myunifyai.com

End User Service Agreement

Welcome to Unified Systems Intelligence (USI) , an enterprise AI platform powered by Unify.AI, which integrates generative AI across a suite of essential business applications. USI enables organizations to streamline their operations by consolidating multiple systems. Unless otherwise stated, the USI Services are owned and/or operated under license by USI and are accessible via various web pages and mobile applications (collectively referred to as the "Site"). Your use of USI Services is governed by this End User Service Agreement ("Agreement"). The USI Services are offered to you on the condition that you accept, without modification, the terms, conditions, and notices outlined herein.

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE SITE OR USI SERVICES. THIS AGREEMENT CONTAINS IMPORTANT INFORMATION REGARDING YOUR LEGAL RIGHTS, REMEDIES, AND OBLIGATIONS, INCLUDING LIMITATIONS ON LIABILITY, YOUR RESPONSIBILITY TO AVOID UPLOADING SENSITIVE DATA WITHOUT PRIOR WRITTEN CONSENT FROM THE DATA SUBJECT, A DISPUTE RESOLUTION CLAUSE, AND A CLASS ACTION ARBITRATION WAIVER.

BY EITHER (1) CLICKING A BOX THAT INDICATES ACCEPTANCE OR (2) USING THE USI SERVICES, YOU ACKNOWLEDGE THAT YOU HAVE READ, UNDERSTAND, AND AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU ARE ENTERING INTO THIS AGREEMENT ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY ("CUSTOMER" AS DEFINED BELOW), YOU CONFIRM THAT YOU HAVE THE AUTHORITY TO BIND THAT ENTITY AND ITS AFFILIATES TO THIS AGREEMENT. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT AGREE WITH THESE TERMS, DO NOT ACCEPT THIS AGREEMENT, AND YOU MAY NOT USE THE USI SERVICES.

1. DEFINITIONS

As used in this Agreement and any associated documents:

- "Applicable Data Protection Legislation" refers to the laws and regulations that govern the processing of Personal Data by each party in connection with this Agreement, including but not limited to: (i) the General Data Protection Regulation (EU) 2016/679 ("GDPR") as amended and supplemented by the relevant EU Member States in which the Customer operates, (ii) the UK Data Protection Act 2018 and UK General Data Protection Regulation ("UK GDPR"), and (iii) the Australian Privacy Act 1988 and National Privacy Principles.
- • "California Consumer Privacy Act of 2018," as amended by the California Privacy Rights Act of 2020, and any related regulations or guidance (collectively referred to as the "CCPA"), (v) the Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA"), and (vi) any other applicable international, federal, state, provincial, and local privacy or data protection laws, rules, regulations, directives, and government requirements currently in effect and as they become effective.
- • "Audit" refers to USI's systematic review of a Supplier's practices and procedures to ensure compliance with applicable regulatory standards, industry best practices, or other criteria or guidelines requested by Clients.
- • "Authorized Users" refers to Customer's administrative users, Workers, Visitors, and agents who are authorized by the Customer to access USI Services or the Site under the rights granted to Customer.
- • "USI" refers to USI, LLC and its affiliates and subsidiaries, including but not limited to Unified Systems Intelligence. In this Agreement, USI may also be referred to as "we."
- • "USI Network" refers to USI's customer network, including all Clients and who have subscribed to USI Services.
- • "USI Services" refers to the services provided by USI, including access to the Site.
- • "Client" refers to a company or other legal entity that engages or does business with USI Network.
- • "Compliance Information" refers to the information provided by USI to Customer when implementing and providing USI Services, including details about regulations, regulatory interpretations, compliance requirements, insurance, qualifications, certifications, and licenses for personnel.
- • "Content" refers to all information, data, text, software, graphics, messages, tags, courses, training materials, or other materials publicly posted, privately transmitted, or otherwise made available through USI Services.
- • "Customer" refers to the company or other legal entity that subscribes to USI Services. A Customer can be either a Supplier or a Client.
- • "Customer Content" refers to all Content uploaded or submitted by Customer (including by its Authorized Users) in connection with their use of USI Services. If the Customer is a Supplier, this includes Limited Access Data and General Access Data.
- • "General Access Data" refers to a Supplier's account information, name, service description, operating locations, main point of contact details, and the Supplier's logos, trademarks, and service marks.
- • "Limited Access Data" refers to a client's data contained in prequalification forms (PQFs), specific insurance details, safety statistics (such as experience modification rate

(EMR) and OSHA data), all data collected during an Audit, and Worker-related data when using USI's worker product(s).

- "Personal Data" refers to any information that (i) identifies or relates to an identifiable individual, either directly or indirectly, based on that data alone or combined with other information USI possesses or controls, or (ii) is defined as personal data or personal information under Applicable Data Protection Legislation.

- "Sensitive Data" includes, but is not limited to, Personal Data related to an individual's physical or mental health, racial or ethnic origin, sexual orientation, trade union membership, genetic and biometric data used for identification, religious or philosophical beliefs, political opinions, or criminal history (including offenses or alleged offenses).
- "Visitor" refers to an individual authorized by the Customer to visit a worksite but who is not employed by the Customer as a Worker.
- "Worker" refers to an individual service provider employed by the Customer.
- "You" and "Your" refer to both (i) the Authorized User acting on behalf of the Customer, and (ii) the Customer entity being represented.

2. FEES AND CHARGES

The terms and conditions governing the billing, refunds, and renewals for USI Services are outlined in USI's Billing, Refund, and Renewal Policy, which is attached as Attachment 1 and incorporated into this Agreement by reference.

3. USI SERVICES

The USI Services are provided to You through the Site or other means. These services are an online subscription-based offering that provides Clients access to various supply chain risk management tools. As part of USI Services, prequalification checks are conducted based on parameters set by Clients, some of which may be automated.

You acknowledge and agree that the Site stores information related to compliance, competency, and worksite attendance of individual users. Clients may set specific rules for users regarding compliance, competency, and attendance at the worksites they operate. If you use USI Services to access a worksite, you must familiarize yourself with these rules. Failure to comply with these rules may result in being marked as an inactive user for certain worksites, preventing your access until the issue is resolved. USI can verify this status through the Site.

You expressly agree that as part of USI Services, USI will conduct Audits, which are objective evaluations of a Supplier's procedures and practices to assess their compliance with relevant standards, best practices, or other criteria requested by Clients. These Audits are conducted solely to gather required documentation for Client review.

USI Services are available through various subscription plans, with differing price levels and features, including promotional plans or subscriptions with limitations. Purchases of online courses within the Unify AI Learning Management System are final, and courses not completed within six months of purchase will expire without refund. Additional product-specific terms and

conditions (available at https://www.myunifyai.com/) may apply to specific portions of the USI Services, and such terms are incorporated into this Agreement. In case of conflicts between product-specific terms and this Agreement, the product-specific terms will take precedence.

USI may fulfill any of its obligations through subcontractors and remains responsible for their actions and omissions under this Agreement. USI may make changes to the Site or USI Services to improve the user experience and will provide a 30-day advance notice for material modifications.

4. THIRD-PARTY SERVICES

USI may offer third-party services ("Third Party Services") through USI Services. These services are not owned or controlled by USI, and their use is governed by the third-party providers' terms. USI assumes no liability for any Third Party Services you choose to use. Third-Party Services may not be installed or used in any way that imposes obligations on USI.

5. USE OF THE USI SERVICES

Customers are granted a limited, non-exclusive, non-transferable, non-sublicensable, revocable license to access and use the USI Services for which they have valid subscriptions. This access is granted solely for legitimate internal business purposes and must comply with the terms of this Agreement. Only Authorized Users may access and use the USI Services, and the Customer is responsible for all actions taken under its account. Unauthorized use of login credentials or accessing the Services from outside the designated country is prohibited. Customers must keep their login credentials confidential and notify USI of any unauthorized access. Login credentials may limit access to certain materials on the USI Services.

Any use of the USI Services beyond the scope of this Agreement, without prior written permission from USI, is prohibited and will result in the termination or suspension of the granted license. Unauthorized use may also violate copyright and trademark laws as well as communication regulations.

The license is subject to the following restrictions and prohibitions:

- (a) You may not copy, print (except for archival purposes), republish, display, distribute, transmit, sell, rent, lease, loan, or make any part of the USI Services or its Content available in any form;
- (b) You may not use the USI Services or its Content to develop or include it in any database, storage, or information system offered for commercial distribution;
- (c) You may not create derivative works of any Content from USI Services;
- (d) You may not use Content in any manner that infringes USI’s or third-party intellectual property rights;
- (e) You may not remove or obscure copyright notices in the USI Services;
- (f) You may not make any part of the USI Services available through timesharing systems, service bureaus, or the internet;
- (g) You may not reverse-engineer or decompile any USI Services or software or use network monitoring software to determine the architecture;
- (h) You may not use any data mining, robots, scraping, or data extraction methods;

- (i) You may not use the USI Services for transmitting unsolicited communications (e.g., emails, calls, or faxes);
- (j) You may not use the USI Services in violation of any applicable law or regulation;
- (k) You may not export or re-export the USI Services or any software in violation of export control laws.

All rights not expressly granted are reserved by USI.

When You use the USI Services, You agree not to:

- Upload, post, email, transmit, or make available any Content that is false, misleading, unlawful, harmful, threatening, abusive, harassing, defamatory, discriminatory, vulgar, obscene, libelous, invasive of another's privacy, hateful, or otherwise objectionable;
- Use the USI Services to harm others in any way;
- Impersonate any person or entity, or misrepresent Your affiliation with any person or entity while using the USI Services;
- Forge headers or manipulate identifiers to disguise the origin of any Content transmitted through the USI Services;
- Modify, create derivative works, or translate the USI Services without USI's prior written permission;
- Use the USI Services for fraudulent or unlawful purposes;
- Attempt unauthorized access to the USI Services or defeat any encryption or security measures implemented by USI;
- Upload, post, email, or transmit any Content You do not have the right to make available, such as proprietary or confidential information disclosed under nondisclosure agreements;
- Upload, post, email, or transmit any Content that (i) infringes on any intellectual property rights; (ii) contains unsolicited or unauthorized advertising, "junk mail," "spam," "chain letters," or "pyramid schemes"; or (iii) contains software viruses or harmful code designed to interrupt or damage any software or hardware;
- Interfere with or disrupt the USI Services or networks connected to USI Services;
- Use the USI Services to violate any applicable law, rule, or regulation;
- Use the USI Services to provide material support to any organization designated by the U.S. government as a foreign terrorist organization;
- Stalk or harass others using the USI Services;

- Collect or store Personal Data about other users for any prohibited conduct listed above.

6. CONTENT

Content provided through the USI Services or on the Site may originate from USI, Clients, or third-party vendors. You understand that all Content, whether publicly posted or privately transmitted, is the responsibility of the person or entity from whom it originated. USI does not control Content posted by others and cannot guarantee its accuracy, integrity, or quality. Information received via the Site is not for consumer use and should not be relied upon for personal, medical, legal, or financial decisions. USI assumes no liability for any errors, omissions, or damages resulting from Content posted or provided by Clients, or third-party vendors.

USI reserves the right to pre-screen Content and may refuse to post, transmit, or remove any Content that violates this Agreement or is otherwise deemed inappropriate. You acknowledge that You must evaluate and bear the risks associated with using any Content provided by others.

You acknowledge that USI may access, retain, and disclose your account information and Content when required by law or when acting in good faith to comply with legal obligations, enforce this Agreement, respond to claims, or protect the rights, property, or safety of USI, its users, or the public. USI reserves the right to investigate any complaints or violations of this Agreement and may take appropriate measures, including reporting unlawful activity to law enforcement or relevant authorities.

7. CUSTOMER CONTENT

As between USI and the Customer, the Customer retains ownership of all rights, title, and interest in the Customer Content. However, by using the USI Services, You grant USI a non-exclusive, transferable, fully-paid, worldwide, irrevocable license to use, modify, copy, reproduce, transmit, sub-license, publish, display, and distribute Customer Content as necessary to:

- Provide, operate, and improve the USI Services;
- Develop new technologies and services for USI;
- Operate and manage award programs, rankings, and related marketing activities; and
- Fulfill USI's obligations under this Agreement.

Additionally, USI may collect usage and operational data ("Usage Data") for research and analysis purposes. Such data may be made public in accordance with applicable laws, provided it does not identify You or disclose any confidential information.

If You are submitting Customer Content (including data from Your Workers or Authorized Users), You acknowledge that:

- Customer Content includes both Limited Access Data and General Access Data;

- General Access Data is used to help Clients and, while not publicly accessible, is shared with Clients in the USI Network; and
- Limited Access Data is divided into standard compliance data (accessible by Clients connected to Your account) and client-specific compliance data (accessible by the specific Client setting the requirements).

You have the ability to review, manage, and control Your Client List, including adding or removing Clients and managing access to Your data via the Site or by contacting USI.

USI will make reasonable efforts to accurately store and provide access to Customer Content. You are responsible for reviewing and verifying the accuracy of Audits conducted by USI and for notifying USI of any errors or omissions.

You acknowledge that the transmission and processing of data on the Site may involve multiple network transmissions and technical adjustments. USI is not responsible for record retention following the termination of this Agreement unless You request the return of Your information before it is disposed of.

8. USI PROPRIETARY RIGHTS

USI (and its licensors, where applicable) owns all rights, title, and interest, including intellectual property rights, in the USI Services (including the underlying technology, software, and analytics), any Content provided by USI, and any models, methods, algorithms, inventions, modifications, enhancements, extensions, materials, or other work product conceived, developed, or prepared in connection with the USI Services.

All trademarks, logos, and service marks displayed through USI Services are the property of USI, its affiliates, licensors, or other third parties. You may not use these marks without prior written permission from USI or the mark's owner. USI reserves all rights not expressly granted in this Agreement, and all Content provided by USI is protected by U.S. and international copyright laws.

9. FEEDBACK

If You provide USI with any comments, suggestions, or other feedback regarding the USI Services ("Feedback"), USI is free to use such Feedback without any obligation or limitation. You irrevocably assign to USI all rights, title, and interest in the Feedback, including any ideas, concepts, techniques, or intellectual property rights contained in it, without attribution or compensation. You also agree to waive any "moral rights" associated with the Feedback. USI will exclusively own any modifications, enhancements, or derivative works of the USI Services that result from the use of such Feedback.

10. BETA OR TESTING FEATURES

From time to time, USI may offer certain products or features ("Beta Services") for testing purposes only. These Beta Services are provided "AS IS," without any warranty or performance obligations. USI will not be liable for any harm or damages that arise from the use of Beta Services. Your use of these Beta Services is entirely at your discretion.

