

## EU-US Privacy Shield

Acxiom and its subsidiaries (collectively, “Acxiom”), commit to conducting their business according to the EU-US Privacy Shield which became effective August 1, 2016. Acxiom commits to applying the Principles to all personal data received from the EU in reliance on the Privacy Shield. Acxiom also maintains an affirmative commitment to the U.S.-Swiss Safe Harbor Framework and its principles, which will not be affected by our participation in the Privacy Shield. Companies, including Acxiom, who are currently registered with the U.S. Department of Commerce Privacy Shield and Safe Harbor programs can be found by going to <https://www.privacyshield.gov> and <http://2016.export.gov/safeharbor/swiss/>. Acxiom is committed to educating its clients and employees in the United States and in the EU and Switzerland about the issues, guidelines and laws surrounding compliance with Privacy Shield and Safe Harbor. Since the requirements for compliance with Privacy Shield vary depending on whether Acxiom is acting as a processor on behalf of Acxiom’s clients or as a data controller, Acxiom’s policies and manner of compliance are described separately below. The practices Acxiom employs under Privacy Shield, as outlined below, also applies to data transferred from Switzerland to the United States under the compliance of the Safe Harbor framework.

### **Acxiom as a Processor on Behalf of Clients**

Acxiom provides customized computer services designed to help companies manage their customer information more effectively, increase profitability of their marketing and reduce the operational costs of processing customer transactions. In this capacity, Acxiom does not own or control any of the information it processes on behalf of Acxiom’s clients. All such information is owned and controlled by Acxiom’s clients. In this capacity Acxiom receives information transferred from the EU to the United States merely as a processor on behalf of our clients.

When Acxiom acts as a processor on behalf of its clients, the policies outlined below apply to all data processing operations concerning personal information that has been transferred from the EU to the United States.

Before starting any processing on behalf of Acxiom’s clients, Acxiom will enter into a processing contract with the EU data controller that ensures the EU data controller will be in compliance with the Member State Data Protection law.

Any data processed by Acxiom will not be further disclosed to third parties except where permitted or required by the processing contract, Privacy Shield or the applicable Member State Data Protection law. Any information Acxiom’s client (acting as the EU controller) identifies as sensitive, will be treated accordingly.

The processing contract will also specify that the processing will be carried out with appropriate data security measures. Acxiom has in place measures to protect personal information from loss, misuse, unauthorized access, disclosure, alteration and destruction.

As a processor on behalf of Acxiom’s clients (who are the EU data controllers), Acxiom is not required to certain apply other Privacy Shield Principles to the personal information received for processing from a clients.

### **Acxiom as a Data Controller**

Acxiom provides business and consumer information products designed to help companies market more successfully, integrate and improve the accuracy of their customer information, and reduce the operational costs of processing customer data. In this function, Acxiom acts as a data controller of the personal information contained in these information products.

Acxiom also collects and maintains human resources data, including personnel files on its employees.

Acxiom has appointed a chief privacy officer, who is responsible for the internal supervision of Acxiom's privacy policies. Acxiom has also appointed a corporate leader for data security. The chief privacy officer and security officers are available to any individual or employee who has questions concerning Acxiom's compliance with Privacy Shield or data security practices.

When Acxiom acts as a data controller of personal information, the policies outlined below apply to all personal information that has been transferred from the EU to the United States.

Acxiom and its subsidiaries located in the EU, develop and maintain databases containing personal information on data subjects, households, and businesses located throughout EU Member States. How these databases are collected varies from country to country. Generally, these databases are developed from public records, publicly available information, information acquired through information providers, and information collected directly from data subjects.

Acxiom's databases contain information that is provided to qualified businesses for marketing, customer data integration, and connectivity purposes. The information contained in these databases may also be used to provide information services, to enhance the understanding a company has about its customers, to aid in accurate integration of a company's customer information, and be used as lists for direct marketing purposes.

Acxiom also collects and maintains human resources data on its employees. These files may contain information such as the employee's resume, performance appraisals, salary increases, and agreements between the employee and Acxiom, though these vary according to the laws and agreements applicable to each subsidiary.

As a data controller, Acxiom is required to comply with all principles of the Privacy Shield.

## **Notice**

Acxiom may be required to disclose personal information in response to lawful requests by public authorities, including requests to meet national security or law enforcement requirements. Prior to the transfer of personal information from the EU to the United States, Acxiom requires contractual confirmation from the EU controller from whom Acxiom acquired the information that the personal data has been provided to Acxiom in accordance with the applicable EU Member State Data Protection law, thereby ensuring the data subjects have been provided with proper notice regarding how their personal data will be used. In addition, when personal data is collected directly from data subjects, Acxiom provides the data subject with notice regarding the manner and circumstances in which the personal data will be used and transferred to third parties.

Any personal data provided by Acxiom associates in the European Union in the course of their employment with Acxiom or its subsidiaries will be handled and transferred in compliance with the requirements of the laws of the relevant Member State. Such personal data, including sensitive personal data, relating to the associate's employment with Acxiom or its subsidiaries may, to the extent that it is reasonably necessary in connection with the Associate's employment:

- Be collected and held (in hard copy and computer readable form) and processed by Acxiom and
- Be disclosed or transferred to and processed by Acxiom and its European subsidiaries and their employees, and where permitted, third party sub-contractors both within and outside of the European Economic Area, and as otherwise required or permitted by law.

