

Privacy Policy

Our commitment to your privacy	1
Adelphi Group of Companies – who are we?	1
How we use your information?	2
People who have contacted us with a request for information.....	2
If you apply to work with us?	2
If you are employed by us	3
Commercial and marketing communications.....	3
People who participate in our market research, health outcomes or observational research projects	3
How we use your personal data	3
Types of personal data we collect	3
Sources of your personal information.....	4
Legal grounds for processing your personal data	4
Sharing your personal data.....	4
Retention of personal data.....	4
People who engage in our medical communications, medical education and publication programmes	5
How we use your personal data	5
Types of personal data we collect	5
Sources of your personal information.....	6
Legal grounds for processing your personal data	6
Sharing your personal data.....	6
How long do we keep your personal data for?	6
If you use our website	7
Log files	7
Cookies	7
How we use cookies to collect statistics	7
How long do we keep your personal data for?	7
Who do we share your information with?	8
Transfers of personal data outside the EEA	8

How we protect your information?	9
Your data protection rights	9
Right to be informed.....	9
Right of access to your information	9
Right of erasure (right to be forgotten).....	9
Right of rectification	9
Opt-out of marketing communications.....	10
Withdraw your consent.....	10
Complaints.....	10
Contact details.....	10
Changes to this privacy policy	10

Privacy Policy

This policy was last updated on the 8th April 2019.


Our commitment to your privacy

ADELPHI is committed to protecting and respecting your privacy. We take our responsibilities regarding the security of information that we have collected seriously. This privacy policy sets out how we use and protect the information that you provide to us. Please read this policy carefully. If you have any questions, please contact compliance.team@adelphigroup.com.

In this policy **ADELPHI**, **we**, and **us** means the Adelphi Group of Companies listed in the section Adelphi Group of Companies. **ADELPHI** is the controller for the personal information.

Adelphi Group of Companies – who are we?

This privacy policy applies to the Adelphi companies listed below who are established within the EU, or those outside who process details of EU Citizens.

<p>Ology Medical Education, trading branch of Excerpta Medica BV Herikerbergweg 17, 1101 CN, Amsterdam The Netherlands Reg. No. 50825461</p>	
<p>Adelphi Real World Adelphi Group Ltd trading as Adelphi Real World Adelphi Mill, Grimshaw Lane, Bollington, Cheshire, SK10 5JB. Company No: 1975338 Registered address: Bankside 3, 90 - 100 Southwark Street, London, England, SE1 0SW</p>	
<p>Adelphi Research Adelphi International Research Ltd trading as Adelphi Research Adelphi Mill, Grimshaw Lane, Bollington, Cheshire, SK10 5JB. Company No: 2419446 Registered address: Bankside 3, 90 - 100 Southwark Street, London, England, SE1 0SW</p>	
<p>Adelphi Research Adelphi Research by Design LLC trading as Adelphi Research 2005 S. Easton Road, Suite 300, Doylestown, PA 18901.</p>	
<p>Adelphi Values Ltd Adelphi Mill, Grimshaw Lane, Bollington, Cheshire, SK10 5JB. Company No: 2761308 Registered address: Bankside 3, 90 - 100 Southwark Street, London, England, SE1 0SW</p>	
<p>Adelphi Values LLC 290 Congress Street, 7th Floor, Boston, Massachusetts 02210</p>	
<p>THE PLANNING SHOP International, Ltd. CP House, 97-107 Uxbridge Road, London W5 5TL. Company No: 3037899 Registered address: Bankside 3, 90 - 100 Southwark Street, London, England, SE1 0SW</p>	
<p>THE PLANNING SHOP International, Inc. 2005 South Easton Road, Suite 300, Doylestown, PA, 18901.</p>	

