DATA PROCESSING AGREEMENT

1. This Data Processing Agreement is entered into in connection with the Awakast System Subscription Agreement (hereinafter referred to as the "Subscription Agreement") and sets out the principles governing the processing by the Service Provider, on behalf of the Client, of personal data of Candidates, Client Employees, and other individuals as specified in this DPA, through the Awakast system.
2. This DPA constitutes the entire obligations and conditions for the entrustment of processing of personal data of the Candidates, the Client's Employees, and other persons indicated in the Processing Agreement, between the Client and the Service Provider in connection with the provision of Services and the Client's use of the Awakast system.

§1. General Provisions

1. The Client entrusts the Service Provider with the processing of Personal Data in connection with the Subscription Agreement to the extent specified in **Annex 1**.
2. The Service Provider may process Personal Data solely for the purpose of fulfilling its obligations under the Subscription Agreement, including the provision of specific functionalities and technical support for the Awakast system.
3. The Service Provider may process Personal Data only for: (i) the duration of the Subscription Agreement and (ii) the period following the termination or expiration of the Subscription Agreement until the deletion of the Personal Data in accordance with the provisions of this Processing Agreement, unless the Client and the Service Provider agree on another data processing period in a separate arrangement.

§2. Technical and Organizational Measures

1. Considering the state of technical knowledge, as well as the nature, scope, context, and purposes of the processing of Personal Data and the risk of infringement of the rights or freedoms of data subjects, the Service Provider shall implement technical and organisational measures appropriate to the type of Personal Data and the risk of such infringement.
2. The appropriate technical and organisational measures shall include, at a minimum, the measures specified in **Annex 2** to this Processing Agreement.

§3 Service Provider's Personnel

1. The Service Provider shall grant access to Personal Data only to individuals acting under its authority whose access is necessary for the performance of services under the Subscription Agreement.
2. The Service Provider shall ensure that such authorised persons are subject to confidentiality obligations regarding the processed Personal Data or are subject to statutory confidentiality

obligations. The Service Provider shall acquaint all persons authorised to process Personal Data with the data protection regulations and their responsibilities for protecting such data from unauthorised access, unjustified modification, destruction, unlawful disclosure, or acquisition

§4 Sub-Processors

1. The Client consents to the use by the Service Provider of Sub-processors for the processing of Personal Data pursuant to Article 28(2) of the GDPR, in order to properly provide the Services, including ensuring specific functionalities and security of the Awakast system.
2. The list of Sub-processors used or intended to be used by the Service Provider as of the effective date of this Processing Agreement is contained in Annex No. 3. By entering into this Processing Agreement, the Client accepts the processing of Personal Data by the entities listed in **Annex 3**.
3. In the event the Service Provider intends to use any Sub-processors other than those listed in Annex 3, the Service Provider shall notify the Client of the new Sub-processor at least 30 days before the data is further entrusted for processing. The notice will be delivered electronically to the Client's Email Address. An update to **Annex 3** does not require an amendment to the Processing Agreement.
4. The agreement between the Service Provider and any Sub-processor shall impose the same data protection obligations as set out in this Processing Agreement, in particular the obligations to comply with the GDPR, including the implementation of technical and organisational measures adequate to the type of entrusted Personal Data and the risk to the rights or freedoms of the data subjects. The rights of Sub-processors shall not exceed those granted to the Service Provider under this Processing Agreement.
5. The Service Provider shall be liable for the acts and omissions of its Sub-processors as for its own acts or omissions.

