TRUSAIC

Data Processing Addendum

Updated 8.25.23

This Data Processing Addendum ("**DPA**") amends the terms and conditions set forth in the Pay Parity® Master Services Agreement and any riders or amendments thereto and the Terms of Service (collectively, "Agreement") between First Capitol Consulting, Inc. dba Trusaic ("Trusaic") and the client ("Client"), and shall be effective on the Effective Date of the AGREEMENT and terminate with the term of the Agreement. In the event of a conflict between the DPA and the Agreement, the DPA shall control. All capitalized terms not defined in this DPA shall have the meanings set forth in the AGREEMENT.

Unless otherwise agreed to in writing under the AGREEMENT, Trusaic will periodically update this DPA, located at {LINK}.

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this DPA shall have the following meaning:

1.1.1 "Client Personal Data" means any Personal Data Processed by the Processor on Controller's behalf pursuant to or in connection with an AGREEMENT;

1.1.2 "Controller" means Client with Client Personal Data for Data Processing;

1.1.3 "Processor" means Trusaic pursuant to an Agreement to Process Client Personal Data;

1.1.4 "GDPR" means EU General Data Protection Regulation 2016/679;

1.1.5 "Data Protection Laws" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR and to the extent applicable, the data protection or privacy laws of any other country;

1.1.6 "EEA" means the European Economic Area;

1.1.7 "Data Transfer" means:

1.1.7.1 a transfer of Client Personal Data from Controller to a Processor; or

1.1.7.2 an onward transfer of Client Personal Data from a Processor to a Subcontracted Processor, if any, or between two establishments of a Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or otherwise restricted under the AGREEMENT);

1.1.8 "Services" means the services identified in the Agreement.

1.1.9 "Subprocessor" means any person appointed by or on behalf of Processor to process Client Personal Data on behalf of Controller in connection with the Agreement.

1.1.10 ""Standard Contractual Clauses" or "SCC" means the European Commission's standard contractual clauses for the transfer of personal data from the European Union to third countries (Module One/Two/Three/Four), as set out in the Annex to Commission Decision (EU) 2021/914.

1.2 The terms, "**Commission**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their related terms shall be construed accordingly.

2. Processing of Client Personal Data

2.1 Processor shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Client Personal Data on behalf of Client; and

2.1.2 not process Client Personal Data other than on Controller's documented instructions.

2.2 Controller instructs Processor to process Client Personal Data to provide the services set forth in the AGREEMENT.

3. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Processor who may have access to Client Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know/access the relevant Client Personal Data, as strictly necessary for the purposes of the AGREEMENT, and to comply with all applicable Data Protection Laws in the context of that individual's duties to the Processor, ensuring that all such individuals are subject to confidentiality obligations.

4. Data Processing and Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall, in relation to the Client Personal Data, implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR and in Annex B.

4.2 In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

4.3 The Processing performed by the Processor on behalf of the Controller relates to the services under the AGREEMENT. Further details on International Transfers of Personal Data are located at Trusaic's Privacy Policy at https://trusaic.com/privacy-policy/.

5. Subprocessing

Processor shall not appoint (or disclose any Client Personal Data to) any Subprocessor unless required or authorized by Controller.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Processor shall assist Controller by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Controller obligations, as reasonably understood by Controller, to respond to requests by Data Subject to Processor to exercise Data Subject rights under the Data Protection Laws.

6.2 Processor shall:

6.2.1 promptly notify Controller if it receives a request from a Data Subject under the Data Protection Laws in respect of Client Personal Data; and

6.2.2 ensure that Processor respond to that request only pursuant to the documented instructions of Controller or as required by the Data Protection Laws to which the Processor is subject, in which case Processor shall to the extent permitted by the Data Protection Laws inform Controller of that legal requirement before the Processor responds to the request.

7. Personal Data Breach

7.1 Upon becoming aware of a Personal Data Breach affecting Client Personal Data and without undue delay, Processor shall notify Controller with sufficient information to allow Controller to meet an obligation to inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Processor shall cooperate with Controller and take reasonable commercial steps as are directed by Controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

Processor shall provide reasonable assistance to Controller with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Controller reasonably considers to be required by Article 35 or 36 of the GDPR, in each case solely in relation to Processing of Client Personal Data by, and taking into account the nature of the Processing

and information reasonably available to, the Processors.

9. Deletion or return of Client Personal Data

9.1 Subject to this section 9, Processor shall promptly and in any event within ten (10) business days of the date of termination of the AGREEMENT (the "Termination Date"), delete and procure the deletion of all copies of those Client Personal Data that is not subject to the Processors legal document retention obligations.