<p>Adelphi Communications Ltd</p> <p>Adelphi Mill, Grimshaw Lane, Bollington, Cheshire, SK10 5JB. Company No: 2761321 Registered address: Bankside 3, 90 - 100 Southwark Street, London, England, SE1 0SW</p>
<p>Adelphi Communications LLC</p> <p>33 Irving Place, New York, NY 10003</p>
<p>2TheNth Ltd</p> <p>Adelphi Mill, Grimshaw Lane, Bollington, Cheshire, SK10 5JB. Company No: 2072694 Registered address: Bankside 3, 90 - 100 Southwark Street, London, England, SE1 0SW</p>
<p>Excerpta Medica BV</p> <p>Amsterdam, Apollo Building, Herikerbergweg 17, 1101 CN Amsterdam, Netherlands. Amsterdam Trade Register number: 5082 5461</p>
<p>Excerpta Medica BV UK Branch</p> <p>Bankside 3, 90 - 100 Southwark Street, London, England, SE1 0SW Company No: BR014830 Registered address: Bankside 3, 90 - 100 Southwark Street, London, England, SE1 0SW</p>
<p>Excerpta Medica LLC</p> <p>2005 S. Easton Road, Suite 300, Doylestown, PA 18901 EIN 27-3145979</p>

How we use your information?

People who have contacted us with a request for information

If you have requested information from **ADELPHI**, we will collect and process the personal data that you provide in order to respond to your request. Unless you consent to the contrary, we shall only use your personal data to provide the information you have requested.

We may collect some or all off the following personal data (this may vary according to your relationship with us):

- Name
- Address
- Email address
- Telephone number
- Business name
- Job title
- Profession

We will process your personal information where there is a legitimate interest in us doing so, if it is reasonably necessary to achieve our or others' legitimate interests (as long as that processing is fair, balanced and does not unduly impact your rights). For example, if you are requesting information about a company or a service from **ADELPHI** (see section Adelphi Group of Companies), then we may pass your personal data onto another member of the group to enable them to appropriately respond to your request. Again unless you consent to the contrary, that member shall only use your personal data to provide the information you have requested.

If you apply to work with us?

Our Recruitment Privacy Notice explains how and why we use your personal data, including how long we keep it and who we share it with. Please see [Recruitment Privacy Notice](#).

If you are employed by us

Our Workplace Privacy Notice explains how and why we use your personal data, including how long we keep it and who we share it with. You will be given the Workplace Privacy Notice if you are offered employment by us and it also available on the **ADELPHI** intranet and from HR.

Commercial and marketing communications

We use the information we collect or receive, such as your email address, phone number, postal address, to communicate directly with you. We may ask you to give us your consent to send you emails containing newsletters or updates or contact you on other ways. If you do not want to receive such communications, you will be given the option to unsubscribe or change your preferences.

Where individuals do not have a relationship with us, for example, if we have identified them from public domain information or purchased a mailing list, as we feel they may have an interest in our services, we shall be relying on our legitimate interests to engage in promotional activities including direct marketing. See section Your data protection rights on page 9.

People who participate in our market research, health outcomes or observational research projects

How we use your personal data

ADELPHI and its suppliers use your personal data for conducting market research, health outcomes or observational research projects ('research') either as **ADELPHI** or on behalf of our clients. We use your personal data for the following purposes:

- Performance of research and analysis either as **ADELPHI** or on behalf of our clients;
- Monitoring and keeping records of communications between you and **ADELPHI** staff;
- Compliance with our contracts with our clients;
- Sharing of information, as needed, with translators, analysts, data processing companies, fieldwork agencies;
- Adherence and compliance with legal and regulatory obligations, requirements and guidance.

Types of personal data we collect

The nature of the personal data collected about you will depend on your relationship with **ADELPHI** and the type of work we conduct. **ADELPHI** typically uses a network of fieldwork partners and clinical sites to recruit participants to participate in a research project and conduct interviews. ('fieldwork partner'). Please read the fieldwork partner's privacy policy for further information about the data that they collect and what it is used for. Typically, the fieldwork partner assigns a respondent identifier to minimise the personal data collected by **ADELPHI**.

