

---

**CHINA DATA HANDLING ADDENDUM  
MONTCLAIR STATE UNIVERSITY AS PERSONAL INFORMATION HANDLER  
WITH CONTRACTOR AS ENTRUSTED PARTY**

This Data Handling Addendum (“**DHA**”) is effective on the date signed by both parties (the “Effective Date”), by and between Montclair State University (“**MONTCLAIR**”), a public institution of higher education located at 1 Normal Avenue, Montclair, New Jersey, the United States of America, and the **CONTRACTOR** described herein, working as an Entrusted Party on behalf of **MONTCLAIR**, whose principal address is identified herein. **MONTCLAIR** and **CONTRACTOR** shall individually be referred to as a “Party” and collectively as “Parties.”

**RECITALS**

Whereas, **MONTCLAIR** and **CONTRACTOR** entered into that certain agreement for the purchase of services that requires the collection of personal information (the “Agreement”) in the People’s Republic of China which includes the continental landmass under the direct control of the PRC, including the islands of Hainan Province and five major autonomous regions (i.e., Tibet, Inner Mongolia, Xinjiang, Ningxia, and Guangxi), but **excluding** the Hong Kong Special Autonomous Region (SAR), Macao SAR and Taiwan (collectively “Mainland China”);

Whereas, the Parties agree to supplement the Agreement with this DHA to incorporate additional terms and conditions related to the protection of individual data privacy and security as required under applicable PRC laws, including the China Personal Information Protection Law (the “PIPL”) as it may be amended from time to time;

NOW, THEREFORE, for and in consideration of their mutual promises and covenants contained herein and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged by the Parties, the Parties agree as follows:

**I. Procedural Terms.**

- a. Recitals. The Parties acknowledge and agree that the aforementioned Recitals are true and correct, and are incorporated herein by reference.
- b. Defined Terms. Unless otherwise defined herein, all defined terms contained in this DHA shall have the meaning ascribed thereto in the Agreement.
- c. Ratification. Except as expressly modified in this DHA, all terms, covenants and conditions of the Agreement shall remain in full force and effect and are hereby ratified and affirmed by the Parties.
- d. Entire Agreement; Order of Precedence. This DHA shall become an integral part of the Agreement and shall have the same legal force and effect. This DHA shall prevail over any conflicting term of the Agreement to the extent necessary to resolve the conflict.

**II. Scope.**

This DHA applies to Handling Personal Information subject to Data Protection Law, as laid out in this DHA and the Agreement. The purposes, methods, and duration of the Personal Information Handling, the categories of Personal Information, retention periods, and the protection measures are laid out in this DHA and its Appendices.

**III. Roles.**

- a. MONTCLAIR is the Personal Information Handler.
- b. CONTRACTOR is the Entrusted Party.
- c. MONTCLAIR entrusts CONTRACTOR to Handle Personal Information as an Entrusted Party as outlined in this DHA and in compliance with Data Protection Law.
- d. MONTCLAIR represents and warrants that it will comply with Data Protection Law and only entrust to CONTRACTOR the Handling of Personal Information to the extent such Handling is lawful and based on one of the legal grounds for Data Handling provided in Data Protection Law.

**IV. Data Entrustment Instructions.**

- a. CONTRACTOR must Handle Personal Information in accordance with the purposes, methods, scope of Personal Information, retention period, and protective measures outlined in Appendix I to this DHA. Any Handling outside of those parameters will be deemed a breach of DHA and CONTRACTOR will be liable for all fees, fines, and damages associated with such a violation.

**V. Data Retention.**

- a. MONTCLAIR may, at any time, request Entrusted Party to delete Personal Information and CONTRACTOR must comply with such request immediately.
- b. CONTRACTOR will only keep Personal Information for the shortest period necessary to realize the purposes outlined in Appendix I, and in any event not beyond the term of this DHA.
- c. If the Agreement or this DHA does not take effect, is void, has been cancelled, or has been terminated, CONTRACTOR must return the Personal Information to MONTCLAIR or delete it, at MONTCLAIR's choice and in accordance with MONTCLAIR's instructions.

**VI. Confidentiality.**

- a. CONTRACTOR must keep Personal Information, and all information relating to its Handling, in strict confidence. CONTRACTOR must ensure that all personnel authorized to Handle Personal Information are subject to a contractual or statutory obligation of confidentiality.
- b. CONTRACTOR may not disclose Personal Information to any third-party, unless CONTRACTOR obtained the prior written authorization of MONTCLAIR.
- c. CONTRACTOR must refrain from making any public communication regarding a potential or confirmed Personal Information Breach involving Personal Information without the prior written authorization of MONTCLAIR, unless otherwise required by applicable law, in which case CONTRACTOR will notify MONTCLAIR of such communication before it is made. Nothing in this subsection will be interpreted to contradict Subsection XIII.