9.2 Upon written request by Controller, Processor shall provide written certification of compliance to Controller.

10. Audit rights

10.1 Subject to this section 10, Processor shall make available to Controller on request all information necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections, by Controller or an auditor mandated by Controller in relation to the Processing of the Client Personal Data by the Contracted Processors.

10.2 Information and audit rights of Controller only arise under section 10.1 to the extent that the DPA does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Laws.

11. Data Transfer

11.1 The Processor may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of Controller. Processor and Controller agree that the Personal Data Processed under the AGREEMENT, while physically located in the EU, maybe accessed by Processor from its headquarters in Los Angeles. To the extent that the GDPR categorizes such access as an international data transfer, and to ensure that the Personal Data is adequately protected, the parties incorporate the Standard Contract Clauses into the DPA.

11.2 The SCC published on June 4, 2021, can be found here. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en. Should the EU regulatory authority update the language of the standard contract clauses after the execution of the DPA, the parties agree that the new contract clauses shall be deemed incorporated into the DPA to the extent necessary to continue to comply with the EU rules regarding data transfers.

12. Governing Law and Jurisdiction

12.1 This DPA is governed by the law of the state of residence of the Controller. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

12.2 Any dispute arising in connection with this DPA, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of Ireland.

12.3 A data subject may also bring legal proceedings against the Processor and/or Controller before the courts of the EU Member State in which he/she has his/her habitual residence.

ANNEX A:

Personal Data Processing Purposes and Details

- Personal Data Categories:

  First & Last Name; Alias; Postal Address; Telephone number; Unique personal identifier; Social Security number (or equivalent); Financial information; Geolocation data; Professional or employment-related data; Compensation; Date of Birth; Race; Gender

- Data Subject Types:

  Client's global employees

- Countries where Processer may receive, access, transfer or store Personal Data:

  Store, transfer or receive: United States, EU Member States

  Access: United States, EU Member States

- Approved Subcontractors:

  Not Applicable

TRUSAIC

Annex B:

Security Measures: Technical and Organizational Data Security Measures:

1. PHYSICAL ACCESS CONTROLS.
    a. Monthly risk assessment meetings are held by the SPO and Legal team to discuss risk and mitigation strategies. For any risks or other control deficiencies identified that require attention or remediation, action plans are implemented to remediate such deficiencies and documented in meeting minutes.
    b. Physical access to the Client facilities, which house the servers in a room that is only accessible by the President, his Executive Assistant, and the Office Manager, is controlled through the use of physical keys and locks, in a 24/7 security building.
    c. The Client is located in one office suite with only two points of entry. The back entrance is only accessible with a key. The front entrance is secured during business hours by the receptionist, who is required to check in all visitors using a visitor's log, and is secured during non-business hours with key access.
    d. Physical access to the data center is restricted to authorized Advanced Networks personnel.
    e. A termination checklist is used and completed when revoking the physical access of terminated employees.
    f. The Client maintains a written agreement with a third-party vendor to dispose of equipment (PCs and other computing devices) containing confidential information using corporate grade data destruction technology (HIPAA and DoD compliant, NIST 800-88 one-pass random wipe or equivalent).
    g. Secure shred bins are provided throughout the facility for collection and disposal of confidential information.
2. SYSTEM ACCESS CONTROLS.
    a. The Client maintains security, confidentiality, and privacy policies (SCP policies), which are available to all employees on the Company's intranet (Asana). The SCP policies address controls over significant aspects of operations, including:
        i. Security requirements for authorized users.
        ii. Data classification and associated protection, access rights, retention, and destruction requirements.
        iii. Responsibility and accountability for security.
        iv. Security and other incidents identification response and mitigation.
        v. Security training.
        vi. Information sharing and disclosure.
    b. New employees must review and complete security, confidentiality, and privacy training, which occurs during the first week of employment.
    c. Monthly risk assessment meetings are held by the SPO and Legal team to discuss risk and mitigation strategies. For any risks or other control deficiencies identified that require attention or remediation, action plans are implemented to remediate such deficiencies and documented in meeting minutes.
    d. Advanced Networks, Trusaic's Managed Services IT Provider, assesses and responds to security risks on an ongoing basis and advises Trusaic management of those risks, reviewing and acting upon security event logs.
    e. System changes that may potentially impact Trusaic's service commitments and system requirements are communicated to all employees through the Company's intranet (Asana).

