DATA PROCESSING AGREEMENT

Between:

TECHNOVA AI SYSTEMS INC.
Registered Office: Alexanderplatz 15, 10178 Berlin, Germany
Company Registration Number: HRB 245871 B
("Provider" or "Processor")

And:

[CLIENT NAME]
Registered Office: [CLIENT ADDRESS]
Company Registration Number: [CLIENT REGISTRATION]
("Client" or "Controller")

Effective Date: [CONTRACT DATE]

This Data Processing Agreement ("DPA") is entered into pursuant to the Master Services Agreement dated [DATE] ("MSA") between Provider and Client for the provision of the InsightPredict Analytics Platform.

RECITALS

WHEREAS, Client engages Provider to provide AI-powered workforce analytics services through the InsightPredict Analytics Platform;

WHEREAS, in the course of providing such services, Provider will process personal data on behalf of Client;

WHEREAS, Regulation (EU) 2016/679 (General Data Protection Regulation, "GDPR") requires that processing of personal data by a processor on behalf of a controller be governed by a contract or other legal act that sets out specific mandatory terms;

WHEREAS, the parties wish to establish their respective rights and obligations regarding the processing of personal data in accordance with applicable data protection laws;

NOW, THEREFORE, in consideration of the mutual promises and covenants contained herein, the parties agree as follows:

==========
1. DEFINITIONS AND INTERPRETATION
==========

1.1 Definitions

In this DPA, unless the context otherwise requires:

"Applicable Data Protection Laws" means all laws and regulations relating to the processing of Personal Data applicable to the parties, including but not limited to:
(a) Regulation (EU) 2016/679 (General Data Protection Regulation);
(b) Regulation (EU) 2024/1689 (AI Act);
(c) Any national implementing legislation; and
(d) Any successor or replacement legislation.

"Client Personal Data" means any Personal Data processed by Provider on behalf of Client in connection with the provision of Services.

"Controller" has the meaning given in Article 4(7) GDPR.

"Data Subject" has the meaning given in Article 4(1) GDPR.

"Personal Data" has the meaning given in Article 4(1) GDPR.

"Personal Data Breach" has the meaning given in Article 4(12) GDPR.

"Processing" has the meaning given in Article 4(2) GDPR, and "Process" shall be construed accordingly.

"Processor" has the meaning given in Article 4(8) GDPR.

"Services" means the InsightPredict Analytics Platform and related services provided by Provider to Client pursuant to the MSA.

"Special Categories of Personal Data" has the meaning given in Article 9(1) GDPR.

"Sub-processor" means any Processor engaged by Provider to Process Client Personal Data.

"Supervisory Authority" has the meaning given in Article 4(21) GDPR.

1.2 Interpretation

References to Articles are to articles of the GDPR unless otherwise specified.
Headings are for convenience only and do not affect interpretation.

==========
2. ROLES AND RELATIONSHIP
==========

2.1 Controller and Processor

The parties acknowledge and agree that:

(a) Client is the Controller of Client Personal Data;
(b) Provider is the Processor of Client Personal Data;
(c) Client determines the purposes and means of Processing Client Personal Data;
(d) Provider Processes Client Personal Data only on behalf of and in accordance with Client's documented instructions.

2.2 Independence

Each party is an independent entity. This DPA does not create a partnership, joint venture, agency, or employment relationship between the parties.

2.3 Compliance with Laws

Each party shall comply with its respective obligations under Applicable Data Protection Laws in relation to the Processing of Client Personal Data.

==========
3. PROCESSING INSTRUCTIONS AND SCOPE
==========

3.1 Processing Instructions

Provider shall Process Client Personal Data only on documented instructions from Client, unless required to Process by applicable law, in which case Provider shall inform Client of such legal requirement before Processing (unless prohibited by law from doing so).

3.2 Initial Instructions

Client's initial instructions for Processing are:

Purpose: Provision of AI-powered workforce analytics services including:
• Candidate screening and recruitment recommendations
• Employee performance analysis and evaluation support
• Workforce planning and optimization
• Skills assessment and training recommendations

3.3 Additional Instructions

Client may issue additional written instructions regarding Processing from time to time, provided such instructions are consistent with the terms of this DPA and the MSA.

3.4 Unlawful Instructions

If Provider believes that any instruction from Client infringes Applicable Data Protection Laws, Provider shall promptly inform Client. Provider may suspend Processing pending resolution of the matter.

3.5 Processing Details

The subject matter, duration, nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects are set out in Annex 1 to this DPA.

==========
4. CLIENT OBLIGATIONS
==========

4.1 Lawfulness of Processing

Client warrants that:

(a) It has all necessary legal bases for the Processing contemplated by this DPA;
(b) It has provided all required notices to Data Subjects;
(c) It has obtained all necessary consents from Data Subjects where required;
(d) The transfer of Client Personal Data to Provider and Provider's Processing in accordance with this DPA will not violate Applicable Data Protection Laws.

