Data Processing Agreement

1. GENERAL

1.1 The provisions of the Agreement apply in full to the Data Processing Agreement. This Data Processing Agreement forms an integral part of the Agreement. Where provisions regarding the processing of personal data are included in the Agreement, the provisions of this Data Processing Agreement shall prevail.

1.2 With regard to the processing of personal data under the Agreement, the client is to be considered as the controller within the meaning of Article 4(7) of the General Data Protection Regulation ("GDPR") and Mysolution as the processor within the meaning of Article 4(8) GDPR.

1.3 Terms from the GDPR such as "process", "personal data", "controller" and "processor" have the meaning given to them in the GDPR.

2. PROCESSING OF PERSONAL DATA

2.1 The categories of Data Subjects and types of Personal Data processed by the Processor and the purpose of that processing are included in **Appendix** 1.

2.2 The Processor shall only process the Personal Data disclosed to it based on written instructions from the Controller and solely within the framework of executing the Agreement, unless a Union or Member State law provision applicable to the Processor requires processing. In that case, the Processor shall inform the Controller of that legal requirement prior to processing, unless that legislation prohibits such notification for important reasons of public interest.

2.3 The Processor has no control over the purpose and means of processing Personal Data. Nothing in this Data Processing Agreement is intended to transfer any control over the Personal Data to the Processor.

2.4 The Processor is not permitted to:

2.4.1 process the Personal Data for its own purposes;

2.4.2 process for purposes other or more extensive than reasonably necessary for the execution of the Agreement;

2.4.3 provide to third parties unless permitted under the Agreement and/or the Data Processing Agreement and/or based on a mandatory legal provision requiring the Processor to provide Personal Data to (supervisory or investigative) authorities.

3. COMPLIANCE WITH LAWS AND REGULATIONS

3.1 Parties shall conduct themselves in accordance with the provisions of the GDPR and future (European) legislation regarding the processing of personal data applicable at any time. If future legislation requires adjustment of the Data Processing Agreement, Parties shall enter into consultation to make new agreements maintaining the intent of this Data Processing Agreement as much as possible.

3.2 The Processor shall assist the Controller in carrying out a Data Protection Impact Assessment, at least insofar as possible in relation to the information available to it and the nature of the processing. The reasonable costs incurred by this obligation to cooperate for the Processor shall be borne by the Controller.

3.3 If and insofar as the Controller is required by law to provide information to a supervisory authority about the processing of Personal Data, the Processor shall, at the first request of the Controller, provide all reasonably requested cooperation to the Controller, so

that this information becomes available and the supervisory authority can be properly informed.

4. CONFIDENTIALITY

4.1 The Processor is obligated to keep the Personal Data confidential and shall ensure that persons authorized to process the Personal Data have committed themselves to confidentiality.

4.2 This confidentiality obligation shall continue to exist even after the termination of this Data Processing Agreement, except for information that is already publicly known, other than as a result of a breach of the aforementioned confidentiality obligation.

5. PROCESSOR SECURITY MEASURES

5.1 The Processor shall take appropriate technical and organizational measures to ensure a level of security appropriate to the risk, which include, among others, the measures specified in **Appendix 2**.

5.2 In determining the measures, the Processor takes into account the state of the art, the implementation costs, as well as the nature, scope, context and purposes of processing and the varying likelihood and severity of risks to the rights and freedoms of persons.

5.3 In assessing the appropriate level of security, the Processor shall particularly take into account the processing risks, especially as a result of destruction, loss, alteration or unauthorized disclosure of or unauthorized access to transmitted, stored or otherwise processed data, whether accidental or unlawful.

5.4 The Processor shall take measures to ensure that any natural person acting under the authority of the Processor who has access to the Personal Data processes these only on instructions from the Controller, unless Union or Member State law requires the Processor to process.

6. SUPERVISION BY CONTROLLER

6.1 The Processor shall provide the Controller, at its request, with the necessary information enabling the Controller to form an opinion on compliance by the Processor with the provisions in Articles 2, 4, 5, 7 and 10 of this Data Processing Agreement.

6.2 The Controller has the right to have compliance with the obligations of the Processor in Articles 2, 4, 5, 7 and 10 of this Data Processing Agreement verified by an independent expert who is bound by confidentiality. The Processor shall cooperate with the audit and make all reasonably relevant information available for the audit in a timely manner. The costs of audits commissioned by the Controller shall be borne by the Controller, unless it appears that the Processor has not adequately fulfilled its obligations in which case the Processor shall bear the costs.

6.3 If the audit report of the independent expert shows that the measures and provisions taken by the Processor do not sufficiently comply with this Data Processing Agreement, the Processor shall immediately take the necessary measures to comply.

7. DATA BREACH NOTIFICATION OBLIGATION

7.1 The Processor shall inform the Controller without delay as soon as it discovers that a personal data breach has occurred. This information provision shall be such that the Controller is able to comply with its obligations under Article 33 and Article 34 GDPR.

7.2 The Processor shall keep the Controller fully informed about the progress of the recovery and all relevant developments regarding the breach referred to in Article 7.1 and its consequences. The Processor shall take all measures that can reasonably be expected of it to repair or limit the adverse

consequences of the breach referred to in Article 7.1 where applicable.

