Contract No.-

FIXED FEE STATEMENT OF WORK

Employ Inc.	**Harbinger Software Inc,**
20 N. Meridian St., Suite 300 Indianapolis, IN 46204	16770 NE 79TH ST, #106, REDMOND, WA, 98052-4413, UNITED STATES
Hereinafter referred as **Customer** or **Employ**	Hereinafter referred to as **Harbinger**

Harbinger and Customer have executed this Statement of Work ("SOW/Agreement") as of the latest date appearing in the signature block below ("Effective Date") on the following terms and conditions.

Description Of Services and Deliverables:

Customer has engaged Harbinger to help with the migration of all current Mulesoft integrations over to the Workato platform. Harbinger is a preferred implementation partner of Workato.

Customer currently has two iPaas platforms- MuleSoft and Workato. It intends to consolidate all the integrations to one single iPaaS platform- Workato. Hence, the need to migrate the Jobvite integrations for all their customers from MuleSoft 3.0 and 4.0 to Workato. This migration encompasses key integrations with platforms such as Workday, UKG Pro, ADP, eScreen, and SFTP for flat files import.

Solution Scope & Approach

To start with Harbinger will conduct an in-depth analysis of existing MuleSoft integrations to get insights of the existing structure and functionality, identify data entities, and understand the existing system workflow. This will help the Harbinger team determine the extent of reusability and developing Workato recipes/recipe functions for the complete workflow.

The key aspects of the solution will include the development of custom actions to the pre-built Jobvite connector, enabling the retrieval and syncing of the employee data from Jobvite ATS and Onboard,such as WID, Name, Role, Employee, DOB, Address_Primary, Email, and Phone_Primary.

Additionally, the solution, which includes both API-based and file-based integrations,will facilitate the extraction of new hire data from Jobvite into a flat file, which will be shared via server or email. Enabling Import capabilities for various Jobvite entities, including requisitions, locations, custom fields, departments, and documents, with data mapping into ADP API and eScreen API.

The proposed delivery approach and methodology for the project is Scrum Agile, with each sprint of 2 weeks duration. Our team will work closely with the Employ team to deliver the solution within the proposed timeline, with regular demos spread across each milestone.

Detailed Project Scope, Execution Plan, and Timeline are presented in Appendix A

Duration of the SOW:

Start Date: April 1, 2025

End Date: September 30, 2025

The term of the SOW may be extended based on mutual understanding between parties and through the amendment.

Project Deliverables

The Project Scope is outlined in Appendix A.

High Level Project Plan

Project Plan is outlined in Appendix A.

Out of Scope Activities

1. Integration with other 3rd parties or any other system except those mentioned in this document.
2. The integration platforms or uses cases other than those mentioned in this document.
3. Any additional custom development beyond the migration scope is not covered.
4. Any automation outside Workato.
5. Any requirements other than those mentioned above.
6. Publishing recipe(s) on marketplace

Project Cost and Payment Schedule

Invoices from Harbinger will be sent directly to Customer's billing email address at Jobvite.com-vision@invoice.ca1.chromeriver.com or if the Customer has a standard invoice mailbox for business in India (unless otherwise notified in writing by Customer), and Customer will pay Harbinger for the Services invoiced as follows:

i. The total cost of the project shall not exceed USD $000.

ii. If the business requires onsite travel, then Customer agrees to pay Harbinger reasonable travel and out-of-pocket expenses at actuals with no markup applied, so long as such expenses are pre-approved in writing by Customer, in accordance with the Employ, Inc. T&E Policy.

Payment Schedule

S#	Payment schedule	Milestones
1	Advance payment	
2	April 30, 2025	Analysis and discovery, Connector Implementation, Jobvite to Custom Field Import, Jobvite to Department Import, Jobvite – location import
3	May 31, 2025	Jobvite Requisition Import, Jobvite New Hire Export, Jobvite to eScreen, Jobvite to Document Import
4	June 30, 2025	Jobvite – UKG Pro Onboarding, Jobvite – Workday, Various,
5	July 31, 2025	Jobvite to ADP API, Jobvite – UKG Pro (HRIS)
6	August 31, 2025	Various Mulesoft 4, UAT delivery
7	September 30, 2025	Upon completion

iii. All the fees stated above are for offshore services to be carried out from Pune, India development center. Any onshore presence if needed would be estimated separately.

iv. Any license costs (if applicable) are not included in the above cost.

v. There may be a 5% variance in cost in case of any unforeseen complexities or unknowns in the current scope of work that may come up during development and these additional costs if any will be discussed upfront and invoiced separately. Any requirements that are outside the current scope of work will be handled as per the Change Request/ Addendum process described below.

vi. Customer will pay Harbinger for the Services invoiced as per the above Payment Schedule within 45days of receiving invoice, failing which Customer shall be liable to pay delayed payment interest at 1.5% per month or maximum permitted by applicable laws, whichever is less, on the undisputed unpaid amount till the date of payment. Harbinger shall be entitled to recover from the Customer any loss on account of tax outgo caused due to delay in payment by the customer beyond 12 months from the date of invoice. Additionally, Harbinger may with 45 days' notice to Customer: (i) with 30 days prior intimation pause / suspend all the Services under this Agreement until all the due payment is received, (ii) collect payment for the Services by any other legal means and claim all the associated costs from the Customer.

vii. Customer will pay Harbinger for the Services invoiced from its below entity:

Full name of Customer's paying entity: Same as above entity
Address:
Bank details, if any:
Relation with Customer's entity (if paying entity is different than the Customer entity):

viii. It is agreed between the Parties that, the advance payment by the Customer is non-refundable if the project is paused due to reasons attributable to the Customer.

ix. It is agreed between the Parties that if Customer is procuring the Services and/or Deliverables for its end customer and if Customer accepts Harbinger Deliverables, then the Customer shall be responsible for payment for all the Services provided and Deliverables delivered by Harbinger as per the applicable SOW.

If the project is paused in-between due to reasons attributable to the Customer, then there will be a re-start fee of 2% of the remaining project value)

Acceptance Testing and Approval Process:

Acceptance Testing: Except for the recommendation report, which does not require Acceptance Testing, customer will perform acceptance testing within 10 days from the date of delivery of Deliverable ("Acceptance Period"). If Customer fails to communicate the acceptance or non-acceptance of the Services and/or Deliverable within 10 days from the date of delivery of Services and/or Deliverable, then Services and/or Deliverable shall be deemed to have been accepted by Customer. In case any Deliverable fails to pass the acceptance testing during Acceptance Period, Customer shall notify Harbinger within the Acceptance Period and Harbinger shall rework on such non-conforming Deliverable and provide corrected Deliverable to Customer within mutually agreed timelines. With respect to any SOW, if Harbinger has failed to meet the timeline for a particular Deliverable, at no additional cost or expense to Customer and at Customer's option, Harbinger shall provide to Customer all necessary additional Harbinger personnel to accelerate performance as may be required or necessary to achieve the timeline. The Parties agree that this will constitute Customer's remedy, exclusive or otherwise, for any damages caused by Harbinger's failure to meet a Deliverable timeline.

Change Requests/Addendum:

- Either Party may request a Change by submitting a Change request/Addendum to the other Party in writing for consideration of feasibility and likely effect on the cost and timing of the Services.
- The Parties will negotiate all Change requests expeditiously and in good faith.

- If the Parties agree to the terms and conditions of a Change, the Change and any new or additional fees due to Harbinger will be documented in a Change Request /Addendum.
- Harbinger will not be obligated to perform any Change prior to execution of a Change Order.

For the purposes of this Agreement:

“Change” shall means changes to the scope, commercials, nature or time schedule of the Services or additional services related to the Services and Deliverables but outside the current scope of a SOW.

“Change Order/Amendment/Addendum” shall mean a written change order to a SOW, signed by the authorized representatives of both the Parties to capture the understanding related to Change.