4.2 Processing Instructions

Client shall ensure that all Processing instructions issued to Provider comply with Applicable Data Protection Laws.

4.3 Data Quality

Client shall ensure that Client Personal Data is accurate, adequate, relevant, and limited to what is necessary for the purposes of the Processing.

4.4 Data Subject Rights

Client shall be responsible for responding to Data Subject requests to exercise their rights under Applicable Data Protection Laws, with assistance from Provider as set out in Clause 7.

4.5 Impact Assessments

Client acknowledges its responsibility under Article 35 GDPR to conduct Data Protection Impact Assessments where required and shall conduct such assessments prior to deploying the Services.

==========
5. PROVIDER OBLIGATIONS
==========

5.1 Compliance with Instructions

Provider shall Process Client Personal Data only in accordance with Client's documented instructions as set out in this DPA.

5.2 Confidentiality

Provider shall ensure that all persons authorized to Process Client Personal Data:

(a) Are subject to a binding duty of confidentiality (whether contractual or statutory); and
(b) Receive appropriate training on data protection and the requirements of this DPA.

5.3 Security Measures

Provider shall implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk, in accordance with Article 32 GDPR, including as a minimum:

(a) Pseudonymization and encryption of Personal Data where appropriate;
(b) Measures to ensure ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
(c) Measures to restore availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
(d) Regular testing, assessment and evaluation of the effectiveness of technical and organizational measures.

The security measures implemented by Provider are described in Annex 2.

5.4 Sub-processing

(a) Client provides general authorization for Provider to engage Sub-processors, subject to the conditions set out in Clause 6.

(b) Provider shall inform Client of any intended changes concerning the addition or replacement of Sub-processors, giving Client the opportunity to object to such changes within 30 days of notification.

(c) If Client objects to a new Sub-processor on reasonable data protection grounds, the parties shall work together in good faith to find a solution. If no solution can be found within 30 days, either party may terminate the affected Services upon written notice.

(d) Provider shall ensure that Sub-processors are bound by written agreements imposing data protection obligations no less protective than those in this DPA.

(e) Provider remains fully liable to Client for the performance of any Sub-processor's obligations.

5.5 Assistance to Controller

Provider shall, taking into account the nature of the Processing and the information available to Provider, assist Client (at Client's expense) in:

(a) Ensuring compliance with Client's obligations under Articles 32 to 36 GDPR (security, breach notification, impact assessments, prior consultation);

(b) Fulfilling Client's obligation to respond to requests from Data Subjects exercising their rights under Chapter III GDPR, to the extent possible and reasonable.

5.6 Personal Data Breach Notification

(a) Provider shall notify Client without undue delay, and in any event within 48 hours, after becoming aware of a Personal Data Breach affecting Client Personal Data.

(b) Such notification shall, to the extent possible, include:
(i) Description of the nature of the breach;
(ii) Categories and approximate numbers of Data Subjects and Personal Data records affected;
(iii) Contact point for further information;
(iv) Likely consequences of the breach;
(v) Measures taken or proposed to address the breach and mitigate its effects.

(c) Provider shall cooperate with Client and take reasonable steps to remediate the breach and prevent future breaches.

(d) Provider shall not notify any Supervisory Authority or Data Subject of a Personal Data Breach without Client's prior written consent, except where required by law.

5.7 Deletion or Return of Personal Data

Upon termination or expiration of the MSA, Provider shall, at Client's election:

(a) Delete all Client Personal Data and certify in writing that such deletion has been completed; or

(b) Return all Client Personal Data to Client in a commonly used electronic format and delete all copies in Provider's possession or control.

Except: Provider may retain Client Personal Data to the extent required by applicable law, and only for so long as required by such law, subject to ongoing confidentiality obligations.

5.8 Audit Rights

(a) Provider shall make available to Client all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR.

(b) Provider shall allow for and contribute to audits, including inspections, conducted by Client or an auditor mandated by Client, subject to:
(i) Client providing reasonable advance written notice (at least 30 days);
(ii) Audits conducted no more than once per year (unless required by Supervisory Authority or in response to a Personal Data Breach);
(iii) Client executing Provider's standard confidentiality agreement;
(iv) Audits conducted during business hours and in a manner that minimizes disruption to Provider's operations;
(v) Client bearing all costs and expenses of the audit.

(c) Provider may provide audit reports prepared by independent third-party auditors (such as SOC 2 Type II reports) in lieu of Client audits, provided such reports adequately address the matters Client seeks to audit.

==========
6. SUB-PROCESSORS
==========

6.1 Authorized Sub-processors

Provider currently engages the Sub-processors listed in Annex 3 for Processing Client Personal Data.