§5 Obligations of the Service Provider

1. Taking into account the nature of the Processing Activities and the information available in connection with the Services, the Service Provider shall assist the Client in fulfilling the following obligations:
    a. conducting a Data Protection Impact Assessment by providing the Client with the necessary information regarding the processing of Personal Data in the Awakast system;
    b. responding to data subject requests under Articles 15-22 of the GDPR, by providing the Client, upon request to: info@awakast.com, with the possibility to: (i) export Personal Data, (ii) delete or restrict the processing of Personal Data, and (iii) rectify Personal Data. In case a data subject submits such a request directly to the Service Provider, the Service Provider shall immediately inform the Client and determine with the Client how to proceed;
    c. notifying the Supervisory Authority and affected data subjects of a Personal Data Breach, in accordance with Articles 33-34 of the GDPR.
2. The Service Provider shall inform the Client without undue delay, but no later than within 5 Business Days, about:

a. any proceedings, particularly administrative or judicial, related to the processing of Personal Data, any administrative decisions or court rulings related to Personal Data addressed to the Service Provider, as well as any planned proceedings, audits, or inspections;
b. any instructions from the Client regarding the processing of Personal Data which, in the opinion of the Service Provider, constitute a breach of the GDPR or other data protection laws.

3. The information shall be delivered to the Client's Email Address.

§6 Personal Data Breach

1. In the event the Service Provider identifies a Personal Data Breach, it shall notify the Client without delay, but no later than within 36 hours of discovery. The notification shall include:
   a. a description of the circumstances of the incident and its identified or suspected causes;
   b. a description of the nature of the Personal Data Breach, including, if possible, the categories and approximate number of affected data subjects and categories and approximate number of data entries concerned;
   c. a description of the possible consequences of the Personal Data Breach;
   d. a description of the remedial actions taken by the Service Provider to mitigate potential adverse effects.
2. The notification shall be delivered to the Client’s Email Address.
3. Upon discovering a Personal Data Breach, the Service Provider shall immediately take all necessary technical and organisational measures to contain the breach and minimise its potential consequences.

§7 Processing Audit

1. The Client is entitled to conduct a Processing Audit in the following cases: (i) the Supervisory Authority imposes an audit obligation, or (ii) an audit is necessary to investigate a Personal Data Breach.

2. The Client shall notify the Service Provider of its intention to conduct a Processing Audit at least 7 Business Days prior to the planned audit date. The Parties shall agree separately on the audit schedule. The notice shall specify the scope, date, and authorised persons conducting the audit and shall be delivered to the Service Provider’s Email Address.

3. If the audit cannot be conducted on the indicated date according to the Audit Schedule, the Service Provider shall notify the Client of the next possible audit date. This notice shall be delivered to the Client’s Email Address.

4. The audit shall conclude with the signing of a Processing Audit Report by both Parties. The report shall include the findings of the audit and the mutually agreed changes to the processing of Personal Data by the Service Provider, if any.

§8 Liability

1. The Service Provider shall be liable for the actions or omissions of its Sub-processors as for its own, under the general principles of liability.

§9 Termination of Data Processing

1. The Service Provider shall delete Personal Data from all data carriers, including all existing copies, no later than 30 days after the end of the Retention Period or the completion of other Services involving Personal Data processing in the Awakast system, unless otherwise agreed in writing. In case of termination or expiration of the Processing Agreement before the expiry of the Retention Period, the Service Provider shall delete the Personal Data within 30 days of the termination or expiration of the Subscription Agreement, unless another deletion deadline is agreed in writing.

2. The Service Provider shall ensure that all Sub-processors delete or anonymise the Personal Data in accordance with this section.

3. During the Retention Period or the provision of other Services involving Personal Data processing in the Awakast system, the Client may request the deletion and export (return) of the Personal Data to a medium agreed upon by the Parties.

4. If the Service Provider is required by applicable law to retain Personal Data beyond the Retention Period or the term of Services involving Personal Data processing in the Awakast system, it shall process the data only to the extent and for the purpose of complying with legal obligations, and shall promptly delete or anonymise the data upon fulfilment of those obligations.