Ownership and License of Service Deliverables.

a. **Developments and Deliverables.** Except as may be otherwise explicitly agreed to in a statement of Services, upon payment in full, Harbinger grants to the Customer sole and exclusive ownership in the Developments and Deliverables developed for Customer in the course of performance the statement of Services. All Workato based recipes and components will be developed and deployed in the customer’s Workato environment.

b. Any formulae, processes, algorithms, ideas, inventions, know-how and techniques that are developed, created, conceived, originated, prepared, or generated by Customer during Customer’s use of the or content provided therein (collectively, “Outputs”) or through Harbinger’s use or exposure to Customer’s pre-existing work in provision of the Services (“Customer Content”), and all patent, copyright, trade mark, trade secret, and all other proprietary rights related to the Outputs or Customer Content and any derivative works created therefrom shall be considered “Work Product” owned exclusively by Customer and shall be considered Customer’s Confidential Information.

c. **Pre-existing work**. All pre-existing work will remain the sole property of the party providing the pre-existing work. During the performance of Services, each party grants to the other a temporary, non-exclusive license to use, reproduce and modify any of its pre-existing work provided to the other party solely for the performance of such Services. Except as may be otherwise explicitly agreed to in a SOW, upon payment in full, Harbinger grants to Customer a non-exclusive, perpetual, fully paid-up license to use, reproduce, modify, and distribute Harbinger pre-existing work to the extent such pre-existing work is incorporated as a part of the service deliverables.

d. Harbinger will not incorporate any open source, freeware, shareware software, AI tools into any Services / Deliverable, without Client’s prior written approval (which may be provided by electronic mail). To the extent any such software or tool is used by Harbinger with Client’s approval, Client is responsible for reviewing the applicable license terms for such software or tool and ensuring that it complies with the contributor’s use requirement. Harbinger makes no warranty, express or implied, including but not limited to title, non-infringement and the implied warranties of merchantability and fitness for a purpose relating to the use of such software or tool including presence of non-detectable/non-traceable malicious code.

e. Harbinger may use their general skills, knowledge, experience, processes, techniques, ideas, methodologies, templates, research and compilation of publicly available data or information gained or learned during the course of providing the Services / Deliverables, to develop work product or otherwise perform services which may be similar to those developed or prepared for Client, so long as Harbinger does so independently and without the use or disclosure of any Client's Confidential Information.

Warranties.

Services. Harbinger warrants that all Services will be performed with professional care and skill and in conformance with standards materially to those found in Appendix C.
Compliance with Laws. Harbinger warrants that it shall comply with all applicable local, state, and federal ordinances, laws, and regulations in providing the Services hereunder.
Third Party Contracts. Harbinger warrants that as of the effective date of this Agreement, its provision of the Services does not violate the terms and conditions of any third-party contract or obligation of Harbinger.
Specification and Documentation Warranty. Harbinger warrants that the Deliverables and Developments will materially comply, function, and perform, in accordance with an and all specifications, criteria, requirements and technical documentation. Any technical documentation will be materially accurate, complete, and sufficient in detail to enable Customer and its employees to use all of the functionality without assistances from Harbinger or any third party.

NO OTHER WARRANTIES. OTHER THAN THOSE IDENTIFIED EXPRESSLY IN THIS AGREEMENT, TO THE EXTENT PERMITTED BY APPLICABLE LAW, HARBINGER DISCLAIMS AND EXCLUDES ALL REPRESENTATIONS, WARRANTIES, AND CONDITIONS WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING WITHOUT LIMITATION ANY: (A) WARRANTY OF MERCHANTABILITY; (B) WARRANTY OF FITNESS FOR A PARTICULAR PURPUSE; AND/OR (C) WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING OR USAGE OF TRADE.

Defense Of Infringement and Misappropriation Claim.

Harbinger will defend, indemnify, and hold harmless Customer against any claims made by an unaffiliated third party that: i) any service deliverable infringes its patent, copyright, or trademark or misappropriates its trade secret, or ii) arises out of or relates to Harbinger's negligence, gross negligence, willful misconduct, or breach of this SOW, and will pay the amount of any resulting adverse final judgment (or settlement to which Harbinger consents). Customer must notify Harbinger promptly in writing of the claim and give Harbinger sole control over its defense or settlement. Customer agrees to provide Harbinger with reasonable assistance in defending the claim, and Harbinger shall reimburse Customer for reasonable out of pocket expenses incurred in providing such assistance. If as a result of an infringement claim, Customer's use of service deliverables is enjoined by a court of competent jurisdiction, Harbinger shall, at Harbinger's option and expense, either: i) procure the right to continue its use; ii) modify it to make it non-infringing; or iii) replace it with a non-infringing functional equivalent.

Harbinger's obligations will not apply to the extent that any claim or adverse final judgment is based on (i) computer code or materials provided by Customer; (ii) Customer's use of a fix or service deliverables after Customer has been notified by Harbinger in writing to discontinue use due to such a claim; (iii) Customer's use of trademark(s) without express written consent to do so; or (iv) any trade secret claim that is a result of Customer acquiring a trade secret (a) through improper means; (b) under circumstances giving rise to a duty to maintain its secrecy or limit its use; or (c) from a person who owed to the party asserting the claim a duty to maintain the secrecy or limit the use of the trade secret. Customer shall indemnify and reimburse Harbinger for any costs or damages that result from these actions.

Confidentiality.

"Confidential Information" means non-public business information, know-how, and trade secrets in any form, including information regarding a party's product plans and any other information a reasonable person should understand to be confidential, which is disclosed by or on behalf of either Party ("**Disclosing Party**") to the other Party ("**Receiving Party**"). "Confidential Information" excludes information that (a) was publicly known and made generally available in the public domain prior to the time of disclosure by the Disclosing Party; (b) becomes publicly known and made generally available after disclosure by the Disclosing Party to the Receiving Party through no action or inaction of the Receiving Party; (c) is already in the possession of the Receiving Party at the time of disclosure by the Disclosing Party, as shown by the Receiving Party's files and records; (d) is obtained by the Receiving Party from a third party without a breach of the third party's obligations of confidentiality; or (e) is independently developed by the Receiving Party without use of or reference to the Disclosing Party's Confidential Information, as shown by documents and other competent evidence in the Receiving Party's possession. In the case of Customer, Confidential Information includes all Developments, Deliverables, Outputs, and Work Product, as defined herein.

Mutual Confidentiality. The Receiving Party agrees to take reasonable steps, at least substantially equivalent to the steps it takes to protect its own proprietary information, but not less than reasonable care, to prevent the unauthorized duplication or use of the Disclosing Party's Confidential Information and the disclosure of the Disclosing Party's Confidential Information to third parties without the Disclosing Party's prior written consent. The Receiving Party may disclose the Disclosing Party's Confidential Information to the Receiving Party's employees or any third parties other than those legal and financial advisors or other authorized representatives of the Receiving Party who have a legitimate need to know such Confidential Information, and who will treat such Confidential Information as required under the terms of this Agreement.

Exceptions. The Receiving Party may disclose the Disclosing Party's Confidential Information as required by applicable law or regulation or as may be required to comply with a court order compelling such disclosure; provided that, unless legally prohibited from doing so, the Receiving Party gives the Disclosing Party prompt written notice of the requirement prior to the disclosure and reasonable assistance in limiting disclosure or obtaining an order protecting the information from public disclosures.

The Parties to the Agreement agree that the obligations under this Section (Confidentiality) shall apply during the Term of this Agreement and survive for a period of three (3) years post termination or expiration of the Agreement.

Data Protection. Customer's Confidential Information (including personal information) to which Harbinger has access, stores, transfers, handles, or otherwise has in its possession shall be handled in accordance with Appendix B.

Limitations of liability.

LIMITATION ON DIRECT DAMAGES. EXCEPT AS OTHERWISE SPECIFICALLY PROVIDED IN THIS PARAGRAPH, WHATEVER THE LEGAL BASIS FOR CUSTOMER'S CLAIMS, EACH PARTY'S TOTAL LIABILITY WILL BE LIMITED, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, TO DIRECT DAMAGES UP TO 3X THE TOTAL AMOUNT OF SOW UNDER THE APPLICABLE SOW UNDER WHICH THE CLAIM ARISES.NOTWITHSTANDING THE FOREGOING, IN CASE OF HARBINGER'S INDEMNIFICATION OBLIGATIONS, HARBINGER'S LIABILITY SHALL BE LIMITED TO 5X OF TOTAL AMOUNT OF THE SOW

NO LIABILITY FOR CERTAIN DAMAGES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NEITHER PARTY WILL BE LIABLE FOR ANY INDIRECT DAMAGES (INCLUDING WITHOUT LIMITATION, CONSEQUENTIAL, SPECIAL, OR INCIDENTAL DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, BUSINESS INTERRUPTION), ARISING IN CONNECTION WITH THIS AGREEMENT OR ANY SOW.