**VII. International Data Transfers.**

CONTRACTOR may not transfer Personal Information outside China, unless CONTRACTOR:

- a. obtains MONTCLAIR's prior written authorization; and
- b. fulfills all requirements under Data Protection Law to perform such Personal Information transfers.

**VIII. Use of Other Entrusted Parties.**

- a. CONTRACTOR may not entrust the Handling of Personal Information to another Entrusted Party without MONTCLAIR's prior specific written authorization. CONTRACTOR must submit the request for specific

authorization at least 30 days prior to the engagement of the other Entrusted Party, together with the information necessary to enable MONTCLAIR to decide on the authorization. The list of other Entrusted Parties already authorized by MONTCLAIR can be found in Appendix II. The Parties shall keep Appendix II up to date.

- b. CONTRACTOR has MONTCLAIR's general written authorization for the engagement of another Entrusted Party from an agreed list. CONTRACTOR must specifically inform MONTCLAIR in writing of any intended changes to that list through the addition or replacement of other Entrusted Parties at least 30 days in advance, thereby giving MONTCLAIR sufficient time to be able to object to such changes prior to the engagement of the other Entrusted Party. CONTRACTOR must provide MONTCLAIR with the information necessary to enable MONTCLAIR to exercise its right to object.
- c. If CONTRACTOR entrusts another Entrusted Party with Handling of Personal Information in accordance with this DHA, CONTRACTOR must enter into an agreement with such other Entrusted Party that imposes the same obligations on that other Entrusted Party as are imposed on CONTRACTOR under this DHA.

**IX. Sensitive Personal Information.**

Parties acknowledge that Sensitive Personal Information may only be Handled where there is a specific purpose and need to be fulfilled. If CONTRACTOR is entrusted to Handle Sensitive Personal Information under this DHA, it must protect such information with strict protection measures.

**X. Training.**

CONTRACTOR regularly, at least once a year, will train its Employees on proper procedures for Handling Personal Information. Employees are CONTRACTOR's staff members, directors, officers, employees, (temporary) employees, interns, consultants, and contractors.

**XI. Assistance and Responsibilities.**

- a. CONTRACTOR agrees that it is responsible for complying with its obligations under this Agreement and the Data Protection Law.
- b. CONTRACTOR must assist MONTCLAIR in fulfilling MONTCLAIR's obligations under the Data Protection Law, including assisting MONTCLAIR in performing any Personal Information protection impact assessments or security assessments to comply with Data Protection Law.
- c. CONTRACTOR must immediately inform MONTCLAIR if it receives a request from a Data Subject to exercise his or her rights under Data Protection Law with regard to Personal Information that CONTRACTOR Handles under this DHA. CONTRACTOR must assist MONTCLAIR in fulfilling MONTCLAIR's obligations under Data Protection Law with regard to such requests.
- d. CONTRACTOR must immediately inform MONTCLAIR if it receives a request from the Supervisory Authority regarding any Personal Information CONTRACTOR is Handling for MONTCLAIR.

**XII. Security.**

- a. CONTRACTOR must take the necessary measures to safeguard the security of Personal Information it Handles, as required by Data Protection Law. At a minimum, CONTRACTOR must implement the security measures listed in Appendix III to this DHA.
- b. Parties must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks presented by Handling. Criteria to take into consideration are the method, scope and purposes of Handling, in addition to the risk of harm to the rights and interests of Data Subjects.

**XIII. Personal Information Breach.**

*To Be Used with All CONTRACTORS Who Collect or Process Personal Data in Mainland China*

- 
- a. CONTRACTOR will notify MONTCLAIR without undue delay, and no later than 24 hours, after becoming aware of a Personal Information Breach involving Personal Information Handled by CONTRACTOR on behalf of MONTCLAIR.
  - b. CONTRACTOR must take immediate action to adopt remedial measures once a Personal Information Breach is discovered.
  - c. CONTRACTOR must assist MONTCLAIR in making any notices required by Data Protection Law in relating to any Personal Information Breach involving Personal Information Handled by CONTRACTOR on behalf of MONTCLAIR. CONTRACTOR must provide MONTCLAIR with, at a minimum:
    - i. The Personal Information categories involved in the Personal Information Breach, the causes of the Personal Information Breach, and possible harm caused by a Personal Information Breach; and
    - ii. The remedial measures taken by CONTRACTOR and measures Data Subjects can adopt to mitigate harm.