Types of personal data that maybe collected include:

- Respondent identifier assigned by the fieldwork partner;
- Information submitted by you during a research interview or when completing a paper or internet questionnaire. This may include information on age, gender, nationality, health data: including, for example, disease specific experience or drug purchasing/prescribing history, Adverse Events;
- System access information, such as user names, passwords and other personally identifiable information;
- Your bank account details;

- Remuneration, including honoraria/fees for service and expenses payment in relation to your participation in, and contribution to, programmes and services;
- Your contact details, such as title, name, email address, mobile/telephone number and company information such as job title/role, office location, mobile/telephone number.

Sources of your personal information

Most of the personal information **ADELPHI** processes is provided directly by you, or by the fieldwork partner. Sometime the sponsoring client may provide a list of names for the purposes of contacting potential respondents. **ADELPHI** will follow the client's instruction on processing the personal data but will ensure that the personal data is processed according to data protection legislation including assurance that the list of names can be legitimately used for the intended research purpose.

Legal grounds for processing your personal data

Under data protection legislation, there are various grounds on which we can rely when processing your personal data. In some contexts, more than one ground applies. Typically, for research **ADELPHI** relies on Legitimate Interests and Consent. **ADELPHI** may also be required to use your personal data to comply with its legal obligation.

Consent

To process your personal data, we obtain your explicit consent. This means that before we collect any information from you we ensure that you are provided with full details about the purpose and nature of the project and what will happen to the information we collect.

Withdrawal of your consent

If we have relied on consent as a ground for processing, you may withdraw consent at any time – though if you do so that will not affect the lawfulness of what we have done before you withdraw consent. See section Your data protection rights on page 9 .

Legitimate interests

Examples of personal data that maybe processed using legitimate interests:

- Maintaining records relating to your participation in research projects;
- Adhering to legislation, governmental and regulatory bodies guidance. Adhering to good governance requirements, such as internal reporting and compliance requirements;
- Audit requirements;
- Monitoring and keeping records of communications between you, the fieldwork partner and **ADELPHI** staff;

Sharing your personal data

In some cases, we may need to share personal information with third parties that provide research services in support of the research project e.g. translators, analysts, data processing companies, fieldwork agencies. Any third party that receives personal information is obligated to follow all the same privacy protection regulations as followed by **ADELPHI**.

Retention of personal data

ADELPHI will not retain your personal information for longer than is necessary. At the end of the research project **ADELPHI** redact (remove) the personal data no longer required for the project. This means that most of the personal data collected during the research project is deleted and there is minimal personal data retained by **ADELPHI**.

People who engage in our medical communications, medical education and publication programmes

How we use your personal data

ADELPHI and its suppliers use your personal data for running medical communications, medical education and publication programmes ('programmes') either as **ADELPHI** or on behalf of our clients. We use your personal data for the following purposes:

- Booking travel and providing other logistical support on your behalf when participating in, or providing services related to programmes;
- Monitoring and keeping records of communications between you and **ADELPHI** staff;
- Evaluation of medical experts both for **ADELPHI** and our clients whom we support to deliver medical communication programmes;
- Sharing of information, as needed, with our clients and suppliers;
- Contacting your nominated contact in event of an emergency;
- Compliance with our contracts with our clients;
- Adherence to legal and regulatory obligations, requirements and guidance.

Types of personal data we collect

The nature of the personal data collected about you will depend on your relationship with **ADELPHI** and the type of work we conduct, but may include the following:

- Your contact details, such as title, name, email address, mobile/telephone number and company information such as job title/role, office location, mobile/telephone number;
- Records of communications with you and other parties e.g. telephone calls, on-line meetings, emails, chat or text messages;
- Information supplied by you, your colleagues, our client or third parties, such as academic, career history, medical background, clinical practice, field of research, practice and other professional specialism information;
- Your participation in, or provision of services related to programmes that may be required to be put on public record;
- Remuneration, including honoraria/fees for service and expenses payment in relation to your participation in, and contribution to, programmes and services;
- Relevant activities associated with the work we undertake, on social media and other publicly available digital channels, used as part of services and business activities we undertake for or that which is necessary as part of our wider business engagement;
- System access information, such as user names, passwords and other personally identifiable information that would allow **ADELPHI** to access IT systems and/or operate on your behalf when nominated to do so by you.