Termination.

Termination for material breach: Either party signing a SOW may terminate the SOW if the other party is in material breach or default of any obligation that is not cured within 30 days' notice of such breach. Harbinger may terminate this Agreement if Customer fails to pay any invoice that is more than thirty (30) calendar days outstanding.

The sole effect of terminating this Agreement will be to terminate the ability of either party to enter into subsequent Statement of Work that incorporate the terms of this Agreement. Termination of this agreement will not, by itself, result in the termination of any Statement of Work previously entered into (or extensions of the same) that incorporate the terms of this agreement, and the terms of this Agreement will continue in effect for purposes of such Statement of Work unless and until the Statement of Work itself is terminated or expires.

It is understood and agreed that in the event of termination of this Agreement or any SOW, Harbinger shall be entitled to the payment for all the work completed / Services performed and Deliverables delivered up to the effective date of termination including up to the last day of notice period in addition to committed and incurred costs if any.

Assignment:

Save and except its Affiliates, neither Party can assign all or part of its obligations under this Agreement without the prior written consent from the other Party. Unless otherwise stated, this Agreement will continue in full force during the Term of the Agreement and will be a binding obligation on either Party to meet their service level expectations even in cases of merger, takeover, acquisition, amalgamation etc. of either Party. The new entity or the taking over party will have the obligations under the current Agreement. However, either Party may terminate this Agreement in the event of such merger, takeover, acquisition, or amalgamation of one Party with the competitor of the other Party.

Miscellaneous.

a. Independent contractor. Harbinger will provide Services as an independent contractor and will be responsible for any and all social security, unemployment, workers' compensation and other withholding taxes for all of its employees.

b. Feedback. All suggestions, enhancement requests, or other feedback provided by Customer during the term of this Agreement and relating to the operation of the Service may be used by Harbinger.

c. Non-Hiring of Resources. Each party expressly agrees that they will not hire any resources working with the other party directly, indirectly, as employees, contractors, or independent consultants or in any other way related to this Agreement during the Term of this Agreement and for a minimum period of two (2) year from the termination of this Agreement, without the prior written consent of the other party.

In the event Customer directly or indirectly hires or solicits or employs any Harbinger personnel (employee or consultant of Harbinger), then Customer shall pay liquidated damages equal to $20,000. The foregoing hiring restriction shall not apply if: 1) Customer makes a general solicitation for employment which is not specifically targeted at Harbinger personnel; 2) Harbinger personnel contacts Customer for the purposes of employment; or 3) personnel has been terminated by Harbinger.

All these remedies will be in addition to and not in limitation of any injunctive relief or other rights or remedies to which Harbinger is or may be entitled at law or in equity or under this Agreement.

d. Publicity. Upon Customer's advance written approval in each instance (a) provided that Harbinger does not disclose any of Customer's Confidential Information in such case study, Harbinger may create and publish a case study regarding the nature of Customer's use of the Services; and (b) Harbinger may identify Customer - by name and logo - as a customer in Harbinger's published customer lists.

e. Applicable law. This Agreement together with the applicable SOW will be governed by the laws of the state of Delaware.

f. Dispute resolution. Any action by either party to enforce this Agreement or a SOW, will be brought in the jurisdiction of King County, Washington. This choice of jurisdiction does not prevent either party from seeking injunctive relief with respect to a violation of intellectual property rights or confidentiality obligations in any appropriate jurisdiction. Any action brought for delinquent payment of an invoice may be brought within any court within Washington State.

g. Compliances: The Customer hereby confirms that it has been compliant with and has not violated any applicable rules/ regulations/orders issued including but not limited to the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC") and hereby agrees and undertakes that it shall continue to abide by and remain in compliance with all applicable rules/ regulations/ orders and as may be updated from time to time, for the entire duration and term of this [Contract/Agreement]. In the event that the Customer does not comply or violates any such rules/ regulations/orders compliance requirements/ commitments during the term and duration of this [Contract/Agreement]. then Harbinger shall not be held responsible/ liable for the same and the Customer shall be solely liable to settle such claims.

h. Entire Agreement. This Agreement and the statements of Services constitute the parties' entire Agreement concerning the subject matter hereof and supersede any other prior and contemporaneous communications. The terms of these documents will control in the following order: (i) this Agreement; (ii) any SOW. The parties may amend this Agreement only in writing when signed by both parties. The parties signing a SOW may amend the SOW only in writing when signed by both parties.

i. Severability. If a court holds any provision of this Agreement or a SOW to be illegal, invalid or unenforceable, the remaining provisions will remain in full force and effect and the parties will amend the Agreement or SOW to give effect to the stricken clause to the maximum extent possible.

j. Waiver. No waiver of any breach of this Agreement or SOW will be a waiver of any other breach, and no waiver will be effective unless made in writing by the waiving party.

k. Force majeure. Other than any payment of fees by Customer to Harbinger, neither Party shall be liable for failure to perform or for delay in performance hereunder due to causes beyond its reasonable control, (each a "Force Majeure"), including, but not limited to, acts of God, fires, floods, earthquakes, accidents, strikes, acts of war, acts of terrorism, riot, embargoes, fuel crises, acts of civil or military authorities, or intervention by governmental authority, epidemics, pandemics or consequences thereof, provided that such Party gives prompt written notice thereof to the other Party. Any failure occasioned by the foregoing shall be remedied as soon as reasonably possible. In the event Force Majeure event persists for more than 30 (Thirty) consecutive days, either Party may terminate this Agreement or relevant SOW immediately on completion of 30 (Thirty) consecutive days or agree to extend the Agreement for a further period as mutually agreed between the Parties. In the event of termination of the Agreement / relevant SOW pursuant to this Clause, Harbinger shall be entitled to the payment for all the Services performed / work completed or Deliverables delivered up to the effective date of termination including the committed and incurred costs if any.

l. Counterparts. This Agreement and any statements of Services may be executed in any number of counterparts, each of which will be an original, and such counterparts together will constitute one and the same instrument. Execution may be affected by delivery of facsimiles of signature pages (and the parties will follow such delivery by prompt delivery of originals of such pages).

m. Notices. The Parties shall give all notices and communications between the Parties in writing by (i) personal delivery, (ii) a nationally recognized courier service, (iii) first-class registered or certified mail, postage prepaid, (iv) electronic mail to the Party's address specified in this Agreement, or to the address that a party has notified in writing to be that party's address for the purposes of this section. A notice given under this Agreement will be effective on the other Party's receipt of it, or if mailed, the earlier of the other Party's receipt of it and the seventh (7th) business day after mailing it.

In case of Harbinger, to Shrikant Pattathil, President and legal@harbingergroup.com ; and in case of Customer, to Maurice Wells Maurice.Wells@employinc.com and Saran Satkunasivam saran.satkunasivam@lever.co.

IN WITNESS WHEREOF, the Parties have caused this SOW to be executed as of the SOW Effective Date by their duly authorized representatives.

Employ Inc.	**Harbinger Systems Private Limited**
______________________________	__________________________________
Name of Signatory:	Name of Signatory:
Designation:	Designation:
Date:	Date:

APPENDIX A

PROJECT SCOPE:

The following table describes the scope of work for migration of the MuleSoft integration to Workato platform.

