Data Processing Agreement (DPA)
Effective Date: June 1st, 2024
Parties:

- **Data Controller:** Logic Pursuits Inc.
  27475 Ferry Rd, Suite 145, Warrenville, IL 60555
- **Data Processor:** Logic Pursuits Inc.

Introduction

This Data Processing Agreement (DPA) is entered into between the Data Controller and the Data Processor (if applicable) to ensure compliance with applicable data protection laws and regulations. This agreement establishes the rights and obligations of both parties concerning the processing of personal data collected through the Data Controller's static website. The static website collects user information through contact forms and similar means for handling inquiries, providing requested information, and managing communications. Both parties agree to comply with the terms outlined herein to safeguard the privacy and security of personal data.

---

1. Definitions

1.1 **Data Protection Laws**: Refers to applicable laws, including the General Data Protection Regulation (GDPR), [UK Data Protection Act], or any similar regulations governing the collection and processing of personal data.
1.2 **Personal Data**: Any information that identifies or can identify a data subject, as provided by users through the website.
1.3 **Data Controller**: The entity determining the purpose and means of processing personal data.
1.4 **Data Processor**: The entity processing data on behalf of the Data Controller.

---

2. Subject Matter of the Processing

The Data Processor will process personal data submitted by users via the website's contact form, such as:

- Name
- Email address
- Phone number (if collected)
- User queries or messages

---

3. Duration and Nature of Processing

The processing of personal data will begin when the user submits data through the website and will continue until either:

- The data is deleted after fulfilling the user's query
- Upon request by the Data Controller or subject as per retention policies

---

4. Purpose of Processing
Personal data will be processed solely for the purpose of:
- Responding to user inquiries
- Providing requested information or services
- Maintaining a record of correspondence

---

5. Obligations of the Data Controller
5.1 Ensure that personal data collected is limited to what is necessary for the purpose.
5.2 Provide necessary notices to data subjects regarding data collection and their rights.
5.3 Maintain a lawful basis for collecting and processing personal data.

---

6. Obligations of the Data Processor (if any)
6.1 Process personal data only on the documented instructions of the Data Controller.
6.2 Ensure confidentiality of personal data by limiting access to authorized personnel.
6.3 Implement appropriate technical and organizational measures to ensure data security (e.g., encryption, access control).
6.4 Assist the Data Controller in fulfilling data subject requests, including access, rectification, and deletion of personal data.
6.5 Notify the Data Controller without undue delay in the event of a personal data breach.

---

7. Data Transfers
Data will not be transferred outside [your jurisdiction/EEA] without the Data Controller's prior written approval and implementation of appropriate safeguards.

---

8. Sub-processors (if applicable)
The Data Processor is permitted to engage sub-processors to assist with data processing activities under the conditions:
- Sub-processors meet the same data protection obligations
- The Data Controller is notified of any changes or additions

---

9. Data Subject Rights
Both parties agree to assist in providing data subjects with access, rectification, or deletion requests. The Data Controller retains primary responsibility for honoring requests.

---

10. Security Measures
The Data Processor will implement technical and organizational measures to ensure a level of security appropriate to the risk, including:
- Encryption of data (if feasible)
- Access controls
- Data pseudonymization (if necessary)

---

11. Breach Notification
In case of a data breach, the Data Processor shall inform the Data Controller without undue delay, including details of:

- The nature of the breach
- The data affected
- Steps taken to mitigate the risk

---

12. Data Retention and Deletion
Upon termination of the agreement or upon the Data Controller's request, personal data shall be securely deleted unless retention is required by law.

---

13. Liability and Indemnification
The parties agree to allocate responsibility in accordance with applicable data protection laws. Any claims by data subjects will be handled by the Data Controller unless the breach is due to the Data Processor's actions.

---

14. Termination
This DPA shall remain effective for as long as the Data Processor processes personal data on behalf of the Data Controller or until terminated by either party in writing.

---

15. Governing Law and Jurisdiction
This DPA is governed by the laws of state of Delaware, USA. Any disputes arising shall be resolved in the courts of Delaware, USA.

SCHEDULE 1

ANNEX I

A. LIST OF PARTIES

Data Controller/ Data Processor:

Name: ***Logic Pursuits Inc.***

Address: ***27475 Ferry Rd, Suite 145, Warrenville, IL 60555***

Contact person's name, position, and contact details: ***Dheeraj Khandelwal, Data Protection Officer (DPO), dpo@logicpursuits.com***

Activities relevant to the data transferred under these Clauses: Provision of the Services to the Customer in accordance with the Agreement.

Signature and date: Signature and date are set out in the Agreement.