We may with your consent, also retain the following:

- Your date of birth, age, gender;
- Your nationality;
- Your bank account details;
- Details of nominated contacts, such as next of kin;

Sources of your personal information

Most of the personal information **ADELPHI** processes is provided directly by you and by your administrative support staff. For example, you tell us your contact details and banking details. We may also obtain your personal data from our clients where we are running a programme or service on their behalf.

Legal grounds for processing your personal data

Under data protection legislation, there are various grounds on which we can rely when processing your personal data. In some contexts, more than one ground applies. Typically, for our programmes we rely on Contract, Legitimate Interests and Consent. **ADELPHI** may also be required to use your personal data to comply with its legal obligation.

Legitimate interests

Examples of personal data that maybe processed using legitimate interests:

- Maintaining records relating to your participation in programmes;
- Adhering to legislation, government and regulatory bodies guidance and compliance requirements;
- Audit requirements;
- Tracking and record-keeping of communications between you and **ADELPHI** staff;

Contract

Example of personal data that maybe processed using the performance of a contract:

- The processing is necessary for the execution of a contract in which you are a party. The contract maybe with you and **ADELPHI** or you and our client.

Consent

Example of personal data that maybe processed where you have given specific consent to the processing of your data.

- Retaining your contact details and company information for potential future projects.

Withdrawal of your consent

If we have relied on consent as a ground for processing, you may withdraw consent at any time – though if you do so that will not affect the lawfulness of what we have done before you withdraw consent. See section Your data protection rights on page 9.

Sharing your personal data

ADELPHI may share information with the following third parties when running programmes:

- Clients of **ADELPHI**;
- Suppliers and agents, such as travel agents;
- Regulatory organisations.

How long do we keep your personal data for?

ADELPHI will not retain your personal information for longer than is necessary. The period for which we keep your personal data will be determined by several criteria, including the purposes for which we are using the information, the amount and sensitivity of the information, the potential risk from any unauthorised use or disclosure of the information, and our legal and regulatory obligations.

Typically, to comply with our legal and regulatory obligations we will retain your personal data for up to 10 years.

If you use our website

When you visit one of the **ADELPHI** websites, we will collect standard internet log information and details of visitor behaviour patterns. We do this to find out things such as the number of visitors to the various parts of the site. We collect this information in a way which does not identify anyone. Our web servers capture IP Addresses that are stored in log files by default for troubleshooting connections. We purge all web server log files every **30** days.

We do not make any attempt to find out the identities of those visiting our websites. We will not associate any data gathered from these sites with any personally identifying information from any source. If we do want to collect personally identifiable information through our websites, we will ask your permission and explain what we intend to do with it.

Appropriate security measures are in place, in our physical facilities to protect against the loss, misuse or alteration of information that we have collected from our websites.

Log files

As is true of most web sites, we gather certain information automatically and store it in log files. This information is related to the use of this site and services. We use this information to analyse trends, to administer the site, to track users' movements around the site, to gather demographic information about our user base as a whole and to monitor for malicious activity etc.

Cookies

Like most websites we use 'cookies' to collect anonymous statistics about how people use the site, and to help us keep it relevant for the user. Cookies 'remember' bits of information from your visit to the site.

A cookie is a simple text file that's stored on your computer or mobile device by a website's server. Only that server can retrieve or read the contents of that cookie. Each cookie is unique to your web browser. So if we put a cookie on your computer, it can't be read by any other website.

If you don't want your web visits to be tracked for statistical purposes like this you can set your computer to block cookies at any time. The way in which you do this depends upon the web browser which you use. Go to <http://www.allaboutcookies.org/> to find out more.

How we use cookies to collect statistics

To improve our service, we collect anonymous web statistics using a cloud tool called Google Analytics. This stores a few cookies on the users' computers or mobile devices to tell us how many people have visited each web page, how they got there, and where they navigate from there. The data collected is completely anonymously and does not store any personal details. If you want to stop our websites collecting usage data about you via Google Analytics, you can disable cookies in your browsers, disable JavaScript in your browser and use Google's Opt-out browser add-on: <https://tools.google.com/dlpage/gaoptout>

How long do we keep your personal data for?

