European
Commission

# GUIDE TO THE
# EU-U.S. PRIVACY SHIELD

*Justice*
*and Consumers*

Europe Direct is a service to help you find answers
to your questions about the European Union.
Freephone number (*):
**00 800 6 7 8 9 10 11**

(*) Certain mobile telephone operators do not allow access to 00 800 numbers or these calls may be billed.


| | | | |
|---|---|---|---|
| Print | ISBN 978-92-79-60823-0 | doi:10.2838/12912 | DS-04-16-641-EN-C |
| PDF | ISBN 978-92-79-60824-7 | doi:10.2838/199012 | DS-04-16-641-EN-N |

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

2016 — pp. 24 — 21 × 21 cm





*Printed in Belgium*

# Contents


Introduction 7

The Privacy Shield company's obligations and your rights with respect to the use of your personal data 9

How can I make a complaint against a Privacy Shield company? What are my redress rights? 15

The Ombudsperson mechanism: how to bring a complaint against a U.S. public authority 19

# Introduction

## What is the EU-U.S. Privacy Shield and why do we need it?

The European Union (EU) and the United States (U.S.) have strong commercial ties. Transfers of personal data are an important and necessary part of the transatlantic relationship, especially in today's global digital economy. Many transactions involve the collection and use of personal data, for example your name, phone number, birth date, home and email address, credit card number, national insurance or employee number, login name, gender and marital status, or any other kind of information that makes it possible to identify you. For instance, your data may be collected in the EU by a branch or a business partner of an American company which receives the data and then uses it in the U.S.

This is the case, for instance, when you buy goods or services online, when using social media or cloud storage services, or if you are an employee of an EU-based company that uses a company in the U.S. (e.g. the parent company) to deal with personnel data. EU law requires that when your personal data are transferred to the U.S they continue to benefit from a high level of protection.

This is where the EU-U.S. Privacy Shield comes in. The Privacy Shield allows your personal data to be transferred from the EU to a company in the United States, provided that the company there processes (e.g. uses, stores and further transfers) your personal data according to a strong set of data protection rules and safeguards. The protection given to your data applies regardless of whether you are an EU citizen or not.

## How does the Privacy Shield work?

To transfer personal data from the EU to the U.S. different tools are available such as contractual clauses, binding corporate rules and the Privacy Shield. If the Privacy Shield is used, U.S. companies must first sign up to this framework with the U.S. Department of Commerce. The obligation applying to companies under the Privacy Shield are contained in the "Privacy Principles". This Department is responsible for managing and administering the Privacy Shield and ensuring that companies live up to their commitments. In order to be able to certify, companies must have a privacy policy in line with the Privacy Principles. They must renew their "membership" to the Privacy Shield on an annual basis. If they do not, they can no longer receive and use personal data from the EU under that framework.

If you want to know if a company in the U.S. is part of the Privacy Shield, you can check the Privacy Shield List on the website of the Department of Commerce (https://www.privacyshield.gov/welcome). This list will give you details of all the companies taking part in 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. 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.

# The Privacy Shield company's obligations and your rights with respect to the use of your personal data

The Privacy Shield provides you with a number of rights and companies are obliged to protect your personal data in line with the "Privacy Principles".

## 1. Your right to be informed

A Privacy Shield company must inform you about:

- the types of personal data it processes;
- the reasons why it processes your personal data;
- if it intends to transfer your personal data on to another company and the reasons why;
- your right to ask the company to access your personal data;
- your right to choose whether you allow a company to use your personal data in a "materially different" way or to disclose it to another company (also known as the right to "opt-out"). When the data are sensitive, (that is, data that reveal, for example, your ethnic origin or the state of your health) the Privacy Shield company has to inform you about the fact that it may only use or disclose such data if you allow this (also known as the right to "opt-in");
- how to contact the company if you have a complaint about the use of your personal data;
- the independent dispute resolution body, either in the EU or the U.S., where you can bring your case;
- the government agency in the U.S. that is responsible to investigate and enforce the company's obligations under the framework;
- the possibility that it may have to respond to lawful requests from U.S. public authorities to disclose information about you.

The Privacy Shield company must provide you with a link to its privacy policy if it has a public website or where you can access it in case it does not have a public website. It must also provide you with a link to the Privacy Shield List on the Department of Commerce website so that you can easily check the Privacy Shield status of the company.

