Data Privacy Framework Policy

Policy Name	Data Privacy Framework Policy				
Policy No.		Version		Effective Date	04/03/2024
Owner	Larry Wescott		Email	privacy@areteir.com	

Purpose

This Data Privacy Framework Policy (the "**Policy**") sets forth Arete's policies and procedures with respect to the Processing of Personal Data transferred from the European Union ("**EU**") under the EU-U.S. Data Privacy Framework and the United Kingdom ("**UK**") under the UK Extension to the Data Privacy Framework (collectively, the "**DPF**").

Scope

This Data Privacy Framework Policy applies to all Personal Data received by Arete from the EU or the UK in reliance upon the DPF in any format, including electronic, paper, or verbal, and all Arete employees who have access to such Personal Data. The protection afforded to Personal Data by the DPF Principles (the "**Principles**") and this Data Privacy Framework Policy applies to any EU or UK individual whose Personal Data has been transferred from the EU or UK to Arete in the United States in reliance upon the DPF. The rights described herein are applicable to all Arete employees, with the exception that the Independent Recourse Mechanism described in section 1.7.3 of this Policy is available to EU and UK employees only.[1] The U.S. entities adhering to the Principles under the DPF are Arete Advisors, LLC and Arete Incident Response, LLC.

[1] The independent recourse mechanism is a unique right available only under foreign law.

Definitions

The following definitions apply to this Policy:

1. "**Agent**" means a third party that Processes Personal Data on behalf, and under the instructions of Company.
2. "**Company**" means Arete located in the United States.
3. "**Confidential Commercial Information**" means information that an organization has taken steps to protect from disclosure, where disclosure would help a competitor in the market.
4. "**Controller**" means a person or entity which, alone or jointly with others, determines the purpose(s) and means of Processing of Personal Data.
5. "**Data Protection Authorities**" or "**DPA**" means Member State data protection authorities and the United Kingdom's Information Commissioner's Office.
6. "**Data Subject**" means an EU or UK individual whose Personal Data has been transferred from the EU or UK to Company in the United States under the DPF.
7. "**Department of Commerce**" means the United States Department of Commerce.
8. "**European Union**" or "**EU**" means, collectively the Member States of the European Union.
9. "**FTC**" means the United States Federal Trade Commission.
10. "**GDPR**" means EU's General Data Protection Regulation, Regulation (EU) 2016/679, and the United Kingdom's GDPR ("UK GDPR"), as implemented by the Data Protection Act of 2018.
11. "**Human Resources Data**" means Personal Data about employees of Company and/or a Company affiliate in the EU (past or present) collected in the context of the employment relationship and transferred to Company in the United States under the DPF for use in the context of the employment relationship.
12. "**Human Resources Data Privacy Notice**" means the Company's policy regarding the use and disclosure of Human Resources Data received from the EU or UK.
13. "**Member States**" means the member countries of the EU, including Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden.
14. "**Personal Data**" means any data about an identified or identifiable Data Subject that is within the scope of the GDPR, received by Company in the United States from the EU or UK under the DPF. Personal Data includes, but is not limited to, Human Resources Data and Sensitive Data.
15. "**Principles**" means the DPF Principles of Notice; Choice; Accountability for Onward Transfer; Security; Data Integrity and Purpose Limitation; Access; and Recourse, Enforcement and Liability, including the Supplemental Principles, issued by the Department of Commerce.
16. "**Privacy Policy**" means Company's website privacy policy or policies regarding the use and disclosure of Personal Data received from the EU or UK.

17. "**DPF List**" means the list maintained and made available to the public by the Department of Commerce of organizations that have self-certified to the DPF and declared their commitment to adhere to the Principles.
    The DPF List is available at https://www.dataprivacyframework.gov/s/participant-search.
18. "**Processing**" (and its conjugates, including without limitation, "Process") means any operation or set of operations which is performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination, and erasure or destruction.
19. "**Sensitive Data**" means Personal Data specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of a Data Subject. Sensitive Data shall also include any Personal Data received by Company from a third party where the third party identifies and treats such Personal Data as sensitive.
20. "**Transferring Entity**" means any person or entity that transfers Personal Data from the EU or UK to Company in the United States under the DPF.