**XIV. Audit.**

- a. CONTRACTOR will allow MONTCLAIR to conduct supervision of the Personal Information Handling by CONTRACTOR, including by conducting audits of CONTRACTOR to verify compliance with Data Protection Law.
  - i. CONTRACTOR will make available to MONTCLAIR all information necessary to demonstrate compliance with this DHA and Data Protection Law.
  - ii. CONTRACTOR will allow and help to contribute to audits by the Supervisory Authority, MONTCLAIR, or another auditor mandated by MONTCLAIR.
  - iii. Each Party bears its own costs related to an audit, except when an audit determines CONTRACTOR materially violated Data Protection Law or this DHA, in which case CONTRACTOR bears all costs related to the audit.
  - iv. Upon a written request from MONTCLAIR, at reasonable intervals, but no more than once per calendar year, CONTRACTOR will make available to MONTCLAIR a copy of all third-party certifications and audits that relate to this DHA, redacting any commercially sensitive information.
  - v. If the documentation provided by CONTRACTOR described in XIV(iv) clearly fails to demonstrate their compliance with this DHA or Data Protection Law, MONTCLAIR may make a written request for additional information from CONTRACTOR relating to their compliance with those provisions that MONTCLAIR expressly identifies as the object of its concern.
  - vi. If the information described in XIV(v) provided by CONTRACTOR does not reasonably address MONTCLAIR's concern(s), MONTCLAIR may request an audit of CONTRACTOR's procedures related to the protection of Personal Information. MONTCLAIR will give at least thirty days' notice before conducting such an audit. The audit will be conducted during CONTRACTOR's business hours and will not be disruptive of CONTRACTOR's operations.
  - vii. CONTRACTOR agrees to permit and reasonably contribute to such an audit described in XIV(vi), while complying with its confidentiality obligations. MONTCLAIR agrees to bear all the costs associated with such audit and to reimburse CONTRACTOR at commercially reasonable rates for any time expended by CONTRACTOR or the other Entrusted Parties that CONTRACTOR engaged to provide assistance in connection with the audit.
  - viii. CONTRACTOR will allow and help to contribute to audits by the Supervisory Authority.

*To Be Used with All CONTRACTORS Who Collect or Process Personal Data in Mainland China*

---

- ix. CONTRACTOR will provide MONTCLAIR a certificate of compliance upon the request by MONTCLAIR.
- b. CONTRACTOR must regularly, at least once a year, engage in internal audits to ensure compliance with all applicable laws and administrative regulations.

**XV. Notice.**

CONTRACTOR must make all notifications, including security-related notifications, required under this DHA to MONTCLAIR's Security Official by email to [sec-official@montclair.edu](mailto:sec-official@montclair.edu). MONTCLAIR must make all notifications required under this DHA to CONTRACTOR as indicated in the signature block below.

- a. Contact information for MONTCLAIR
  - i. Title: Director, Red Hawk Central
  - ii. Phone: 973/655-7971, Option 1
  - iii. Email: [China-PIPL@montclair.edu](mailto:China-PIPL@montclair.edu)
  - iv. Address: 1 Normal Avenue, Montclair, NJ 07043

With a copy to:

Title: University Counsel

Phone: 973/655-5225

Email: [China-PIPL@montclair.edu](mailto:China-PIPL@montclair.edu)

Address: 1 Normal Avenue, Montclair, NJ 07043

- b. Contact information for CONTRACTOR is set forth on the signature page of this DHA.

**XVI. Modifications.**

This DHA may only be modified by a written amendment signed by all Parties, with the exception of changes to Appendices, which may be amended by an unsigned written agreement between the Parties.

**XVII. Invalidity and Severability.**

If any provision of this DHA is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, then the invalidity or unenforceability of such provision does not affect any other provision of this DHA, and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

**XVIII. Term.**

The term of this DHA is the same as that of the Agreement.

**XIX. Translation.**

This DHA is entered into in both English and Chinese, and with language versions having equal legal force and effect.

**XX. Definitions.**

- a. **"Anonymization"** means the process in which the personal information is processed so that it is impossible to identify a certain natural person and unable to be recovered.