f. The Client maintains a Change Management Policy to address material changes to its system. The policy requires oversight by SPO to determine the potential effect of system changes on its service commitments and system requirements, including those related to internal controls.
g. Access to the network is restricted to authorized personnel and requires a unique user ID and password.
h. Remote access to the network is restricted to authorized personnel, requires a unique user ID and password, and users are authenticated using MFA with remote access over an encrypted VPN connection.
i. The Trusaic Platform infrastructure, which resides on the cloud infrastructure provided by the cloud service provider, is segregated from the Company's network.
j. User and user entity access to the Trusaic Platform requires a unique user ID, password, and MFA.
k. Passwords for user access to the network are configured according to the Active Directory policies, which requires minimum password length, password changes after a specified period of days, and password is complexity enabled.
l. Passwords for user access to the Trusaic Platform require minimum password length, and password complexity is enabled.
m. Logical access to the Azure IT environment is restricted to the Engineering Administrators and the SPO.
n. Access modification to the network is reviewed monthly by the SPO.
o. Requests for user access to the system and network must be approved by authorized personnel and are documented in a new hire checklist and sent to Advanced Networks for provision of user access.
p. Administrator access to the domain, which provides the user with the ability to create or modify user access privileges to the network, is restricted to authorized personnel who require such access to perform their job responsibilities.
q. The access of terminated employees or contractors is removed or disabled by Advanced Networks after receipt of notification from Trusaic. Access is then removed or disabled by Advanced Networks.
r. Access to the Trusaic Platform's internal supporting application, WAM, is restricted to the Data Operations team.
s. Events triggering an alert by the firewall or IDS are automatically emailed to the Advanced Networks ticketing system and the event is assessed by Advanced Networks IT personnel. Any significant alerts or events warranting the attention of Trusaic management are communicated to the Trusaic SPO.
t. The Client uses industry standard encryption to provide for the security of data transmitted over public networks.
u. Antivirus software and the latest operating system updates are installed on all Client desktop and laptop computers.

3. DATA ACCESS CONTROLS.
    a. Monthly risk assessment meetings are held by the SPO and Legal team to discuss risk and mitigation strategies. For any risks or other control deficiencies identified that require attention or remediation, action plans are implemented to remediate such deficiencies and documented in meeting minutes.
    b. The Client maintains a Data Breach Detection and Notification Policy, under which the SPO is notified of a potential security event within one business day. Pursuant to this Policy, events are reviewed and responded to by the SPO in accordance with a CIR Process. Results are documented in forms and referenced in the risk assessment minutes maintained by the SPO.

c. Access to the network is restricted to authorized personnel and requires a unique user ID and password.
d. Remote access to the network is restricted to authorized personnel, requires a unique user ID and password, and users are authenticated using MFA with remote access over an encrypted VPN connection.
e. The Trusaic Platform infrastructure, which resides on the cloud infrastructure provided by the cloud service provider, is segregated from the Company's network.
f. User and user entity access to the Trusaic Platform requires a unique user ID, password, and MFA.
g. Passwords for user access to the network are configured according to the Active Directory policies, which requires minimum password length, password changes after a specified period of days, and password is complexity enabled.
h. Passwords for user access to the Trusaic Platform require minimum password length, and password complexity is enabled.
i. Logical access to the Azure IT environment is restricted to the Engineering Administrators and the SPO.
j. External connections to the Trusaic Platform use restricted ports and is covered by secure sockets layer (SSL) certification and Transport Layer Security (TLS) 1.2 or later protocols.
k. All data held in the Trusaic Platform that is publicly accessible is encrypted.
l. Access to encryption keys is restricted to Engineering Administrators and the SPO.
m. Requests for user access to the system and network must be approved by authorized personnel and are documented in a new hire checklist and sent to Advanced Networks for provision of user access.
n. Administrator access to the domain, which provides the user with the ability to create or modify user access privileges to the network, is restricted to authorized personnel who require such access to perform their job responsibilities.
o. The access of terminated employees or contractors is removed or disabled by Advanced Networks after receipt of notification from Trusaic. Access is then removed or disabled by Advanced Networks.
p. The Trusaic Platform that is accessible to the public is configured to enable user entity administrators to manage user entity user accounts and set access levels to help ensure segregation of duties and user entity data.
q. A firewall has been implemented and is managed by Advanced Networks to control access to the Trusaic network from outside of the service organization and is configured to detect threats and block unauthorized access attempts.
r. Events triggering an alert by the firewall or IDS are automatically emailed to the Advanced Networks ticketing system and the event is assessed by Advanced Networks IT personnel. Any significant alerts or events warranting the attention of Trusaic management are communicated to the Trusaic SPO.
s. The Client uses industry standard encryption to provide for the security of data transmitted over public networks.
t. External connections to the Trusaic Platform use restricted ports and are covered by SSL certification and TLS 1.2 or later protocols.
u. The Client allows user entity data files to be transferred using SFTP if approved by the DE, who will obtain and configure IP restrictions and strong passwords for each user entity group (client).
v. The Client has implemented a Security Information and Event Management (SIEM) tool to continuously monitor the Trusaic Platform. Detection filters have been implemented to aggregate and analyze potential security events.