## 2. Limitations on the use of your data for different purposes

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

- Using your data for a purpose that is incompatible with the original purpose is never allowed;
- If the new purpose is different but related to the original one (i.e. "materially different"), the Privacy Shield company may only use your data if you do not object or, in the case of sensitive data, if you consent.
- If the new purpose is different from the original one but still close enough that it would not be considered as materially different, such use is permissible.

For instance, if your employer has transferred your personal data to the U.S. for processing, the U.S. company might be allowed to use these data to offer you an insurance policy or pension scheme, as long as you do not object to such use. Conversely, it must not sell your data to a third party merchant for offering you goods or services that have no relationship with your employment.

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 U.S. or in another non-EU country. 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. Data minimisation and obligation to keep your data only for the time needed

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

## 4. Obligation to secure your data

The company must ensure that your personal data are 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. Obligation to protect your data if transferred to another company

As noted above (point 2), under certain conditions and taking into account the purpose for which it received your personal data, the Privacy Shield company may transfer them to another company. This can happen for instance when a company shares your data (with a company that itself decides how to use the data, a so-called "controller") without you objecting to that or concludes a service contract with a (sub-)processor (a so-called "agent"). Irrespective of its location, within or outside the U.S., the company that receives the data must ensure the same level of protection of your personal data as guaranteed under the Privacy Shield framework. This requires a contract between the Privacy Shield company and the third party setting out the conditions under which the third party can use your personal data and its responsibilities to protect your data. This contract will have to require the third party to inform the Privacy Shield company of situations where it cannot 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 the actions of an agent that do not follow 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 processed, the categories of personal data concerned and the recipients to whom the data are disclosed. You can then request the company to correct, change or delete them if they are not accurate, outdated or have been processed in violation of the Privacy Shield rules. The company also has to confirm whether or not it holds or processes your personal data.

You are normally not obliged to give any reasons as to why you would like to access your data, however, the company may ask you to do so if your request is too broad or vague. The company has to respond to your access request within a reasonable time frame. A company may sometimes be able to limit your access rights, but only in specific situations such as when providing access would undermine confidentiality, breach professional privilege or conflict with legal obligations.

The right to access can be particularly useful if your personal data are used for a decision which might significantly affect you. In those situations where this typically becomes relevant (e.g. a positive or negative decision about a job, a loan etc.), U.S. law provides additional rights that allow you to better understand to what extent your data have been taken into account.

## 7. Your right to lodge 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 to investigate unresolved complaints. For instance they can choose alternative dispute resolution (ADR) or submit to the oversight of a national Data Protection Authority (DPA).

Consequently, as an individual you have several possibilities to lodge a complaint, namely with the:

1. U.S. Privacy Shield company itself;
2. Independent recourse mechanism, such as ADR or DPA;
3. U.S. Department of Commerce, only through a DPA;
4. U.S. Federal Trade Commission (or the U.S. Department of Transportation if complaint relates to an airline or ticket agent);
5. Privacy Shield Panel, only once certain other redress options have failed.

**• Alternative Dispute Resolution body**

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

**• National Data protection authority**

A Data Protection Authority is established in each EU Member State and is responsible for protecting and enforcing the data protection rules at national level.

**• U.S. Department of Commerce and U.S. Federal Trade Commission**

On the U.S. side, both the Department of Commerce and the U.S. Federal Trade Commission handle complaints. While you can always go directly to these U.S. bodies, a simpler way is to contact your national DPA that will "channel" your complaint across the Atlantic.

**• Privacy Shield panel**

The Privacy Shield Panel is an "arbitration mechanism" made up of three neutral arbitrators, meaning that it settles disputes without going to court. Its decisions, however, are binding and enforceable in U.S. courts. Only you can invoke arbitration through the Privacy Shield Panel, under certain conditions (in particular the prior exhaustion of certain other redress possibilities). The Privacy Shield company does not have the same right because arbitration is exclusively meant to protect you.

## 8. Redress in case of access by U.S. public authorities

Finally, the protection of your personal data may also be affected by U.S. public authorities when they access your data. The Privacy Shield ensures that this will occur only to the extent necessary for pursuing a public interest objective such as national security or law enforcement. While existing U.S. law provides you with protections and remedies in the law enforcement area, the Privacy Shield framework for the first time creates a special instrument to address national security access, the so-called Ombudsperson mechanism (see part C).