11. YOUR REPRESENTATIONS AND WARRANTIES

You represent, warrant, and agree that:

- If You are a Client (i) You are entering into this Agreement in a professional capacity for trade, business, or professional purposes as a specialized service provider, and (ii) Your use of the USI Services and USI's processing of Customer Content (including any Personal Data) in accordance with this Agreement will not violate any third-party rights or applicable laws.
- If You are a Worker, Visitor, or agent of a Customer, You are an Authorized User, and the Content uploaded or submitted by You is at the request of the Customer and considered Customer Content.
- You have the legal right and authority to enter into this Agreement and to comply with its terms.
- You will use the USI Services for lawful purposes only, in compliance with this Agreement and all applicable laws, regulations, and policies.
- The information You provide is true and accurate, and You have the right to provide it.
- If You are not the owner of the information being uploaded to the Site, You warrant that You have the full consent of the owner to agree to these terms on their behalf and have fully informed the owner of these terms and their implications.
- You are at least the age of majority in Your jurisdiction and have the legal capacity to form binding contracts on behalf of the entity You represent.

12. INTERNATIONAL TRADE COMPLIANCE

Both You and USI agree not to engage with or use, directly or indirectly, the following in any business transactions:

- The government, entity, group, or individual from any country subject to sanctions by the U.S. Office of Foreign Assets Control (OFAC) or any other governmental entity that imposes economic sanctions ("Embargoed Country").
- Any government, entity, group, or individual listed on the OFAC List of Specially Designated Nationals and Blocked Persons or similar lists maintained by other government entities ("Sanctioned Party").

Each party represents and warrants that it is not:

- A Sanctioned Party;
- Owned or controlled by, or acting on behalf of, a Sanctioned Party; or
- Directly or indirectly owned, controlled by, or acting on behalf of an Embargoed Country.

If either You or USI becomes designated as a Sanctioned Party or becomes owned, controlled, or associated with a Sanctioned Party or Embargoed Country, this Agreement will automatically terminate.

USI Confidential Information is defined as: (a) any and all information that Customer receives or has access to regarding any other Supplier or Client, and (b) any other information disclosed by

USI or revealed through USI's provision of the USI Services, including but not limited to business and marketing plans, technical information, product designs, and business processes. USI Confidential Information does not include information that: (i) becomes public knowledge without breaching any obligations to USI, a Client, or a Supplier, (ii) was known to Customer before its disclosure by USI, a Client, or a Supplier, (iii) is lawfully received from a third party without breaching any obligations to USI, a Client, or a Supplier, or (iv) was independently developed by Customer without using USI's Confidential Information.

You agree not to use or disclose USI Confidential Information for any purpose other than your legitimate internal business needs related to using the USI Services. You agree to protect USI Confidential Information with at least the same degree of care as You would use to protect your own confidential information, but not less than a reasonable level of care. Access to USI Confidential Information should be limited to Authorized Users and personnel who need it to use the USI Services.

Customer Confidential Information is defined as Customer's proprietary, non-public information, including business and marketing plans, technical information, product plans, and business processes, disclosed to USI during the provision of USI Services. Customer Confidential Information excludes information that: (i) becomes public knowledge without breaching any obligations to Customer, (ii) was known to USI before its disclosure by Customer, or (iii) is received from a third party without breaching any obligations to Customer. USI will protect Customer Confidential Information with the same level of care as it protects its own confidential information. USI may disclose Customer Confidential Information as necessary to provide the USI Services, limiting access to those USI employees and third-party providers who require it to fulfill their obligations.

Notwithstanding the above, Confidential Information (either USI's or Customer's) may be disclosed if required by law, provided that the party compelled to disclose it gives prompt notice to the disclosing party, where legally permissible, and cooperates reasonably in any efforts to protect the information during the legal process.

14. DATA SECURITY

USI will maintain appropriate technical, physical, administrative, and organizational controls to ensure the confidentiality, security, and integrity of Customer Confidential Information. These controls include:

(a) Systems and procedures for detecting, preventing, and responding to attacks, intrusions, or system failures, and regular testing of these systems, including vulnerability scans and penetration testing;

(b) A dedicated team responsible for maintaining security controls;

(c) An annual assessment of risks that could compromise Customer Confidential Information, and review of the sufficiency of existing systems to mitigate these risks;

(d) Security measures designed to meet high availability, business continuity, and disaster recovery standards.

USI's services are hosted in third-party data centers located in the US, On request, USI will provide its audit report and certifications. If you suspect any security incidents, please report them immediately to **farnold@myunifyai.com**.

15. DATA PRIVACY

USI's collection and use of information on the Site and through the USI Services is governed by its Privacy Policy, available at: https://www.myunifyai.com/If You are a Supplier, You acknowledge and agree that:
(i) USI processes Personal Data in accordance with the Data Processing Addendum (DPA) at https://www.myunifyai.com/, which is incorporated by reference, and
(ii) You are responsible for obtaining the necessary consents and notices to lawfully transfer Personal Data to USI.

If You are an individual user (e.g., administrative user, Worker, Visitor, or other Authorized User), You agree that:

- After receiving Your Personal Data, USI will process it per its data processing terms with Customer. If Customer is a Supplier, the terms are found at https://www.myunifyai.com/;
- You may only upload or submit Personal Data related to Yourself unless You have obtained valid consent from the data owner;
- Your Personal Data may be shared with Customer, Clients, Prime Contractors, USI's affiliates, and service providers as part of providing USI Services;
- Your Personal Data may be transferred to and stored in countries outside your residence, where the protection levels may differ and where it may be accessible by law enforcement;
- If You contact USI's support team, voice data may be collected for authentication purposes, but only with Your express consent;
- If You are a Worker or Visitor, USI may collect Sensitive Data (such as drug test results) as directed by Customer for worksite access, and by submitting this Sensitive Data, You consent to its processing by USI. If You do not submit this data, You may not be eligible to work for Customer or its Clients.

YOU AGREE NOT TO UPLOAD OR SUBMIT SENSITIVE DATA ABOUT ANY INDIVIDUAL WITHOUT PRIOR WRITTEN CONSENT FROM THE INDIVIDUAL AS REQUIRED UNDER APPLICABLE DATA PROTECTION LAWS.

You may access, correct, or update Your Personal Data or express concerns by contacting USI using the details provided in the Privacy Policy. For further information about Your data rights, refer to the Privacy Policy.

Please note that Personal Data accessed by Clients through the USI Services will be handled according to their own privacy policies. USI is not responsible for the actions of these third parties.

16. INDEMNIFICATION FOR THIRD PARTY CLAIMS

USI agrees to defend Customer against any claim, demand, lawsuit, or legal action brought by a third party alleging that the use of the USI Services in compliance with this Agreement infringes or misappropriates the third party's registered patent, copyright, or trademark (each referred to as a "Claim Against Customer"). USI will indemnify Customer for any damages awarded in a final judgment against Customer and for reasonable attorney fees and costs incurred as a result of the Claim Against Customer or for any amounts paid by Customer in a settlement approved in writing by USI. This indemnification is subject to the following conditions:

- (a) Customer promptly notifies USI in writing of the Claim Against Customer;
- (b) USI has sole control over the defense and settlement of the Claim Against Customer (provided that USI may not settle any Claim unless it fully releases Customer from liability); and
- (c) Customer provides USI with all reasonable assistance, at USI's expense.

Customer may choose to participate in the defense of the claim and attend proceedings at its own cost with counsel of its choice. If USI becomes aware of an infringement or misappropriation claim related to the USI Services, USI may, at its discretion and without cost to Customer:

- (i) modify the USI Services to avoid infringement,
- (ii) obtain a license for Customer's continued use of the USI Services, or
- (iii) terminate Customer's subscription with 30 days' written notice and refund any prepaid fees for the remainder of the subscription term.

The above obligations do not apply if:

1. The claim does not specify that the USI Services are the cause of the alleged infringement;
2. The Claim arises from the combination of the USI Services with software, hardware, data, or processes not provided by USI, where the USI Services alone would not have caused the infringement; or
3. The Claim arises from Customer's Content, a non-USI application, or Customer's breach of this Agreement.

Customer Indemnification of USI
Customer agrees to defend USI against any third-party claim, demand, lawsuit, or legal action arising from:

- (i) Customer's use of the USI Services, including any third-party claims related to access to Customer Content;
- (ii) Customer's use of or reliance on any Content provided through the USI Services; or
- (iii) USI's sharing of Personal Data with its Clients as described in this Agreement and in USI's Privacy Policy (each referred to as a "Claim Against USI").

Customer will indemnify USI for any damages awarded in a final judgment and for reasonable attorney fees and costs incurred as a result of the Claim Against USI or for any amounts paid by

USI under a settlement approved in writing by Customer. This indemnification is subject to the following conditions:

- (a) USI promptly notifies Customer in writing of the Claim Against USI;
- (b) Customer has sole control over the defense and settlement of the Claim Against USI (provided that Customer may not settle any Claim unless it fully releases USI from liability); and
- (c) USI provides Customer with all reasonable assistance, at Customer's expense.

USI may choose to participate in the defense of the claim and attend proceedings at its own cost with counsel of its choice. The above defense and indemnification obligations do not apply if the Claim Against USI arises from USI's breach of this Agreement.

17. LIMITATION OF LIABILITY

TO THE FULLEST EXTENT PERMITTED BY LAW, NEITHER USI NOR YOU WILL BE LIABLE FOR ANY LOSS OF USE, LOST REVENUE OR PROFIT, LOSS OF DATA, OR ANY CONSEQUENTIAL, EXEMPLARY, SPECIAL, OR PUNITIVE DAMAGES, WHETHER ARISING FROM A BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, EVEN IF SUCH DAMAGES WERE FORESEEABLE OR THE POSSIBILITY OF SUCH DAMAGES WAS DISCLOSED. EXCEPT FOR LIABILITY ARISING FROM INDEMNIFICATION OBLIGATIONS, THE TOTAL AGGREGATE LIABILITY OF USI OR YOU RELATED TO THIS AGREEMENT SHALL NOT EXCEED THE AMOUNT ACTUALLY PAID BY OR OWED BY YOU TO USI IN THE 12-MONTH PERIOD IMMEDIATELY PRIOR TO THE EVENT GIVING RISE TO SUCH LIABILITY.

Because some states or jurisdictions do not allow the exclusion or limitation of liability for consequential or special damages, the above limitation may not apply to You. If You are dissatisfied with any portion of the USI Services, Your sole and exclusive remedy is to discontinue using the USI Services.

18. FORCE MAJEURE

Neither You nor USI will be considered in default or liable for any delay, error, failure in performance, or interruption in service due to events beyond Your or USI's control, including but not limited to natural disasters, war, insurrection, terrorism, riots, strikes, power outages, internet or communication service interruptions, or acts by individuals not under the control of You or USI.

19. NO WARRANTIES

YOU ACKNOWLEDGE THAT USI MAKES NO WARRANTIES, GUARANTEES, OR REPRESENTATIONS OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE. TO THE MAXIMUM EXTENT PERMITTED BY LAW, USI SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, ACCURACY, COMPLETENESS, AND CORRESPONDENCE WITH DESCRIPTION. ANY IMPLIED WARRANTIES ARISING FROM A COURSE OF DEALING OR USAGE OF TRADE ARE ALSO DISCLAIMED. ALL SERVICES

PROVIDED BY USI ARE DELIVERED ON AN "AS-IS" AND "AS AVAILABLE" BASIS, WITHOUT ANY WARRANTY WHATSOEVER.

You also agree that using the USI Services does not guarantee Your hiring or acceptance by any Client or Supplier of USI. You are solely responsible for Your interactions with other members of the USI Network, and USI disclaims any liability or responsibility for disputes or issues between You and other USI Clients.

20. DISCLAIMER REGARDING COMPLIANCE INFORMATION

USI may provide Compliance Information to You as part of the implementation and provision of USI Services. This Compliance Information is intended solely for informational purposes, and USI does not guarantee its accuracy, legality, or completeness. USI has no obligation to update You regarding any changes to Compliance Information or legal or regulatory updates. Since Compliance Information may differ by jurisdiction, You agree to:

- (a) Assume full responsibility for verifying the accuracy, legality, and jurisdictional relevance of all Compliance Information before using it;
- (b) Acknowledge that USI holds no liability for any Compliance Information provided; and
- (c) Use or rely on Compliance Information entirely at Your own risk.

21. COMPLIANCE WITH LAW

You agree to comply with all applicable laws, regulations, ordinances, rules, and orders at all times, including those related to anti-slavery and human trafficking. You must not engage in any activity, practice, or conduct that would constitute an offense under the UK Modern Slavery Act 2015, the Australian Modern Slavery Act 2018 (Cth), or the Australian Criminal Code Act of 1995 (Cth) if conducted in the relevant jurisdictions. You also represent and warrant that You have not been convicted of, nor are under investigation for, any offense related to slavery or human trafficking.

22. NOTICES, PERMISSIONS, AND APPROVALS

All legal notices, permissions, or approvals under this Agreement must be provided via electronic mail to the email address specified by the receiving party. Such notices will be considered given once they are sent.

- Notices to USI should be sent to **farnold@myunifyai.com**.
- Notices to You will be sent to the email address You provided in Your Customer profile.

If You fail to maintain a valid email address, USI may provide notices through any means reasonably expected to provide You with actual notice.

23. MODIFICATIONS AND CHANGES

USI reserves the right, at its sole discretion, to modify this Agreement (including any documents incorporated by reference) at any time by posting an updated version on this page. USI will make

reasonable efforts to notify Customer of these changes via email or by displaying a notice on the Site. The updated version will be deemed accepted and will take effect 30 days after such notice, unless Customer provides USI with written notice of rejection of the changes. If Customer rejects the changes or if USI does not provide timely notice, the current version of the Agreement will remain in effect. The updated version will become effective for Customer upon the renewal of their current subscription term or when they upgrade or subscribe to additional services after the updated version is posted. Continuing to use the USI Services after the effective date of any changes constitutes Your acceptance of the updated Agreement.