6.2 Sub-processor Requirements

Provider shall:

(a) Conduct appropriate due diligence on all Sub-processors before engagement;

(b) Enter into written agreements with all Sub-processors imposing data protection obligations substantially equivalent to those in this DPA;

(c) Remain fully liable for the acts and omissions of Sub-processors;

(d) Supervise Sub-processors to ensure compliance with their obligations.

6.3 New Sub-processors

(a) Provider may engage new Sub-processors or replace existing Sub-processors from time to time in accordance with Clause 5.4.

(b) Provider shall maintain an up-to-date list of Sub-processors accessible to Client at [URL or other specified location].

(c) Provider shall notify Client at least 30 days in advance of adding or replacing any Sub-processor.

(d) Client may object to the use of a new Sub-processor on reasonable grounds relating to data protection by notifying Provider in writing within 30 days of receiving notification.

(e) If Client reasonably objects, Provider shall use reasonable efforts to make available to Client a change in the Services or recommend a commercially reasonable alternative that avoids the use of the objected Sub-processor.

==========
7. DATA SUBJECT RIGHTS
==========

7.1 Assistance with Data Subject Requests

Provider shall, to the extent legally permitted and taking into account the nature of the Processing, assist Client in fulfilling Client's obligations to respond to requests from Data Subjects exercising their rights under GDPR, including:

(a) Right of access (Article 15);
(b) Right to rectification (Article 16);
(c) Right to erasure ("right to be forgotten") (Article 17);
(d) Right to restriction of processing (Article 18);
(e) Right to data portability (Article 20);
(f) Right to object (Article 21);
(g) Rights related to automated decision-making and profiling (Article 22).

7.2 Procedures

(a) If Provider receives a request directly from a Data Subject, Provider shall promptly forward the request to Client and shall not respond to the Data Subject without Client's prior written authorization.

(b) Upon Client's request, Provider shall provide reasonable assistance to enable Client to respond to Data Subject requests, including:
(i) Providing information about the Processing;
(ii) Providing access to Client Personal Data;
(iii) Rectifying inaccurate Personal Data;

(iv) Deleting Personal Data;
(v) Restricting Processing;
(vi) Exporting Personal Data in a structured, commonly used, machine-readable format.

(c) Client shall reimburse Provider for reasonable costs incurred in providing assistance beyond Provider's ordinary obligations under this DPA.

7.3 Automated Decision-Making

(a) Client acknowledges that the Services involve automated profiling and decision support for employment-related purposes.

(b) Client is responsible for ensuring compliance with Article 22 GDPR, including:
(i) Obtaining necessary legal basis for automated decision-making;
(ii) Ensuring appropriate human intervention in decisions;
(iii) Informing Data Subjects of automated decision-making;
(iv) Implementing suitable safeguards for Data Subject rights;
(v) Providing meaningful information about the logic involved and the significance and envisaged consequences.

(c) Provider shall, upon request, provide Client with information about the algorithmic processing to enable Client to fulfill its obligations under Article 22, subject to Provider's legitimate interests in protecting proprietary information and trade secrets.

==========
8. INTERNATIONAL DATA TRANSFERS
==========

8.1 Transfer Mechanisms

To the extent that Provider Processes Client Personal Data originating from the European Economic Area (EEA) in countries outside the EEA that have not been subject to an adequacy decision under Article 45 GDPR:

(a) The parties shall implement appropriate safeguards for such transfers in accordance with Chapter V GDPR, which may include:
(i) Standard Contractual Clauses approved by the European Commission;
(ii) Binding Corporate Rules approved by a competent Supervisory Authority;
(iii) Approved certification mechanisms together with binding enforceable commitments;

(iv) Other mechanisms permitted under GDPR.

(b) The Standard Contractual Clauses for controller-to-processor transfers approved by the European Commission (as set out in Annex 4 or as may be amended or replaced from time to time) are hereby incorporated by reference and shall apply to such transfers.

8.2 Data Localization

(a) Provider shall Process Client Personal Data within the European Economic Area unless otherwise agreed in writing.

(b) Current Processing locations are specified in Annex 1.

(c) Provider shall provide at least 90 days' written notice before Processing Client Personal Data in any new location outside the EEA.

8.3 Government Access Requests

(a) In the event Provider receives a legally binding request from a government authority or law enforcement agency to disclose Client Personal Data, Provider shall:
(i) Attempt to redirect the requesting party to request the data directly from Client;
(ii) Promptly notify Client of the request (unless legally prohibited);
(iii) Challenge the request if it appears invalid or overbroad;
(iv) Disclose only the minimum Personal Data necessary to comply with the request.

(b) This clause shall not apply to routine requests for information received in Provider's capacity as employer regarding Provider's own employees.

==========
9. SPECIAL CATEGORIES OF PERSONAL DATA
==========

9.1 Authorization for Special Categories

Client authorizes Provider to Process the following Special Categories of Personal Data (as defined in Article 9(1) GDPR) to the extent such data is included in Client Personal Data:

(a) Biometric data for the purpose of uniquely identifying a natural person (limited to facial recognition and voice pattern analysis where Client has enabled such optional features);

(b) Data concerning health (to the extent incidentally revealed through absence patterns or other workforce data).