Sub Processor:

The list is as below

#	Name	Description of Services	Location
1	Zoho Corp	HRMS Services	India / US
2	Microsoft	Email , Office apps, cloud storage, and security	US
3	AWS	Cloud Services Provider	US
4	Sterling Risk	Background Verification (for India Employees)	India
5	EmpMonitor	Workforce Management	India
6	Go Insure	Employee Benefits Provider (for India Employees)	India
7	Scrut	Compliance Partner	India / US
8	Hiring Plug	Recruitment Services	India
9	Pylon	Recruitment Services	India
10	IndiHire	Recruitment Services	India

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Customer's authorized users of the Services.

Categories of personal data transferred

- Name
- Email address
- Phone number (if collected)
- User queries or messages

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

No sensitive data collected.

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

Continuous basis

Nature of the processing

The prospective client/recruitee provides data to us. We just store their personal information for the purpose of future interaction.

Purpose(s) of the data transfer and further processing

The purpose of the transfer is to facilitate the performance of the Services more fully described in the Agreement and accompanying order forms.

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

The period for which the Customer Personal Data will be retained is more fully described in the Agreement, Addendum, and accompanying order forms.

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

The subject matter, nature, and duration of the Processing more fully described in the Agreement, Addendum, and accompanying order forms.

C.COMPETENT SUPERVISORY AUTHORITY

Data exporter is established in an EEA country.
The competent supervisory authority is ***as determined by application of Clause 13 of the EU SCCs.***

ANNEX II

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

Description of the technical and organisational security measures implemented by Logic Pursuits Inc. as the data processor/data controller to ensure an appropriate level of security, taking into account the nature, scope, context, and purpose of the processing, and the risks for the rights and freedoms of natural persons.

- Security

- Security Management System.
  - Organization. Logic Pursuits Inc. designates qualified security personnel whose responsibilities include development, implementation, and ongoing maintenance of the Information Security Program.
  - Policies. Management reviews and supports all security related policies to ensure the security, availability, integrity and confidentiality of Customer Personal Data. These policies are updated at least once annually.
  - Assessments. Logic Pursuits Inc. engages a reputable independent third-party to perform risk assessments of all systems containing Customer Personal Data at least once annually.
  - Risk Treatment. Logic Pursuits Inc. maintains a formal and effective risk treatment program that includes penetration testing, vulnerability management and patch management to identify and protect against potential threats to the security, integrity or confidentiality of Customer Personal Data.
  - Vendor Management. Logic Pursuits Inc. maintains an effective vendor management program
  - Incident Management. Logic Pursuits Inc. reviews security incidents regularly, including effective determination of root cause and corrective action.
  - Standards. Logic Pursuits Inc. operates an information security management system that complies with the requirements of ISO/IEC 27001:2022 standard.
- Personnel Security.
  - Logic Pursuits Inc.'s personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Logic Pursuits Inc. conducts reasonably appropriate background checks on any employees who will have access to client data under this Agreement, including in relation to employment history and criminal records, to the extent legally permissible and in accordance with applicable local labor law, customary practice and statutory regulations.
  - Personnel are required to execute a confidentiality agreement in writing at the time of hire and to protect Customer Personal Data at all times. Personnel must acknowledge receipt of, and compliance with, Logic Pursuits Inc.'s confidentiality, privacy and security policies. Personnel are provided with privacy and security training on how to implement and comply with the Information Security Program. Personnel handling Customer Personal Data are required to complete additional requirements appropriate to their role (e.g., certifications). Logic Pursuits Inc.'s personnel will not process Customer Personal Data without authorization.

- Access Controls
  - **Access Management**. Logic Pursuits Inc. maintains a formal access management process for the request, review, approval and provisioning of all personnel with access to Customer Personal Data to limit access to Customer Personal Data and systems storing, accessing or transmitting Customer Personal Data to properly authorized persons having a need for such access. Access reviews are conducted periodically to ensure that only those personnel with access to Customer Personal Data still require it.
  - **Infrastructure Security Personnel**. Logic Pursuits Inc. has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. Logic Pursuits Inc.'s infrastructure security personnel are responsible for the ongoing monitoring of Logic Pursuits' security infrastructure, the review of the Services, and for responding to security incidents.
  - **Access Control and Privilege Management**. Logic Pursuits' and Customer's administrators and end users must authenticate themselves via a Multi-Factor authentication system or via a single sign on system in order to use the Services
  - **Internal Data Access Processes and Policies – Access Policy**. Logic Pursuits Inc.'s internal data access processes and policies are designed to protect against unauthorized access, use, disclosure, alteration or destruction of Customer Personal Data. Logic Pursuits Inc. designs its systems to only allow authorized persons to access data they are authorized to access based on principles of "least privileged" and "need to know", and to prevent others who should not have access from obtaining access. Logic Pursuits Inc.requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; a need to know basis; and must be in accordance with Logic Pursuits Inc.'s internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies follow industry standard practices. These standards include password complexity, password expiry, password lockout, restrictions on password reuse and re-prompt for password after a period of inactivity