Policy

1.1 Notice

1.1.1 Timing of Notice.

a. Company will provide the Notice required by the DPF through its Privacy Policy and Human Resources Data Privacy Notice. Company's Privacy Policy shall be posted on Company's website and Company's Human Resources Data Privacy Notice shall be posted in a location accessible by Company's affected employees. The relevant notice shall be provided to Data Subjects in clear and conspicuous language when Data Subjects are first asked to provide Personal Data to Company, or as soon thereafter as is practicable.
b. Unless otherwise permitted by the Principles, Company will provide Data Subjects additional Notice that contains the requirements of section 1.1.2 below, before Personal Data is used for different purposes than that for which it was originally collected and before it is disclosed to a third party.

1.1.2 Content of Notice

Company shall include in its Privacy Policy, Human Resources Data Privacy Notice, and additional notices:

a. Statements that (i) Company is participating in the DPF; (ii) Company is subject to the investigatory and enforcement powers of the FTC with respect to representations concerning the Personal Data at issue; and (iii) Company is liable in cases of onward transfers;
b. The Subsidiaries of Company that are also adhering to the Principles;

c. A description of the Processing, including types of Personal Data collected, purposes for which Personal Data is collected and used, and the types or identity of third parties to which Personal Data will be disclosed and the purposes for such disclosures;
d. A description of Data Subject Rights and how Data Subjects may exercise those rights;
e. Contact information for any inquiries or complaints, including any relevant contact point in the EU or UK that can respond to such inquiries or complaints;
f. The independent dispute resolution body designated to address complaints and provide appropriate recourse free-of-charge, and whether such body is based in the EU, UK, or the U.S. or is the panel established by DPAs;
g. The possibility under certain conditions for the individual to invoke binding arbitration;
h. The link to website or complaint submission form of chosen independent recourse mechanism.

1.2 Choice

1.2.1 Opt-Out Requirements

Company shall offer Data Subjects the opportunity to choose (opt- out) whether their personal data is (i) disclosed to a third party, except for third parties acting as an Agent that Company has contracted with to perform tasks on behalf of Company; or (ii) used for materially different purposes than for which Personal Data was originally collected. When Company provides the additional Notice required by Section 1.1.1(b) above, such notice shall include a clear, conspicuous, and readily available mechanism for Data Subjects to opt out of such uses of their Personal Data.

a. If a Company employee must use Personal Data for a materially different purpose than for which Personal Data was originally collected or disclose Personal Data to third parties, employee shall escalate to the Legal and Privacy Office at privacy@areteir.com, who will direct employee how to proceed in compliance with the DPF.

1.2.2 Opt-In Requirements (Sensitive Data)

Except as provided in Section 1.2.3 below, Company will obtain affirmative consent from Data Subjects before disclosing Sensitive Data to a third party or Processing Sensitive Data for a purpose other than that for which it was originally collected or subsequently authorized by the Data Subject through the exercise of opt-in choice.

a. If a Company employee must disclose Sensitive Data to a third party or Process Sensitive Data for a purpose other than that for which it was originally collected or subsequently authorized by the Data Subject, employee shall escalate to the Legal and Privacy Office at privacy@areteir.com, who will direct employee how to proceed in compliance with the DPF.

1.2.3 Opt-In Exemption

Company is not required to obtain opt-in consent from Data Subjects where the Processing is: (i) in the vital interests of the Data Subject or another person; (ii) necessary for the establishment of legal claims or defenses; (iii) required to provide medical care or diagnosis; (iv) necessary to carry

out the Company's obligations in the field of employment law; or (v) related to data that are manifestly made public by the Data Subject.

1.3 Accountability for Onward Transfer

1.3.1 Transfers to Third Party Controllers

If Company transfers Personal Data to a third party acting as a Controller, Company shall:

a. Comply with the Notice (Section 1.1) and Choice (Section 1.2) Principles;
b. Enter into a contract with the third-party Controller that provides that (i) Personal Data may only be Processed for a limited and specific purpose consistent with the consent provided by the Data Subjects and (ii) that the third-party Controller will provide the same level of protection as the Principles and will notify Company if it makes a determination that it can no longer meet this obligation.

1.3.2 Transfers of Human Resources Data for Operational Purposes

For occasional employment-related operational needs of Company with respect to Human Resources Data (such as the booking of a flight, hotel room, or insurance coverage), Company may transfer the Personal Data of a small number of employees to third-party Controllers without entering into a contract with such third-party Controllers, provided that Company complies with the Notice and Choice Principles.