ANNEX NO. 1 – PERSONAL DATA

Category of Data Subjects	**Type of Personal Data**	**Processing Activities**	**Form of Processing**
Candidates	All data entered by the Client into the Service Provider's Systems, e.g., data included in a CV, cover letter, or application form, in particular: first and last name, contact details (email address, phone number, residential address), date of birth, education, work experience, qualifications and skills, expected start date, financial expectations, image.	Collection, recording, organisation, structuring, storage, consultation, transmission, modification, deletion.	Electronic
Client's Employees	First and last name, email address, or other data.	Collection, recording, organisation, structuring, storage, consultation, transmission, modification, deletion	Electronic

ANNEX NO. 2 – LIST OF TECHNICAL AND ORGANISATIONAL MEASURES

§1 Personal Data Security

1. **Organisational Measures:**

   a) The Service Provider conducts initial and periodic training on personal data protection and information security for its employees;

   b) The Service Provider grants named authorisations to employees for the processing of personal data. Authorisations are reviewed periodically.

2. **Access Control Measures:**

   a) Each employee of the Service Provider has a separate, unique access account for the IT systems used for processing Personal Data;

   b) The Service Provider enforces a strong password policy, password changes, and account locking;

   c) Remote access to Personal Data is centrally managed and controlled.

3. **Operational Security Measures:**

   a) IT systems used by the Service Provider to process Personal Data are regularly updated and verified for security

   b) The Service Provider employs protection against unauthorised access to systems and networks via a firewall;

§2 Application Security

The following security measures are implemented in the Service Provider's Systems:

1. **Architecture Security:**

   a) The application architecture ensures multi-layered application structure;

   b) Application architecture components are monitored for vulnerabilities;

   c) Network security measures are in place at the Internet boundary.

2. **Authentication Security**: Session management mechanisms are implemented to ensure supervised and secure user interaction with the application. Sessions are unique per user and cannot be guessed or shared.

3. **Session Management Security:** Session management mechanisms are implemented to ensure supervised and secure user interaction with the application. Sessions are unique per user and cannot be guessed or shared.

4. **Access Control Security:** Access is granted only to resources for which consent has been given. Individuals accessing the system have valid credentials, and users are assigned to defined roles and permissions.
5. **Malicious Input Handling Security**: Input data validation is used to ensure correctness and alignment with intended purposes.
6. **Inactive Cryptographic Mechanisms Security**: All cryptographic modules that terminate with failure do so safely. Access to keys is securely managed.
7. **Error Handling and Logging Security:** Security event logging mechanisms are used, and all logged information is securely handled and stored.
8. **Data Protection Mechanisms Security**: Measures are in place to protect data from unauthorised viewing or disclosure, both during transmission and at rest. Data is protected from malicious creation, alteration, or deletion by unauthorised persons, and is accessible only to authorised users when needed.
9. **Communication Security**:
    a) Secure connections are used for all (internal and external) communications that are authenticated or involve sensitive data or functions;
    b) Mechanisms are implemented to prevent degradation of security parameter;
    c) The strongest available encryption algorithm is used.
10. **File and Resource Security:** Untrusted file data is handled securely, and source files from untrusted origins are stored outside the application root directory with restricted permissions.
11. **Web Service Security**: All input parameters transmitted from less trusted to more trusted layers are validated.
12. **Configuration Process Security:** Security is ensured during software changes and the use of up-to-date libraries and platforms. Communication between components is encrypted and authenticated.

ANNEX NO. 3 – SUB-PROCESSORS

No.	Name of Sub-Processor	Address of Sub-Processor	Data Processing Location	Purpose of Sub-processing
1.	Microsoft Ireland Operations Limited	70 Sir Rogerson's Quay Dublin 218, Irlandia	Na terenie EOG Sweden - 805 91 Gävle, Sweden	Cloud hosting (Microsoft Azure)
2.	OVH Groupe SA	2, rue Kellermann, 59100 Roubaix	Na terenie EOG Germany, Frankfurt - Limburger Str. 45, 65555 Limburg b.	Cloud hosting (OVHcloud)