*To Be Used with All CONTRACTORS Who Collect or Process Personal Data in Mainland China*

---

- b. **“Automated Decision-Making”** means an activity to automatically analyze or evaluate a person’s behaviors, habits, hobbies or economic, health or credit status through computer programs and making a decision based on such data.
- c. **“China”** means the People’s Republic of China, for the purpose of this DHA refers to the continental landmass under the direct control of the PRC, including the islands of Hainan Province and five major autonomous regions (i.e., Tibet, Inner Mongolia, Xinjiang, Ningxia, and Guangxi), but excluding the Hong Kong Special Autonomous Region (SAR), Macao SAR and Taiwan.
- d. **“Data Protection Law”** means all applicable privacy and data protection laws in China, including China’s Personal Information Protection Law and all other associated data protection laws, regulations, regulatory guidance and important national standards of China, as may be amended or replaced from time to time.
- e. **“Data Subject”** means an individual to whom the Personal Information relates.
- f. **“Entrusted Party”** refers to the Party to this DHA to whom the Personal Information Handler entrusts the Handling of Personal Information subject to this DHA on behalf of the Personal Information Handler.
- g. **“Handling,” “Handle,” “Handles,”** and **“Handled”** mean any operation or set of operations performed on Personal Information or on sets of Personal Information, whether or not by automated means. This includes, but is not limited to, collection, storage, use, processing, transmission, provision, publishing, and deletion of Personal Information.
- h. **“Joint Handler”** means an organization that is working as a Personal Information Handler in conjunction with another third-party Personal Information Handler where both parties have jointly determined the purpose and method of Handling Personal Information for their own respective behalf and who bear joint responsibility and liability in accordance with the law.
- i. **“Personal Information”** means any information, recorded by electronic or other means, relating to an identified or identifiable individual. Personal Information does not include information that underwent Anonymization. For the purposes of this DHA, the term “Personal Information” includes “Sensitive Personal Information” as defined below.
- j. **“Personal Information Breach”** means a Personal Information leak, distortion, or loss has occurred or is reasonably suspected to have occurred.
- k. **“Personal Information Handler”** refers to any organization or individual, Party to this DHA, that independently determines the purpose and method of handling Personal Information.
- l. **“Sensitive Personal Information”** means Personal Information which, if inappropriately disclosed or illegally used, would likely cause harm to the dignity of an individual or grave harm to persons or property. Sensitive Personal Information includes information on biometric characteristics, religious beliefs, specially-designated status, medical health, financial accounts, individual location tracking, and personal information about children under the age of 14.
- m. **“Supervisory Authority”** means a government agency responsible for monitoring the application of Data Protection Law and protecting and enforcing data privacy rights, including the Cyberspace Administration of China and other departments fulfilling Personal Information protection duties.

***To Be Used with All CONTRACTORS Who Collect or Process Personal Data in Mainland China***

By signing this Agreement, Parties acknowledge and agree that they have read and understood their obligations under this Agreement and accept all terms and conditions as outlined herein.

<b>MONTCLAIR UNIVERSITY</b>	<b>CONTRACTOR</b>
Name:	Name:
Title: Vice President for Finance and Treasurer	Title:
Address: 1 Normal Avenue, Montclair, NJ 07043	Address:
Signature:	Signature:
Date:	Date:
	Contact Information for Security Notices:
	Name:
	Title:
	Email:
	Address:
	Phone:

**APPENDIX I**  
**Description of Handling**

Description of Handling

A. Purpose(s) for Handling:

1. Define the specific purpose, legal basis, scope of personal information needed to achieve purpose.

B. Acquisition of Personal Information:

1. How is PI/SPI being acquired? Direct from individuals, from MONTCLAIR, CONTRACTOR, from a third-party collector, Website, Social Media, other?
2. How is notice of collection provided? How is consent obtained? How is consent documented?
3. How are individuals notified in the event of any change in processing? How is consent re-obtained and documented?

C. Method(s) of Handling:

1. Storage and retrieval of personal information, combining personal information with other data sources, indexing personal information.
2. Security measures needed for stored personal information and personal information in transit.
3. Requests for edits, updates, and/or deletion of personal information, etc.
4. Notification of Parties of any changes in personal information or deletion requests.

D. Categories of Personal Information Handled:

1. Name, mailing address, cookie IDs, hashed email addresses, mobile advertising IDs, passwords, ID numbers, employment history, etc.

*To Be Used with All CONTRACTORS Who Collect or Process Personal Data in Mainland China*

---

E. Categories of Sensitive Personal Information Handled:

1. Information on biometric characteristics, religious beliefs, specific identities, medical health, financial accounts and individual location tracking, personal information of minors under 14.

F. The Retention period of Personal Information:

1. Deletion requests, deletion once purpose is achieved, or is unable or no longer necessary to achieve.
2. Personal Information will be retained by CONTRACTOR for at least the minimum time period permitted by law.

