DATA PROCESSING 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 Processing Terms and Conditions**: these terms and conditions, including annexes, which form an inseparable part of the Agreement.
7. **EEA**: European Economic Area.
8. **Employees**: the persons we both engage for the Processing of Personal Data and who work under supervision of the parties.
9. **Agreement**: the Agreement between you and us, including annexes.
10. **Personal Data**: any data relating to an identified or identifiable natural person (i.e. Data Subject).
11. **Controller**: we both – the controller for the Processing within the meaning of the GDPR.
12. **Process(ing)**: any operation or set of operations involving Personal Data.
13. **Processor**: the Processor within the meaning of the GDPR.
14. **Sub-processor**: any third party engaged by us in the Processing under the Agreement, other than Employees.
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 will Process on your behalf. Processing will only take place within the framework of the Agreement.
2. We will not Process Personal Data for any purpose other than that arising from the Agreement.
3. We shall not make any independent decisions about the Processing, the provision of Personal Data to third parties and/or the duration of the Processing.
4. Processing in and transfer of Personal Data to countries outside the EEA is only permitted with your prior consent.

3. PROCESSOR OBLIGATIONS

1. We Process in a proper, careful and transparent manner.
2. We Process only on the basis of prior instruction from you, unless we are legally obliged to Process. In that case, we will inform you to the extent permitted.
3. We will inform you on first request of the measures taken by us from these Data Processing Terms and Conditions and/or the applicable laws and regulations.
4. We will not engage Sub-processors without your prior consent.
5. When we engage Sub-processors with your consent, we shall ensure that they comply, as a minimum, with the requirements set out in these Data Processing Terms and Conditions. We require each Sub-processor not to Process Personal Data further other than as set out in these Data Processing Terms and Conditions.

4. SECURITY AND REPORTING DATA BREACHES

1. We shall ensure appropriate technical and organizational measures to secure Personal Data against loss or any form of unlawful Processing. These measures, taking into account the state of the art and the costs involved in implementing and carrying out the measures, will ensure an adequate level of protection. In doing so, we will observe the security requirements of Article 32 AVG and take into account the risks of the Processing and the nature of the Personal Data. We will evaluate the information security measures we have taken and enhance, complement or improve them insofar as the requirements or (technological) developments give cause to do so.
2. In the event of a Data Breach, we will inform you thereof without unreasonable delay after discovering it. You will decide whether the Data Subject(s) and/or the relevant regulator(s) will be informed. If you so request and/or the laws and regulations require, we will cooperate in informing you.
3. We undertake efforts to ensure that the information provided is complete, correct and accurate. We will also keep you informed of further developments concerning the Data Breach.

5. DATA SUBJECT REQUESTS

1. When the Data Subject makes a request to us to examinate or correct, supplement, amend or block his Personal Data, we will refer him to you. Responsibility for handling requests lies in principle with you.
2. When the Data Subject submits a request for examination to us, we will, if you so wish, cooperate within 14 days.

ANNEX 1 Norms and Standards

The measures we adhere to are as follows:

- we 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.