We are required by law to keep your personal data only for as long as is necessary for the purposes for which we are using it. The period for which we keep your personal data will be determined by several criteria, including the purposes for which we are using the information, the amount and sensitivity of the information, the potential risk from any unauthorised use or disclosure of the information, and our legal and regulatory obligations.

We keep a backup of our data to restore the original data after a data loss event. When we delete your personal data, it will be deleted from the live storage immediately but there will be a delay before it is removed from the backup data.

Who do we share your information with?

We use selected agents to process your information on our behalf, such as software providers to host our website. Such third parties will be authorised to see and use your information but only to fulfil their contractual obligations to us and will not be permitted to use it for any other purpose. We retain full responsibility for how your personal information may be used by such agents.

The personal data that we collect from you may be transferred to, and stored at, a destination outside the European Economic Area ("EEA"). It may also be processed by staff of **ADELPHI** who are operating outside the EEA. By submitting your personal data, you agree to this transfer, storing or processing. We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this privacy policy.

We may share your personal information so that we can comply with a legal obligation to which we are subject. For example: where we are obliged to share your personal information with regulatory bodies which govern our work and services; government departments such as law enforcement and HMRC; court orders etc.

We will process your personal information where there is a legitimate interest in us doing so if it is reasonably necessary to achieve our or others' legitimate interests (as long as that processing is fair, balanced and does not unduly impact your rights). For example, if you are requesting information about a company or a service from a member of **ADELPHI** (see section Adelphi Group of Companies), then we may pass your personal data onto another member of the group to enable them to appropriately respond to your request. Again, unless you consent to the contrary, that member shall only use your personal data to provide the information you have requested.

We may share your data when conducting research, running programmes, if you apply to work with us and if you are employed by us. See the relevant sections in this privacy policy.

ADELPHI does not sell, trade or rent your personal information.

Transfers of personal data outside the EEA

In connection with our business and for employment, administrative, management and legal purposes, we may transfer your personal data outside the EEA to members of our group and processors in the United States and on occasion other jurisdictions in which we are established. Some of our systems are hosted in the United States. We will ensure that the transfer is lawful and that there are appropriate security arrangements.

Where we need to transfer your information outside of the European Economic Area we only do so to countries which have been determined by the European Commission to have an adequate level of data protection or by using a variety of legal mechanisms, including the US Privacy Shield and Standard Contractual Clauses, to help ensure your rights and protections.

Our US offices have Privacy Shield certification. **ADELPHI's** Privacy Shield certification, along with additional information about the Privacy Shield, can be found at <https://www.privacyshield.gov/>.

How we protect your information?

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

To protect your personal data **ADELPHI** employ:

- technical measures, including but not limited to, robust network security, firewalls, anti-virus protection, regular internal and external oversight and inspection, including penetration testing, access controls, audit trails, encryption of devices and data both whilst at rest and during any transmission to and from third parties in order to keep your personal data secure.
- organisational measures including, but not limited to, training of all individuals who process personal data in data protection and information governance, the creation of and adherence to appropriate policies and procedures.

Your data protection rights

You have specific rights connected to provision of your personal information to **ADELPHI**, although in some cases these rights are subject to certain conditions and limitations. To exercise any of these rights please contact us using the contact details in section Contact details on page 10.

Right to be informed

You have the right to be told how your personal information is/will be used. This Privacy Policy and our Recruitment and Workplace Privacy notices are intended to provide a clear and transparent description of how your personal data may be used.

Right of access to your information

You can request a copy of the information held relating to you. Please ensure that you include your name and clear instructions on what you would like us to do. If you require us to supply you with details of the personal information that we hold about you, then we will provide this information free of charge and we will provide this information to you within one month of your request unless the request is complex or is numerous requests. If this is the case, we will inform you within one month of your request about the reason for the extension of time.

Right of erasure (right to be forgotten)

You have the right to have your personally identifiable data deleted.