**APPENDIX II**  
**Other Entrusted Parties**  
**(To be Completed When CONTRACTOR Uses Subprocessors)**

MONTCLAIR authorizes CONTRACTOR to engage the following other Entrusted Party(s)

1. Name of Subprocessor:

Address of Subprocessor:

Contact Person for Subprocessor:

Name:

Position:

Address:

Phone:

Email:

Personal Information Protection Officer for Subprocessor:

Name:

Phone:

Email:

Description of Handling by Subprocessor (including a clear delimitation of responsibilities in case several other Entrusted Parties are authorized):

Subprocess will provide following services:

2. Additional Subprocessors

Name:

Address:

Contact Person

Name:

Position:

Address:

Phone:

Email:

Personal Information Protection Officer:

Name:

Phone:

***To Be Used with All CONTRACTORS Who Collect or Process Personal Data in Mainland China***

---

Email:

3. Description of Handling (including a clear delimitation of responsibilities in case several other Entrusted Parties are authorized:

4. Description of nature of services:

---

**APPENDIX III (To Be Completed by Contractor to Summarize Contractor Security Measures)**

**A.** CONTRACTOR shall provide a description of the technical and organizational security measures implemented by CONTRACTOR to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the Handling, and the risks for the rights and freedoms of natural persons. **The following are examples and should be edited by CONTRACTOR to reflect CONTRACTOR’S SECURITY MEASURES.**

1. Measures of pseudonymization and encryption of personal information.
2. Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services.
3. Measures for ensuring the ability to restore the availability and access to personal information in a timely manner in the event of a physical or technical incident.
4. Processes for identifying and remedying Personal Information Breach. Notification processes in the event of security incident.
5. Processes for regularly testing (audits), assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing of personal information.
6. Measures for user identification and authorization, access restriction, records of access to personal information.
7. Measures for the protection of personal information during transmission, controls on onward transmissions.
8. Measures for the protection of personal information during storage.
9. Measures for ensuring physical security of locations at which personal information are processed.
10. Measures for ensuring event logging.
11. Measures for ensuring proper system configuration, including default configuration.
12. Measures for internal IT and IT security governance and management.
13. Measures for certification/assurance of processes and products.
14. Measures for ensuring personal information minimization.
15. Measures for ensuring personal information integrity and quality.
16. Measures for ensuring limited personal information retention.
17. Measures for ensuring accountability.
18. Measures for allowing personal information portability and ensuring erasure.
19. Name of person designated as the personal information protector (if applicable).

CONTRACTOR’S Security Measures are summarized in this space:

**B.** If CONTRACTOR is Handling Sensitive Personal Information, CONTRACTOR must describe in the space below the additional security measures they using to safeguard such information. All security measures should be applied to all Personal Information, including Sensitive Personal Information being transferred out of China. **The following are examples and should be edited by CONTRACTOR to reflect CONTRACTOR’S SECURITY MEASURES.**

*To Be Used with All CONTRACTORS Who Collect or Process Personal Data in Mainland China*

---

Strict purpose limitation, access restrictions (including access only for staff that received specialized training), keeping a record of access to the data, restrictions for onward transfers, and any additional security measures.

CONTRACTOR'S Additional Security Measures for Sensitive Personal Information are summarized in this space:

C. If CONTRACTOR has entrusted the Handling of Personal Information to other Entrusted Parties, CONTRACTOR must describe the specific technical and organizational security measures to be taken by them to provide security measures. **The following are examples and should be edited by CONTRACTOR to reflect CONTRACTOR'S SECURITY MEASURES.**

1. Measures of pseudonymization and encryption of personal information.
2. Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services.
3. Measures for ensuring the ability to restore the availability and access to personal information in a timely manner in the event of a physical or technical incident.
4. Processes for identifying and remedying Personal Information Breach. Notification processes in the event of security incident.
5. Processes for regularly testing (audits), assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing of personal information.
6. Measures for user identification and authorization, access restriction, records of access to personal information.
7. Measures for the protection of personal information during transmission, controls on onward transmissions.
8. Measures for the protection of personal information during storage.
9. Measures for ensuring physical security of locations at which personal information are processed.
10. Measures for ensuring event logging.
11. Measures for ensuring proper system configuration, including default configuration.
12. Measures for internal IT and IT security governance and management.
13. Measures for certification/assurance of processes and products.
14. Measures for ensuring personal information minimization.
15. Measures for ensuring personal information integrity and quality.
16. Measures for ensuring limited personal information retention.
17. Measures for ensuring accountability.
18. Measures for allowing personal information portability and ensuring erasure.
19. Name of person designated as the personal information protector (if applicable).

Security Measures undertaken by CONTRACTOR's Entrusted Parties is summarized in this space: