DATA EXCHANGE TERMS AND CONDITIONS

1. DEFINITIONS

1. **You**: any (legal) person who has entered into, enters into or wishes to enter into an Agreement with us.
2. **We** or **us**: JEX Backoffice B.V., with its registered address according to its articles of association in (3071 JL) Rotterdam at the address Nassaukade 5, listed in the Commercial Register under number 76171183.
3. **Parties** or **we (both)**: we and you jointly. Individually also called the party.
4. **Data Subject**: the data subject within the meaning of the GDPR.
5. **Data Breach**: a security breach regarding Personal Data resulting in (the significant likelihood of) serious adverse effects on the protection of Personal Data.
6. **Data Exchange Terms and Conditions**: these terms and conditions, including annexes, which form an inseparable part of the Agreement.
7. **Incident**: a Personal Data security breach that has yet to be determined to result in (the significant likelihood of) serious adverse effects on the protection of Personal Data.
8. **Employees**: the persons we both engage for the Processing of Personal Data and who work under supervision of the parties.
9. **Norms and Standards**: the norms and standards with regard to methods, techniques, procedures and security requirements that will be followed during the Processing of Personal Data, as included in Annex 1.
10. **Agreement**: the Agreement between you and us, including annexes.
11. **Personal Data**: any data relating to an identified or identifiable natural person (i.e. Data Subject).
12. **Controller**: the controller for the Processing within the meaning of the GDPR – we both.
13. **Processing**: any operation or set of operations involving Personal Data.
14. **Processor**: the Processor within the meaning of the GDPR.
15. **Processing of Personal Data**: the Processing of a particular type or types of Personal Data of a particular category or categories of Data Subjects for specified, specifically defined and legitimate purposes for a predetermined duration.

2. SUBJECT

1. We both commit ourselves towards each other to process Personal Data lawfully, carefully, properly and transparently.
2. In Annex 2, we both describe the processing operations covered by these Data Exchange Terms and Conditions.
3. We both guarantee towards each other that Employees will comply with the requirements of the GDPR and the provisions of these Data Exchange Terms and Conditions.

3. OBLIGATIONS

1. We both guarantee each other that the Personal Data we both obtain from each other will not be further processed in a manner incompatible with the purposes for which it was obtained.
2. We both guarantee each other that the Processing of Personal Data is not unlawful and does not infringe on the rights of third parties.

4. CHAIN PROVISION

1. We both are entitled to disclose the Personal Data we obtain from each other to other Controller(s) upon written consent, to the extent permitted by the GDPR. We or you may object to this on reasonable grounds towards the other.
2. Parties shall impose the same obligations on such other Controller(s) as applicable towards each other and monitor compliance by such other Controller(s).
3. We both shall impose on the other Controller(s) the obligation to comply with Article 14 of the GDPR insofar as they have not themselves communicated the information referred to in this article to the Data Subject.
4. We both shall notify each other (and any other Controller(s) to which Personal Data have been provided) of the rectification or erasure of Personal Data or restriction of Processing in accordance with Article 16, 17 first paragraph and Article 18 of the GDPR unless this is impossible or requires disproportionate effort. The Controller to which the Data Subject exercises a right under the GDPR shall handle the request and inform the other Controller(s).

5. SECURITY, INCIDENTS AND DATA BREACHES

1. We both will secure the (Processing of) Personal Data in accordance with the requirements set by or pursuant to the GDPR and by or pursuant to other applicable legislation regarding the processing of Personal Data.
2. If an Incident or Data Breach occurs with you or us, we both will immediately report the Incident or Data Breach to the other party and to the Personal Data Authority and, if necessary, to Data Subject(s).

ANNEX 1 Norms and Standards

The measures we both adhere to are as follows:

- we both maintain a policy that explicitly addresses the measures that safeguard privacy and secure the Processing of Personal Data. Responsibilities, both at operational and executive levels, are clearly defined therein. This policy (hereinafter: the Privacy and Information Security Policy) is based on relevant law and regulations and generally applied (security) standards. All Employees and, where applicable, external users are informed about the Privacy and Information Security Policy, as relevant to their position;
- Employees are bound by a duty of confidentiality and a screening has taken place upon employment (if applicable);
- IT facilities and equipment are physically protected against unauthorized access, damage and malfunctions;
- procedures are in place to allow authorized users to access the information systems and to prevent unauthorized access to network and information systems;
- there are procedures for development, maintenance and destruction of information systems;
- adequate security is applied when providing Personal Data to third parties;
- activities performed by users with Personal Data are recorded in log files. The same applies to other relevant events, such as attempts to gain unauthorized access to Personal Data and disruptions that may result in damage or loss of Personal Data;
- the network and information systems are actively monitored and managed;
- procedures are in place for the timely and effective handling of Incidents and security weaknesses;
- a procedure is available to report and register Data Breaches;
- software, such as browsers, virus scanners and operations systems, are kept up-to-date;
- preventive and recovery measures are in place to ensure continuity and mitigate the effects of force majeure situations.

ANNEX 2 Type of Personal Data and categories of Data Subjects

Data Subject categories:

- applicants;
- candidates;
- temporary workers;
- self-employed persons.

Personal Data:

- name;
- address;
- gender;
- date of birth;
- contact details;
- CV;
- diplomas and certificates;
- registrations (i.e. in the case of Individual Healthcare Professions or in the case of self-employed persons regarding Chamber of Commerce and VAT);
- Certificate of Good Conduct (if applicable);
- proof of identity and work permit for temporary workers outside the EEA;
- residence permit of self-employed persons outside the EEA;
- social number (in the case of temporary workers);
- hours worked and work locations;
- non billable hours.