#	Integrations	Type (Custom, Partial or Productized)	Total Customers	Harbinger Understanding and Considerations
1	Jobvite - Workday	Partially Productized	13	Considered basic details of employee such as WID, Name, Role, Employee_ID, DOB, Address_Primary, Email, Phone_Primary etc.
2	Various	Custom	28	Considered unidentified medium level complexity of integration with 3-4 use cases
3	Jobvite - New Hire Export	Partially Productized	56	Considered scheduler based New Hire Export. Flat files exporting new hire data from Jobvite ATS or Jobvite ATS and Onboard.
4	Jobvite - Requisition Import	Partially Productized	22	Considered flat file (.csv) to import data to the Jobvite system through API
5	Jobvite - UKG Pro Core (HRIS)	Productized	9	Considered New Hire sync use case with medium complexity with unique data mapping
6	Jobvite - UKG Pro Onboarding	Productized	37	Considered New Hire sync onboarding process by creating new hires in UKG Pro Onboarding.
7	Jobvite - Location Import	Partially Productized	12	Considered flat file (.csv) to post or send data to the Jobvite system through API
8	Jobvite to Custom Field Import	Partially Productized	14	Considered flat file (.csv) to post or send data to the Jobvite system through API
9	Jobvite to Department Import	Partially Productized	9	Considered flat file (.csv) to post or send data to the Jobvite system through API
10	Jobvite to Document Import	Partially Productized	3	Considered flat file (.csv) to post or send data to the Jobvite system through API
11	Jobvite to ADP API	Productized	4	Considered a medium complexity use case for unique data mapping for each customer's specific needs from Jobvite to ADP API
12	Jobvite to eScreen	Productized	3	Considered a medium complexity use case for unique data mapping for each customer's specific needs from Jobvite to eScreen
13	Various MuleSoft 4	Custom	30	Considered fully custom design/asset Integration for each customer with a medium complexity

Notes:

1. For every integration, efforts are projected for consecutive customer integrations under the assumption that each customer possesses a comparable level of complexity. However, any alterations in the complexity of the use case may lead to variations in the required efforts.
2. In Workato, the Harbinger team will use the templatized approach for common functionality currently used by Employ for its existing integrations. This can be seamlessly integrated into the proposed workflow to streamline the process further. Harbinger will ensure to follow the best reusability practices convention to Employ existing integrations.
3. For scalability, batch processing will be employed for handling extensive data volumes efficiently and maintaining optimal performance.
4. Any change to the list of integrations will be considered as out of scope and will be estimated and charged separately with prior approval from the customer.
5. It assumed that the source of the flat file to be an exported file will be via an API.
6. For the above various MuleSoft 3.0 and 4.0 integrations (Row #2 and #13 in the above table) following scope is considered:

#	Feature	Implementation Tasks
1	HRIS Integration	The integration will be made up of the following syncs: 1. Ingestion of requisition and/or position data from the HRIS vendor system to Jobvite (this could be in the form of populating drop down lists with meta data or creating a requisition object in Jobvite) 2. Pushing Hire and Onboarding data to vendor HRIS 3. Accommodation for multiple hire types (e.g. New Hire, Re-hire, internal hire/mobility, etc.) 4. Pull data from both the Jobvite ATS and Onboarding module Note: Integrations will primarily be polling based for #1 and trigger based for #2
2	Assessment and Background check	The integration will be made up of the following syncs: • Trigger background check or assessment to vendor system (at a pre-defined workflow state / trigger). This will send the required details from Jobvite to the vendor system (e.g. name, email, etc. + test or background check type) • Collect results and post them back to Jobvite (retrieve assessment or background check result and post it to Jobvite)
3	File Sync	The integration will be made up of the following syncs: • Create a file (csv or xml) based on data from Jobvite (via API) and drop file to location (e.g. sFTP, S3) • Ingest file (csv or xml) and push data into Jobvite via the API

Solution Overview

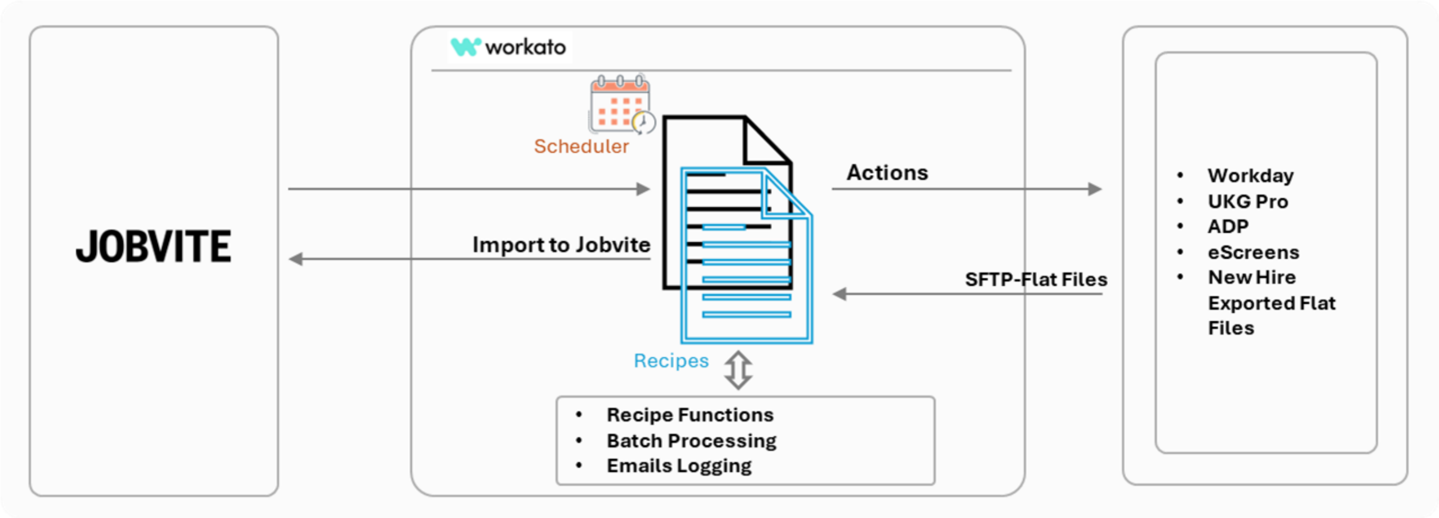
Harbinger proposes following implementation task for the migrations and integration of customers from Mulesoft to Workato:

1. **Detailed Analysis of Data Entities and System Workflows:** Thorough exploration and comprehension of data entities within the associated systems and workflows.
2. **Analysis of Existing MuleSoft Integrations**: In-depth examination of the current Mulesoft integrations to gain insights into their functionality and structure.
3. **Jobvite-Workato Custom Connector Enhancement:** Enhancement of Jobvite-Workato's custom connector with a comprehensive analysis of Jobvite APIs and authentication methods.

4. **Entity Mapping Across Platforms:** Mapping of entities with attributes between Jobvite and all the targeted platforms that are currently integrated using MuleSoft 3.0 and MuleSoft 4.0.
5. **Understanding and Identification of Reusable Components in Workato Ecosystem:** In-depth exploration of the existing Workato ecosystem to identify reusable components for efficient integration.
6. **UKG Pro (HRIS and Onboarding) Integration:** Analysis of UKG Pro's pre-built connector and authentication methods in collaboration with Workato for seamless integration.
7. **eScreen & ADP Integration:** Examination of authentication methods and necessary APIs for syncing eScreen and ADP with Jobvite.
8. **Replicating the existing Error and Exception Handling Strategy in MuleSoft:** Replicating the existing strategy for error and exception handling within the MuleSoft framework into Workato.
9. **Workato Recipe Development:** To establish end-to-end workflows for seamless data integration with Workato best practices.
10. **Environment Management in Workato:** Management of Dev/Test/Prod environments and recipes within the Workato platform for streamlined integration processes.

Solution Approach

The following high-level integration of Jobvite with proposed systems.



The solution includes:

Jobvite- Workday	• Candidates' data sync from Jobvite to Workday based on condition **Trigger** Trigger new/updated record in Jobvite. **Actions** • Get Applicants • Put Applicant • Hire Employee • Change Job • Contract Contingent Worker • End Contingent Worker Contract • Rescind • Cancel
Jobvite – Export/Import	• The new Hire flat will be exported and shared over the server or email. • Flat files will be received from SFTP and imported into Jobvite. (Requisition, Location, custom field, Documents, Departments)
Jobvite – eScreen	• Candidates' data sync from Jobvite to eScreen based certain conditions
UKG Pro Onboarding	Triggers: • Trigger Candidate Placement in "Initiate UKG Pro Onboarding" in ATS. Actions: • Retrieve candidate and requisition data from Jobvite. • Integrate data with UKG Pro Onboarding. • Move candidate based on success/failure to "UKG Pro Onboarding Success" or " UKG Pro Onboarding Error" steps. • Update Integration Details with timestamp or error message. • A separate nightly process will run to update dropdown custom field values in Jobvite with values from UKG
UKG Pro Core	Triggers • Trigger on completion of "Ready for UltiPro Integration" task in Jobvite Onboard. Actions: • Retrieve Onboard, Candidate, and Requisition information from Jobvite. • Transform and send data to UltiPro through API. • Update Candidate Integration Status and Integration Detail fields based on UltiPro response (Success/Error). • Mark the "Ready for UltiPro Integration" task as retrieved. •
Jobvite to ADP	Triggers • Trigger on Candidate Placement in the "ADP WFN" workflow state. Actions: • Retrieve candidate and requisition details from Jobvite ATS.

