Adelphi Group Data Privacy Framework Policy

This policy was last updated on May 10th , 2024.

Our commitment to your privacy

Adelphi Research by Design LLC trading as Adelphi Research

Doylestown Commerce Center, 2005 South Easton Road, Suite 300, Doylestown, PA 18901.

Adelphi Values LLC

One Lincoln Street, Suite 2400, Boston MA 02111.

THE PLANNING SHOP International, Inc.

Doylestown Commerce Center, 2005 South Easton Road, Suite 300, Doylestown, PA 18901.

Excerpta Medica LLC

Doylestown Commerce Center, 2005 South Easton Road, Suite 300, Doylestown, PA 18901.

(Collectively **ADELPHI)** respects your concerns about privacy. **ADELPHI** participates in the Data Privacy Framework Program issued by the U.S. Department of Commerce.

In this Policy, **ADELPHI**, **we**, and **us** means the **ADELPHI** companies listed above.

Definitions

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 organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- **'DPF'** means Data Privacy Framework Program.
- '**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 also includes the European Economic Area (EEA) countries: 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.
- '**Data Privacy Framework Program Principles'** means the Principles and Supplemental Principles of the Data Privacy Framework Program.
- '**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.

Data Privacy Framework Program certification

ADELPHI commits to comply with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, as set forth by the U.S. Department of Commerce. **ADELPHI** has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF.

This Policy describes how **ADELPHI** implements the Data Privacy Framework Program Principles for Consumer personal data.

The EU-U.S. DPF and UK Extension to the EU-U.S. DPF were respectively developed by the U.S. Department of Commerce, the European Commission, and the UK Government to provide U.S. organizations with reliable mechanisms for personal data transfers to the United States from the European Union, and the United Kingdom while ensuring data protection that is consistent with both EU and UK law.

If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles, the Principles shall govern. **ADELPHI**'s Data Privacy Framework (DPF) Program certification, along with additional information about the Data Privacy Framework (DPF), can be found at https://www.dataprivacyframework.gov/s/.

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;
- Personal data in the 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.

Personal data collected under the Data Privacy Framework

On July 10th, 2023, the European Commission adopted its adequacy decision for the EU-U.S. Data Privacy Framework program. The adequacy decision concludes that the United States ensures an adequate level of protection for personal data transferred from the EU to US companies participating in the Data Privacy Framework.

On the September 21st, the U.K. Parliament approved secondary regulations to extend the framework to the UK. The UK – EU – U.S. extension of the Data Privacy framework has now taken effect.

ADELPHI has adopted a separate Data Privacy Policy describing our compliance with the program, individual rights, and redress information.

Our commitments to Data Privacy Framework (DPF) are enforceable by the US Federal Trade Commission, and any personal data collected by **ADELPHI** under DPF, complies with the principles set out in the DPF. To learn more about the Data Privacy Framework program, and to view our certification, please visit

https://www.dataprivacyframework.gov/s/.

Transfers by us – where we disclose personal data

We may transmit personal data to certain third parties (as listed in the 'who we share your personal data with' section) that are located in countries that do not protect personal data to the same standard as the GDPR, including to: (1) our different global offices; and (2) our different offices in the Omnicom Group entities, networks, or partners agencies.

These countries may not give you the same rights in relation to your personal data and may not have a data protection supervisory authority to help you if you have any concerns about the processing of your personal data.

However, when transferring your personal data, we will ensure that, where required by the GDPR, at least one of the following applies: (1) we will only transfer your personal data to countries or organisations that have been deemed to provide an adequate level of protection for personal data by the UK Government or the European Commission; or (2) we may use specific contracts approved by the UK Government or the European Commission referred to as the "Standard Contractual Clauses" or "SSCs" which give personal data the same protection it has in the UK and EU.

To find out more about the SCCs we use, please email us at: compliance.team@adelphigroup.com

In addition, where we disclose personal data that we process in connection with our participation in the EU-U.S. Data Privacy Framework and/or the UK Extension to that framework, we remain liable under those frameworks in relation to our onward transfer of personal data to these countries, unless we can show that we are not responsible for the event giving rise to the damage.

Transfers to us – where we receive personal data

Any data that you provide directly to us, or that is received from third parties, may be stored in the USA. In addition, it may be transferred by us to other countries (as described above).

ADELPHI complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF as set forth by the U.S. Department of Commerce. **ADELPHI** has certified to the U.S. Department of Commerce that it adheres to the Data Privacy Framework Principles (EU-U.S. DPF and the UK Extension to the EU-U.S. DPF) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF.