24. GOVERNING LAW AND VENUE; ARBITRATION

The governing law that applies to any dispute or lawsuit arising from or in connection with this Agreement, as well as the courts with jurisdiction over such disputes, depends on where You are domiciled:

If You are domiciled in:	**Governing law is:**	**Courts with exclusive jurisdiction are:**
Anywhere globally except for Australia, Brazil, or New Zealand	Texas and controlling United States federal law	Houston, Texas, U.S.A.
Australia or New Zealand	New South Wales, Australia	New South Wales, Australia
Brazil	Federative Republic of Brazil	Sao Paulo, Brazil

USI and You agree to the applicable governing law without regard to any choice or conflict of law rules, and You consent to the exclusive jurisdiction of the applicable courts. The United Nations Convention on Contracts for the International Sale of Goods is expressly excluded from this Agreement, and the Uniform Computer Information Transactions Act does not apply. YOU HEREBY WAIVE ANY RIGHT TO INVOKE OR APPLY ANY OTHER LAW TO GOVERN THE FORMATION, PERFORMANCE, NON-PERFORMANCE, TERMINATION, OR EXPIRATION OF THIS AGREEMENT.

IN THE EVENT OF A DISPUTE BETWEEN YOU AND USI ARISING OUT OF OR RELATING TO THE USI SERVICES, EXCEPT WHERE PROHIBITED BY LAW, YOU OR USI MAY ELECT TO RESOLVE THE DISPUTE THROUGH BINDING ARBITRATION, AS OUTLINED BELOW, INSTEAD OF IN COURT. ANY CLAIM (EXCEPT FOR A CLAIM CHALLENGING THE VALIDITY OR ENFORCEABILITY OF THIS ARBITRATION AGREEMENT, INCLUDING THE CLASS ACTION WAIVER) CAN BE RESOLVED BY BINDING ARBITRATION IF EITHER PARTY REQUESTS IT. THIS MEANS THAT IF EITHER YOU OR USI ELECTS ARBITRATION, NEITHER PARTY WILL HAVE THE RIGHT TO LITIGATE THE CLAIM IN COURT OR HAVE A JURY TRIAL. ARBITRATION INVOLVES LIMITED DISCOVERY AND APPEAL RIGHTS.

Class Action Waiver
EXCEPT WHERE PROHIBITED BY LAW, ALL ARBITRATIONS MUST BE CONDUCTED ON AN INDIVIDUAL BASIS. THIS MEANS THAT NEITHER YOU NOR USI MAY CONSOLIDATE CLAIMS OR ARBITRATE AS PART OF A CLASS ACTION OR IN A PRIVATE ATTORNEY GENERAL CAPACITY. YOU AND USI ALSO AGREE NOT TO LITIGATE ANY CLAIMS AS A REPRESENTATIVE OR MEMBER OF A CLASS IN COURT.

Only a court, not an arbitrator, will have the authority to determine the validity and enforceability of this Class Action Waiver. Even if all parties agree to litigate a claim in court, either You or USI can still choose to arbitrate any new claims introduced by a new party or any new claims that arise later in the litigation process.

Governing Laws and Rules for Arbitration
The arbitration terms in this Agreement are governed by the Federal Arbitration Act ("FAA"). Arbitration must be conducted through Judicial Arbitration and Mediation Services, Inc. ("JAMS"). The rules outlined in this arbitration agreement, as well as JAMS' procedures, will govern the arbitration. If there is any conflict between this agreement and JAMS' procedures, the terms of this agreement will take precedence. If JAMS' procedures change after the claim is filed, the rules in effect at the time of the claim's filing will apply.

Fees and Costs
Each party is responsible for its own litigation or arbitration costs, including attorney fees, filing fees, and any travel expenses. The arbitrator's fees, along with the costs of third-party facilities used for hearings, will be equally shared between the parties.

Hearings and Decisions
Arbitration hearings will be held in Tampa, FL, USA, and conducted by a single arbitrator. The arbitrator must:

- (i) Follow all applicable substantive laws unless overridden by the FAA;
- (ii) Apply the relevant statutes of limitations;
- (iii) Honor valid claims of privilege; and
- (iv) Provide a written decision explaining the reasons for the award.

The arbitrator's decision will be final and binding, subject to review as permitted by the FAA. However, if the dispute involves more than $100,000, either party may appeal the decision to a new panel of three arbitrators. The appellate panel has the discretion to accept or reject the original award in whole or in part. The appeal must be filed with the arbitration organization within 30 days of the original decision. The party filing the appeal will cover the appellate costs unless the panel decides otherwise in its ruling. The arbitration award may be enforced in any court with appropriate jurisdiction.

Other Beneficiaries of this Provision
In addition to You and USI, the rights and obligations outlined in the arbitration terms extend to USI’s affiliates, as well as the officers, directors, and employees of both USI and its affiliates.

These terms also apply to any third-party co-defendant involved in a claim subject to this arbitration provision, along with all joint account holders and Authorized Users of Customer's account(s).

Survival of this Provision
The arbitration section will survive under the following conditions:
(a) Closure of Your account;
(b) Voluntary payment of Your account or any part of it;
(c) Any legal proceedings initiated to collect amounts owed by You; and
(d) Any bankruptcy declared by You.

25. ENGLISH LANGUAGE
The official version of this Agreement is in English, and the English text will take precedence in all matters, even if translated under the laws or regulations of another country.

26. MISCELLANEOUS TERMS
You and USI are independent contractors, and this Agreement does not establish any partnership, franchise, joint venture, agency, fiduciary, or employment relationship between You and USI. You may not assign or delegate Your rights or obligations under this Agreement without prior written consent from USI. USI may assign its rights under this Agreement, including in connection with a sale of USI, whether through a merger, asset sale, stock sale, or otherwise. Additionally, USI may fulfill its obligations through an affiliate or third-party contractor.

Any provisions of this Agreement that are intended to survive termination or expiration, such as indemnification obligations, limitations of liability, confidentiality obligations, and governing law provisions, will continue to apply after the termination of this Agreement.

The titles or headings used in this Agreement are for convenience only and will not affect the interpretation of any provisions. This Agreement represents the entire understanding between You and USI concerning Your use of USI Services and supersedes all prior agreements, proposals, or representations, whether written or oral. If You are a Client and there is a conflict between this Agreement and the agreement executed between You and USI, the executed agreement will prevail.

If any provision of this Agreement is found to be invalid, illegal, or unenforceable, that provision will be removed to the extent of its invalidity, and the remaining provisions will continue to be fully enforceable. This Agreement will not be construed more strongly against either party, regardless of which party was more involved in its drafting.

27. JURISDICTION SPECIFIC PROVISIONS
The jurisdiction-specific provisions outlined in Attachment 2, which is incorporated by reference into this Agreement, are only applicable to the specific jurisdictions listed, addressing local law requirements.

28. COMMENTS AND CONCERNS
All legal notices, such as those concerning claimed breaches or terminations of the Agreement or

Sales Orders, permissions, and approvals, must be delivered as set forth in Section 22. Notices related to copyright infringement claims should be directed to the copyright agent designated in USI's Copyright Policy and submitted according to the procedures outlined therein. For all other feedback, comments, technical support requests, or any other communications related to the USI Services, please contact USI through the available support channels.

ATTACHMENT 1

BILLING, REFUND, AND RENEWAL POLICY
Applicable to Clients only

FEES AND CHARGES FOR USI SERVICES; RENEWAL
WHEN YOU INITIALLY SUBSCRIBE TO THE USI SERVICES, YOU WILL BE CHARGED AN ACTIVATION FEE AND A SUBSCRIPTION FEE.

Your account will automatically be charged under the following conditions unless you have terminated your subscription:

- **Subscription Renewal:** Your subscription will automatically renew every 12 months from the date you originally subscribed to the USI Service. Your account will be charged a subscription fee unless you contact USI to terminate the subscription before the renewal date. The renewal invoice will be issued 30 days before the renewal date, serving as your renewal notice.
- **Subscription Upgrades and Changes:** Your account will be automatically charged in the following scenarios:
    - When you upgrade your subscription by adding with a new Client or Prime Contractor, adding a new Client site, selecting a new trade that changes your risk classification, or adding new products or services.
    - When a Client adds you to their approved Supplier List.
    - When a Client to whom you are connected adds a new product or service that changes your risk classification.
    - When a Client not yet connected to you informs USI that you are part of their supply chain.

You may remove your account from a Client's approved Supplier List at any time by contacting USI, which will notify the Client of your request. However, any Client in the USI Network may add your account to their approved Supplier List. You will receive a notification email when this occurs. If you do not wish to be connected to that Client, you may remove yourself by notifying USI. If you fail to notify USI within 30 days of receiving such notification, your account will automatically be charged as described above.

Worker Platform Fees
If you are subscribed to USI's Worker Platform, you will be charged annually for the seats you have in the platform. Each seat allows one Worker access to the platform. If additional seats are

added during the subscription term by you or a connected Client, you will be charged a prorated amount for the remaining term. You can adjust the number of seats at each annual renewal, and the subscription fee will be updated accordingly. Some features of the Worker Platform may require additional fees or licenses.

.

PAYMENT

Unless otherwise approved by USI, You are required to provide valid, up-to-date, and complete credit card or bank account information ("Payment Account") along with any other relevant contact and billing details. Payments made using a credit card (or debit card in Australia) may be subject to a card processing fee. This fee does not apply to other payment methods (such as ACH, bank wires, or debit cards outside of Australia) and will only be charged where allowed by law. The processing fee will be less than USI's actual costs for processing credit card payments, as USI cannot profit from these fees under the law.

YOU HEREBY AUTHORIZE USI TO AUTOMATICALLY CHARGE YOUR PAYMENT ACCOUNT, OR TO INITIATE ELECTRONIC DEBIT OR CREDIT ENTRIES THROUGH THE ACH SYSTEM, FOR THE FEES DESCRIBED ABOVE WHEN THEY ARE INCURRED. YOU ALSO ACKNOWLEDGE AND AGREE THAT USI MAY RETAIN YOUR PAYMENT ACCOUNT INFORMATION.

If your Payment Account information changes, it is your responsibility to contact USI to update your details.

USI may, at its discretion, issue invoices to You instead of automatically billing, and You must pay any invoice within 30 days of its issue date.

If USI is unable to charge Your Payment Account, or if payment has not been received within 30 days of the due date, USI may, without prejudice to its other rights and remedies:
(i) Disable Your password, account, and access to some or all USI Services, without liability, until the balance due is paid in full; and
(ii) Charge interest on unpaid amounts at a rate of 1.5% per month or the maximum allowed by law, whichever is lower, from the due date until the date of payment. Additionally, You are responsible for all costs incurred by USI in collecting late payments, including attorney fees.

CLIENT PROGRAM

USI offers a program in certain cases where a Client opts to pay or obtain discounts on Supplier registration and subscription fees for its connected Suppliers ("Client Program"). While USI is committed to adhering to the terms set with Clients, please note that the Client Program is solely at the discretion of the Client, and its duration and application to Suppliers on the Client's Supplier List are determined by the Client.

WITHHOLDING OF TAXES

The fees for the USI Services do not include taxes. You are responsible for paying any taxes

related to your subscription payments (such as sales tax, use tax, GST, VAT, consumption tax, or other similar taxes). If USI is legally obligated to pay or collect taxes that You are responsible for, USI will invoice You for that amount unless You provide a valid tax exemption certificate issued by the appropriate taxing authority. Taxes should not be deducted or withheld from payments to USI unless required by applicable law, in which case You are responsible for providing USI with the appropriate tax receipt to confirm that tax payments have been properly settled on USI's behalf.

If You fail to withhold or submit tax payments to the relevant authorities, leading to penalties, surcharges, or disallowance of a tax deduction, You are solely responsible and must indemnify USI for any costs, expenses, and penalties incurred as a result.

USI is solely responsible for taxes based on its income, property, and employees.

REFUND POLICY
Except as otherwise specified below, refunds for subscription fees will only be granted if Supplier's Payment Account was improperly double charged or charged in error. For instance, if Supplier submits payment twice for the same membership, or pays both via Payment Account and by check, Supplier is entitled to a refund of one of those payments.

Subscription fees are refundable if Supplier cancels their subscription and provides written notice of cancellation to USI within 7 days of initially subscribing to the USI Services. Activation fees, however, are non-refundable.

No refunds are provided after the payment of a renewal subscription fee. If You are subscribed to a Worker Platform, the number of seats in the platform cannot be decreased during the subscription term. It is the Supplier's responsibility to contact USI and request deactivation before the Membership Subscription Renewal Date (listed on the Edit Account page) if Supplier chooses not to renew.

Supplier is responsible for ensuring that their contact email is accurate and up to date.

Refunds will be issued using the same payment method used by Supplier. For example, if payment was made by credit card, the refund will be issued to that same credit card.

ATTACHMENT 2
Jurisdiction-Specific Provisions

Australia
If You are domiciled in Australia, Section 19 "No Warranties" of this Agreement is replaced with the following:

19. WARRANTIES
NOTHING IN THIS AGREEMENT EXCLUDES, RESTRICTS, OR MODIFIES ANY

CONDITION, WARRANTY, RIGHT, OR LIABILITY IMPLIED IN THE AGREEMENT OR PROTECTED BY LAW (INCLUDING ANY APPLICABLE GUARANTEES UNDER AUSTRALIAN CONSUMER LAW) TO THE EXTENT SUCH EXCLUSION, RESTRICTION, OR MODIFICATIONS WOULD RENDER THE AGREEMENT OR ANY PROVISION OF THE AGREEMENT VOID, ILLEGAL, OR UNENFORCEABLE ("NON-EXCLUDEABLE RIGHTS"). SUBJECT TO ANY NON-EXCLUDEABLE RIGHTS, ANY CONDITION, WARRANTY, GUARANTEE, REPRESENTATION, RIGHT, OR LIABILITY THAT WOULD OTHERWISE BE IMPLIED IN THE AGREEMENT OR PROTECTED BY LAW IS EXCLUDED.

You also acknowledge and agree that Your use of the USI Services does not guarantee Your hiring or acceptance by any Client or Supplier of USI. You are solely responsible for Your interactions with other members of the USI Network. USI disclaims any responsibility or liability regarding interactions or disputes between You and any USI Clients

USI confirms that all manual Audits and observations are conducted in good faith based on the information available to the auditor at the time of the Audit. Observations are made based on the general health and safety systems submitted by the Supplier and are not specific to any site or workplace. These Audits provide information according to a set of criteria but are not to be relied upon as a comprehensive account of all possible weaknesses or areas for improvement in the health and safety system. Additionally, these Audits do not identify on-site hazards, risks, or control measures at a specific workplace. The Audit process is based solely on USI's review of the written materials provided by the Clients and does not involve on-site inspections, observations, or audits. Clients are reminded of their own obligations under the WA WHS Act and related regulations.