9.2 Legal Basis

Client warrants that it has established an appropriate legal basis for the Processing of Special Categories of Personal Data under Article 9(2) GDPR, which may include:

(a) Article 9(2)(b) - Processing necessary for carrying out obligations and exercising specific rights in the field of employment and social security law;

(b) Article 9(2)(f) - Processing necessary for establishment, exercise or defense of legal claims;

(c) Other legal bases as applicable.

9.3 Additional Safeguards

For Processing of Special Categories of Personal Data, Provider shall implement additional safeguards including:

(a) Enhanced access controls limiting access to authorized personnel only;
(b) Additional encryption for Special Categories of Personal Data;
(c) Logging and monitoring of access to Special Categories of Personal Data;
(d) Regular audits of Processing of Special Categories of Personal Data.

9.4 Prohibition on Certain Processing

Unless explicitly authorized by Client in writing, Provider shall not:

(a) Use Special Categories of Personal Data for purposes other than those specified in Annex 1;

(b) Create inferences or derived data regarding Special Categories where not necessary for the specified purposes;

(c) Make such data available to any Sub-processor without Client's prior consent.

==========
10. AI ACT COMPLIANCE
==========

10.1 High-Risk AI System Classification

The parties acknowledge that the InsightPredict Analytics Platform constitutes a high-risk AI system under Article 6(2) and Annex III of Regulation (EU) 2024/1689 (AI Act) as it is intended for use in employment, workers management and access to self-employment.

10.2 Provider Obligations as AI System Provider

Provider represents and warrants that it shall comply with all obligations applicable to providers of high-risk AI systems under the AI Act, including but not limited to:

(a) Article 9 - Establishment and maintenance of a risk management system;
(b) Article 10 - Ensuring training, validation and testing data is of high quality and free from bias;
(c) Article 11 - Preparation and maintenance of technical documentation;
(d) Article 12 - Automatic logging and record-keeping;
(e) Article 13 - Transparency and provision of information to deployers;
(f) Article 14 - Ensuring appropriate human oversight;
(g) Article 15 - Ensuring accuracy, robustness and cybersecurity;
(h) Article 17 - Establishment of a quality management system;
(i) Article 43 - Conformity assessment procedures;
(j) Article 48 - CE marking;
(k) Article 71 - Registration in EU database;
(l) Article 72 - Post-market monitoring;
(m) Article 73 - Reporting of serious incidents.

10.3 Client Obligations as Deployer

Client acknowledges its obligations as a deployer of a high-risk AI system under Article 26 AI Act, including but not limited to:

(a) Taking appropriate technical and organizational measures to ensure use of the AI system in accordance with instructions for use;
(b) Assigning human oversight to competent and adequately trained persons;
(c) Monitoring the operation of the AI system and informing Provider of serious incidents;
(d) Keeping logs generated by the AI system for appropriate period;
(e) Conducting fundamental rights impact assessment where required;

(f) Ensuring transparency to persons subject to the AI system;
(g) Complying with registration obligations where applicable.

10.4 Risk Management and Bias Mitigation

(a) Provider shall operate and continuously update a risk management system addressing risks to health, safety and fundamental rights, with particular attention to:
(i) Risks of discrimination based on protected characteristics;
(ii) Risks to workers' fundamental rights including privacy, dignity and non-discrimination;
(iii) Risks arising from automation bias and over-reliance on algorithmic recommendations.

(b) Provider shall implement measures to detect, prevent and mitigate algorithmic bias, including:
(i) Regular bias testing and audits;
(ii) Monitoring of disaggregated performance metrics;
(iii) Procedures for addressing identified biases;
(iv) Transparency regarding bias testing methodologies and results.

(c) Provider shall inform Client of risk management measures and shall provide Client with information necessary to understand and mitigate risks in deployment.

10.5 Data Governance for AI Training

(a) Provider warrants that training, validation and testing data used for the AI system meets the requirements of Article 10 AI Act, including:
(i) Relevance and representativeness;
(ii) Appropriate to intended purpose;
(iii) Free from errors and complete;
(iv) Subject to data governance practices ensuring data quality;
(v) Examined for possible biases.

(b) Provider shall maintain documentation of data governance practices and shall make such documentation available to Client upon reasonable request.

(c) Client Personal Data used for model training or improvement shall be processed only with Client's explicit consent and in accordance with documented instructions.

10.6 Human Oversight

(a) Provider shall design and develop the AI system with appropriate human oversight measures enabling natural persons to:
(i) Fully understand the AI system's capacities and limitations;
(ii) Remain aware of the possible tendency of automation bias;
(iii) Correctly interpret the AI system's output;
(iv) Decide not to use the AI system or override its output;
(v) Intervene in or interrupt the system's operation.