Data Subject Rights

Data subjects may exercise these rights verbally or in writing using our contact information provided in the 'How to contact us' section. We will endeavour to promptly respond to your requests. Where you ask us to provide a copy of your personal data, we are legally obliged to respond within one calendar month of such request. If your request is denied, we will inform you about the reasons for denial.

Please note that in order for you to assert these rights, we may need to verify your identity to confirm your right to access your personal data. This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. In order to verify your identity, we may need to gather more personal data from you than we currently have.

Lodging complaints

In addition, you may have the right to lodge certain complaints in relation to our processing of your personal data with regulators in your jurisdiction.

If you have a concern about any aspect of our privacy practices, including the way we have handled your personal data, we encourage you to first contact us using our contact information provided in the 'How to contact us' section.

If the GDPR applies, you can report your concerns to the following organisations:

European Economic Area	You can find a list of supervisory authorities and their contact details for the EEA at http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm
United Kingdom	The Information Commissioner's Office ("**ICO**") is the supervisory authority in the United Kingdom. Contact details for the ICO can be found at https://ico.org.uk.

United States of America	In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, **ADELPHI** commits to refer unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF to JAMS, an alternative dispute resolution provider based in the United States. If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit https://www.jamsadr.com/DPF-Dispute-Resolution for more information or to file a complaint. The services of JAMS are provided at no cost to you. Following the dispute resolution process, JAMS or you may refer the matter to the U.S. Federal Trade Commission, which has investigatory and enforcement powers over us. Under certain circumstances, you also may be able to invoke binding arbitration to address complaints about our compliance with DPF Principles.

Data Privacy Framework principles

ADELPHI's privacy practices regarding the processing of Consumer personal data comply with the Data Privacy Framework 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 Data Privacy Framework Principles, **ADELPHI** obtains opt-in consent for certain uses and disclosures of Sensitive Data. Consumers may contact **ADELPHI,** see section How to Contact Adelphi on page 8, 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 Data Privacy Framework 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 Data Privacy Framework 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 Data Privacy Framework 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 Data Privacy Framework 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 Data Privacy Framework 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 Data Privacy Framework Principles if the company's third-party Processor onward transfer recipients process relevant personal data in a manner inconsistent with the Data Privacy Framework 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, considering 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 authorised 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 authorised. Consumers may contact **ADELPHI ,** see section How to Contact Adelphi on page 8, 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 authorised 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 Data Privacy Framework 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,** see section How to Contact Adelphi on page 8,

Recourse, enforcement, and liability

ADELPHI has mechanisms in place designed to help assure compliance with the Data Privacy Framework Principles. **ADELPHI** conducts an annual self-assessment of its Consumer personal data practices to verify that the attestations and assertions **ADELPHI** makes about its Data Privacy Framework privacy practices are true and that **ADELPHI**'s privacy practices have been implemented as represented and in accordance with the Data Privacy Framework 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 Data Privacy Framework 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 https://www.jamsadr.com/eu-us-data-privacy-framework. 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 Data Privacy Framework 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 Data Privacy Framework Principles.

How to Contact Adelphi

To contact **ADELPHI** with questions or concerns about this Policy or **ADELPHI**'s Consumer personal data practices:

Adelphi Group (UK office), ATTN: Compliance Department

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

Adelphi Group (**Netherlands office**), ATTN: Compliance Department

Professor W.H. Keesomlaan 4
1183 DJ Amstelveen, The Netherlands.
Email: compliance.team@adelphigroup.com

Adelphi Group (US office), ATTN: Compliance Department

Doylestown Commerce Center, 2005 South Easton Road, Suite 300, Doylestown, PA 18901
Email: compliance.team@adelphigroup.com

Issue Date	Effective date	Version	Author	Reviewed by	Name and Title	Approver signature
10/05/2024	04/06/2024	V1.0	Kristen Massey Adelphi Group Compliance	Kirstie Hill Adelphi Group Compliance	Lloyd Morgan Adelphi Group Board Compliance Lead	

Date	Version	Document Revision History	Document Author
10/05/2024	V1.0	• Removal of any references to the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF). • Further text added under Principles to ensure consistent referral to Adelphi's commitments to the rights of EU and UK individuals. • Language included in Certification section to inform individuals about the relevant European data protection authority designated to address complaints.	Kristen Massey