w. Secure shred bins are provided throughout the facility for collection and disposal of confidential information.
x. The Client collects individual personal information of enterprise client employees only from the client or its authorized agents.
y. Formal data retention and disposal procedures are defined in the Employee Handbook and are in place to guide the secure disposal of the Client and customer data. Specific data retention and disposal requirements have been established for each type of record and data.
z. Personal information is deleted during the enterprise client off-boarding process in accordance with the Privacy Policy and the Company's Document Retention Policy.
aa. Any requests by employees of enterprise clients to access their personal information maintained by the Client are reviewed and authorized by the SPO. Access requests are subject to a three-point identity verification and supporting declaration prior to access being provided.
bb. Denial of correction requests to personal information follows the Privacy Policy.
cc. The Client maintains a record of all disclosures of enterprise client employee personal information provided to federal and state tax authorities.

4. TRANSMISSION CONTROLS.
    a. Access to the network is restricted to authorized personnel and requires a unique user ID and password.
    b. Remote access to the network is restricted to authorized personnel, requires a unique user ID and password, and users are authenticated using MFA with remote access over an encrypted VPN connection.
    c. Logical access to the Azure IT environment is restricted to the Engineering Administrators and the SPO.
    d. External connections to the Trusaic Platform use restricted ports and is covered by secure sockets layer (SSL) certification and Transport Layer Security (TLS) 1.2 or later protocols.
    e. All data held in the Trusaic Platform that is publicly accessible is encrypted.
    f. Access to encryption keys is restricted to Engineering Administrators and the SPO.
    g. Access to the Trusaic Platform's internal supporting application, WAM, is restricted to the Data Operations team.
    h. A firewall has been implemented and is managed by Advanced Networks to control access to the Trusaic network from outside of the service organization and is configured to detect threats and block unauthorized access attempts.
    i. An IPS is used to provide continuous monitoring of the Company's network and prevention of potential security incidents or intrusion.
    j. The Client uses industry standard encryption to provide for the security of data transmitted over public networks.
    k. External connections to the Trusaic Platform use restricted ports and are covered by SSL certification and TLS 1.2 or later protocols.
    l. The Client allows user entity data files to be transferred using SFTP if approved by the DE, who will obtain and configure IP restrictions and strong passwords for each user entity group (client).
    m. all files uploaded by user entities to the Trusaic Platform are scanned for malware and are rejected if malware is detected.

n. The Client has implemented a Security Information and Event Management (SIEM) tool to continuously monitor the Trusaic Platform. Detection filters have been implemented to aggregate and analyze potential security events.

5. INPUT CONTROLS.
    a. External connections to the Trusaic Platform use restricted ports and is covered by secure sockets layer (SSL) certification and Transport Layer Security (TLS) 1.2 or later protocols.
    b. The Trusaic Platform that is accessible to the public is configured to enable user entity administrators to manage user entity user accounts and set access levels to help ensure segregation of duties and user entity data.
    c. External connections to the Trusaic Platform use restricted ports and are covered by SSL certification and TLS 1.2 or later protocols.
    d. The Client allows user entity data files to be transferred using SFTP if approved by the DE, who will obtain and configure IP restrictions and strong passwords for each user entity group (client).
    e. All files uploaded by user entities to the Trusaic Platform are scanned for malware and are rejected if malware is detected.
    f. The Client has implemented a Security Information and Event Management (SIEM) tool to continuously monitor the Trusaic Platform. Detection filters have been implemented to aggregate and analyze potential security events.
6. DATA BACKUPS.
    a. Hourly backups are scheduled for the network during the Company's normal business hours using an automated system.
    b. Backups are replicated to a secondary server daily.
    c. Backup verification is configured to be performed on all backups. Failed verification test notification is sent to Advanced Networks for monitoring.
    d. Data stored on the Trusaic Platform is configured to be geo-redundant backup storage.
    e. The Client maintains a Business Continuity Assurance Plan to guide employees on the recovery strategy for mission- critical operations during an extended interruption or outage. The Plan is reviewed annually.
7. DATA SEGREGATION.
    a. The Trusaic Platform infrastructure, which resides on the cloud infrastructure provided by the cloud service provider, is segregated from the Company's network.
    b. User and user entity access to the Trusaic Platform requires a unique user ID, password, and MFA.
    c. Logical access to the Azure IT environment is restricted to the Engineering Administrators and the SPO.
    d. The Trusaic Platform that is accessible to the public is configured to enable user entity administrators to manage user entity user accounts and set access levels to help ensure segregation of duties and user entity data.
    e. All data held in the Trusaic Platform that is publicly accessible is encrypted.
    f. The Client uses industry standard encryption to provide for the security of data transmitted over public networks.
    g. External connections to the Trusaic Platform use restricted ports and are covered by SSL certification and TLS 1.2 or later protocols.