BILLING, REFUND, AND RENEWAL POLICY

Applicable to Clients only

FEES AND CHARGES FOR USI SERVICES; RENEWAL
WHEN YOU SUBSCRIBE TO THE USI SERVICES, USI WILL CHARGE THE FOLLOWING FEES,:

- A **registration fee (Activation)** for the initial registration of your account in the USI system, which is included in the total amount of the first annuity
- An **annuity fee** for using the USI Services.

The annuity fee is based on a **risk rating**, which will be calculated at two points in time:

1. Initially, based on information provided by the Supplier during the Service Evaluation stage of the registration process.

2. After internal verification of the information, based on compliance guidelines and instructions from USI Network Clients. If a significant difference in risk is calculated at this point, the Supplier will be charged the difference.

Unless You terminate Your subscription, Your account will automatically be charged in the following circumstances:

- **Subscription Renewal:** Your subscription will automatically renew every 12 months based on the original subscription date, unless You contact USI to terminate your subscription before the renewal date. A renewal invoice will be issued 30 days before the renewal date, serving as your renewal notice.
- **Service Additions:**, pro-rated based on the remaining months of their annuity. This occurs when:
    - You upgrade your subscription by connecting with a new Client, adding a new Client site, selecting a new trade that changes your risk classification, or adding a new product or service.
    - Your subscription is upgraded due to being added to a Client's approved Supplier List.
    - Your subscription is upgraded because a connected Client adds a new product or service that changes your risk classification.
    - A new Client informs USI that You are part of their supply chain.

At any time, You may remove your account from a Client's approved Supplier List by contacting USI. The Client will be notified of your removal request. However, any Client in the USI Network may add your account to their approved Supplier List. You will receive a notification email informing you of this addition. If you do not wish to connect with the Client, You must notify USI within 30 days. Failure to do so will result in your account being automatically charged as described above.

If you are subscribed to one of USI's worker products ("**Worker Platform**"), You will be charged annually for the seats in the platform. Each seat allows one Worker to access the relevant platform. If seats are added during a subscription term, USI will charge You a prorated amount for the remainder of the term. You may adjust the number of seats at each annual renewal, and fees will be adjusted accordingly. Additional fees or licenses may be required for certain Worker Platform features.

Payment Terms
Unless otherwise approved by USI, If you fail to pay by the due date, USI may, without prejudice to its rights and remedies:
(i) Disable your password, account, and access to the USI Services without liability until the outstanding balance is paid.
(ii) Charge interest on unpaid amounts at 1.5% per month or the maximum allowed by law, whichever is lower, from the due date until payment is made. You will also be responsible for any collection costs, including attorneys' fees.

WITHHOLDING OF TAXES
The fees for USI Services do not include taxes. You are responsible for paying any applicable taxes related to your subscription payments (such as sales tax, use tax, GST, VAT, consumption tax, or similar taxes). If USI is legally obligated to pay or collect taxes that you are responsible for, USI will invoice you, and you must pay the amount due unless you provide a valid tax exemption certificate from the appropriate taxing authority. Taxes should not be deducted or withheld from payments to USI unless required by applicable law. In such cases, you must provide USI with the appropriate tax receipt to confirm that tax payments have been properly settled on USI's behalf.

Any failure to withhold or submit tax payments to the relevant tax authorities, resulting in penalties, surcharges, or disallowance of tax deductions, will be your sole responsibility, and you must indemnify USI for any related costs, expenses, and penalties.

USI is responsible for any taxes assessed against USI based on its income, property, or employees.

REFUND POLICY
Except as otherwise provided below, Clients are entitled to a refund of subscription fees only if their account was improperly double charged or charged in error.

Subscription fees are refundable if the Supplier cancels the subscription and provides written notice of the cancellation to USI within 7 days of the initial subscription to the USI Services. Activation fees are non-refundable. No refunds are offered after payment of a renewal subscription fee. If you are subscribed to the Worker Platform, the number of seats cannot be decreased during the relevant subscription term. It is the Supplier's responsibility to contact USI to deactivate the membership before the Membership Subscription Renewal Date, which is listed on the Edit Account page, if the Supplier does not wish to renew.

Clients are responsible for ensuring their contact email is accurate and up to date.

Refunds will only be issued to the same person or entity who made the original payment.

Germany
If You are domiciled in Germany, Section 17 "Limitation of Liability" of this Agreement is replaced with the following:

17.1 Unlimited Liability.
The parties shall be mutually liable without limitation:
(a) in the event of willful misconduct or gross negligence,
(b) within the scope of a guarantee undertaken by the respective party,
(c) in the event that a defect is maliciously concealed,
(d) in case of injury to life, body, or health, and
(e) according to the German Product Liability Law.

17.2 Liability for Breach of Cardinal Duties.
If cardinal duties are infringed due to slight negligence, endangering the objective of this Agreement, or if there is a slightly negligent failure to comply with essential duties for the proper performance of this Agreement, the parties' liability will be limited to foreseeable damages typical for the contract. In all other cases, any liability for damages caused by slight negligence shall be excluded.

17.3 Liability Cap.
Unless the parties are liable in accordance with the "Unlimited Liability" section above, the aggregate liability of each party, along with all affiliates, arising out of or related to this Agreement, shall not exceed the total amount paid by Customer for the services giving rise to the liability in the 12 months preceding the first incident. This limitation does not apply to payment obligations under the "Fees and Charges" section.

17.4 Scope.
Except for liability under the "Unlimited Liability" section, the above limitations apply to all claims for damages, irrespective of the legal basis, including tort claims. These limitations also apply to claims against the other party's employees, agents, or bodies.

India
If You are domiciled in India, the USI entity entering into this Agreement is **USI India Private Limited**.

Japan
If You are domiciled in Japan, You represent and warrant that neither Customer nor its officers, directors, or material shareholders are:
(a) Involved with Anti-Social Forces (defined below) and have not been for at least the last five years; or
(b) Engaged with Anti-Social Forces in any way, including management, funding, or providing favors.

USI may immediately terminate this Agreement in the event of a breach of these representations. "Anti-Social Forces" refers to an organized crime group (bouryokudan), members or affiliates, corporate racketeers (soukaiya), rogue persons or groups advocating social or political movements, or other anti-social forces.

New Zealand
If You are domiciled in New Zealand, Your payments will be processed through the secure **Fat Zebra** system. Any credit card details stored for recurring payments are handled through the Fat Zebra system, and no credit card information is stored by USI.

Spain
If You are domiciled in Spain, in the event of any conflict between the statutory laws in Spain and the terms of this Agreement, the applicable statutory law will prevail.

Privacy Policy

Last modified date: October 28, 2024

Privacy Policy

1. SCOPE OF THIS PRIVACY POLICY
This privacy policy ("Privacy Policy") explains how **Unified Systems Intelligence, LLC** and its affiliated group of companies worldwide ("USI," "we," or "us") handle your personal data when you visit USI websites, application sites, and mobile platforms that link to this Privacy Policy (collectively referred to as the "Services"). This Privacy Policy may be supplemented by additional terms or notices related to specific features of the Services.

Please note, this Privacy Policy does not apply to third-party websites, applications, or mobile platforms, even if they are linked to the Services. For example, the Services may offer access to social media features, message boards, chats, forums, blogs, and profile pages where you can post personal data and other materials. Information posted or disclosed through these services may be public, so exercise caution when sharing personal data in such spaces. We encourage you to review the privacy policies of third-party websites, applications, and platforms before interacting with them.

2. CONTROLLER AND PROCESSOR
USI, LLC functions as:

- A **data processor** when processing your personal data on behalf of our customers (e.g., when processing personal data contained in prequalification forms).
- A **data controller** when processing personal data for USI's own purposes (e.g., for billing, account management, product development, and legitimate business purposes).

You can contact our **Privacy Officer** via the following means:

Postal Service: 7901 4th St N #300 St Petersburg FL 33702, USA

For any questions or concerns regarding this Privacy Policy, please feel free to reach out to us using the contact information provided.

Unified Systems Intellligence, LLC
Attention: Privacy Officer
7901 4th St N #300

St Petersburg FL 33702, USA

Email: farnold@myunifyai.com

3. THE DATA WE COLLECT ABOUT YOU

Personal data, or personal information, refers to any information about an individual that can be used to identify that person. It does not include anonymous data where the individual's identity has been removed.

We may collect, use, store, and transfer various types of personal data about you, categorized as follows:

- **Identity Data**: Includes first name, last name, username or similar identifier, title, date of birth, gender, identification number, QR code or badge, and in limited cases (with your express consent), biometric data such as fingerprints or voice data for authentication purposes.
- **Contact Data**: Includes your mailing address, email address, and phone numbers.
- **Profile Data**: Includes username, password, photos, enrolled courses and assessments, course results/status, certificates, roles, assigned worksites, associated companies, and account status.
- **Health Data**: Includes vaccination status and alcohol/drug screening results, but only when requested by parties you work with or seek to work with through our Services, and when you voluntarily agree to provide it.
- **Professional Data**: Includes occupation, professional certifications, licenses, training status, course results/status, and work experience.
- **Location Data**: Includes your internet protocol (IP) address, geolocation, and worksite locations.
- **Transaction Data**: Includes details of your subscriptions associated with your account.
- **Technical Data**: Includes IP address, login data, browser type and version, time zone settings, browser plug-in types and versions, operating system and platform, and other technology on devices used to access the Services.
- **Usage Data**: Includes information on how you use the Services.
- **Marketing and Communications Data**: Includes your preferences for receiving marketing materials, communication preferences, and records of customer support calls.

We may also collect, use, and share **Aggregated Data**, such as statistical data, for any purpose. Aggregated Data may be derived from your personal data but is not considered personal data when anonymized, as it does not directly or indirectly identify you. For example, we may aggregate your Usage Data to determine the percentage of users accessing a specific feature. However, if Aggregated Data is combined with your personal data such that it can identify you, we treat it as personal data and will handle it in accordance with this Privacy Policy.

You are not legally obligated to provide USI with your personal data. However, failure to provide such data may limit our ability to offer you full access to the Services.

4. HOW IS YOUR PERSONAL DATA COLLECTED?

We use different methods to collect data from and about you including through:

Direct interactions
You or your authorized representatives may provide us with personal data, such as **Identity, Contact, Profile, Health, Professional,** and **Marketing and Communications Data**, by filling in forms or corresponding with us via phone, email, or other means. This includes personal data you provide when you:

- Create an account with us.
- Complete prequalification forms.
- Upload documentation requested by the parties you work with through our Services.
- Participate in events and activities we host.
- Provide feedback or contact us.

Automated technologies or interactions
As you use the Services, we automatically collect **Location, Usage,** and **Technical Data** about your device, browsing actions, and patterns. We gather this personal data using cookies and other similar technologies. Please refer to our **Cookie Policy** for further information.

Third parties or publicly available sources
We may receive personal data about you from third parties and public sources, including:

- **Identity, Contact,** and **Professional Data** from verification services and data enrichment providers like greenID, ZoomInfo, 6sense, or similar vendors, as well as from publicly available sources such as government document verification services (e.g., those provided by the Australian Government).
- **Identity, Contact, Profile, Health, Professional, Location,** and **Transaction Data** from your employer(s) or other companies you or your employer(s) work with.
- **Technical** and **Usage Data** from analytics providers like Google.
- **Contact** and **Transaction Data** from providers of technical and payment services.

---

5. HOW WE PROCESS YOUR PERSONAL DATA

We will only use your personal data where the law permits us to. Commonly, we will process your personal data under the following circumstances:

- Where it is necessary to fulfill the contract(s) we have entered into or are about to enter into with our customers.
- Where processing is required for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override these interests.
- Where processing is necessary to comply with a legal obligation.

The table below outlines the purposes and legal bases for our data processing activities, including the legitimate interests involved where applicable.

Please note, in some cases, we may process your personal data on more than one legal ground depending on the specific purpose for which we are using it.

Purposes for which we process your personal data	**Categories of personal data processed**	**Legal basis for processing including basis of legitimate interest**
To register you as a user of the Services, either as an authorized user of a client or a supplier	• Identity • Contact • Profile • Location	(i) Your consent or (ii) where we do not obtain your consent, our legitimate interests (to fulfill our contracts with our customers).
To assess your eligibility pursuant to the requirements by the parties you work with or seek to work with through our Services	• Identity (which may include biometric data under limited circumstances) • Contact • Profile • Health Data (if required by our customers) • Professional • Location	For biometric data (such as fingerprints to access a worksite), your consent. For Health Data, your consent. For other categories of personal data, (i) your consent or (ii) where we do not obtain your consent, our legitimate interests (to fulfill our contracts with our customers).
To assist our users in soliciting, bidding for, or completing a transaction or order	• Identity • Contact • Professional • Location • Transaction	(i) Your consent or (ii) where we do not obtain your consent, our legitimate interests (to fulfill our contracts with our customers).
To contact you about your account or tasks to complete and to manage our relationship with you such as notifying you about changes to the Services or our terms and asking you for your feedback or comments	• Identity • Contact • Profile • Location • Transaction	Necessary for our legitimate interests (to perform our contracts with our customers, keep our records updated, and improve our Services and support).

Purposes for which we process your personal data	**Categories of personal data processed**	**Legal basis for processing including basis of legitimate interest**
	• Marketing and Communications	
To verify your identity and account when you contact our customer support team	• Identity (which may include biometric data if opted in) • Contact	Your consent.
To provide and improve our Services and support and develop new products	• Identity • Contact • Profile • Professional • Location • Technical • Transaction • Usage	Necessary for our legitimate interests (to provide and improve the Services and our support).
To test new products and services (e.g. Beta testing)	• Identity • Contact • Profile • Health Data (if required by our customers who have opted in the testing) • Professional • Location • Transaction • Technical • Usage	For Health Data, your consent. For other categories of personal data, (i) your consent or (ii) where we do not obtain your consent, our legitimate interests (to develop and improve our Services).

Purposes for which we process your personal data	**Categories of personal data processed**	**Legal basis for processing including basis of legitimate interest**
To deliver relevant content and marketing materials to you and measure or understand the effectiveness of our marketing strategy	• Identity • Contact • Professional • Location • Transaction • Technical • Usage • Marketing and Communications	Necessary for our legitimate interests (to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy).
To deliver targeted advertising to visitors of our website (through cookies and other tracking technologies) and measure or understand the effectiveness of the advertising we serve	• Identity (such as device identifiers) • Location (such as approximate device location) • Technical • Usage	(i) Your consent or (ii) where we do not obtain your consent, our legitimate interests (to grow our business and to inform our marketing strategy).
To provide you with features on the Services such as sharing content with a colleague	• Identity • Technical • Usage	Necessary for our legitimate interests (to improve and promote our Services and support).
To invite you to participate in surveys, sweepstakes, competitions and similar promotions	• Identity • Contact • Professional • Transaction	Necessary for our legitimate interests (to improve and promote our Services).
To aggregate information in order to anonymize it for data analysis, audits, developing new products, enhancing the Services,	• Identity • Contact	Necessary for our legitimate interests (to improve our Services and support).