(b) Provider shall provide Client with instructions and training materials to enable effective human oversight by Client's personnel.

(c) Client shall ensure that natural persons assigned to human oversight are competent, adequately trained and have appropriate authority.

10.7 Transparency to Affected Persons

(a) Client shall ensure transparency to natural persons (employees, candidates) subject to the AI system, including:
(i) Informing individuals that they are subject to an AI system;
(ii) Providing information about the AI system's purpose and functioning;
(iii) Informing individuals of their rights;
(iv) Providing meaningful information about the logic involved and the significance and consequences of the processing.

(b) Provider shall provide Client with template transparency notices and information necessary to enable Client to fulfill transparency obligations.

10.8 Incident Reporting

(a) Client shall promptly inform Provider of any serious incident (as defined in Article 3(49) AI Act) or malfunction of the AI system that occurs during Client's use.

(b) Provider shall report serious incidents to relevant market surveillance authorities in accordance with Article 73 AI Act.

(c) The parties shall cooperate in investigating incidents and implementing corrective measures.

10.9 Post-Market Monitoring

(a) Provider shall establish and document a post-market monitoring system to actively collect and analyze data on the AI system's performance throughout its lifetime.

(b) Client shall cooperate with Provider's post-market monitoring activities, including:
(i) Providing feedback on AI system performance;
(ii) Reporting issues, errors or unexpected behavior;
(iii) Participating in periodic performance reviews;
(iv) Allowing Provider access to system logs for monitoring purposes (subject to data protection safeguards).

10.10 Updates and Modifications

(a) Provider may update or modify the AI system to maintain compliance, improve performance, or address identified issues.

(b) Provider shall notify Client of substantial modifications that may affect compliance or performance.

(c) Client shall implement updates and modifications within reasonable time periods specified by Provider, particularly where updates address safety, security or compliance issues.

==========
11. LIABILITY AND INDEMNIFICATION
==========

11.1 Provider Liability for Data Protection Violations

(a) Provider shall be liable to Client for damages caused by Processing that violates this DPA or Applicable Data Protection Laws, except where Provider proves it is not in any way responsible for the event giving rise to the damage.

(b) This liability is subject to the limitations and exclusions set out in the MSA, except that no limitation shall apply to:
(i) Liability under Article 82 GDPR;
(ii) Liability arising from gross negligence or willful misconduct;
(iii) Liability for fraudulent misrepresentation.

11.2 Client Liability

Client shall be liable for damages caused by Processing that violates Applicable Data Protection Laws where such violation results from Client's instructions, failure to comply with its obligations under this DPA, or other acts or omissions of Client.

11.3 Third-Party Claims

(a) Provider shall indemnify and hold harmless Client from and against any claims, damages, losses, liabilities, costs and expenses (including reasonable attorneys' fees) arising from or related to:
(i) Provider's violation of this DPA or Applicable Data Protection Laws;
(ii) Claims by Data Subjects under Article 82 GDPR resulting from Provider's Processing;
(iii) Regulatory fines or penalties imposed on Client arising from Provider's non-compliance.

(b) Client shall indemnify and hold harmless Provider from and against any claims, damages, losses, liabilities, costs and expenses (including reasonable attorneys' fees) arising from or related to:
(i) Client's instructions that violate Applicable Data Protection Laws;
(ii) Client's failure to comply with its obligations under this DPA;
(iii) Client's failure to fulfill its obligations as Controller or Deployer;
(iv) Claims that Client lacks legal basis for Processing.

(c) The indemnifying party's obligations are conditional upon the indemnified party:
(i) Promptly notifying the indemnifying party of the claim;
(ii) Cooperating with the indemnifying party in the defense;
(iii) Allowing the indemnifying party to control the defense and settlement (provided settlement does not impose obligations on indemnified party without its consent).

11.4 Allocation of Liability for Data Subject Claims

Where a Data Subject brings a claim under Article 82 GDPR against both Client and Provider arising from the same Processing, the parties shall cooperate to defend the claim and shall allocate liability between them based on their respective responsibility for the violation, as determined by a court of competent jurisdiction or as agreed between the parties.

==========
12. DURATION AND TERMINATION
==========

12.1 Duration

This DPA shall commence on the Effective Date and shall continue in force for so long as Provider Processes Client Personal Data.

12.2 Termination

This DPA shall automatically terminate upon the later of:
(a) Termination or expiration of the MSA; and
(b) Completion of deletion or return of all Client Personal Data in accordance with Clause 5.7.

12.3 Survival

The following provisions shall survive termination or expiration of this DPA:
- Clause 5.2 (Confidentiality)
- Clause 5.7 (Deletion or return of Personal Data)
- Clause 11 (Liability and Indemnification)
- Clause 14 (Governing Law and Jurisdiction)

Any provisions necessary for the interpretation or enforcement of surviving provisions shall also survive.