1.3.3 Transfers to Third Party Agents

If Company transfers Personal Data to a third party acting as an Agent, Company shall:

a. Enter into a contract with Agent that provides that (i) Processing will be limited to the purposes specified in the contract, (ii) the Agent will provide at least the same level of protection as required by the Principles and will notify the organization if it can no longer meet their obligations, and (iii) Agent will indemnify Company for any liability related to its non-compliance with the Principles;
b. Transfer such Personal Data only for limited purposes as specified in the contract with the Agent;
c. Ascertain that the Agent is obligated to provide at least the same level of privacy protection as is required by the Principles by requiring Agent to provide satisfactory written assurance to Company that it will protect the Personal Data in a manner substantially consistent with the DPF or, alternatively, with the standards contained in the GDPR;
d. Take reasonable and appropriate steps to ensure that the Agent effectively processes the Personal Data transferred in a manner consistent with Company's obligations under the Principles by conducting audits and inspections of Agent;
e. Require the Agent to notify Company if Agent makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles;
f. Upon notice, including under subsection 1.3.3, take reasonable and appropriate steps to stop and remediate unauthorized Processing. If Company is unable to remediate the

situation, Company will request that the Agent return or delete all of the Personal Data and otherwise stop engaging in the business activity that requires the Agent to access the Personal Data;

g. Provide a summary or a representative copy of the relevant privacy provisions of its contract with that Agent to the Department of Commerce upon request.

1.3.4 If a Company employee must transfer Personal Data to a new third-party Controller or Agent, employee shall escalate to the Legal and Privacy Office at privacy@areteir.com, who will direct employee how to proceed in compliance with the DPF.

1.4 Security

Company shall take reasonable and appropriate measures to protect 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. This includes, for example, having an incident response and security breach notification plan in place, training employees on appropriate safeguards and contractually ensuring that third parties with access to the Personal Data maintain appropriate safeguards.

1.5 Data Integrity and Purpose Limitation

1.5.1 Purpose Limitation

Company shall limit the Processing of Personal Data to that which is relevant for the purpose of the Processing. Company shall not Process Personal Data in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the Data Subjects.

1.5.2 Data Integrity

To the extent necessary for the purposes for which Personal Data was collected or subsequently authorized by the Data Subject, Company shall take reasonable steps to ensure that such Personal Data is reliable for its intended use, accurate, complete, and current.

1.5.3 Data Retention

Company shall retain Personal Data in accordance with Company's Record Retention Policy. In addition, Company may retain Personal Data in a form identifying or making identifiable the Data Subject only for so long as it serves a purpose for which such Personal Data has been collected or subsequently authorized by relevant Data Subject. These data retention obligations do not prevent Company from Processing Personal Data for longer periods for the time and to the extent such Processing reasonably serves the purposes of archiving in the public interest, scientific or historical research, and statistical analysis. In these cases, such Processing shall be subject to the other Principles (as applicable).

1.6 Access

1.6.1 Access Rights

Company permits reasonable access by Data Subjects to the Personal Data about that Data Subject that Company stores or otherwise Processes and allows Data Subjects to request that their Personal Data be corrected, amended, or deleted where it is inaccurate or processed in violation of the Principles. Company shall provide in its Privacy Policy and Human Resources Data Privacy Notice how Data Subjects may submit requests for access, amendment, correction, or deletion. Upon request, Company will provide a Data Subject access to Personal Data about them in the form of disclosures.

1.6.2 Responding to Access Requests

a. No Justification Required
   Company shall not require Data Subjects to justify requests for access to their Personal Data. However, in responding to Data Subjects' access requests, Company may communicate with Data Subjects as necessary to better understand the motivation for the request and to locate the responsive information.
b. Good Faith Effort
   Company shall make a good faith effort to provide access if a Data Subject requests access. If certain information needs to be protected and can be readily separated from other Personal Data subject to an access request, Company may redact the protected information and make available the other information. If Company determines that access should be restricted in any particular instance, Company will provide the Data Subject requesting access with an explanation of why it has made that determination and a contact point for any further inquiries. Company shall not restrict or limit access to Personal Data solely on costs grounds if Data Subject offers to pay such costs.
c. No Database Access
   Company may provide access in the form of disclosure of the relevant Personal Data to the Data Subject. Data Subject assess to Company's databases is not required.
d. Available Information Only
   Company needs to provide access to Data Subjects only to the extent that Company stores or otherwise Processes the relevant Personal Data. Where Company does not store or otherwise Process the relevant Personal Data, Company shall provide Data Subjects with confirmation that Company does not have Personal Data relating to such Data Subjects.
e. Access Fee
   Company may charge a fee for providing access that is not excessive and limited to Company's reasonable costs associated with providing such access.
f. Timeframe and Form for Responses
   When Company receives an access request, Company shall respond to access requests within a reasonable time period, in a reasonable manner and in a form that is readily intelligible to Data Subjects.
g. If a Company employee receives an access request from a Data Subject, employee shall escalate to the Legal and Privacy Office at privacy@areteir.com, who will direct employee how to proceed in compliance with the DPF.