Right of rectification

If you believe the records that **ADELPHI** keep are inaccurate, you have the right to ask for these to be updated.

Opt-out of marketing communications

You have the right to opt-out of marketing communications we send you at any time. You can exercise this right by clicking on the “unsubscribe” or “opt-out” link in the marketing e-mails we send you. You can also opt-out of other forms of marketing (such as postal marketing or telemarketing), by contacting us.

Withdraw your consent

If we have collected and processed your personal information with your consent, then you can withdraw your consent at any time. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your personal information conducted in reliance on lawful processing grounds other than consent.

Complaints

If you have complaints relating to our processing of your personal data, you should raise these with the **ADELPHI** compliance department; see section [Contact details on page 10](#), or you can raise directly with the relevant supervisory authority.

In the UK: Information Commissioner’s Office (ICO). They can be contacted via their website <https://ico.org.uk/>

In the Netherlands: Autoriteit Persoonsgegevens. They can be contacted via their website <https://autoriteitpersoonsgegevens.nl>

Contact details

Adelphi Group
ATTN: Compliance Department
Adelphi Mill, Bollington Cheshire SK10 5JB, UK
Email: compliance.team@adelphigroup.com .

Adelphi Group (Excerpta Medica)
ATTN: Compliance Department Apollo Building, Herikerbergweg 17 1101 CN Amsterdam, Netherlands
Email: compliance.team@adelphigroup.com

Changes to this privacy policy

We keep our privacy policy under regular review and reserve the right to revise it at any time. Any changes we may make to our privacy policy in the future will be posted on this page. There is a date at the beginning of this policy which indicates the date it was updated. Please revisit this policy each time you consider giving personal information.

ADELPHI GROUP

EU-U.S. Privacy Shield: Consumer Privacy Policy

Last Updated: 30th September 2016

ADELPHI GROUP and its operating subsidiaries Adelphi Values, Adelphi Research, Adelphi Communications, Excerpta Medica and The Planning Shop International (collectively, “Adelphi”) respect your concerns about privacy. Adelphi participates in the EU-U.S. Privacy Shield framework (“Privacy Shield”) issued by the U.S. Department of Commerce. Adelphi commits to comply with the Privacy Shield Principles with respect to Consumer Personal Data the company receives from the EU in reliance on the Privacy Shield. This Policy describes how Adelphi implements the Privacy Shield Principles for Consumer Personal Data.

For purposes of this Policy:

“Consumer” means any natural person who is located in the EU, but excludes any individual acting in his or her capacity as an Employee.

“Controller” means a person or organization which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

“Employee” means any current, former or prospective employee, temporary worker, intern or other non-permanent employee of any subsidiary or affiliate of Adelphi, who is located in the EU.

“EU” means the European Union and Iceland, Liechtenstein and Norway.

“Personal Data” means any information, including Sensitive Data, that is (i) about an identified or identifiable individual, (ii) received by Adelphi in the U.S. from the EU, and (iii) recorded in any form.

“Privacy Shield Principles” means the Principles and Supplemental Principles of the Privacy Shield.

“Processor” means any natural or legal person, public authority, agency or other body that processes Personal Data on behalf of a Controller.

“Sensitive Data” means Personal Data specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life, the commission or alleged commission of any offense, any proceedings for any offense committed or alleged to have been committed by the individual or the disposal of such proceedings, or the sentence of any court in such proceedings.

“Supplier” means any supplier, vendor or other third party located in the EU that provides services or products to Adelphi.

Adelphi’s Privacy Shield certification, along with additional information about the Privacy Shield, can be found at <https://www.privacyshield.gov/>. For more information about Consumer Personal Data processing with respect to information obtained through Adelphi’s website, please visit the [Online Privacy Notice](#).

Types of Personal Data Adelphi Collects

Adelphi collects Personal Data directly from Consumers. This collection occurs, for example, when a Consumer visits Adelphi’s website. The company may use this information for the purposes indicated in the [Online Privacy Notice](#).