	• Format the data for ADP integration. • Update Candidate Integration Status and Integration Details based on success or failure. • Success: Set "ADP WFN Success." • Failure: Set "ADP WFN Error" and store error details in Integration Details (e.g., Missing Email Address). • Upon successful submission, update the Integration Details field with the timestamp of when the record was received by ADP.

Solution Details

Harbinger Team will implement a Workato based solution covering following important aspects:

1. Adding custom actions in pre-built Jobvite custom connector
2. Retrieve data from the Jobvite with retrieval strategy supporting batches and sync into all the targeted platforms mentioned above that presently have Mulesoft integrations with Jobvite.
    - Considered basic details of employee such as WID, Name, Role, Employee_ID, DOB, Address_Primary, Email, Phone_Primary.
    - Retrieve and export new hire data from Jobvite to flat file. The new hire data is exported to a flat file. This file will be shared over server or email.
3. Retrieve and import:
    - Requisition in Jobvite
    - Location in Jobvite
    - Custom field in Jobvite
    - Department in Jobvite
4. Document in Jobvite Retrieve and map the candidate data from Jobvite and Onboarding platforms.
5. Retrieve data from the Jobvite with retrieval strategy and sync it into UKG Pro (HRIS) and UKG Pro (Onboarding)

For the above solution approach following are the key considerations:

1. The solution will leverage the default Workato connectors available for UKG Pro.
2. Flat file conversion will leverage Workato capabilities like Parse JSON, batched actions, Workato files, parallel recipe functions for optimized handling large volume of data.
3. Workato logging will enable traceability of the data processing.
4. Deployment of recipe in Production environment will be carried out manually using Recipe life cycle management feature.
5. Detailed mapping of entities along with data transformation and configuration needs will be performed at the start of the project with the help of the Employ’s team.

Assumptions

1. All pre-requisites mentioned in Pre-requisites below. (Workato access, Mulesoft access, documentation of use cases, existing test cases, etc.) needed to start implementation should be provided at the start of the project.
2. The availability of an expert(s) from Employ team to discuss/review workflows, data variations, and use cases.
3. Functional testing will be done manually on Stage/Prod environments via Recipe Life Cycle Management export/import package feature. Adequate testing environments exist for validation of migrated integrations.
4. Exact entities/objects to be used for integration will be identified after a detailed analysis of the sandbox environment at the start of the project.
5. Estimates may vary after the detailed analysis that will be carried out at the start of the project.
6. Necessary tools and resources for migration should be readily accessible.
7. The scope includes the integration of the platforms listed in the Solution Overview table. Any additional 3rd party integration will be estimated separately.

Pre-requisites

Following prerequisites should be fulfilled by the Employ team before the implementation starts:

1. APIs and APIs keys required for the integration use cases should be provided by Employ to Harbinger
2. Access to Workato instance, sandbox portal, and API access of systems involved, will be provided at the start of the project by Employ to Harbinger.

Any delay in providing these prerequisites may result in delayed timelines. Newer customization requirements identified during implementation may be subject to an additional increase in the timelines and effort estimates provide.

Deliverables

The following deliverables will be available as a part of this project:

1. The functionally complete solution as per scope elaborated in appropriate phases.
2. Custom-developed source code
3. Technical documentation
4. Existing Jobvite custom connector enhancements

Quality Assurance

Overall Functional Testing - Harbinger would ensure that the system conforms to the specified requirements and functionality, as per requirement documents and screen mockups. It involves Feature and / UI validations with both positive and negative tests.

Acceptance Criteria

1. The team will add any new recipe and/or triggers to the UAT and Production environment.
2. The application is expected to meet a certain response time.
3. All vulnerabilities must be remediated by the partner and rescanned before the project's end date.
4. Harbinger will be responsible for fixing all the issues coming up during the acceptance period. However, change requests may need to be estimated separately and fixed.

The acceptance testing will be done on a frequent basis at the end of every/selected sprint. The detailed sprint plan including continuous acceptance will be created at the start of the project and updated as needed.

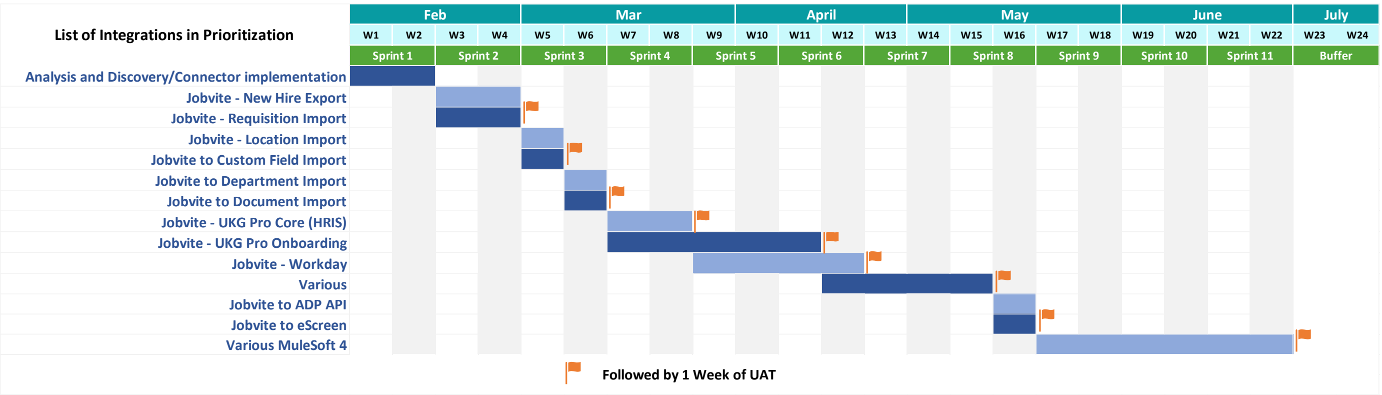
HIGH-LEVEL PROJECT PLAN

To ensure the delivery of the project for both MuleSoft 3.0 and MuleSoft 4.0 within 5 calendar months, Harbinger proposes following four milestones project plan span across 11 sprints, each sprint of two weeks. A review meeting with the Employ team will follow each sprint. Received changes and feedback will be addressed in the next sprint.

The following Cohort chart outlines a comprehensive implementation schedule for each integration. The initial two weeks will be dedicated to analysis and the implementation of custom connectors. Each integration will be followed by 1 week of UAT.

The sequencing of integrations is strategically planned, beginning with simpler levels of integration, and progressing towards more complex levels of integration. This approach facilitates a systematic understanding and familiarization with the system. Additionally, parallel execution of integrations at similar levels of complexity and use cases will be undertaken.

The following project plan was provided at the proposal stage and shall be used as a reference. A final project plan will be shared at the start of the project.



APPENDIX B

VENDOR GDPR DATA PROCESSING ADDENDUM AND STANDARD CONTRACTUAL CLAUSES

This Data Processing Addendum and Standard Contractual Clauses ("DPA") supplements the master subscription agreement or terms of service agreement (the "Agreement") between [VENDOR] ("Vendor" or "Data Importer") and Employ, Inc. ("Employ" or "Data Exporter") when the GDPR applies to Employ's use of Vendor's Services to Process Employ Data. Except as amended by this DPA, the Agreement will remain in full force and effect.

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Agreement. **Nothing in this Addendum is intended to alter or have any adverse effect on the Standard Contractual Clauses incorporated into this Addendum in Exhibit A ("Standard Contractual Clauses"). In the event that a competent government authority determines that a conflict exists between the Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail.** If there is a conflict between any other agreement between the Parties including the Agreement and this DPA, the terms of this DPA will control.

1. **Definitions.** Unless otherwise defined in the Agreement, all capitalized terms used in this DPA will have the meanings given to them below.

1.1. "Agreement" means any agreement between Vendor and a specific customer under which Services are provided by Vendor to that customer. Such an agreement may have various titles, including but not limited to "Order Form," "Sales Order," or "Master Subscription Agreement."

1.2. "Employ" means the entity which determines the purposes and means of Processing of Employ Data. Employ may also be referred to as Data Exporter.