Purposes for which we process your personal data	**Categories of personal data processed**	**Legal basis for processing including basis of legitimate interest**
identifying usage trends and determining the effectiveness of our promotional campaigns	• Professional • Transaction • Technical • Usage	
To use data analytics to improve our Services, marketing, customer relationships and experiences	• Transaction • Technical • Usage	Necessary for our legitimate interests (to define types of customers for our products and services, to keep our products updated and relevant, to develop our business and to inform our marketing strategy).
To prepare or implement reorganization or sale of assets or shares	Potentially all categories of data as described in Section 3.	Our legitimate interests (to prepare and complete corporate transactions).
To administer and protect our business and the Services (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data), and prevent and detect security threats, fraud or other malicious activity	• Identity • Contact • Profile • Location • Transaction • Technical • Usage	Our legitimate interests (to improve and maintain the Services, and to protect our business).
To comply with our legal obligations, respond to government or judicial requests for information (including in the context of private litigation), resolve disputes, and enforce our agreements	Depending on the legal obligations.	Compliance with a legal obligation.

We will only use your personal data for the purposes for which it was originally collected unless we determine that another reason is compatible with the original purpose. If you would like an explanation of how processing for a new purpose is compatible with the original one, please contact us.

If we need to use your personal data for a purpose unrelated to the original one, we will inform you and explain the legal basis that allows us to do so.

Please note that, in accordance with legal requirements, we may process your personal data without your knowledge or consent where such processing is required or permitted by law.

---

6. DISCLOSURES OF YOUR PERSONAL DATA

We may share your personal data with the parties listed below for the purposes described in the previous sections.

Categories of Data Recipients	**Description**
Group Affiliates For further information, please visithttps://www.myunifyai.com/.	Members of the affiliated group of USI (including Unify AI) The affiliates and subsidiaries of USI, LLC, are data processors and provide IT and system administration, customer services, software development services, payment services, and other data processing services.
Service Providers and Contractors to USI For further information, please visit https://www.myunifyai.com/.	Cloud service providers based in US.
	Providers of software development services, IT and system administration, internal audit functions, quality assurance, customer support, document review services, maintenance services, and other administrative and processing services based in US.
	Providers of compliance tools.
	Providers of communication tools such as Zoom (based in the US) and Microsoft Teams (based in the US).

Categories of Data Recipients	Description
	Analytical service providers such as Google (based in the US).
	Verification service providers.
	Providers of data processing tools.
	Providers of customer relationship management tools such as Salesforce (based in the US).
	Marketing service providers such as Marketo (based in the US).
	Independent agents, representatives, and consultants globally to support our business.
Users of the Services	clients in the network of the Services who you work with or seek to work with through our Services.
Other Recipients	Third parties to whom we may choose to sell, transfer, or merger parts of our business or our assets.
	Third parties that we may acquire.
	Third parties if we expressly told you about such potential disclosure in our agreement(s) with you, or at the point at which you submitted the personal data to us.
	Third parties we need to disclose your personal data to in order to: (i) respond to or comply with any law,

Categories of Data Recipients	Description
	regulation, subpoena or court order, or government or judicial request (including in the context of private litigation); (ii) investigate and help prevent security threats, fraud or other malicious activity; (iii) enforce and protect the rights and properties of USI; or (iv) protect the rights or personal safety of our employees and third parties on or using our property. We may disclose your personal data to domestic or foreign government or public authorities in any of the countries in which we operate in order to respond to inquiries or requests or as otherwise required by law or legal process, including to meet national security or law enforcement requirements.

7. COOKIES AND OTHER TRACKING TECHNOLOGIES

We may automatically collect information using cookies or similar technologies, such as web beacons. Some of the content or functionality of our Services may be provided by third parties. These third parties may use cookies, web beacons, or other tracking technologies to collect information about you when you use the Services. The information they gather may be linked to your personal data, or they may collect information about your online activities over time and across different websites and services. You can set your browser to reject some or all browser cookies or to alert you when cookies are being used. If you disable or refuse cookies, some parts of the Services may not function properly. For more details about our use of cookies, please see our **Cookie Policy**.

8. DO NOT TRACK DISCLOSURE

Our Services do not respond to **Do Not Track** signals. However, you may disable certain tracking technologies as described in our **Cookie Policy**, such as by disabling cookies.

9. CHILDREN'S PRIVACY

We do not knowingly collect personal data from children under the age of 18, and our Services are not targeted toward children under 18.

10. YOUR CHOICES AND SELECTING YOUR PRIVACY PREFERENCES

As a user of the Services, you can manage your communication preferences, including opting in or out of certain communications, when you register with the Services or by updating your account preferences.

In some cases, we may send direct marketing messages without your explicit consent. However, you have the right to ask us to stop processing your personal data for such purposes. You can exercise this right by using the "opt-out" or unsubscribe option provided in the marketing communications. Please note that even if you opt out of direct marketing, we may still send you transactional or relationship-related messages (such as account notifications).

11. YOUR RIGHTS

You have the right to request a copy of the personal data we hold about you and to request corrections where necessary. In certain circumstances, you may also have the right to object to the processing of your personal data or request its erasure. If the Services allow registered users to access and update their registration information, the responsibility for ensuring the accuracy of that information rests with the user.

You also have the right to withdraw your consent at any time when we rely on it to process your personal data. If you choose to withdraw your consent, we may be unable to provide certain products or services to you, and we will inform you of this at the time you withdraw your consent.

To protect your privacy and security, we may take reasonable steps to verify your identity before processing any requests to exercise your rights. You can manage your personal data by returning to the webpage or application where you originally provided it and following the instructions, or you can contact us at:

Email: farnold@myunifyai.com

For more information about your rights or to exercise any of these rights, please contact us using the information provided above.

12. DATA RETENTION AND SECURITY

We store your information in computer systems and databases managed either by us or our external service providers. We will only keep your personal data for as long as it is reasonably necessary to fulfill the purposes for which it was collected, including legal, regulatory, tax, accounting, or reporting obligations. We may retain your data for longer periods if needed for a complaint or if we anticipate potential litigation related to our relationship.

To determine the appropriate retention period, we consider factors such as the volume, nature, and sensitivity of the data, the risk of unauthorized use or disclosure, the purposes of processing, and legal requirements. In some cases, we may anonymize your personal data for research or statistical purposes, which would allow us to use this information indefinitely without further notice.

The security of your personal data is important to us. We implement various measures to protect its confidentiality and integrity. However, no data transmission or storage method can be 100% secure. If you believe your interaction with us is no longer secure, please notify us immediately at **farnold@myunifyai.com**.

13. CHANGES TO THIS PRIVACY POLICY

We may modify this Privacy Policy to reflect changes in our data practices. When we do so, we will update the version posted here with a new revision date. We encourage you to review this page periodically for the latest information.

14. INTERNATIONAL DATA TRANSFER
Your personal data may be transferred to recipients as mentioned in Section 6, including to jurisdictions like the United States, which may not offer the same level of protection as your home country. However, we will continue to govern your data in accordance with this Privacy Policy.

For transfers to the **United States**, USI self-certifies under the **EU-US Data Privacy Framework**, **UK Extension**, and **Swiss-US Data Privacy Framework**. Details are available in our **Data Privacy Framework Notice**.

If data protection laws evolve, we will adjust our practices, working with our customers to ensure compliant data transfers across borders.

15. LOCAL LAWS AND REGULATIONS
While this Privacy Policy aims to provide consistent global information, all data will be processed in line with applicable local laws. For specific local regulations applicable to your region, please refer to **Appendix I** of this Privacy Policy.

16. HOW TO CONTACT US
If you have any comments, questions, or concerns regarding this Privacy Policy or how we process your information, you can reach out to us using the following contact details:

Unified Systems Intelligence, LLC
Attention: Privacy Officer
7901 4Th St N #300

St Petersburg FL 33702, USA
Email: farnold@myunifyai.com

Appendix I: Jurisdiction Specific Terms
United States - Notice to California Residents
Last Updated: September 28, 2023

This notice for California residents supplements the information in the Privacy Policy and applies solely to visitors, users, and others who reside in the State of California ("consumers" or "you"). We provide this notice in compliance with the **California Consumer Privacy Act of 2018 (CCPA)**, as amended by the **California Privacy Rights Act of 2020 (CPRA)**. Any terms defined in the CCPA have the same meanings when used in this notice.

Information We Collect

We collect information that identifies, relates to, describes, references, or could reasonably be linked, directly or indirectly, with a particular consumer, household, or device ("personal information"). Personal information does **not** include:

- Publicly available information from government records.

- Deidentified or aggregated consumer information.
- Information excluded from the CCPA's scope, such as:
    - Health or medical information covered by the **Health Insurance Portability and Accountability Act of 1996 (HIPAA)** and the **California Confidentiality of Medical Information Act (CMIA)**, clinical trial data, or other qualifying research data.
    - Personal information covered by certain sector-specific privacy laws, including the **Fair Credit Reporting Act (FCRA)**, the **Gramm-Leach-Bliley Act (GLBA)** or **California Financial Information Privacy Act (FIPA)**, and the **Driver's Privacy Protection Act of 1994 (DPPA)**.

Categories of Personal Information Collected

In particular, we have collected the following categories of personal information from consumers within the past twelve (12) months:

(Additional specific details regarding categories of information collected would follow here, such as identifiers, financial information, commercial information, etc., based on your operations.)

Category	**Examples**	**Collected**
A. Identifiers.	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.	YES
B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.	YES

Category	Examples	Collected
	Some personal information included in this category may overlap with other categories.	
C. Protected classification characteristics under California or federal law.	Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).	YES (to the extent the data is requested to be collected by our customers)
D. Commercial information.	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	YES (to the extent personal data is contained in the transaction data)
E. Biometric information.	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	NO (unless you contact our customer support team and give us your express consent to use your voice to authenticate your identity)
F. Internet or other similar network activity.	Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.	YES
G. Geolocation data.	Physical location or movements.	YES
H. Sensory data.	Audio, electronic, visual, thermal, olfactory, or similar information.	YES (if you upload a profile photo or if you participate in recorded meetings or calls)

Category	Examples	Collected
I. Professional or employment-related information.	Current or past job history or performance evaluations.	YES
J. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)).	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.	NO
K. Inferences drawn from other personal information.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	NO (with respect to our users) YES (with respect to business prospects)
L. Sensitive personal information	Government identifiers (social security, driver's license, state identification card, or passport number); complete account access credentials (user names, account numbers, or card numbers combined with required access/security code or password); precise geolocation; racial or ethnic origin; religious or philosophical beliefs; union membership; genetic data; mail, email, or text messages contents; unique identifying biometric information; health, sex life, or sexual orientation information.	YES (to the extent the data is requested to be collected by our customers or if you contact our customer support team and give us your consent to use your voice to authenticate your identity)

Use of Personal Information
As described in **Section 4** of our Privacy Policy, we collect personal information from various sources, including:

- Direct interactions with you.
- Automated technologies or interactions.
- Third parties or publicly available sources.

Purpose of Use or Disclosure of Personal Information

We may use or disclose the personal information we collect for one or more of the following purposes:

- **User Registration**: To register you as a user of the Services, either as an authorized user of a client or supplier.
- **Eligibility Assessment**: To assess your eligibility according to the requirements set by the parties you work with or seek to work with through our Services.
- **Transaction Facilitation**: To assist users in soliciting, bidding for, or completing a transaction or order.
- **Account Management**: To contact you regarding your account, manage our relationship, notify you of changes to the Services or terms, and request feedback.
- **Identity Verification**: To verify your identity when contacting customer support.
- **Service Improvement**: To provide and enhance our Services, support, and develop new products.
- **Beta Testing**: To test new products and services (e.g., Beta testing).
- **Marketing and Analytics**: To deliver relevant content and marketing materials, measure the effectiveness of our strategies, and target advertising through cookies and other tracking technologies.
- **Content Sharing**: To provide features such as content sharing with colleagues.
- **Surveys and Promotions**: To invite you to participate in surveys, sweepstakes, competitions, and similar promotions.
- **Data Aggregation and Analysis**: To anonymize and aggregate data for audits, product development, identifying trends, and analyzing promotional campaigns.
- **Reorganization or Sale**: To prepare or implement reorganization or sale of assets or shares.
- **Security and Fraud Prevention**: To administer and protect our business and Services by troubleshooting, performing data analysis, testing, system maintenance, and detecting security threats or fraud.
- **Legal Compliance**: To comply with legal obligations, respond to governmental or judicial requests for information, resolve disputes, and enforce agreements.
- **Other Uses**: As described to you during collection or as otherwise set forth in the CCPA.

Sensitive Personal Information

If you contact our customer support team, we may collect voice data for authentication purposes after obtaining your express consent. Any other sensitive personal information collected is strictly used to fulfill contractual obligations with our customers and for purposes permitted under the **California Consumer Privacy Act (CCPA)**. We do not process sensitive personal information to infer characteristics about individuals.

Changes in Data Collection or Use

We will not collect additional categories of personal information or use the personal information we collect for materially different, unrelated, or incompatible purposes without notifying you.

Retention of Personal Information
As outlined in **Section 12** of our Privacy Policy, we retain your personal information only for as long as necessary to fulfill the purposes for which it was collected, including meeting legal, regulatory, tax, accounting, or reporting requirements. We may keep your personal information for a longer period if necessary due to a complaint or anticipated litigation involving our relationship with you.

When determining the appropriate retention period, we consider various factors, including:

- The volume, nature, and sensitivity of the personal information.
- The potential risk of harm from unauthorized use or disclosure of the information.
- The purposes for which we process the data and whether those purposes can be fulfilled through other means.
- Legal, regulatory, tax, accounting, or other applicable requirements.

In certain circumstances, we may anonymize your personal information for research or statistical purposes. Once anonymized, the data is no longer associated with you, and we may use this information indefinitely without further notice.

Disclosure of Personal Information
We may disclose your personal information to third parties for business purposes. These disclosures are made under written contracts that outline the purposes, require confidentiality, and prohibit the third parties from using the disclosed information for purposes beyond the contract. In the past twelve (12) months, we have disclosed personal information for business purposes to the categories of third parties listed in the chart below.