==========
13. GENERAL PROVISIONS
==========

13.1 Relationship to MSA

This DPA supplements and forms part of the MSA. In the event of any conflict or inconsistency between this DPA and the MSA regarding data protection matters, this DPA shall prevail.

13.2 Amendments

(a) Provider may update this DPA from time to time to reflect:
(i) Changes in Applicable Data Protection Laws;
(ii) Guidance from Supervisory Authorities;
(iii) Changes to Provider's Processing activities or security measures;
(iv) Updates to Standard Contractual Clauses or other transfer mechanisms.

(b) Provider shall notify Client of material amendments at least 30 days in advance. Client may object to amendments on reasonable data protection grounds within 30 days. If the parties cannot resolve the objection, either party may terminate the MSA upon written notice.

13.3 Severability

If any provision of this DPA is held to be invalid or unenforceable, the remaining provisions shall remain in full force and effect. The parties shall replace the invalid or unenforceable provision with a valid and enforceable provision that achieves the original intent as closely as possible.

13.4 Entire Agreement

This DPA, together with the MSA and its exhibits and annexes, constitutes the entire agreement between the parties regarding the Processing of Client Personal Data and supersedes all prior agreements, understandings and communications.

13.5 Notices

Notices under this DPA shall be in writing and delivered in accordance with the notice provisions of the MSA, with copies to:

For Provider:
Data Protection Officer
TechNova AI Systems Inc.
Alexanderplatz 15, 10178 Berlin, Germany
Email: dpo@technova-ai.com

For Client:
[Data Protection Officer or designated contact]
[Address]
[Email]

==========
14. GOVERNING LAW AND JURISDICTION
==========

14.1 Governing Law

This DPA shall be governed by and construed in accordance with the laws of Germany, without regard to conflict of law principles.

14.2 Jurisdiction

The parties submit to the exclusive jurisdiction of the courts of Berlin, Germany for any disputes arising out of or in connection with this DPA, except that:

(a) Either party may bring proceedings before the courts of any other jurisdiction where necessary to enforce a judgment or to seek interim relief;

(b) Data Subjects retain the rights granted under Article 79 GDPR to lodge complaints with Supervisory Authorities and bring judicial remedies.

14.3 Supervisory Authority

For the purposes of this DPA, the lead Supervisory Authority shall be the Berlin Commissioner for Data Protection and Freedom of Information (Berliner Beauftragte für Datenschutz und Informationsfreiheit), unless otherwise determined under the cooperation and consistency mechanisms of Chapter VII GDPR.

==========

IN WITNESS WHEREOF, the parties have executed this Data Processing Agreement as of the Effective Date.

TECHNOVA AI SYSTEMS INC.

By: _____
Name: Marcus Thompson
Title: Chief Technology Officer
Date: _____

[CLIENT NAME]

By: _____
Name: [NAME]
Title: [TITLE]
Date: _____

==========

ANNEX 1: DETAILS OF PROCESSING

==========

Subject Matter:
Provision of AI-powered workforce analytics services through the InsightPredict Analytics Platform.

Duration:
From Effective Date until termination of the MSA and completion of deletion or return of Client Personal Data.

Nature and Purpose of Processing:
• Analysis of employee and candidate data to generate insights and recommendations for HR decision-making
• Candidate screening and recruitment support
• Employee performance evaluation and predictive analytics
• Skills assessment and training recommendations
• Workforce planning and optimization
• Generation of reports, dashboards and analytics for Client

Types of Personal Data:
• Identity data: names, employee IDs, contact information
• Professional data: employment history, job titles, responsibilities, education, qualifications, certifications
• Performance data: performance reviews, ratings, productivity metrics, attendance records
• Compensation data: salary, benefits, bonuses
• Behavioral data: communication patterns (metadata only), collaboration metrics, system usage patterns, learning management system engagement
• Application data: resumes, cover letters, application forms, interview notes
• Assessment data: test results, skill assessments, certifications
• Biometric data (optional modules): facial recognition data, voice patterns
• Inferred data: performance predictions, turnover risk scores, skill gap analyses, promotion readiness assessments

Categories of Data Subjects:
• Current employees of Client
• Former employees of Client
• Job applicants and candidates
• Contractors and temporary workers (where applicable)

Sensitivity:
Processing includes:
• Large volumes of Personal Data (potentially thousands to tens of thousands of Data Subjects per Client)
• Special Categories of Personal Data (biometric data where applicable)
• Data revealing potentially sensitive information (performance issues, health-related absences, disciplinary matters)
• Automated decision-making and profiling with significant effects on Data Subjects (employment opportunities, career advancement)

Processing Operations:
• Collection and ingestion of Personal Data from Client systems
• Storage and organization of Personal Data in Provider's databases