## **Choice**

In addition to choices regarding the use of information, Acxiom will remove an individual's name and related information from its direct marketing information products. Consumers may request an opt-out form by writing Acxiom at the address below, leaving a message on our Consumer Advocate Hotline at 001-501-342-2722 or sending an e-mail to us at [privacyshielddoptout@acxiom.com](mailto:privacyshielddoptout@acxiom.com).

**To request an opt-out form by mail, write to:**

Consumer Advocate  
EU-US Privacy Shield Opt-Out  
Acxiom Corporation  
P.O. Box 2000  
Conway, Arkansas, USA 72033-9928

Acxiom and its subsidiaries will make reasonable efforts to accommodate privacy preferences regarding human resources data it maintains on its employees.

**Data Integrity**

Acxiom takes reasonable steps to ensure the information transferred from the EU to the United States is reliable, accurate, and complete. The steps Acxiom takes to assure data integrity are based on the purposes for which the personal information is used.

**Onward Transfer**

Acxiom complies with the notice and choice principles as described above for all data disclosed or transferred to a third party. Acxiom takes reasonable and appropriate steps to ensure that the third party effectively processes the personal information transferred in a manner consistent with Acxiom's obligations under the Principles.

When Acxiom uses data processors to perform processing tasks on behalf and under the instruction of Acxiom, Acxiom requires that its data processors either:

- Subscribe to the Privacy Shield, the EU Data Protection Directive, or another adequacy finding; or
- Enter into a written agreement with Acxiom requiring them to process the data only for limited and specified purposes and to provide the same level of protection as Acxiom provides.

In cases of onward transfer to third parties, Acxiom is generally liable for the acts of the third party that are in violation of the Privacy Shield Principles.

**Security**

Acxiom has an information security policy in place to protect personal information from loss, misuse, unauthorized access, disclosure, alteration, and destruction. Acxiom's security officer is responsible for conducting investigations into any alleged computer or network breaches, incidents or problems and ensuring that proper disciplinary action is taken against those who violate Acxiom's information security policy.

Any security compromises or potential security compromises and any inquiries concerning security should be reported to the Acxiom consumer advocate. Contact information for the Acxiom consumer advocate is provided below.

**Access**

An individual may request access to the information Acxiom maintains in its information products. The individual has the right to learn whether or not data about him or her is found in Acxiom's information products and to correct, amend or delete that information when it is inaccurate. This right applies only to personal information about the individual making the request and is subject to other limitations as defined by law. Individuals can request access by writing or calling:

**Consumer Advocate**  
Acxiom Corporation  
P.O. Box 2000  
Conway, Arkansas USA 72033-9928

**Consumer Advocate Hotline:** 001- 501-342-2722

Acxiom's consumer advocate will explain the process for making an access request. In order to confirm the identity of the individual and have the necessary information to retrieve the individual's information, Acxiom provides a form which the individual fills out, signs, and mails to Acxiom. The form must be accompanied by a \$10 personal check. Filing a request in English will expedite the process.

Acxiom agrees to process all reasonable requests for access within a reasonable time period, but reserves the right to deny access or limit access in cases where the burden or cost of providing access would be disproportionate to the risks to the individual's privacy or in the case of an unwarranted or fraudulent request.

Acxiom maintains personnel files on its employees. Depending on the subsidiary, these files may contain information such as the Associate's CV, performance appraisals, salary increases and agreements between the employee and Acxiom. Every employee can access and, if necessary, correct or delete information in his personnel files, by contacting the Human Resources Department.

### **Enforcement**

Individuals who wish to file a complaint or who take issue with Acxiom's Privacy Shield or Safe Harbor policies should contact Acxiom's consumer advocate at the above address. Acxiom's consumer advocate will explain the process to be followed when filing a complaint. Filing a complaint in English will expedite the process.

Acxiom is a participant in DMA's Privacy Shield and Safe Harbor dispute resolution programs. If consumers cannot resolve a complaint after contacting Acxiom's consumer advocate, they may pursue recourse with DMA, free of charge:

### **DMA**

Online complaint form: <https://thedma.org/shield-complaint-form/>

Mail: Privacy Shield Line  
DMA  
1615 L Street, NW – Suite 1100  
Washington, DC 20036

Web: [www.thedma.org/privacy-shield-safe-harbor-for-consumers/](http://www.thedma.org/privacy-shield-safe-harbor-for-consumers/)

Fax: 202.955.0085

Under certain conditions, an individual may invoke binding arbitration to resolve residual claims. Acxiom is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission. In addition, Acxiom agrees to cooperate with local EU Data Protection Authorities to resolve an EU Acxiom employee's dispute concerning human resources data or an alleged breach of the Privacy Shield Principles.



**ACXIOM DEUTSCHLAND GMBH**

Zwei Standorte in Deutschland:

Frankfurt: Martin-Behaim-Str. 12 • 63263 Neu-Isenburg

München: Eisenheimerstr. 55a • 80687 München

Tel. 0800/022 94 66 • Fax: 089/857 09 – 200 • [info-germany@acxiom.com](mailto:info-germany@acxiom.com) • [www.acxiom.de](http://www.acxiom.de)