1.6.3 Restricting Access

Company shall only deny or limit a Data Subject's right of access in exceptional circumstances, and any denial of or limitation to the right of access shall be necessary and duly justified based on one or more of the grounds set forth in this Section 1.6.3:

a. Grounds for Restricting Access
    i. Burden or Expense of Providing Access
    Company may deny or limit a Data Subject's right of access to Personal Data if the legitimate rights of persons other than the Data Subject would be violated or if the burden or expense of providing access would be disproportionate to the risks to the Data Subject's privacy in the case in question.
    ii. Confidential Commercial Information
    Company may deny or limit a Data Subject's access to Personal Data to the extent that granting full access would reveal Company's own Confidential Commercial Information or the Confidential Commercial Information of a third party that is subject to a contractual obligation of confidentiality.
    iii. Countervailing Public Interests
    Company may deny or limit a Data Subject's access to Personal Data to the extent that disclosure is likely to interfere with the safeguarding of important countervailing public interests (such as national security, defense or public security).
    iv. Research or Statistical Purposes
    Company may deny or limit a Data Subject's access to Personal Data where such Personal Data is Processed solely for research or statistical purposes.
    v. Other Reasons to Deny Access
    Other reasons Company may deny or limit access are: (a) interference with the execution or enforcement of the law or with private causes of action, including the prevention, investigation or detection of offenses or the right to a fair trial; (b) disclosure where the legitimate rights or important interests of others would be violated; (c) breaching a legal or other professional privilege or obligation; (d) prejudicing employee security investigations or grievance proceedings or in connection with employee succession planning and corporate re- organizations; or (e) prejudicing the confidentiality necessary in monitoring, inspection or regulatory functions connected with sound management, or in future or ongoing negotiations involving Company.

b. Repetitious or Vexatious Requests for Access
    Company may set reasonable limits on the number of times within a given period that access requests from a particular Data Subject will be met.
c. Fraudulent Requests
    Company is not required to provide access unless the Company has sufficient information to allow it to confirm the identity of the Data Subject making the request.

1.7 Recourse, Enforcement, and Liability

1.7.1 Compliance Mechanisms

Company shall have robust mechanism for assuring compliance with the Principles, including a Verification process as described in Section 2.2.2 below, an Internal Redress Mechanism as described in section 1.7.2 below, and an Independent Recourse Mechanism as described in Section 1.7.3 below. Company encourages interested persons to raise any concerns by contacting the Legal and Privacy Office at privacy@areteir.com. Company will investigate and attempt to resolve any complaints and disputes regarding use and disclosures of Personal Data in accordance with the Principles and as further described in Section 1.7.2, 1.7.3, and 1.7.4 below.

1.7.2 Internal Redress Mechanism

If Company receives an inquiry or complaint from a Data Subject, Company will designate a contact point to handle inquiries and complaints and shall respond within 45 days of receiving that inquiry or complaint at no cost to the Data Subject. If a Company employee receives an inquiry or complaint from a Data Subject, employee shall escalate to the Legal and Privacy Office at privacy@areteir.com, who will direct employee how to proceed in compliance with the DPF.

1.7.3 Independent Recourse Mechanism

a. General
   Company has selected the American Arbitration Association's International Center for Dispute Resolution (AAA-ICDR) as its approved independent recourse mechanism for handling Data Subject complaints and disputes that cannot be resolved internally. The AAA-ICDR must investigate and expeditiously resolve complaints at no cost to Data Subjects, and must award damages where applicable law or private-sector initiatives so provide.
b. Human Resources Data
   Company selects the DPAs as its independent recourse mechanism with respect to Human Resources Data only, and declares its commitment to cooperate with the DPA with regard to such Human Resources Data. Company shall: (i) respond directly to such DPAs with regard to the investigation and resolution of complaints regarding Human Resource Data; (ii) comply with the advice given by DPAs within 25 days of the delivery of such advice, unless Company provides a satisfactory explanation to the DPAs for any delay; and (iii) provide DPAs with written confirmation that such action has been taken.