1.3. "Employ Data" means any "personal data" (as defined in GDPR) that is provided by or on behalf of Employ and Processed by Vendor pursuant to the Agreement.

1.4. "Data Protection Laws" means all laws and regulations, including laws and binding regulations of the European Union, the European Economic Area ("EEA") and their member states, Switzerland and the United Kingdom, and any amending or replacement legislation from time to time, applicable to the Processing of Employ Data under the Agreement.

1.5. "GDPR" means the General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the Processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC.

1.6. "Permitted Purpose" means the use of the Employ Data to the extent necessary for provision of the Services by Vendor to the Employ.

1.7. "Security Incident" means any unauthorized or unlawful access to, or acquisition, alteration, use, disclosure, or destruction of Employ Data.

1.8. "Services" means the Vendor services ordered by the Employ from Vendor.

1.9. “Standard Contractual Clauses” means the agreement, attached at Annex 2, pursuant to the European Commission decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to processors established in third countries.

1.10. “Sub-processor” means any entity engaged by Vendor to Process Employ Data in connection with the Services.

1.11. “Supervisory Authority” means an independent public authority which is established by an EU Member State pursuant to the GDPR.

1.12. Terms such as “Data Subject,” “Processing,” “Controller,” and “Processor” shall have the meaning ascribed to them in the GDPR.

1.13. “Third-Party Services” means connections and/or links to third party websites and/or services not included in the core Services offerings identified in the Agreement, including, without limitation, via application programming interfaces.

2. **Data Processing.**

2.1. *Data Processing Activities.*

2.1.1. Subject Matter. Vendor’s provision of the Services to the Employ.

2.1.2. Nature and Purpose. Vendor will process Employ Data for the purposes of providing the Services (including administration, operations, technical and Employ support), to Employ in accordance with the Agreement.

2.2. *Roles of the Parties.* The Parties acknowledge and agree that Vendor will Process the Employ Data in the capacity of a Processor and that Employ will be the Controller of the Employ Data. Employ understands that to the extent Third-Party Services are accessed, Employ serves as the Controller and the Third-Party Services are Processors, and the Third-Party Services are not Sub-processors of Vendor.

2.3. *Employ Instructions.* The Parties agree this DPA and the Agreement constitute Employ’s documented instructions regarding Vendor’s processing of Employ Data. Vendor will process Employ Data only in accordance with these documented instructions.

2.4. *Compliance with Laws.* Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this DPA, including the GDPR, UK GDPR, and Swiss Privacy Laws. Vendor is not responsible for determining the requirements of laws applicable to Employ’s business or that Vendor’s provision of the Services meet the requirements of such laws.

3. **Employ Obligations.**

3.1. *Instructions*. Employ shall provide instructions to Vendor pursuant to this DPA comply with the Data Protection Laws.

3.2. *Data Subject and Supervisory Authority Requests*. The Employ shall be responsible for communications and leading any efforts to comply with all requests made by Data Subjects under the Data Protection Laws, and all communications from Supervisory Authorities that relate to Employ Data, in accordance with Data Protection Laws. To the extent such requests or communications require Vendor’s assistance, the Employ shall notify Vendor of the Data Subject or Supervisory Authority request.

3.3. *Notice, Consent and Other Authorizations*. Employ is responsible for providing the necessary notice to the Data Subjects under the Data Protection Laws. Employ is responsible for obtaining, and demonstrating evidence that it has obtained, all necessary consents, authorizations and required permissions under the Data Protection Laws in a valid manner for Vendor to perform the Services.

4. **Vendor’s Obligations.**

4.1. *Scope of Processing.* Vendor will Process Employ Data on documented instructions from the Employ, and in such manner as is necessary for the provision of Services except as required to comply with a legal obligation to which Vendor is subject. If Vendor believes any documented instruction or additional processing instruction from Employ violates the GDPR or other Data Protection Laws, Vendor will inform Employ without undue delay and may suspend the performance of the Services until Employ has modified or confirmed the lawfulness of the additional processing instruction in writing. Employ acknowledges and agrees that Vendor is not responsible for performing legal research or for providing legal advice to Employ.

4.2. *Data Subject Requests.* If Vendor receives a request from any Data Subject made under Data Protection relating to Employ Data, Vendor will provide a copy of that request to the Employ within two (2) business days of receipt. Vendor provides Employ with tools to enable Employ to respond to a Data Subjects' requests to exercise their rights under the Data Protection Laws. To the extent Employ is unable to respond to Data Subject's request using these tools, Vendor will provide reasonable assistance to the Employ in responding to the request.

4.3. *Supervisory Authority Requests.* Vendor will assist Employ in addressing any communications and abiding by any advice or orders from the Supervisory Authority relating to the Employ Data.

4.4. *Retention.* Vendor will retain Employ Data only for as long as the Employ deems it necessary for the Permitted Purpose, or as required by applicable laws. At the termination of this DPA, or upon Employ's written request, Vendor will either destroy or return the Employ Data to the Employ, unless legal obligations require storage of the Employ Data.

4.5. *Disclosure to Third Parties and Confidentiality.* Vendor will not disclose the Employ Data to third parties except as permitted by this DPA or the Agreement, unless Vendor is required to disclose the Employ Data by applicable laws, in which case Vendor shall (to the extent permitted by law) notify the Employ in writing and liaise with the Employ before complying with such disclosure request. Vendor treats all Employ Data as strictly confidential and requires all employees, agents, and Sub-processors engaged in Processing the Employ Data to commit themselves to confidentiality, and not Process the Employ Data for any other purposes, except on instructions from Employ.

4.6. *Assistance.* Taking into account the nature of the Processing and the information available, Vendor will provide assistance to Employ in complying with its obligations under GDPR Articles 32-36 (inclusive) (which address obligations with regard to security, breach notifications, data protection impact assessments, and prior consultation). Upon request, Vendor will provide Employ a list of processing operations.

4.7. *Security.* Vendor will keep Employ Data confidential and implement and maintain administrative, physical, technical and organizational safeguards for the security (including protection against accidental or unlawful loss, destruction, alteration, damage, unauthorized disclosure of, or access to, Employ Data transmitted, stored or otherwise Processed), confidentiality and integrity of Employ Data as detailed in Appendix 2 to Annex 1.

5. **Sub-Processors.**

5.1. *SCC's.* Pursuant to Clause 9 of the Standard Contractual Clauses, Employ acknowledges and expressly agrees Vendor may engage new Sub-processors as described in Section 5 of this DPA. All references within the SCCs shall be automatically updated as necessary to comply with UK GDPR and Swiss Privacy requirements.

5.2. *General Consent.* Employ agrees that Vendor may engage third-party Sub-processors in connection with the provision of Services, subject to compliance with the requirements below. As a condition to permitting a Sub-processor to Process Employ Data, Vendor will enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Employ Data as those in this DPA, to the extent applicable to the nature of the Services provided by such Sub-processor. Vendor will provide copies of any Sub-processor agreements to Employ pursuant only upon reasonable request by Employ. To the extent necessary to protect business secrets or other confidential information, including personal data, Vendor may redact the text of the agreement prior to sharing a copy.

5.3. *Current Sub-processor List.* Employ acknowledges and agrees that Vendor may engage its current Sub-processors identified in Annex II to Exhibit A.

5.4. *Written Notice Via Mailing List.* Vendor will provide Employ with notice ("New Sub-processor Notice") of the addition of any new Sub-processor to the Sub- processor List at any time during the term of the Agreement. Vendor will provide Employ with additional information about any Sub-processor on the Sub-processor List that Employ may reasonably request upon receipt of a New Sub-processor Notice

5.5. *Employ Objection.* If Employ has a reasonable basis to object to Vendor's use of a new Sub-processor, Employ will notify Vendor promptly in writing within 15 days after receipt of a New Sub-processor Notice. Vendor will use reasonable efforts to make available to Employ a change in the affected Services or recommend a commercially reasonable change to Employ's configuration or use of the affected Services to avoid processing of Personal

Data by the objected-to new Sub-processor without unreasonably burdening Employ. If Vendor is unable to make available such change within a reasonable period of time, which will not exceed 30 days, Employ may terminate the portion of any Agreement relating to the Services that cannot be reasonably provided without the objected-to new Sub-processor by providing written notice to Vendor.