Selling or Sharing of Personal Information
We do not sell personal information for monetary gain. However, we may use tracking technologies on our website for advertising purposes, which might be considered "selling" or "sharing" of your personal information under the **California Consumer Privacy Act (CCPA)**. In the past twelve (12) months, we may have sold or shared certain categories of personal information to the categories of third parties identified in the chart below.

Special Considerations
We do not sell or share personal information about individuals under the age of 16, nor do we sell or share personal information submitted by our customers in the course of using our Software-as-a-Service (SaaS) products.

Personal Information Category	**Category of Third-Party Recipients**	
	Business Purpose Disclosures	**Sale or Sharing**
A: Identifiers.	• Service providers for cloud services, software development, IT and system administration,	• Marketing/advertising service providers (such as online/device identifiers, IP

Personal Information Category	Category of Third-Party Recipients	
	Business Purpose Disclosures	**Sale or Sharing**
	internal audit functions, quality assurance, customer support, document review services, maintenance services, other administrative and processing services, and professional services (collectively, the "**Essential Service Providers**") • Compliance tool providers • Communication tool providers • Data analytics providers • ID verification providers • CRM providers • Marketing service providers • clients in the network of the Services who you work with or seek to work with through our Services	addresses, and other similar identifiers)
B: California Customer Records personal information categories.	• Essential Service Providers • ID verification providers • Clients	N/A
C: Protected classification characteristics under California or federal law.	• Essential Service Providers • ID verification providers • Clients	N/A
D: Commercial information.	• Essential Service Providers • ID verification providers	N/A

Personal Information Category	Category of Third-Party Recipients	
	Business Purpose Disclosures	**Sale or Sharing**
	• Clients	
E: Biometric information.	• Communication tool providers (if you contact our customer support team and give us your express consent to use your voice to authenticate your identity)	N/A
F: Internet or other similar network activity.	• Essential Service Providers • Compliance tool providers • Communication tool providers • Data analytics providers • ID verification providers • CRM providers • Marketing service providers • Clients	• Marketing/advertising service providers (such as browsing history, online behavior, and interactions with our and other websites)
G: Geolocation data.	• Essential Service Providers • Compliance tool providers • Communication tool providers • Data analytics providers • ID verification providers • CRM providers • Marketing service providers • Clients	• Marketing/advertising service providers (such as approximate device location)
H: Sensory data.	• Essential Service Providers • Communication tool providers	N/A
I: Professional or employment-	• Essential Service Providers	N/A

Personal Information Category	Category of Third-Party Recipients	
	Business Purpose Disclosures	**Sale or Sharing**
related information.	• ID verification providers • Clients	
J: Non-public education information.	N/A	N/A
K: Inferences drawn from other personal information.	• Essential Service Providers • Data analytics providers • CRM providers • Marketing service providers	• Marketing service providers (such as site visitors' preferences and characteristics)
L: Sensitive personal information	• Essential Service Providers • Compliance tool providers • Communication tool providers • ID verification providers • CRM providers • Clients	N/A

Your Rights and Choices
The **California Consumer Privacy Act (CCPA)** provides California residents with specific rights concerning their personal information. This section outlines your rights under the CCPA and how you can exercise them.

Right to Know and Data Portability

You have the right to request information regarding our collection and use of your personal data, also known as the **right to know**. After we receive and verify your request, we will disclose the following to you:

- The categories of personal information we have collected about you.
- The categories of sources from which we collected personal information.
- Our business or commercial purpose for collecting, selling, or sharing personal information.
- The categories of third parties to whom we disclose personal information.

- If applicable, a list detailing:
    - **Selling/sharing**: The personal information categories each recipient purchased or received.
    - **Business purpose disclosures**: The personal information categories obtained by each recipient.
- The specific pieces of personal information we collected about you (also called a **data portability request**).

Right to Correct

You have the right to request that we correct any inaccurate personal information we hold about you, taking into account the nature of the information and its purpose (referred to as the **right to correct**). Once we receive your request and confirm your identity, we will review the information you have contested and may request additional documentation to validate your request. We will use reasonable efforts to correct verified inaccuracies or otherwise process your request following the CCPA.

Please note, we may deny your request to correct if there are reasonable grounds to believe the request is fraudulent or abusive.

Right to Delete

Right to Delete
You have the right to request that we delete any personal information we have collected from you and retained, subject to certain exceptions (the **right to delete**). Upon receiving and verifying your request, we will review it to determine if any exceptions apply, allowing us to retain the information. We may deny your deletion request if retaining the information is necessary for us or our service providers to:

- Complete the transaction for which we collected the personal information or fulfill a service request.
- Detect security incidents, prevent malicious, fraudulent, or illegal activity, or prosecute those responsible.
- Debug to identify and repair errors that affect intended functionality.
- Exercise free speech or allow others to exercise their free speech rights.
- Comply with the California Electronic Communications Privacy Act.
- Engage in public, peer-reviewed scientific, historical, or statistical research in the public interest, where deletion could impair the research, and you provided informed consent.
- Enable internal uses aligned with consumer expectations based on your relationship with us.
- Comply with legal obligations.
- Make other lawful internal uses compatible with the context in which you provided the information.

We will delete or de-identify personal information not subject to these exceptions and direct our service providers to do the same.

Exercising Your Rights to Know, Correct, or Delete

To exercise your right to know, correct, or delete personal information, please submit a request by emailing **farnold@myunifyai.com**. Only you or someone legally authorized to act on your behalf may make a request related to your personal information. You can only submit a **right to know** request twice within a 12-month period. Your request must:

- Provide sufficient information for us to verify your identity or authority to make the request.
- Describe your request in enough detail to allow us to understand, evaluate, and respond to it.

We cannot respond if we cannot verify your identity or the authority to make the request.

You do not need an account to make a request, but if you do have one, we will consider requests from password-protected accounts sufficiently verified. We will only use the personal information provided in the request to verify your identity or authority.

Response Timing and Format

We will confirm receipt of your request within **10 business days**. If you don't receive confirmation within that timeframe, please contact **farnold@myunifyai.com**. We aim to respond substantively within **45 days**. If more time is needed (up to another 45 days), we will inform you of the reason for the delay. Our response will be sent to your account if you have one or via your chosen method (mail or email) if you do not.

If we cannot fulfill your request, we will explain why. For data portability requests, we will provide your information in a format that is readily usable for transferring between entities.

We do not charge for processing or responding to requests unless they are excessive, repetitive, or unfounded. If a fee is warranted, we will explain our decision and provide a cost estimate before completing your request.

Right to Opt-out of Sale/Sharing – Notice of Right to Opt-out of Sale/Sharing

Right to Opt-Out of Sale or Sharing of Personal Information
You have the right to opt-out of the sale or sharing of your personal information with third parties for cross-context behavioral advertising (the **right to opt-out**). To exercise this right, you can enable an opt-out preference signal on your browser or device. We process the signal automatically, as long as it is in a format commonly used and recognized by businesses. The opt-out preference signal will be treated as a valid request to opt-out for both the browser or device and any associated consumer profile (pseudonymous profiles).

You may need to install an extension or application on your browser or device to implement the opt-out preference signal. Providers of the platform or mechanism that sends the signal will typically inform you that the signal is intended to opt you out of the sale or sharing of your personal information.

Alternatively, you can opt-out by using the **Cookie Settings** on our website to reject cookies that could be used for marketing and behavioral advertising purposes, such as social media cookies, targeting cookies, and performance cookies. If you previously visited our website and did not opt-out, you may need to clear the cookies stored on your browser or device, then revisit our website to opt-out of sale or sharing. Please note that Cookie Settings control the settings for the specific browser or device you are using. To fully exercise your opt-out right, you will need to update the Cookie Settings on all browsers or devices you use to access our website.

Non-Discrimination
We will not discriminate against you for exercising your CCPA rights. Specifically, unless permitted by the CCPA, we will not:

- Deny you goods or services.
- Charge you different prices or rates for goods or services, including through discounts, benefits, or penalties.
- Provide a different level or quality of goods or services.
- Suggest that you may receive a different price or level of goods or services.

However, we may offer certain financial incentives permitted by the CCPA, which can result in different prices, rates, or quality levels. Any financial incentives will be reasonably related to the value of your personal information and will include written terms describing the material aspects of the program. Participation in any financial incentive program will require your prior opt-in consent, which you can revoke at any time.

Other California Privacy Rights
Under California's "Shine the Light" law (Civil Code Section § 1798.83), California residents may request information about how we disclose personal information to third parties for their direct marketing purposes. To make such a request, please email us at **farnold@myunifyai.com**.

Changes to Our Privacy Policy

We reserve the right to modify or update this Privacy Policy at our discretion and at any time. When we make changes to this notice, we will post the updated version on this page and revise the effective date accordingly. Your continued use of our Services after any changes have been posted constitutes your acknowledgment and acceptance of the updated Privacy Policy.

Contact Information

Additional Disclosures

Last Updated: September 28, 2023

Do We Disclose Personal Information to Overseas Recipients?

We may disclose your personal information to recipients located outside the United States. Please refer to Section 6 of the Privacy Policy for more details.

Do We Use Your Personal Information for Marketing?

We may use your personal information to offer you products and services that we believe may be of interest to you. However, we will not do so if you request otherwise. These products and services may be offered by us, our related companies, business partners, or service providers.

If you receive electronic marketing communications from us, you can opt out by following the opt-out instructions in the communication. Please note that even if you opt out of marketing messages, we may still send you transactional or relationship messages (such as account notifications).

Access to and Correction of Your Personal Information

You can request access to or correction of your personal information by contacting us. Our contact details are provided above. In some cases, we may not be required to grant you access to your personal information.

There is no fee for requesting access to your personal information, but we may charge a reasonable fee to cover our costs in providing access. We will respond to your requests within a reasonable timeframe and will take all reasonable steps to ensure that the personal information we hold about you is accurate and up to date.

Complaints

If you have a complaint regarding how we have managed any privacy-related issue, including a request to access or correct your personal information, please contact us using the details provided below. We will review your complaint and determine whether further investigation is required. Following our review, we will inform you of the outcome and any actions taken as part of our internal investigation.

If you are not satisfied with the way we have handled your privacy issue, you may seek advice from an independent advisor or contact the Office of the Federal Trade Commission (www.ftc.gov) for guidance on alternative actions that may be available.

Contact Details

If you have any questions, comments, requests, or concerns, please contact us at:

Email: farnold@myunifyai.com
Postal Address:
Unified Systems Intelligence, LLC
Attention: Privacy Officer
7901 4Th St N #300

St Petersburg FL 33702, USA

Notice at Collection

Last modified date: October 29, 2024

/

Notice at Collection

1. What personal data does USI collect and for what purposes? Does USI sell any personal data or share any personal data with third parties for cross-context behavioral advertising?

USI, LLC and its affiliates and subsidiaries (collectively, "USI," "we," or "us") collect your personal data to support our business operations, as detailed in the table below. These business purposes may include providing our services, managing customer accounts, ensuring security, and improving our products.

Personal Data Collection Purposes:
We collect personal data such as identity data (e.g., name, contact details), technical data (e.g., IP address, device information), and usage data (e.g., browsing actions) to fulfill the following purposes:

- Customer account management
- Performance of our services
- Marketing and advertising activities
- Compliance with legal obligations

Sale or Sharing of Personal Information:
We do not sell personal information for any monetary consideration. However, we do sometimes use tracking technologies on our website for advertising purposes, which may be considered "selling" or "sharing" of personal data under the California Consumer Privacy Act of 2018 (CCPA), as amended by the California Privacy Rights Act of 2020 (CPRA). The personal information we may "sell" or "share" is described in the chart below, primarily for cross-context behavioral advertising.

Data of Minors:
We do not sell or share personal information of individuals we know to be under 16 years of age. Additionally, we do not sell or share personal data that our customers have submitted to us as part of using our SaaS services.

If you wish to opt out of personal information sale/sharing, please visit the Notice of Right to Opt-out of Sale/Sharing.

Personal Data Category	**Collected [YES/NO]**	**Business Purpose**	**Sold or Shared for Cross-context Behavioral Advertising**
A. Identifiers (examples: a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers)	Admin users/agents of a Client or a Supplier (collectively, "**Admin Users**"): Yes (business contact data). Individual workers ("**Workers**"): Yes (such as name, contact data, and identification data). Client's visitors ("**Client Visitors**"): Yes (such as name and contact data). Business contact of potential customers ("**Business Prospects**"): Yes (such as name, contact data, online identifier).	**Admin Users:** To fulfill our contracts and manage our relationship with our customers. **Workers/Client Visitors:** To fulfill our contracts with our customers. **Business Prospects:** To generate sales leads.	**General website visitors***: the information being shared/sold may include online/device identifiers, IP addresses, and other similar identifiers. *"General website visitors" are also considered business prospects and do not include visitors to our SaaS platform.

Personal Data Category	Collected [YES/NO]	Business Purpose	Sold or Shared for Cross-context Behavioral Advertising
B. Personal data in a nature similar to the personal information listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)) (examples: name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information)	**Admin Users:** Yes (to the extent the business contact data falls under this category). **Workers:** Yes (to the extent the data is required by the Worker's employer). **Client Visitors:** Yes (to the extent the data is required by the Client). **Business Prospects:** Yes (to the extent the business contact data falls under this category).	**Admin Users:** To fulfill our contracts and manage our relationship with our customers. **Workers/Client Visitors:** To fulfill our contracts with our customers. **Business Prospects:** To generate sales leads.	No
C. Protected classification characteristics under California or US federal law (examples: age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related	**Admin Users:** No. **Workers:** Yes (to the extent the data is required by the Worker's employer). **Client Visitors:** Yes (to	**Admin Users:** N/A **Workers/Client Visitors:** To fulfill our contracts with our customers. **Business Prospects:** N/A	No

Personal Data Category	Collected [YES/NO]	Business Purpose	Sold or Shared for Cross-context Behavioral Advertising
medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information))	the extent the data is required by the Client). **Business Prospects:** No.		
D. Commercial information (examples: records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies)	**Admin Users:** No (unless personal data is contained in the business transaction data). **Workers:** No (unless personal data is contained in the business transaction data). **Client Visitors:** No (unless personal data is contained in the business transaction data). **Business Prospects:** No (unless personal data is contained in the business transaction data).	**Admin Users:** To fulfill our contracts and manage our relationship with our customers. **Workers/Client Visitors:** To fulfill our contracts with our customers. **Business Prospects:** To generate sales leads.	No
E. Biometric information (examples: genetic, physiological, behavioral, and	**Admin Users:** No.	**Admin Users/Business Prospects:** N/A	No

Personal Data Category	Collected [YES/NO]	Business Purpose	Sold or Shared for Cross-context Behavioral Advertising
biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data)	**Workers:** No (except for certain worksites in Australia where fingerprints may be collected for identification purposes). **Client Visitors:** No (except for certain worksites in Australia where fingerprints may be collected for identification purposes). **Business Prospects:** No. **All types of users including the above:** Yes, but only if you contact our customer support team and give us your consent to use your voice to authenticate your identity.	**Workers/Client Visitors:** To fulfill our contracts with our customers. **All types of users regarding voice data:** To authenticate your identity and to enhance the efficiency of our customer support services.	