1.7.4 Arbitration

Company shall arbitrate any residual claims (i.e., claims not resolved via Company's internal redress mechanism or selected independent recourse mechanism) raised by a Data Subject relating to whether Company has violated its obligations under the Principles in accordance and with and subject to the Data Privacy Framework Annex I: Arbitration Model, available at: https://www.dataprivacyframework.gov/s/article/ANNEX- I-introduction-dpf?tabset-35584=2.

1.7.5 Inquiries by Authorities

a. Responding to Inquiries
   Company shall respond promptly to inquiries and other requests for information from the Department of Commerce relating to the DPF. Company shall respond expeditiously to complaints regarding compliance with the Principles referred by EU Member State authorities and United Kingdom authorities through the Department of Commerce. If a Company employee receives an inquiry or complaint the Department of Commerce or other authority, employee shall escalate to the Legal and Privacy Office at privacy@areteir.com, who will direct employee how to proceed in compliance with the DPF.
b. Publishing Reports of Non-Compliance
   If Company becomes subject to an FTC or court order based on noncompliance, Company shall make public any relevant DPF- related sections of any compliance or assessment report, to the extent consistent with confidentiality requirements.

1.8 Application of the Principles

1.8.1 Effective Date
The principles apply immediately upon certification to the DPF by Company.

1.8.2 Personal Data Subject to the Principles
Company shall apply the Principles to all Personal Data transferred in reliance on the DPF after it certifies to the DPF, including by complying with this Policy.

1.8.3 Duration
Company shall apply the Principles to Personal Data transferred in reliance on the DPF for as long as Company stores, uses, discloses or otherwise Processes such Personal Data, even if it subsequently leaves the DPF for any reason.

1.8.4 Employee Training
Company shall train employees with access to DPF Personal Data on DPF policies and privacy practices.

1.8.5 Limitations on the Application of the Principles
Adherence to the Principles may be limited:

a. to the extent necessary to comply with a court order or meet public interest, law enforcement, or national security requirements, including where statute or government regulation create conflicting obligations;
b. by statute, court order, or government regulation that creates explicit authorizations, provided that, in exercising any such authorization, Company can demonstrate that its non-

compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or

c. if the effect of the GDPR is to allow exceptions or derogations, under the conditions set out therein, provided such exceptions or derogations are applied in comparable contexts.

2. Public Record and Publicly available Information

2.1 Applicable Principles

Company shall apply the Security, Data Integrity and Purpose Limitation, and Recourse, Enforcement and Liability Principles to Personal Data from publicly available sources by complying with this Policy with respect to such Personal Data. These Principles shall also apply to Personal Data collected from public records (i.e., records kept by government agencies or entities at any level that are open to consultation by the public in general).

2.2 Applicable Principles

It is not necessary for Company to apply the Notice, Choice, or Accountability for Onward Transfer Principles to public record information, as long as such information is not combined with non-public record information, and any conditions for consultation established by the relevant jurisdiction are respected. It is also generally not necessary to apply the Notice, Choice, or Accountability for Onward Transfer Principles to publicly available information unless the Transferring Entity indicates that such information is subject to restrictions that require application of those Principles by Company for the uses it intends.

2.3 Applicability of Access Principle

2.3.1 Public Record Information

It is not necessary for Company to apply the Access Principle to public record information as long as it is not combined with other personal information (apart from small amounts used to index or organize the public record information); however, any conditions for consultation established by the relevant jurisdiction are to be respected. In contrast, where public record information is combined with other non- public record information (other than as specifically noted above), Company shall provide access to all such information, assuming it is not subject to other permitted exceptions.

2.3.2 Publicly Available Information

It is not necessary for Company to provide access to information that is already publicly available to the public at large, as long as such information is not combined with non-publicly available information.

3. Self-Certification, Maintaining Certification and Ongoing Obligations

3.1 Self-Certification

3.1.1 General Requirements

In order to enter the DPF, Company shall:

a. Publicly declare Company's commitment to comply with the Principles, by stating so in Company's Privacy Policy. Accordingly, Arete adopts the following, and has included same within its Data Privacy Framework Notice: We comply with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. We have certified to the U.S. Department of Commerce that we adhere to the EU-U.S. Data Privacy Framework Principles ("DPF Principles") with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. If there is any conflict between the terms in this DPF Notice and the DPF Principles, the DPF Principles shall govern. To learn more about the DPF program please visit www.dataprivacyframework.gov.
b. Publicly disclose Company's Privacy Policy in line with the Principles, by posting the Privacy Policy on Company's Website, and
c. Fully implement the Privacy Policy.

3.1.2 Self-Certification

To self-certify for the DPF, Company shall provide to the Department of Commerce a self-certification submission, signed by a corporate officer on behalf of Company, that contains at least the following information:

a. Name of Company, mailing address, e-mail address, telephone and fax numbers;
b. A description of the activities of Company with respect to Personal Data that would be received from the EU under DPF;
c. A description of Company's relevant Privacy Policy: (i) the relevant web address where the Privacy Policy is available and (ii) its effective date of implementation;
d. A contact office within Company for the handling of complaints, access requests, and any other issues arising under the Principles, including: (i) the name(s), job title(s) (as applicable), e-mail address(es), and telephone number(s) of the relevant individual(s) or relevant contact office(s) within Company; and (ii) the relevant U.S. mailing address for Company;
e. That the FTC is the specific statutory body that has jurisdiction to hear any claims against Company regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy;
f. The name of any privacy program in which Company is a member;
g. The method of verification (i.e., self-assessment; or outside compliance reviews, including the third party that completes such reviews); and
h. The relevant independent recourse mechanism(s) available to investigate unresolved Principles-related complaints.

3.1.3 Cooperation with DPAs

Company shall also declare in its certification that Company:

a. Extends DPF benefits to Human Resources Data;
b. Elects to cooperate with the DPAs for purposes of meeting the Recourse, Enforcement, and Liability Principle;
c. Will cooperate with the DPAs in the investigation and resolution of DPF complaints; and
d. Will comply with any advice given by DPAs concerning remedial or compensatory measures for affected individuals, and will provide the DPAs with written confirmation of such actions.
e. Further, In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, Arete commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner's Office (ICO) regard to unresolved complaints concerning our handling of human resources data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF in the context of the employment relationship.
f. In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, Arete 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 International Centre for Dispute Resolution of the American Arbitration Association ("ICDR-AAA"), 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://go.adr.org/dpf_irm.html for more information or to file a complaint. The services of ICDR-AAA are provided at no cost to you.

3.2 Annual Re-Certification and Verification

3.2.1 Re-Certification

Company shall annually re-certify its participation in the DPF with the Department of Commerce via the DPF Program website.

3.2.2 Verification

Prior to re-certifying, Company shall verify that its published Privacy Policy and Human Resources Data Privacy Notice conform to the Principles and are in fact complied with, utilizing the self-assessment approach.

a. Self-Assessment: Verification shall indicate that:
    i. Company's published Privacy Policy and Human Resources Data Privacy Notice are accurate, comprehensive, prominently disclosed, completely implemented and accessible;
    ii. Company's Privacy Policy and Human Resources Data Privacy Notice conform to the Principles;

iii. Data Subjects are informed of internal arrangements for handling complains and of the independent mechanism through which they may pursue complaints;
iv. Company has in place procedures for training employees in the implementation of the Privacy Notice, Human Resources Data Privacy Notice, this Policy and Company's other DPF policies and privacy practices, and disciplining employees for failure to follow such notices, policies and privacy practices; and
v. Company has in place internal procedures for periodically conducting objective reviews of compliance with the above.

b. Verification Statement: A corporate officer or other authorized representative of Company shall sign a statement verifying the self-assessment at least once a year. This statement shall be made available to Data Subjects upon request or in the context of an investigation or complaint about non-compliance.

3.3 Privacy Policy Records

Company shall retain their records on the implementation of their DPF privacy practices and make them available upon request in the context of an investigation or a complaint about non-compliance to the independent dispute resolution body responsible for investigating complaints or to the FTC. Company shall also respond promptly to inquiries and other requests for information from the Department of Commerce relating to Company's adherence to the principles.

Version History

Version	Description	Revision Date	Review Date	Reviewer/Approver Name
1	Initial Version	03/18/2024		Andrew Taylor
1	Approved		03/29/2024	Mark Cluse
1.1	Corrected per Recommendations of the DPF Program	04/19/2024	04/19/2024	Mark Cluse