• Analysis and profiling using machine learning algorithms
• Generation of predictions, scores and recommendations
• Production of reports and visualizations
• Transmission of results back to Client
• Logging of system operations and user activities
• Retention of Personal Data for agreed periods
• Deletion or return of Personal Data upon termination

Processing Location(s):
• Primary: European Union (Germany - Frankfurt data center)
• Backup: European Union (Netherlands - Amsterdam data center)
• Development/Testing: European Union (Germany - Berlin)
• Sub-processors: As specified in Annex 3

==========
ANNEX 2: TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES
==========

Provider implements the following technical and organizational measures to ensure appropriate security of Personal Data:

1. PHYSICAL SECURITY

Data Centers:
• Tier III or higher certified facilities
• 24/7 security personnel and video surveillance
• Multi-factor access control (biometric and key card)
• Visitor logging and escort requirements
• Environmental controls (fire suppression, climate control)
• Redundant power and network connectivity

Offices:
• Secure office facilities with access control
• Clean desk and screen lock policies
• Visitor management procedures
• Secure disposal of physical media (shredding)

2. LOGICAL ACCESS CONTROLS

Authentication:
• Unique user accounts for all personnel

• Strong password requirements (minimum 12 characters, complexity, expiration)
• Multi-factor authentication for privileged accounts and remote access
• Single sign-on (SSO) integration where applicable

Authorization:
• Role-based access control (RBAC) limiting access to Personal Data based on job function and need-to-know
• Principle of least privilege
• Segregation of duties for critical functions
• Regular access reviews and recertification

Account Management:
• Prompt provisioning and de-provisioning procedures
• Automated deactivation of inactive accounts
• Logging of authentication and authorization events

3. DATA ENCRYPTION

Encryption in Transit:
• TLS 1.3 or higher for all data transmissions over public networks
• VPNs for administrative access
• Encrypted email for sensitive communications

Encryption at Rest:
• AES-256 encryption for all Personal Data stored in databases
• Encrypted file systems for data storage volumes
• Encrypted backups
• Secure key management with hardware security modules (HSMs)

4. NETWORK SECURITY

Perimeter Security:
• Firewalls with deny-by-default rules
• Intrusion detection and prevention systems (IDS/IPS)
• DDoS protection
• Web application firewalls (WAF)

Network Segmentation:
• Separation of production, development and testing environments
• DMZ for public-facing services
• Isolated network segments for sensitive data processing
• Virtual private clouds (VPCs) with security groups

Monitoring:
• 24/7 security operations center (SOC)
• Security information and event management (SIEM)
• Log aggregation and analysis
• Threat intelligence integration

5. APPLICATION SECURITY

Secure Development:
• Secure coding standards and training
• Code review processes
• Static and dynamic application security testing
• Vulnerability scanning and penetration testing
• Dependency management and patching

Input Validation:
• Validation and sanitization of all user inputs
• Protection against injection attacks (SQL, XSS, etc.)
• Content security policies

Session Management:
• Secure session handling with appropriate timeouts
• Protection against session hijacking and fixation

6. DATA PROTECTION CONTROLS

Data Minimization:
• Collection limited to necessary data elements
• Automated deletion of unnecessary data
• Pseudonymization and anonymization where feasible

Purpose Limitation:
• Technical controls preventing use of data for unauthorized purposes
• Separate environments for different processing purposes

Data Quality:
• Validation rules ensuring data accuracy
• Error detection and correction procedures
• Regular data quality audits

7. BACKUP AND DISASTER RECOVERY

Backups:
• Daily incremental backups
• Weekly full backups
• Encrypted backup storage
• Geographic redundancy (backups stored in multiple EU locations)
• Regular backup restoration testing

Disaster Recovery:
• Documented disaster recovery plan
• Recovery time objective (RTO): 4 hours
• Recovery point objective (RPO): 1 hour
• Annual disaster recovery testing

Business Continuity:
• Redundant infrastructure components
• Failover capabilities
• Incident response procedures

8. VENDOR AND SUB-PROCESSOR MANAGEMENT

Due Diligence:
• Security assessments of all Sub-processors
• Review of security certifications and audit reports
• Contractual security requirements

Monitoring:
• Ongoing oversight of Sub-processor security practices
• Periodic re-assessment
• Security incident notification requirements

9. PERSONNEL SECURITY

Background Checks:
• Background verification for employees with access to Personal Data (to extent permitted by law)

Confidentiality:
• Confidentiality agreements for all personnel
• Ongoing confidentiality obligations

Training:
• Data protection and security awareness training for all personnel
• Specialized training for personnel handling Personal Data
• Annual refresher training

10. INCIDENT RESPONSE

Incident Response Plan:
• Documented procedures for detecting, responding to and recovering from security incidents
• Defined roles and responsibilities
• Escalation procedures

Personal Data Breach Response:
• Procedures for identifying and assessing Personal Data Breaches
• Notification procedures meeting GDPR Article 33 and 34 requirements
• Post-incident review and corrective actions