The types of Consumer Personal Data Adelphi collects includes:

- Contact information, such as name, postal address, email address and telephone number; and
- Personal Data in content Consumers provide on Adelphi’s website and other data collected automatically through the website (such as IP addresses, browser characteristics, device characteristics, operating system, language preferences, referring URLs, information on actions taken on our website, and dates and times of website visits).

In addition, Adelphi obtains Personal Data, such as contact information and financial account information, of its Suppliers’ representatives. Adelphi uses this information to manage its relationships with its Suppliers, process payments, expenses and reimbursements, and carry out Adelphi’s obligations under its contracts with the Suppliers.

Adelphi also may obtain and use Consumer Personal Data in other ways for which Adelphi provides specific notice at the time of collection.

Adelphi’s privacy practices regarding the processing of Consumer Personal Data comply with the Privacy Shield Principles of Notice; Choice; Accountability for Onward Transfer; Security; Data Integrity and Purpose Limitation; Access; and Recourse, Enforcement and Liability.

Notice

Adelphi provides information in this Policy and the [Online Privacy Notice](#) about its Consumer Personal Data practices, including the types of Personal Data Adelphi collects, the types of third parties to which Adelphi discloses the Personal Data and the purposes for doing so, the rights and choices Consumers have for limiting the use and disclosure of their Personal Data, and how to contact Adelphi about its practices concerning Personal Data.

Relevant information also may be found in notices pertaining to specific data processing activities.

Choice

Adelphi generally offers Consumers the opportunity to choose whether their Personal Data may be (i) disclosed to third-party Controllers or (ii) used for a purpose that is materially different from the purposes for which the information was originally collected or subsequently authorized by the relevant Consumer. To the extent required by the Privacy Shield Principles, Adelphi obtains opt-in consent for certain uses and disclosures of Sensitive Data. Consumers may contact Adelphi as indicated below regarding the company's use or disclosure of their Personal Data. Unless Adelphi offers Consumers an appropriate choice, the company uses Personal Data only for purposes that are materially the same as those indicated in this Policy.

Adelphi shares Consumer Personal Data with its affiliates and subsidiaries. Adelphi may disclose Consumer Personal Data without offering an opportunity to opt out, and may be required to disclose the Personal Data, (i) to third-party Processors the company has retained to perform services on its behalf and pursuant to its instructions, (ii) if it is required to do so by law or legal process, or (iii) in response to lawful requests from public authorities, including to meet national security, public interest or law enforcement requirements. Adelphi also reserves the right to transfer Personal Data in the event of an audit or if the company sells or transfers all or a portion of its business or assets (including in the event of a merger, acquisition, joint venture, reorganization, dissolution or liquidation).

Accountability for Onward Transfer of Personal Data

This Policy and the [Online Privacy Notice](#) describe Adelphi's sharing of Consumer Personal Data.

Except as permitted or required by applicable law, Adelphi provides Consumers with an opportunity to opt out of sharing their Personal Data with third-party Controllers. Adelphi requires third-party Controllers to whom it discloses Consumer Personal Data to contractually agree to (i) only process the Personal Data for limited and specified purposes consistent with the consent provided by the relevant Consumer, (ii) provide the same level of protection for Personal Data as is required by the Privacy Shield Principles, and (iii) notify Adelphi and cease processing Personal Data (or take other reasonable and appropriate remedial steps) if the third-party Controller determines that it cannot meet its obligation to provide the same level of protection for Personal Data as is required by the Privacy Shield Principles.

With respect to transfers of Consumer Personal Data to third-party Processors, Adelphi (i) enters into a contract with each relevant Processor, (ii) transfers Personal Data to each such Processor only for limited and specified purposes, (iii) ascertains that the Processor is obligated to provide the Personal Data with at least the same level of privacy protection as is required by the Privacy Shield Principles, (iv) takes reasonable and appropriate steps to ensure that the Processor effectively processes the Personal Data in a manner consistent with Adelphi's obligations under the Privacy Shield Principles, (v) requires the Processor to notify Adelphi if the Processor determines that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shield Principles, (vi) upon notice, including under (v) above, takes

reasonable and appropriate steps to stop and remediate unauthorized processing of the Personal Data by the Processor, and (vii) provides a summary or representative copy of the relevant privacy provisions of the Processor contract to the Department of Commerce, upon request. Adelphi remains liable under the Privacy Shield Principles if the company's third-party Processor onward transfer recipients process relevant Personal Data in a manner inconsistent with the Privacy Shield Principles, unless Adelphi proves that it is not responsible for the event giving rise to the damage.

