

Privacy Shield Policy

This Privacy Shield Policy ("Policy") describes how UDG Healthcare plc and its subsidiaries and affiliates in the United States ("US") ("Company," "we," or "us") collect, use, and disclose certain personally identifiable information that we receive in the US from the European Economic Area ("EEA Personal Data").

We recognize that the EEA has established strict protections regarding the handling of EEA Personal Data, including requirements to provide adequate protection for EEA Personal Data transferred outside of the EEA.

This Policy applies to the following US affiliated entities that receive personal information from the EU (Ashfield Healthcare, LLC; Ashfield Meetings & Events, Inc; Ashfield Healthcare Communications, LLC; Informed Direct, Inc; Ashfield Pharmacovigilance, Inc and GET Destinations, LLC) who commit to comply with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the U.S.

The above listed Ashfield companies have self-certified to the U.S. Department of Commerce that they adhere to the Privacy Shield Principles of notice, choice, accountability for onward transfer, security, data integrity and purpose limitation, access, recourse, enforcement, and liability for onward transfer to third parties, the Privacy Shield Supplemental Principles and the Swiss-U.S. Privacy Shield Principles. If there is any conflict between the terms of this Privacy Policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program visit <https://www.privacyshield.gov/welcome> and to view Ashfield's certifications, please visit <https://www.privacyshield.gov/list>

This Policy supplements our Website Privacy Policy located at <https://www.udghealthcare.com/privacy-policy/> and unless specifically defined in this Policy, the terms in this Policy have the same meaning as the Website Privacy Policy.

We comply with the Privacy Shield Principles for all onward transfers of personal data from the EU and Switzerland, including the onward transfer liability provisions.

Personal Data Collection and Use

Our Website Privacy Notice located at <https://www.udghealthcare.com/privacy-policy/> describes the categories of EEA Personal Data that we may receive in the US as well as the purposes for which we use that EEA Personal Data. We process EEA Personal Data for the following purposes: to receive and process information about existing and potential corporate customers, clients, suppliers, business partners, job applicants and employees. We will only process EEA Personal Data in ways that are compatible with the purpose that we collected it for, or for purposes the individual later authorizes. Before we use your EEA Personal Data for a purpose that is materially different than the purpose we collected it for or that you later authorized, we will provide you

with the opportunity to opt out. We maintain reasonable procedures to help ensure that EEA Personal Data is reliable for its intended use, accurate, complete, and current.

Data Transfers to Third Parties

Third-Party Agents or Service Providers. We may transfer EEA Personal Data to our third-party agents or service providers who perform functions on our behalf as described in our Website Privacy Notice. Where required by the Privacy Shield, we enter into written agreements with those third-party agents and service providers requiring them to provide the same level of protection the Privacy Shield requires and limiting their use of the data to the specified services provided on our behalf. We take reasonable and appropriate steps to ensure that third-party agents and service providers process EEA Personal Data in accordance with our Privacy Shield obligations and to stop and remediate any unauthorized processing. Under certain circumstances, we may remain liable for the acts of our third-party agents or service providers who perform services on our behalf for their handling of EEA Personal Data that we transfer to them.

Disclosures for National Security or Law Enforcement. Under certain circumstances, we may be required to disclose your EEA Personal Data in response to valid requests by public authorities, including to meet national security or law enforcement requirements.

Security

We maintain reasonable and appropriate security measures to protect EEA Personal Data from loss, misuse, unauthorized access, disclosure, alteration, or destruction in accordance with the Privacy Shield.

Our employees are trained in-line with and required to adhere to the principles of the applicable Data Protection laws and Privacy Shield Principles in their country of employment.

Access Rights

You may have the right to access the EEA Personal Data that we hold about you and to request that we correct, amend, or delete it if it is inaccurate or processed in violation of the Privacy Shield. These access rights may not apply in some cases, including where providing access is unreasonably burdensome or expensive under the circumstances or where it would violate the rights of someone other than the individual requesting access. If you would like to request access to, correction, amendment, or deletion of your EEA Personal Data, you can submit a written request to the contact information provided below. We may request specific information from you to confirm your identity. In some circumstances we may charge a reasonable fee for access to your information.

Choice/Opt-Out

Should you no longer wish to receive information or future communications about our relevant services, please contact us using one of the following options. You may send your request via email stating your desire to opt out of further communications to data.protection@udghealthcare.com or alternatively you may write to us at:

Data Protection Officer
UDG Healthcare plc
20 River Walk
Citywest Business Campus
Dublin 24 D24 NR23
Ireland

We also provide an opt-out option with all marketing email communications by either clicking the unsubscribe link at the bottom of the email or replying to the email stating your request to opt-out of further communications. If we intend to use personally identifiable information in a manner different from that stated within this Privacy Policy or as otherwise previously notified, we will notify all affected users; users will be able to opt out of any new use of their personal information.

Contact Us, Questions or Complaints

You can direct any questions or complaints about the use or disclosure of your EEA Personal Data to us at: data.protection@udghealthcare.com or alternatively you can write to us at:

Data Protection Officer
UDG Healthcare plc
20 River Walk
Citywest Business Campus
Dublin 24 D24 NR23
Ireland

In compliance with data privacy laws and the Privacy Shield Principles, we commit to resolve complaints about your privacy and our collection or use of your personal information.

We will investigate and attempt to resolve any complaints or disputes regarding the use or disclosure of your EEA Personal Data within 45 days of receiving your complaint.

We have further committed to refer unresolved privacy complaints under the Privacy Shield Principles to an independent dispute resolution mechanism, the ICDR/AAA, operated by the American Arbitration Association located in the U.S. If you do not receive timely acknowledgement of your privacy complaint from us, or if we have not addressed your complaint to your satisfaction, please contact or visit the ICDR/AAA web site at <http://go.adr.org/privacyshield.html> for more information or to file a complaint. EU and Swiss complainants may invoke binding arbitration under the Privacy Shield Principles if a complaint has not been resolved by Ashfield or by other recourse and enforcement mechanisms. Ashfield's US businesses are also subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission.

Ashfield commits to co-operate with the EU Data Protection Authorities and comply with the advice given by such authorities with regard to Human Resources data transferred from the EU to the US in the context of the employment relationship. If you have a complaint relating to Human Resources data transferred from Ashfield's EU businesses that cannot be resolved by Ashfield's internal dispute resolution process, you may refer your complaint to the Data Protection Panel secretariat established by the EU Data Protection Authorities (DPA) at the following address: European Commission, Directorate General Justice, Data Protection Panel, B-1049 Brussels, Belgium. Telephone: (32-2) 299.11.11; Fax (32-2) 298.80.94.

Binding Arbitration You may have the option to select binding arbitration for the resolution of your complaint under certain circumstances, provided you have taken the following steps: (1) raised your complaint directly with us and provided us the opportunity to resolve the issue; (2) made use of the independent dispute resolution mechanism identified above; and (3) raised the issue through the relevant data protection authority and allowed the US Department of Commerce an opportunity to resolve the complaint at no cost to you. For more information on binding arbitration, see US Department of Commerce's Privacy Shield Framework: Annex I (Binding Arbitration).

Contact Us

If you have any questions about this Policy or would like to request access to your EEA Personal Data, please contact us as follows: data.protection@udghealthcare.com or you can write to us at:

Data Protection Officer
UDG Healthcare plc
20 River Walk
Citywest Business Campus
Dublin 24 D24 NR23
Ireland

Changes To This Policy

We reserve the right to amend this Policy from time to time consistent with the Privacy Shield's requirements.

Effective Date: 18 May 2018

Last modified: 18 May 2018