Personal Data Category	Collected [YES/NO]	Business Purpose	Sold or Shared for Cross-context Behavioral Advertising
F. Internet or other similar network activity (examples: technical data, usage data, search history, information on a user's interaction with a website, application, or advertisement)	**Admin Users:** Yes. **Workers:** Yes. **Client Visitors:** Yes. **Business Prospects:** Yes.	**Admin Users/Workers/Client Visitors:** To fulfill our contracts with our customers and to improve and develop our products and services. **Business Prospects:** To generate sales leads.	**General website visitors**: the information being shared/sold may include browsing history, online behavior, interactions with our and other websites, and other similar network activity data.
G. Geolocation data (examples: physical location or movements)	**Admin Users:** Yes (IP address). **Workers:** Yes (IP address, and work site locations if required by the Worker's employer). **Client Visitors:** Yes (IP address). **Business Prospects:** Yes (such as IP	**Admin Users/Workers/Client Visitors:** To fulfill our contracts with our customers and to improve, maintain, and develop our products and services. **Business Prospects:** To generate sales leads.	**General website visitors**: the information being shared/sold may include approximate device location and other similar data.

Personal Data Category	Collected [YES/NO]	Business Purpose	Sold or Shared for Cross-context Behavioral Advertising
	address or the location of the event in which the Business Prospect participated).		
H. Sensory data (examples: audio, electronic, visual, thermal, olfactory, or similar information)	**Admin Users:** No (unless the Admin User participates in recorded meetings/calls). **Workers:** No (unless the Worker uploads a profile photo). **Client Visitors:** No (unless the Client Visitor uploads a profile photo). **Business Prospects:** No (unless the Business Prospect participates in recorded meetings/calls).	**Admin Users:** To fulfill our contracts with our customers. **Workers/Client Visitors:** To fulfill our contracts with our customers. **Business Prospects:** To generate sales leads.	No
I. Professional or employment-related information (examples:	**Admin Users:** Yes (role	**Admin Users:** To fulfill our contracts and	No

Personal Data Category	Collected [YES/NO]	Business Purpose	Sold or Shared for Cross-context Behavioral Advertising
current or past job history or performance evaluations)	with the business subscriber). **Workers:** Yes (to the extent required by the Worker's employer). **Client Visitors:** Yes (to the extent required by the Client). **Business Prospects:** Yes (business contact person's role).	manage our relationship with our customers. **Workers/Client Visitors:** To fulfill our contracts with our customers. **Business Prospects:** To generate sales leads.	
J. Non-public education information (examples: Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records)	**Admin Users:** No. **Workers:** No. **Client Visitors:** No. **Business Prospects:** No.	N/A	No
K. Inferences drawn from other personal information (examples: profile reflecting a person's preferences, characteristics, psychological trends, predispositions,	**Admin Users:** No. **Workers:** No.	**Admin Users/Workers/Client Visitors:** N/A **Business Prospects:** To generate sales leads.	**General website visitors**: the information being shared/sold may

Personal Data Category	Collected [YES/NO]	Business Purpose	Sold or Shared for Cross-context Behavioral Advertising
behavior, attitudes, intelligence, abilities, and aptitudes)	**Client Visitors:** No. **Business Prospects:** Yes (inferences related to the business contact person's role).		include site visitors' preferences and characteristics.
L. Sensitive personal data/special categories of personal data (examples: government identifiers (social security, driver's license, state identification card, or passport number); complete account access credentials (user names, account numbers, or card numbers combined with required access/security code or password); precise geolocation; racial or ethnic origin; religious or philosophical beliefs; union membership; genetic data; mail, email, or text messages contents; unique identifying biometric information; health, sex life, or sexual orientation information)	**Admin Users:** No. **Workers:** Yes (to the extent required by the Worker's employer). **Client Visitors:** Yes (to the extent required by the Client). **Business Prospects:** No. **All types of users including the above:** Yes, but only if you contact our customer support team and give us your consent to use your voice to	**Admin Users/Business Prospects:** N/A **Workers/Client Visitors:** To fulfill our contracts with our customers. **All types of users regarding voice data:** To authenticate your identity and to enhance the efficiency of our customer support services.	No

Personal Data Category	Collected [YES/NO]	Business Purpose	Sold or Shared for Cross-context Behavioral Advertising
	authenticate your identity.		

In addition to the business purposes described earlier, we may also use personal data for our legitimate interests, which include the following:

- Preventing and detecting security threats, fraud, or other malicious activities
- Preparing for or implementing reorganization, sale of assets, or shares
- Complying with legal obligations
- Other purposes outlined in our Privacy Policy and as permitted under applicable data protection laws

As previously mentioned, if you contact our customer support team, we may collect voice data for authentication, but only after obtaining your express consent. Any other sensitive personal data or special categories of personal data we collect from individuals are used strictly to fulfill our contracts with our customers (typically the employer of the individuals) and for purposes permitted by applicable data protection laws. We do not process sensitive personal data to infer characteristics about individuals.

We may also aggregate and anonymize the data for various purposes, including:

- Data analysis
- Auditing
- Developing new products
- Enhancing services
- Identifying usage trends
- Measuring the effectiveness of our promotional campaigns

2. How long does USI retain the personal data?

We retain personal data only for as long as necessary to fulfill the purposes for which it was collected, including legal, regulatory, tax, accounting, or reporting requirements. In some cases, we may keep personal data for a longer period, for example, if there is an ongoing complaint or if litigation is likely in relation to our relationship with you.

To determine the appropriate retention period for personal data, we assess:

- The amount, nature, and sensitivity of the data
- The potential risk of harm from unauthorized use or disclosure

- The purposes for which we process the data and whether we can achieve those purposes through other means
- Legal, regulatory, tax, accounting, and other requirements

In some circumstances, we may anonymize your personal data (so it can no longer be linked to you) for research or statistical purposes, in which case we may use this information indefinitely without further notice.

3. Further Information

For additional details, please view our full [Privacy Policy].

If you have any questions regarding this notice or require access to the information in an alternative format due to a disability, please contact us at:

Email: farnold@myunifyai.com

Data Processing Addendum to EUSA

Last updated: October 24, 2024

Data Processing Addendum to EUSA

This Data Processing Addendum ("DPA") is incorporated into and forms part of the terms and conditions of the End User Service Agreement ("EUSA") between USI and Supplier. It sets forth the additional terms, requirements, and conditions under which USI will obtain, handle, process, disclose, transfer, or store Personal Data when providing services under the EUSA. All capitalized terms not defined in this DPA shall have the meaning ascribed to them in the EUSA.

1. Definitions and Interpretation.

1.1 **Definitions.**

- **Applicable Data Protection Legislation:** Refers to laws and regulations applicable to each party's processing of Personal Data in connection with the EUSA, including but not limited to GDPR, UK GDPR, Australian Privacy Act, CCPA, PIPEDA, and other international, federal, or state data protection laws.
- **Data Subject:** An individual who is the subject of the Personal Data and whom the Personal Data relates to or identifies.
- **Data Privacy Framework:** Mechanisms for transferring Personal Data from the EEA, UK, and Switzerland to the United States, in compliance with EU, UK, and Swiss law.
- **EEA:** European Economic Area, including EU member states, Iceland, Norway, and Liechtenstein.
- **EU SCCs:** Standard Contractual Clauses for personal data transfer from the EU to third countries.
- **Personal Data:** Any information processed by USI that directly or indirectly identifies an individual or is defined as personal data under the Applicable Data Protection Legislation.
- **Processing:** Any activity involving the use of Personal Data, including recording, organizing, retrieving, using, or erasing it.
- **Security Breach:** Any security breach resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to Personal Data.
- **Subject Rights Request:** A Data Subject exercising rights under the Applicable Data Protection Legislation.
- **UK Addendum:** UK's International Data Transfer Addendum to the European Commission's SCCs.

1.2 **Schedules:** The Schedules are part of this DPA and will have full effect as if set out in the body of the DPA. 1.3 **Writing:** Includes email. 1.4 **Conflicts:** In case of conflict between this DPA and the EUSA, the DPA takes precedence, including any Schedule A provisions.

2. Roles and Scope of Processing.

2.1 **Roles of the Parties.** Supplier and USI agree that:

- (a) **Data Processor:** USI is a data processor when processing Personal Data on behalf of and under the direction of Supplier (e.g., Personal Data of Supplier's personnel, including prequalification or OSHA data).
- (b) **Data Controller:** USI is a data controller when processing Personal Data for its own purposes, including billing, account management, technical support, product development, analytical uses, and marketing communications.

This DPA clarifies the responsibilities of both Supplier and USI in terms of compliance with data protection laws and processing personal data in accordance with the EUSA.

2.2 Supplier Processing of Personal Data.
Supplier acknowledges and agrees that:
(a) Supplier is solely responsible for ensuring the accuracy, quality, and legality of the Personal Data submitted to USI and/or the Site, whether submitted by Supplier or by its Data Subjects;
(b) Supplier will only upload or submit Personal Data to USI and/or the Site that has been obtained from Data Subjects in compliance with the Applicable Data Protection Legislation;
(c) Supplier must ensure it has all required consents and notices in place and has fulfilled all other obligations under the Applicable Data Protection Legislation to enable the lawful transfer of Personal Data (including Sensitive Data) to USI, and to permit USI's processing of the Personal Data in multiple jurisdictions, as per the EUSA and this DPA;
(d) Where consent is the lawful basis for processing Personal Data or is required for using USI Services, Supplier will (i) maintain a mechanism for obtaining Data Subjects' consent, and (ii) provide a way for Data Subjects to withdraw consent, in each case in compliance with the Applicable Data Protection Legislation; and
(e) Supplier's use of the USI Services will not infringe upon the rights of any Data Subjects.

2.3 Details of Data Processing.
Schedule B describes the general categories of Personal Data, the types of Data Subjects, and other details regarding the processing activities USI will undertake in connection with providing USI Services in accordance with the EUSA.

3. USI's Obligations.

3.1 Processing Purposes.
USI will process Personal Data solely for the specific purposes outlined in Schedule B. USI may process Personal Data for other purposes if (i) it has obtained prior consent from the Data Subject, (ii) it is necessary for establishing, exercising, or defending legal claims in specific administrative, regulatory, or judicial proceedings, or (iii) it is necessary to protect the vital

interests of the Data Subject or another natural person. Where USI acts as a data processor for Supplier, USI will process Personal Data based on Supplier's instructions, provided those instructions fall within the scope of the EUSA. Any additional instructions will require USI's prior written consent. If USI believes any Supplier instruction violates Applicable Data Protection Legislation, it will promptly notify Supplier. Supplier is responsible for any required communications, notifications, or authorizations related to its Data Subjects.

3.2 Compliance Assistance.
USI will assist Supplier in meeting its compliance obligations under the Applicable Data Protection Legislation, considering the nature of USI's processing activities and the information available to USI. Supplier will bear the costs associated with such assistance. These obligations may include conducting a Data Protection Impact Assessment (DPIA) if the processing is likely to result in high risk to the rights and freedoms of natural persons.

4. USI's Employees.
4.1 USI ensures that all employees involved in processing Personal Data:
(i) have received appropriate training regarding their duties under Applicable Data Protection Legislation;
(ii) are aware of their personal obligations concerning data privacy; and
(iii) are bound by confidentiality obligations (whether contractual or statutory).

4.2 USI takes reasonable steps to ensure the reliability and trustworthiness of any employee who has access to Personal Data.

5. Security.
5.1 Taking into account the nature, scope, and risks involved in processing, as well as implementation costs, USI has implemented appropriate technical and organizational measures to ensure a level of security that is appropriate to the risks. These measures, described in Annex II of Schedule B, may be reviewed and updated by USI, provided such updates do not materially diminish the security level.

5.2 Supplier is responsible for determining if the security measures provided by USI are sufficient to meet their legal obligations and requirements under the Applicable Data Protection Legislation.

6. Security Breach and Personal Data Loss.
6.1 USI shall notify Supplier promptly upon becoming aware of any Security Breach. The notification will be sent to the email registered by Supplier, and if no email is registered, USI may choose another reasonable means of notification. Supplier should report suspected breaches to farnold@myunifyai.com.

6.2 USI will provide information about the breach, including the nature and consequences, measures taken, and the status of the investigation. Communications regarding Security Breaches do not imply any fault or liability by USI.

7. Cross-Border Transfers of Personal Data; Required Contractual Clauses.
7.1 Supplier acknowledges that USI may transfer, access, and process Personal Data globally to provide its services.

7.2 Where cross-border data transfers require specific mechanisms, USI will make those Transfer Mechanisms available as outlined in Schedule A.

7.3 If additional legal requirements or changes to the law necessitate modifications to the Transfer Mechanisms, USI will cooperate with Supplier to ensure compliance, updating the mechanisms in Schedule A when appropriate.

8. (Sub-) processors.
8.1 Supplier agrees that USI may use sub-processors listed on its website for processing Personal Data. USI will notify Supplier at least 10 days in advance if new sub-processors are added. Supplier may object based on compliance issues; if unresolved, Supplier may terminate the EUSA.

8.2 USI may use service providers as data controllers for specified purposes, as listed on its website.

9. Data Subject Rights Requests.
9.1 Both parties agree to cooperate reasonably to fulfill Subject Rights Requests as required under the Applicable Data Protection Legislation.

10. Third-Party Data Access Request.
10.1 USI shall notify Supplier of any third-party requests for Supplier's Personal Data unless prohibited by law.

11. Term and Termination.
11.1 This DPA takes effect when the EUSA becomes effective or when Personal Data is provided to USI and will remain in effect as long as the EUSA remains active.

11.2 Certain provisions related to Personal Data protection will survive termination to ensure continued data protection.

12. Data Return and Destruction.
12.1 At Supplier's request, USI will provide a copy of Personal Data before deletion, as long as the request is made prior to USI's scheduled disposal of the data.