Security

Adelphi takes reasonable and appropriate measures to protect Consumer Personal Data from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into account the risks involved in the processing and the nature of the Personal Data.

Data Integrity and Purpose Limitation

Adelphi limits the Consumer Personal Data it processes to that which is relevant for the purposes of the particular processing. Adelphi does not process Consumer Personal Data in ways that are incompatible with the purposes for which the information was collected or subsequently authorized by the relevant Consumer. In addition, to the extent necessary for these purposes, Adelphi takes reasonable steps to ensure that the Personal Data the company processes is (i) reliable for its intended use, and (ii) accurate, complete and current. In this regard, Adelphi relies on its Consumers to update and correct the relevant Personal Data to the extent necessary for the purposes for which the information was collected or subsequently authorized. Consumers may contact Adelphi as indicated below to request that Adelphi update or correct relevant Personal Data.

Subject to applicable law, Adelphi retains Consumer Personal Data in a form that identifies or renders identifiable the relevant Consumer only for as long as it serves a purpose that is compatible with the purposes for which the Personal Data was collected or subsequently authorized by the Consumer.

Access

Consumers generally have the right to access their Personal Data. Accordingly, where appropriate, Adelphi provides Consumers with reasonable access to the Personal Data Adelphi maintains about them. Adelphi also provides a reasonable opportunity for those Consumers to correct, amend or delete the information where it is inaccurate or has been processed in violation of the Privacy Shield Principles, as appropriate. Adelphi may limit or deny access to Personal Data where the burden or expense of providing access would be disproportionate to the risks to the Consumer's privacy in the case in question, or where the rights of persons other than the Consumer would be violated. Consumers may request access to their Personal Data by contacting Adelphi as indicated below.

Recourse, Enforcement and Liability

Adelphi has mechanisms in place designed to help assure compliance with the Privacy Shield Principles. Adelphi conducts an annual self-assessment of its Consumer Personal Data practices to verify that the attestations and assertions Adelphi makes about its Privacy Shield privacy practices are true and that Adelphi's privacy practices have been implemented as represented and in accordance with the Privacy Shield Principles.

Consumers may file a complaint concerning Adelphi's processing of their Personal Data. Adelphi will take steps to remedy issues arising out of its alleged failure to comply with the Privacy Shield Principles. Consumers may contact Adelphi as specified below about complaints regarding Adelphi's Consumer Personal Data practices.

If a Consumer's complaint cannot be resolved through Adelphi's internal processes, Adelphi will cooperate with JAMS pursuant to the JAMS International Mediation Rules, available on the JAMS website at www.jamsadr.com/international-mediation-rules. JAMS mediation may be commenced as provided for in the relevant JAMS rules. The mediator may propose any appropriate remedy, such as deletion of the relevant Personal Data, publicity for findings of noncompliance, payment of compensation for losses incurred as a result of noncompliance, or cessation of processing of the Personal Data of the Consumer who brought the complaint. The mediator or the Consumer also may refer the matter to the U.S. Federal Trade Commission, which has Privacy Shield investigatory and enforcement powers over Adelphi. Under certain circumstances, Consumers also may be able to invoke binding arbitration to address complaints about Adelphi's compliance with the Privacy Shield Principles.

How to Contact Adelphi

To contact Adelphi with questions or concerns about this Policy or Adelphi's Consumer Personal Data practices:

Write to:

President, Adelphi Research, 2005 S. Easton Road, Suite 300, Doylestown, PA 18901, USA

Or

Chief Operating Officer, Adelphi Group, Adelphi Mill, Grimshaw Lane, Bollington, Macclesfield, SK10 5JB, UK

E-mail: privacyshield@adelphigroup.com