11. LOGGING AND MONITORING

Audit Logging:
• Comprehensive logging of access to Personal Data
• Logging of administrative actions
• Logging of system events and errors
• Log retention for at least 12 months

Monitoring:
• Real-time monitoring of system performance and security events
• Automated alerting for anomalous activities
• Regular log review and analysis

12. TESTING AND ASSESSMENT

Vulnerability Management:
• Regular vulnerability scanning (at least monthly)
• Annual penetration testing by independent third parties
• Prompt remediation of identified vulnerabilities based on risk rating

Compliance Audits:
• Annual third-party security audits (SOC 2 Type II)
• Internal compliance reviews
• Regular assessment against security frameworks (ISO 27001, NIST, etc.)

13. DOCUMENTATION AND POLICIES

Security Policies:
• Comprehensive information security policy
• Data protection policy
• Acceptable use policy
• Incident response policy
• Business continuity and disaster recovery policy

Procedures:
• Documented procedures for key security processes
• Regular review and update of documentation
• Version control and change management

14. CHANGE MANAGEMENT

Change Control:
• Formal change management process
• Security impact assessment for changes
• Testing of changes before production deployment
• Rollback procedures

Patch Management:
• Regular patching of systems and applications
• Prioritization based on vulnerability severity
• Testing of patches before deployment

15. AI-SPECIFIC SECURITY MEASURES

Model Security:
• Access controls for machine learning models
• Protection against model extraction and theft
• Adversarial robustness testing

Training Data Security:
• Secure storage and access controls for training datasets
• Data provenance tracking
• Protection against data poisoning

Inference Security:
• Rate limiting and abuse prevention for API calls
• Input validation to prevent adversarial examples
• Output validation to detect anomalous predictions

Provider reviews and updates these security measures regularly to address evolving threats and maintain appropriate security in light of the state of the art and

the risks presented by the Processing.

==========
ANNEX 3: LIST OF SUB-PROCESSORS
==========

Provider currently engages the following Sub-processors for Processing Client Personal Data:

1. Cloud Infrastructure Provider
Name: [Cloud Provider Name]
Location: European Union (Frankfurt, Germany; Amsterdam, Netherlands)
Processing Activity: Infrastructure-as-a-Service (IaaS) - hosting of Provider's application and data storage
Data Processed: All categories of Client Personal Data
Security Certifications: ISO 27001, SOC 2 Type II, CSA STAR

2. Database Hosting Service
Name: [Database Provider Name]
Location: European Union (Germany)
Processing Activity: Managed database services
Data Processed: All categories of Client Personal Data
Security Certifications: ISO 27001, SOC 2 Type II

3. Backup and Disaster Recovery Service
Name: [Backup Provider Name]
Location: European Union (Netherlands)
Processing Activity: Encrypted backup storage and disaster recovery
Data Processed: All categories of Client Personal Data
Security Certifications: ISO 27001, SOC 2 Type II

4. Customer Support Platform
Name: [Support Platform Name]
Location: European Union (Ireland)
Processing Activity: Support ticket management and client communication
Data Processed: Identity data, professional data (limited to information provided in support requests)
Security Certifications: ISO 27001, SOC 2 Type II, Privacy Shield (if applicable)

5. Security Monitoring Service
Name: [Security Provider Name]
Location: European Union (Germany)
Processing Activity: Security information and event management (SIEM)

Data Processed: System logs including access logs (may incidentally include Personal Data)
Security Certifications: ISO 27001, SOC 2 Type II

Provider maintains an up-to-date list of Sub-processors accessible at: https://www.technova-ai.com/subprocessors

Clients may subscribe to receive notifications of changes to Sub-processors at the above URL.

==========

ANNEX 4: STANDARD CONTRACTUAL CLAUSES

==========

[Standard Contractual Clauses for international data transfers would be inserted here - referencing the European Commission approved Standard Contractual Clauses for controller-to-processor transfers, as updated from time to time]

For transfers of Client Personal Data from the European Economic Area to countries without an adequacy decision, the parties agree to be bound by the Standard Contractual Clauses approved by the European Commission, with the following specifications:

Module: Controller to Processor (Module Two)
Optional Clauses: [Specify which optional clauses apply]
Docking Clause: [Included/Not included]
Governing Law: [Law of EU Member State in which Controller is established]

The annexes to the Standard Contractual Clauses are completed as follows:
- Annex I.A (Data Exporter): Client information as Controller
- Annex I.B (Data Importer): Provider information as Processor
- Annex I.C (Competent Supervisory Authority): As specified in Clause 14.3 of DPA
- Annex II (Technical and Organizational Measures): As specified in Annex 2 of DPA
- Annex III (List of Sub-processors): As specified in Annex 3 of DPA

[Full text of applicable Standard Contractual Clauses would be included]

==========

END OF DATA PROCESSING AGREEMENT

==========