12.2 Following the termination of the EUSA, USI will securely delete or destroy Supplier's Personal Data within a reasonable time, unless retention is necessary for legal, regulatory, or litigation purposes. Backup systems will be addressed according to USI's policies.

13. Audit.
13.1 Upon Supplier's written request, USI will provide documentation of its compliance with this DPA, including relevant audit reports and certifications. Supplier may audit USI's

compliance once per year unless otherwise required by a data protection authority, with audit expenses borne by Supplier. USI reserves the right to require confidentiality agreements prior to disclosing audit information.

14. General.
14.1 This DPA supersedes any prior data processing agreements between the parties. USI may update this DPA to reflect changes in data protection laws or its services, provided that no updates materially reduce the privacy or security of Personal Data.

14.2 USI's liability under this DPA is subject to the limitations set forth in the EUSA.

14.3 This DPA does not create third-party beneficiary rights, except as required by the Applicable Data Protection Legislation.

14.4 This DPA is governed by the laws specified in the EUSA.

14.5 If any provision of this DPA is found to be invalid or unenforceable, the remaining provisions will remain in effect, and Section 14.2 will remain enforceable regardless.

SCHEDULE A
TRANSFER MECHANISMS AND REQUIRED CONTRACTUAL CLAUSES

This Schedule A outlines the Transfer Mechanisms that are supported by USI for transferring Personal Data. These Transfer Mechanisms are only applicable if required under the Applicable Data Protection Legislation. When applicable, the mechanisms listed below are considered automatically incorporated into this DPA.

1. Data Privacy Framework.
For transfers of Personal Data to the United States, USI has self-certified to the EU-US Data Privacy Framework, the UK Extension to the EU-US Data Privacy Framework, and the Swiss-US Data Privacy Framework administered by the US Department of Commerce. Further details can be found in USI's Data Privacy Framework Notice at https://www.myunifyai.com/

2. EU Standard Contractual Clauses (EU SCCs).
For transfers of Personal Data from the EEA to USI where there is no other legitimate transfer basis, such transfers are subject to the EU SCCs. The specific modules applicable are as follows:

a. Data Controller to Data Controller Transfers (Module One):
When USI acts as a data controller and the Supplier is also a data controller, the following provisions will apply:

- Clause 7 (docking clause) is used.

- Clause 11(a) (redress) is not used.
- Clause 17: The first option is used, and the governing law is that of **Germany**.
- Clause 18(b): The courts of **Germany** shall have jurisdiction.

b. Data Controller to Data Processor Transfers (Module Two):
When the Supplier is a data controller and USI is acting as a data processor, the following provisions will apply:

- Clause 7 (docking clause) is used.
- Clause 9(a): Option 2 (general written authorization) is selected, with a ten (10) day notice period for changes to sub-processors.
- Clause 11(a) (redress) is not used.
- Clause 17: The first option is used, and the governing law is that of **Germany**.
- Clause 18(b): The courts of **Germany** shall have jurisdiction.

c. Annexes for EU SCCs:
Annex I, Annex II, and Annex III of the EU SCCs shall be completed with the information set out in **Schedule B**.

SCHEDULE A
3. UK Addendum.
When processing involves transfers of Personal Data outside the UK to USI, and no other legitimate basis exists (e.g., the Data Privacy Framework has been invalidated), transfers are subject to the UK Addendum, with the following terms:

a. The parties to this UK Addendum shall be the same parties to the DPA.
b. The EU SCCs referenced in Section 2 of this Schedule A shall apply, and Tables 1-3 of the UK Addendum will be completed accordingly with the relevant information.
c. For Table 4, "Importer" shall be selected.
d. Part 2 of the UK Addendum shall include the mandatory clauses of Addendum B.1.0 issued by the ICO and laid before Parliament under the Data Protection Act 2018, as revised.

4. Swiss Standard Contractual Clauses.
For transfers of Personal Data outside Switzerland to USI, when no other valid transfer mechanism exists (e.g., the Data Privacy Framework is invalid), such transfers will be subject to the EU SCCs referenced in Section 2 of this Schedule A, with adjustments for Switzerland:

a. "Member state" should not exclude Swiss Data Subjects from suing for their rights in Switzerland, per clause 18(c) of the EU SCCs.
b. For transfers subject solely to the Federal Act on Data Protection (FADP), references to the GDPR in the SCCs will be interpreted as references to the FADP.
c. If transfers are governed by both the FADP and GDPR, references to GDPR should be read as referring to the FADP for transfers governed by the FADP.

5. CCPA Contract Clauses.
For processing Personal Data of California residents, the following provisions apply:

a. USI will:

- Only collect, use, retain, or disclose Personal Data for permitted purposes under the EUSA and CCPA.
- Not sell or share Personal Data for cross-context behavioral advertising.
- Not collect, use, retain, or disclose Personal Data outside of the business relationship except as necessary for providing USI Services.
- Not combine Personal Data with data from other persons for business purposes unless permitted under CCPA and not involving cross-context behavioral advertising.
- Provide the same level of privacy protection required by the CCPA. USI certifies understanding and compliance with these restrictions.

b. Supplier has the right to monitor USI's compliance with the DPA and take steps to ensure Personal Data use aligns with the CCPA. If USI can no longer meet its obligations, it will notify the Supplier and take steps to stop and remediate non-compliant processing.

SCHEDULE B
PERSONAL DATA PROCESSING DETAILS
This Schedule B is part of the DPA and outlines the processing activities USI will undertake in connection with providing USI Services.

ANNEX I – DATA PROCESSING DESCRIPTION

A. LIST OF PARTIES
Data Exporter:

Name:	As provided by Supplier
Address:	As provided by Supplier
Contact person's name, position, and contact details:	As provided by Supplier
Activities relevant to the data transferred under this DPA:	Use of the USI Services pursuant to the USA.
Signature and date:	This Schedule B shall automatically be deemed executed when the USA is executed by Supplier.

Role (controller/processor):	Controller

Data importer:

Name:	USI, LLC
Address:	7901 4Th St N #300 St Petersburg FL 33702, USA
Contact person's name, position, and contact details:	Privacy Officer farnold@myunifyai.com
Activities relevant to the data transferred under this DPA:	Processing necessary to provide the USI Services to Supplier. Processing necessary for the legitimate interests of USI as described in the USI's privacy policy (the "**Privacy Policy**") which is available at https://www.myunifyai.com/.
Signature and date:	This Schedule B shall automatically be deemed executed when the USA is executed by Supplier.
Role (controller/processor):	Processor to the extent the processing is carried out on behalf of Clien. Controller as to the other processing activities, including but limited to the processing activities necessary for the legitimate interests of USI.

B. DESCRIPTION OF TRANSFER

Categories of Data Subjects whose Personal Data is transferred:	Supplier's admin users who access or use the USI Services through Supplier's account. Supplier's Workers (if Workers' Personal Data is contained in the prequalification forms and other Customer Content, or if Supplier is subscribed to USI's worker product(s)).
Categories of Personal Data transferred:	Supplier's admin users: **business contact data** (such as name, title, email, phone number, mailing address); **location data** (IP address); **technical and usage data** (such as browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology on the devices the Authorized User uses to access the USI Services); **biometric data** (if the admin user contacts USI's support team and gives express consent to use the admin user's voice for authentication

	purposes); **transaction data** (such as Supplier's subscription status and history, but only if Personal Data is contained in the transaction data); and marketing and **communications data** (such as Supplier's marketing and communication preferences, but only if Personal Data is contained in such data). Supplier's Workers: ▪ Any Personal Data submitted to the USI by Supplier and/or its Workers, which may include **identity data** (such as name, identification number, QR code or badge, title, date of birth, place of birth, gender, and citizenship status); **contact data** (such as email, phone number, home/mailing address, emergency contact and relationship, and next of kin information); **profile data** (such as username, password, profile photo, language preference, employer(s), the crews the Workers belong to, worksites, work roles, and trainings and assessments the Workers have enrolled into); **health data** (such as vaccination status, alcohol and drug screening results, and medical records or attestations to the extent such data is required by Supplier or its Clients); **biometric data** (if the Worker contacts USI's support team and gives express consent to use the Worker's voice for authentication purposes, or if the Worker attends a worksite that requires fingerprints to authenticate the Worker's identity); **professional data** (such as occupation, job competencies, evidence of work competencies, professional certifications, training status, academic qualifications and history, accreditations, and work experience); and **communications data** (such as communication preference); ▪ **Profile data** generated by USI concerning the Workers (if Supplier is subscribed to USI's worker product(s)), which may include unique ID, subscription status, compliance status against the requirements set by Supplier or its Clients,

	and/or site access key(s); and **transaction data** (only if the Workers' Personal Data is contained in the transaction data); ▪ **Location data** (such as IP address, worksite locations, and geolocations when logging into the site access control systems); and ▪ **Technical and usage data** (such as browser type and version, time zone setting and location, language settings, browser plug-in types and versions, operating system and platform, other technology on the devices the Worker uses to access the USI Services, time logged in/out, time on site, webpage visited, search terms, third-party content assessed).
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:	As described above, biometric data may be collected from Data Subjects with their express consent. The content uploaded or submitted by Supplier and/or its Workers may contain special categories of data, the extent of which is determined and controlled solely by Supplier at its discretion. Such special categories of data include, but may not be limited to, information revealing racial or ethnic origins, trade-union membership, and the processing of data concerning an individual's health. Additionally, geolocation data may be collected in connection with the USI Services (for example, geolocation data is collected when a Worker logs into the site access control systems). Any such special categories of data shall be protected by applying the security measures described in Schedule B.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous for the duration of the EUSA.
Nature of the processing:	Processing necessary to provide the USI Services to Supplier. Processing necessary for USI's legitimate interests as described in the Privacy Policy.

Purpose(s) of the data transfer and further processing:	Processing necessary for the provision of the USI Services. Processing necessary for USI's legitimate interests as described in the Privacy Policy.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	USI shall return or delete the Personal Data in accordance with Section 12 of this DPA.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	Details of (sub-) processors are available at:https://www.myunifyai.com/.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13 of the EU SCCs:	Where the EU GDPR applies, the competent supervisory authority determined in accordance with Clause 13 of the EU SCCs. Where the UK GDPR applies, the UK Information Commissioner's Office.

ANNEX II – TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

Overview
USI's software-as-a-service (SaaS) applications are developed with security at their core. The Connect and Workforce Management SaaS Services incorporate multiple security controls across each processing tier, addressing a variety of potential security risks. While these security controls may evolve over time, any updates will be made to maintain or enhance the overall security of the SaaS platform.

The primary security measures described below apply to all components of the USI Connect and Workforce Management SaaS Services, which are primarily hosted on cloud platforms like Amazon Web Services (AWS), with Equinix being used in specific regions.

Audits and Certifications
USI's SaaS Services are undergoing certification under the following standards and will be provided in 2025.

- ISO/IEC 22301

USI conducts an annual internal controls audit, reviewed by the Information Security and Privacy Management Systems Committee, which includes senior executive leadership.

Disaster Recovery and Business Continuity
USI employs a designated backup/failover AWS data center in a different geographic region from its primary production facility, ensuring quick response capabilities in the event of environmental, physical, or accidental disruptions. USI has a detailed Disaster Recovery and Business Continuity Plan, which is reviewed annually to keep personnel prepared for emergency situations that could affect normal business operations.

The recovery point objective (RPO) for USI's systems is less than 2 hours, while the recovery time objective (RTO) is less than 4 hours. USI also conducts regular risk assessments to ensure that mitigation strategies and controls are in place to address any identified risks.

Incident Response
USI has a comprehensive Incident Response Plan that allows personnel to swiftly react to potential security breaches or suspicious cybersecurity activities. An Incident Response Team, comprising experienced security professionals, assesses the situation, formulates action plans, and implements mitigation strategies. In the case of a confirmed breach, the team follows predefined protocols to mitigate malicious activity and preserve forensic evidence. Additionally, a notification procedure is followed in case of confirmed breaches.

Encryption
USI's SaaS Services encrypt data at rest, with further data encryption techniques like SALT applied to specific elements. This encryption ensures the confidentiality and integrity of customer data. Logical data separation is enforced within the platform, ensuring that no unauthorized entity can access customer data.

Customer data access is regulated through identity and access management protocols, following the "least privilege" principle, which grants access only to employees with a clear business need for specific data or system functions.

Web Application Security Controls
Customer access to USI's SaaS Services is protected by secure communication protocols, ensuring encrypted data transmission between end-users and the services. Customers have control over provisioning and de-provisioning users, and the SaaS Services offer multi-factor authentication via SAML 2.0 identity providers. Customizable password policies can also be configured to align with customer corporate policies.

Network
The SaaS Services employ network controls to restrict access and enforce security boundaries. Security groups are used to limit network activities to authorized endpoints. The services use a multi-tier network architecture, which separates environments into private, DMZ, and untrusted zones for enhanced security.

Monitoring and Auditing
USI monitors its SaaS Services for system health, network anomalies, and security incidents. An

intrusion detection system (IDS) alerts USI team members to any suspicious activity. Web application firewalls (WAF) are deployed for public web services. Application, network, user, and system events are logged and analyzed for threats using a security information and event management (SIEM) system, allowing for continuous security monitoring.

Vulnerability Management
USI conducts periodic web application vulnerability assessments, static code analysis, and external security assessments. Semi-annual independent vulnerability and penetration tests are conducted to ensure compliance with the OWASP Top 10 Web Vulnerabilities. Any identified vulnerabilities are prioritized, tracked, and remediated through USI's internal ticket system as part of its software development lifecycle (SDLC).

Secure Software Development
USI follows strict secure development practices within its SDLC. Static and real-time code analysis tools are used, and peer reviews are conducted before deployment into production. USI maintains separate environments for production, testing/quality assurance, and demonstration. USI developers undergo annual secure coding training to reinforce these practices.

USI Cybersecurity Team
USI's dedicated Cybersecurity Team, led by a Cybersecurity Manager with a master's degree in Cybersecurity, regularly conducts security training, vulnerability assessments, and penetration tests. The team ensures that technical and organizational security measures are continuously tested and improved. The Cybersecurity Team also participates in annual audits and certifications, ensuring compliance with security standards.

Privacy and Data Protection
USI maintains strict Information Security and Personal Data Protection Policies, which outline the procedures and controls for safeguarding customer information. These policies cover data retention, access control, authentication, acceptable use, and data privacy practices, ensuring that customer data is protected at all stages of processing.

ANNEX III – LIST OF SUB-PROCESSORS

USI's current list of sub-processors may be found at https://www.myunifyai.com/.