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

The Privacy Shield provides you with a number of ways to help you make a complaint about a company for instance if you think that it is not using your personal data in the correct way or that it is not complying with the rules.

You are free to choose the redress mechanism that is most convenient for you and suited to your complaint.

These are the ways in which you can lodge a complaint:

1. **U.S. Privacy Shield company.**. A company must always provide you with details of someone you can contact directly for any inquiries or complaints. 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 apply. The company is obliged to look into each complaint it receives unless it is clearly groundless.

2. **Independent ADR body** in case the Privacy Shield company has chosen ADR as its independent recourse mechanism. The company's website must provide you with the information and the link to the website of the ADR body, which should provide you with details of the services it offers, including the procedures to follow. These bodies must be able to impose effective remedies and sanctions to ensure that the Privacy Shield company is in compliance with its obligation to protect your personal data. You will be able to use this mechanism free of any charge.

3. **National Data Protection Authority.** A Privacy Shield company is in principle free to opt for an EU DPA to act as its independent recourse mechanism. However, when a company handles human resources (personnel) data, submission to DPA oversight is mandatory. This means that as an employee you can always go to your local DPA if you have any complaints with respect to employment-related data transferred to a Privacy Shield company. Moreover, even if a DPA does not have oversight powers over a particular Privacy Shield company, it is always possible for you to approach your DPA who can then refer your complaint to one of the responsible U.S. authorities (see below).

DPAs will deliver their advice to the company as quickly as possible but this must be within 60 days of receiving a complaint. You will be informed about that advice, which will be made public to the extent possible. A company then has 25 days to comply, failing which the DPA may refer the case to the U.S. Federal Trade Commission for possible enforcement action. It may also inform the Department of Commerce about the company's refusal to comply with the DPA's advice which may lead to the removal of the company from the Privacy Shield List if the company persists in its non-compliance.

In addition, if your complaint shows that the transfer of your personal data to the Privacy Shield company violates EU data protection law, the DPA can also act against the EU company that sends the data and, if necessary, order the suspension of the data transfer. This includes cases where the EU company has reasons to believe that the Privacy Shield company is not complying with the Privacy Principles.

4. **Department of Commerce**. Even if a DPA does not have oversight powers over the Privacy Shield company you are complaining against, it can still refer your complaint to the U.S. Department of Commerce. This will be done through a newly-established, dedicated contact point responsible for liaising directly with DPAs. It will review your complaint and get back to your DPA within 90 days with a response. The Department of Commerce may also forward complaints to the Federal Trade Commission (or the Department of Transportation).

4. **Federal Trade Commission**. You can make your complaint directly with the U.S. Federal Trade Commission under the same complaint system used by U.S. citizens: www.ftc.gov/complaint. The Federal Trade Commission will also review complaints it receives from the U.S. 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.

5. **Privacy Shield (Arbitral) Panel**. If your complaint is still wholly or partially unresolved after using the other redress mechanisms, or if you are not satisfied with the way your complaint was handled, you have the right to seek redress through another option: binding arbitration.

### *Who can invoke arbitration?*

It is important to know that only you, the individual, can initiate a case against a Privacy Shield company through binding and enforceable arbitration.

### *When can you invoke arbitration?*

A Privacy Shield company is obliged to arbitrate claims when you invoke this right. However, you may only do so after you have exhausted other avenues of redress such as with the company, the ADR body, or with the Department of Commerce. There are other situations where you may not use the Privacy Shield Panel, namely if your complaint has already been in an arbitration procedure before; a court has already ruled on your complaint and you were a party in this court procedure; the parties have already settled the complaint; or a DPA is able to resolve your claim directly with the company. However, investigations by the FTC can proceed in parallel with arbitration.

### *How do I invoke arbitration?*

If you want to initiate the arbitration procedure, you must first formally notify a company of your intention to do so. Your notice must include a summary of the steps you have already taken to resolve your complaint and a description of the alleged violation. You may also choose to provide any supporting documents or legal texts relating to your complaint.

### *Where will the arbitration take place? What are the benefits?*

The arbitration will take place in the U.S. because the company you are complaining about is based there. At the same time, there are several "consumer friendly" elements that will greatly benefit you:

- right to ask for your DPA's assistance to prepare your claim;
- possibility to join the proceedings by telephone or video-conference, so there is no requirement to be physically present in the U.S.;
- possibility to obtain free of charge interpretation and translation of documents from English into another language;
- arbitral costs (except for lawyer's fees ) will be offset from a fund specifically set up by the Department of Commerce and funded from the Privacy Shield companies' annual contributions.