5.6. *Responsibility*. Vendor will remain responsible for its compliance with the obligations of this DPA and for any acts and omissions of its Sub-processors that cause Vendor to breach any of Vendor's obligations under this DPA.

6. **Security Incident Notification.** Vendor shall, to the extent permitted by law, notify Employ without undue delay, but no later than 48 hours after becoming aware of any Security Incident. Vendor's notification of a Security Incident to the Employ to the extent known should include: (a) the nature of the incident; (b) the date and time upon which the incident took place and was discovered; (c) the number of data subjects affected by the incident; (d) the categories of Employ Data involved; (e) the measures, such as encryption, or other technical or organizational measures, that were taken to address the incident, including measures to mitigate the possible adverse effects; (f) whether such proposed measures would result in a disproportionate effort given the nature of the incident; (g) the name and contact details of the data protection officer or other contact; and (h) a description of the likely consequences of the incident. The Employ alone may notify any public authority.

7. **Transfers Outside of the EEA.** The Parties agree the Standard Contractual Clauses, as identified in Annex 2, will apply to Employ Data that is transferred outside the EEA, either directly or via onward transfer, to any country not recognized by the European Commission as providing as adequate level of protection for personal data (as described by the GDPR.

8. **Third Party Certifications and Audits.**

8.1. ***Report****.* In addition to the information contained in this DPA, upon Employ's request, and subject to the confidentiality obligations set forth in the Agreement, Vendor will make available reports or other documentation describing the controls implemented by Vendor. so that Employ can reasonably verify Vendor's compliance with its obligations under this DPA. The CIS Control standards (Centre for Internet Security Critical Security Controls) offer **a standardized and prioritized approach** to fortifying organization's defenses against cyberattacks.),

8.2. *Audits.* To the extent the reports provided in Clause 8 of the Standard Contractual Clauses, Employ may audit Vendor's compliance with this DPA up to once per year with the thirty (30) days prior written notice, unless requested by a Supervisory Authority or in the event of a Security Incident. Such audit will be conducted by an independent third party ("Auditor") reasonably acceptable to Vendor and the cost of such Audit shall be borne by Employ. Vendor will work cooperatively with Employ and Auditor to agree on a final audit plan in advance of the audit. The results of the inspection and all information reviewed during such inspection will be deemed Vendor's confidential information and shall be protected by Auditor in accordance with the confidentiality provisions to be made between Vendor and Auditor. Notwithstanding any other terms, the Auditor may only disclose to the Employ specific violations of the Addendum, if any, and the basis for such findings, and shall not disclose to Employ any of the records or information reviewed during the inspection.

9. **Liability.** To the extent permitted by applicable laws, liability arising from claims under this DPA will be subject to the terms of the Agreement.

10. **Miscellaneous.**

10.1. ***Obligations Post-termination.*** Termination or expiration of this DPA shall not discharge the Parties from their obligations

10.2. ***Severability.*** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invaliding the remaining provisions hereof, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. The Parties will attempt to agree upon a valid and enforceable provision that is a reasonable substitute and shall incorporate such substitute provision into this DPA.

Accepted and agreed to as of the Effective Date by the authorized representative of each party:

Harbinger, Inc. (“Vendor”)

By: _________________________________

Name: ______________________________

Title: _______________________________

Date: _______________________________

Employ, Inc.

By: _________________________________

Name: ______________________________

Title: _______________________________

Date: _______________________________

Exhibit A:

STANDARD CONTRACTUAL CLAUSES (CONTROLLER TO PROCESSOR)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (1) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter ‘personal data breach’). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (8) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer’s responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). For Module Three: The data exporter shall forward the notification to the controller.

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. The data exporter shall make the assessment available to the controller.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f)

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority and the controller of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland (specify Member State).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): Employ, Inc.

Address: 1125 Mission Street, San Francisco, CA 94103

Contact Person: David Hollady, DPO, privacy@Employ.co

Signature and Date:

Role: Controller

Data importer(s):

Name: Harbinger Systems Private Limited

Address: 202 Unit 2, 2nd floor, 45/1 to 10/1, Global Port, Mumbai-Bangalore Bypass, Baner, Pune -411045 INDIA

Contact Person: Ashish Chakraborty

Signature and Date:

Role: Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Categories of personal data transferred:

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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Ongoing during the provision of Services to Customer.

Nature of the processing

Purpose(s) of the data transfer and further processing

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Irish Data Protection Commission

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Vendor will process employ data in accordance with the following minimum security criteria:

Data Segregation. Vendor shall logically separate, secure, and monitor production environments.

Credential Hashing. Vendor must have appropriate algorithms in place for hashing secrets, including passwords and API tokens, both for Vendor's accounts and for Customer accounts to access Vendor's system.

Encryption.

Data in Transit. Vendor must ensure that HTTPS is enabled in any web interface related to the product or service. Vendor must disable non-encrypted transmission services (e.g., FTP). Vendor must have commercial certificates to provide Customer the option to utilize TLS 1.2 or greater for web facing applications.

Data at Rest. Employ Data both at rest and in-transit must be encrypted at all times using industry accepted cryptography standards. Vendor must have key management in place for high sensitivity data (e.g., key rotation, key encryption, access control, etc.). Where different algorithms are used, they are to have comparable strengths e.g., if an AES-128 key is to be encrypted, an AES-128 key or greater, or RSA-3072 or greater could be used to encrypt it.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorized the use of the following subprocessors: n/a

Appendix C

Security Exhibit

This Security Exhibit ("Security Exhibit") will become part of the executed agreement between Harbinger and Employ that references this document. Harbinger's performance of the services must be in accordance with the Agreement and this Security Exhibit. Terms used here but not defined here are defined in the Agreement.

Purpose:

Harbinger will make commercially reasonable efforts to prevent loss, theft, or damage to Employ Data from the Services. This Exhibit establishes the requirements necessary to maintain a security program and ensure that sufficient physical, operational, and technical security measures are in place for the protection of Employ Data in the Services. This Security Exhibit applies when Harbinger provides the Services and Support to Employ.

1. Information Security Management

1.1 Information Security Management System. Harbinger shall maintain and continually make improvements to a documented information security management system in accordance with industry standard practices and accepted frameworks for the delivery of Harbinger Services and Support which its personnel are to be made aware of and comply with ("Information Security Management System").

1.2 Certification. During the term of the Agreement, Harbinger shall maintain CIS Control standards (Centre for Internet Security Critical Security Controls) certification or equivalent as well as maintain a lawful transfer mechanism for export of personal data out of the European Union.

1.3 Testing. Harbinger will conduct at least annual third-party security tests on applications and infrastructure used to support the provision of Services and Support to identify security vulnerabilities. Harbinger will provide summary reports of security test reports to Employ upon request.

2. Organizational Security

2.1 Information Security Responsibilities. Harbinger must have dedicated roles with clearly defined responsibilities for the administration of the Information Security Management System.

2.2 Security Policies. As part of administration of the Information Security Management System, Harbinger will create information security policies that will define responsibility for the protection of Harbinger and Employ Data ("Information Security Policies"). The Information Security Policies will include requirements to designed to monitor for compliance with privacy/information security policies and procedures.

3. Asset Classification

3.1 Asset Management. Harbinger will maintain an asset management policy in accordance with industry standard practices, including asset classification (e.g. information, software, hardware) and an inventory of devices and systems that administer the Services and Support to enable Harbinger to protect Employ Data and assets.

3.2 Asset Controls. Harbinger will establish physical, organizational, and technical security controls to protect Employ Data from unauthorized access and disclosure.

4. People Security

4.1 Harbinger Employees. Harbinger Employees must behave consistently with this Security Exhibit to ensure effective security. Harbinger will make its Employees aware of their responsibilities for maintaining effective security controls, particularly regarding the use of passwords, disposal of information, social engineering attacks, incident reporting, and the physical and technical security of users and company equipment through security awareness/onboarding trainings. Harbinger will issue documented security policies, update them as necessary, and provide security training.

4.2 Background Checks. Harbinger must ensure that its Employees involved in providing the Services and Support have passed basic background checks designed to validate the completeness and accuracy of resumes, confirmation of professional qualifications, and verification of identity where permitted by law these checks may also include checks of criminal history.