### *How long will the arbitration process take?*

The arbitration procedure will be finished within 90 days from the day you have sent your notice to the company.

### *What remedies are available?*

If the Privacy Shield Panel finds evidence of a violation of the Privacy Principles it can impose relief such as access, correction, deletion, or return of your personal data.

Even if the Privacy Shield Panel cannot award you monetary damages, you have the possibility to obtain such relief in court. If you are not satisfied with the outcome of the arbitration, you can challenge it under U.S. law under the Federal Arbitration Act.

# The Ombudsperson mechanism: how to bring a complaint against a U.S. public authority

The Privacy Shield sets up a new independent redress mechanism in the area of national security: the Ombudsperson Mechanism.

## *What is the Ombudsperson Mechanism?*

The Privacy Shield Ombudsperson is a senior official within the U.S. Department of State who is independent from U.S. intelligence agencies. Assisted by a number of staff, the Ombudsperson will ensure that complaints are properly investigated and addressed in a timely manner, and that you receive confirmation that the relevant U.S. laws have been complied with or, if the laws have been violated, the situation has been remedied.

In carrying out its duties, and following up on the complaints received, the Ombudsperson will work closely with and obtain all the information from other independent oversight and investigatory bodies necessary for its response when it concerns the compatibility of surveillance with U.S. law. These bodies are the ones responsible to oversee the various U.S. intelligence agencies.

## *Does the Ombudsperson Mechanism only cover complaints relating to transfers of personal data to U.S. Privacy Shield companies?*

No. This mechanism is not Privacy Shield specific. It covers all complaints relating to all personal data and all types of commercial transfers from the EU to companies in the U.S., including 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?*

You should first submit your request in writing to the supervisory authority in your Member State responsible for the oversight of national security services and/or your national DPA. This means you can turn to an authority that assists you in your own language.

Your written request should contain information such as describing the basis of your request, the kind of answer or relief you are looking for, the U.S. Government entities you think have been involved in the surveillance activities, and information about other measures you may have already taken to pursue your request as well as any answer you may already have received. But your request does not need to show that your data have in fact been accessed by U.S. intelligence agencies.

Before being submitted to the Ombudsperson, your request will be checked to verify your identity, that you are acting only for yourself and not on behalf of a government or intergovernmental organisation, that your request contains all the relevant information, that it relates to personal data transferred to the U.S., and that your request is not frivolous, vexatious or made in bad faith, i.e. reflects a genuine concern.

## *What happens once my request is sent to the Ombudsperson?*

The Ombudsperson will process your request and, if it has any questions or if 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 U.S. bodies. When the request relates to the compatibility of surveillance with U.S. law, it will be able to cooperate with one of the independent oversight bodies with investigatory powers. The Ombudsperson will have to receive the necessary information to be able to provide a response. It will confirm that your request has been properly investigated and that U.S. law has been complied with or, if not, that any violation of U.S. law has been remedied. The response will not state whether you have been the target of surveillance by U.S. national intelligence services.

### *.Requests for information*

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

However, it is not possible to receive access to classified national security information, personal information of third parties, and information concerning law enforcement investigations. These limitations apply equally to Americans and non-Americans.

Disputes about FOIA requests can be appealed administratively and then in federal court in the U.S. The court can then decide whether the records you requested have been properly withheld or it can force the government to give access to these documents. The courts can award attorney's fees but monetary damages are not available.

*The special procedures for complaints, which are described in this guide, do not replace your right to seek the guidance and support of the national Data Protection Authorities on the exercise of your legal rights.*

## HOW TO OBTAIN EU PUBLICATIONS

**Free publications:**

- one copy:
  via EU Bookshop (http://bookshop.europa.eu);
- more than one copy or posters/maps:
  from the European Union's representations (http://ec.europa.eu/represent_en.htm);
  from the delegations in non-EU countries (http://eeas.europa.eu/delegations/index_en.htm);
  by contacting the Europe Direct service (http://europa.eu/europedirect/index_en.htm) or
  calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (*).

  (*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

**Priced publications:**

- via EU Bookshop (http://bookshop.europa.eu).

DS-04-16-641-EN-N

Publications Office

ISBN 978-92-79-60824-7

doi:10.2838/199012