5. **Physical and Environmental Security**

5.1 Physical Access. Where Harbinger maintains a physical office location, Harbinger shall ensure that only authorized users have physical access to the network, critical systems and applications, server rooms, communication rooms and work environments it is required that and that Harbinger shall provide secure protection for its physical facilities (e.g. through card readers, key cards or a manned reception area) from which Harbinger provides the Services and Support. Harbinger will maintain controls to monitor for attempts at unauthorized access. Additional controls will be maintained to prevent or detect the removal of any such equipment.

5.2 Data Transfer. Harbinger will not permit Employ Data to be transferred to any external or removable storage media.

6. **Communications and Operations Management**

6.1 Vulnerability/Patch Management. Harbinger will establish a vulnerability/patch management process that ensures all systems used to provide the Services and Support services, including network devices, servers, and desktop/laptop computers, are patched against known security vulnerabilities in a reasonable period of time based on the criticality of the patch and sensitivity of the Employ Data accessed through the systems or subject to industry standard compensating controls.

6.2 Secure System Configuration. Harbinger will establish controls to ensure that all systems used to provide Services and Support are securely configured in a repeatable manner. This involves changes to default settings to improve system security (e.g., system “hardening”), changes to default account passwords and removal of unnecessary software or services/daemons. Additionally, employee devices used to interact or manage systems that provide the Services and Support are to also be configured in a repeatable manner. Specific additional requirements beyond what also exists in this Exhibit include:

6.2.1 Full/whole disk encryption; and

6.2.2 Remote data wipe and lock capability in case of lost/stolen device

6.3 Malware Prevention. Harbinger will implement detection and prevention controls to protect against malicious software and appropriate user awareness procedures. Harbinger will keep and update technical controls and must regularly evaluate all systems for the existence of malware. Harbinger will run real-time or regular scans of Harbinger’s owned devices to detect viruses, malware, and possible security incidents.

6.4 Logging and Auditing. Harbinger will have in place a comprehensive log management program defining the scope, generation, transmission, storage, analysis and disposal of logs based on then current industry practices. The systems and the services will provide logging capabilities in accordance with the following principles:

6.4.1 the scope of logging and the retention policy will be based on a risk-based approach, with minimum retention of six (6) months;

6.4.2 logs will be collected to permit forensic analysis on information security incidents;

6.4.3 logs will record administrative changes to the Services;

6.4.4 log records will be kept physically and virtually secured to prevent tampering;

6.4.5 logs will contain only industry standard elements, and will exclude sensitive data elements;

6.4.6 will perform regular log analysis to evaluate security;

6.4.7 configuring all affected systems to provide real-time logging of any event that may indicate a system compromise, denial-of-service event, or other security violation, including notifying an administrator when pre-determined event thresholds are exceeded; and

6.4.8 protect logs from unauthorized access or modification.

7. Disaster Recovery and Business Continuity Planning

7.1 Programs. Harbinger must establish disaster recovery and business continuity programs, and must ensure that the plans are capable of ensuring confidentiality and integrity of Employ Data during recovery operations. Harbinger will ensure the programs do not allow any reduction of security.

7.2 Backups. Harbinger must ensure the availability of Employ Data stored or processed by Harbinger that is stored locally through the use of backups.

8. Security Incidents

8.1 Incident Detection. Harbinger must establish and maintain an operational incident detection capability and a clearly documented incident response program for responding to suspected or known security incidents or system breaches. Incident response plans must include methods to protect evidence of activity from modification or tampering, and to properly allow for the establishment of a chain of custody for evidence.

8.2 Incident Response. In the event of an incident that affects Employ Data, Harbinger will utilize industry standard efforts to respond to the incident and mitigate the risk to Employ and Employ Data.

8.3 Incident Notification. In the event of an incident that affects Employ Data, Harbinger will provide notice of the security incident to Employ within forty-eight (48) hours of detection.

9.Access Control

9.1 Authentication. Harbinger must support Single sign on (SSO) mechanisms for Employ to interact with Harbinger assets (e.g., SAML 2.0 compliant).

9.2 Corporate Authentication. Harbinger must have centralized authentication management mechanisms. Harbinger must use multiple authentication factors where available, and Harbinger will use at least two-factor authentication to access accounts used to provide data hosting services. All administrative access by Harbinger Employees must require two-factor authentication.

9.3 Administrative Access. Harbinger must use multiple factors of authentication for all Harbinger administrative access.

9.4 Brute-force Protection. Harbinger must implement controls to limit the capability of attackers to brute-force authentication endpoints.

9.5 RESERVED.

9.6 User Passwords. Harbinger will provide training to Employees reasonably designed to ensure Employees have sufficient complexity and expiration requirements or require an additional layer of security with multi- factor authentication.

9.6.1 Inactivity. All Harbinger devices must be locked after a reasonable period of inactivity.

9.6.2 Employee or Consultant Termination. At the time of the termination of an Employee, contractor, or any third-party consultant, the terminated person’s access to the networks, systems, and accounts used to provide the Services and Support, and access to any Employ Data, must be terminated.

9.6.3 Authorization. Harbinger alone will control and provide access to Employ Data. Harbinger will not use a third party to control access to Employ Data. Access will be granted only on a need-to-know basis and following the principles of least privilege.

9.6.4 Network Access Controls. All networks Harbinger uses to provide the Services and Support must be protected through the use of controls capable of blocking unauthorized network traffic, both inbound (ingress) and outbound (egress). Harbinger will maintain capabilities to monitor network traffic.

10. **Data Security**

10.1 Data Segregation. Harbinger logically separate, secure, and monitor production environments.

10.2 Credential Hashing. Harbinger must have appropriate algorithms in place for hashing secrets, including passwords and API tokens, both for Harbinger's accounts and for Employ accounts to access Harbinger's system.

10.3 Encryption.

10.3.1 Data in Transit. Harbinger must ensure that HTTPS is enabled in any web interface related to the product or service. Harbinger must disable non-encrypted transmission services (e.g., Telnet). Harbinger must have commercial certificates to provide Employ the option to utilize TLS 1.2 or greater for web facing applications.

10.3.2 Data at Rest. Employ Data both at rest and in-transit must be encrypted at all times using industry accepted cryptography standards. Harbinger must have key management in place for high sensitivity data (e.g. key rotation, key encryption, access control, etc.). At a minimum, this includes:

10.3.2.1 Use Advanced Encryption Standard (AES) defined in FIPS 197.

10.3.2.2 Where different algorithms are used, they are to have comparable strengths.

11. *Privacy*.

11.1 Harbinger represents and warrants that:

11.1.1 as of the date of this contract, it has not received any directive under Section 702 of the U.S. Foreign Intelligence Surveillance Act, codified at 50 U.S.C.§ 1881a ("FISA Section 702").

11.1.2 no court has found Vendor to be the type of entity eligible to receive process issued under FISA Section702: (i) an "electronic communication service provider" within the meaning of 50 U.S.C § 1881(b)(4) or (ii) a member of any of the categories of entities described within that definition.

11.1.3 it is not the type of provider that is eligible to be subject to Upstream collection ("bulk" collection) pursuant to FISA Section 702, as described in paragraphs 62 & 179 of the judgment in the EU Court of Justice CaseC-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ("Schrems II"), and that therefore the only FISA Section 702 process it could be eligible to receive, if it is an "electronic communication service provider" within the meaning of 50 U.S.C § 1881(b)(4), would be based on a specific "targeted selector" i.e., an identifier that is unique to the targeted endpoint of communications subject to the surveillance.

11.2 Where possible Harbinger will use all reasonably available legal mechanisms to challenge any request under FISA Section 702 for bulk surveillance, i.e., a surveillance demand whereby a targeted account identifier is not identified via a specific "targeted selector" (an identifier that is unique to the targeted endpoint of communications subject to the surveillance). Harbinger will use all reasonably available legal mechanisms to challenge any demands for data access through national security process it receives as well as any non-disclosure provisions attached thereto.

11.3 All Employees are required to comply with Harbinger security and privacy policies and standards. Noncompliance is subject to disciplinary action, up to and including termination of Employment.

11.4 Harbinger regularly reviews our collection, storage, and processing practices to prevent unauthorized access to Harbinger's system.

11.5 Harbinger will promptly notify Employ if Harbinger can no longer comply with the Standard Contractual Clauses or the clauses in this section 11. Harbinger shall not be required to provide Employ with specific information about why it can no longer comply, if providing such information is prohibited by applicable law.