7.3 The Processor is not permitted to communicate with Data Subject(s) and/or supervisory authority(ies) in the context of a breach as referred to in Article 7.1 other than on instruction from the Controller, or with its express and explicit consent.

8. SUB-PROCESSORS

8.1 The Processor hereby obtains permission to outsource parts of the processing of Personal Data to other processors during the term of the Agreement, as described in **Appendix** 1.

8.2 The Processor shall inform the Controller about intended changes regarding the addition or replacement of sub-processors, whereby the Controller is given the opportunity to object to these changes.

8.3 The Processor shall ensure that all sub-processors engaged by it that play a role in the execution of the Agreement will comply with the obligations contained in this Data Processing Agreement, particularly the obligation to provide adequate guarantees with regard to applying appropriate technical and organizational measures to ensure an equivalent level of protection of the Personal Data.

9. REQUESTS FROM DATA SUBJECTS

9.1 The Controller has obligations under the GDPR towards Data Subjects, such as regarding the provision of information, providing access to, rectification and deletion of Personal Data. The Processor shall - if possible - provide cooperation with the obligations to be fulfilled by the Controller. The Processor reserves the right to charge its regular hourly rate to the Controller for this cooperation.

9.2 If a Data Subject contacts the Processor directly regarding the exercise of their rights under the GDPR, the Processor shall not respond to this (substantively), but shall notify this without delay to the Controller.

10. INTERNATIONAL TRANSFERS

10.1 The Processor shall ensure that any processing of Personal Data which is carried out by or on behalf of the Processor including by its engaged third parties in connection with the execution of the Agreement shall take place within the European Economic Area (EEA) or to or from countries that provide an adequate level of protection in accordance with the GDPR.

10.2 Without the prior written consent of the Controller, the Processor may therefore not transfer Personal Data to or store in a country or organization outside the EEA or make Personal Data accessible from a non-EEA country, unless that country or organization provides an adequate level of protection or a Union or Member State law provision applicable to the Processor requires processing. In that case, the Processor shall inform the Controller of that legal requirement prior to processing, unless that legislation prohibits such notification for important reasons of public interest.

11. WARRANTY AND INDEMNIFICATION

11.1 The Controller warrants that the data processing takes place in accordance with applicable laws and regulations. This means at least that the Controller warrants that it has the right to collect the data and is entitled to have these data processed.

11.2 The Controller indemnifies the Processor against damage and costs resulting from any claims by third parties, explicitly including Data Subject(s) and supervisory authorities (such as the Dutch Data Protection Authority), relating to or arising from unlawful processing and/or other violation of the GDPR and/or the Data Processing Agreement that can be attributed to the Controller.

12. LIABILITY

12.1 The Processor guarantees correct compliance with the obligations from the Data Processing Agreement. This Data Processing Agreement forms an integral part of the Agreement between Controller and Processor and the (total) liability of Processor is (therefore) limited in accordance with the provisions in the Agreement and/or general terms and conditions.

13. DURATION OF DATA PROCESSING AGREEMENT

13.1 This Data Processing Agreement enters into force at the moment the Agreement enters into force and is concluded for the duration of the Agreement.

13.2 As soon as the Agreement is terminated or ends, for whatever reason, this Data Processing Agreement shall remain in force as long as Personal Data is processed by the Processor, after which this Data Processing Agreement shall end by operation of law.

13.3 After the end of this Data Processing Agreement, the Processor shall, at the first request and at the choice of the Controller, either delete all Personal Data or return these to them. The Controller must make their choice known to the Processor no later than two (2) weeks before the termination of the Data Processing Agreement. If the Processor does not receive this choice in time, the Processor is entitled to delete the Personal Data.

13.4 The Processor shall only retain a copy of the Personal Data if it is required to do so by a mandatory legal provision.

14. FINAL PROVISION

14.1 Changes and additions to this Data Processing Agreement are only valid if agreed in writing between Parties.

14.2 Dutch law exclusively applies to this Data Processing Agreement.

APPENDIX 1 OVERVIEW OF PERSONAL DATA AND SUB-PROCESSORS

I. Types of personal data

- Identification data for a natural person, BSN number, name and address details
- Gender, date of birth, telephone number, email address, nationality, (passport) photo
- Profession and position, data concerning work experience/employment history, CV
- Data concerning completed and to be completed education, courses and internships
- Financial data (bank account number)
- Website behavior (IP number)

II. Categories of data subjects

- Candidates/Applicants/Assessees
- Customers
- Marketing contacts
- Employees
- Suppliers

III. Purposes for which personal data processing takes place

- Recruitment purposes
- Marketing purposes
- Payment purposes
- Administrative purposes
- Statistical purposes
- Security, improvement and development of the Service and Application
- Assessment and acceptance of (future) customers
- Execution of agreement or contract

IV. Sub-processors

Name: **Salesforce.org**

Address: Prins Bernhardplein 200 1097JB Amsterdam

Description of service: Cloud services (Recruitment and selection, relationship management, customer and contract administration)

Name: **Microsoft BV**

Address: Evert van de Beekstraat 354 1118 CZ Amsterdam

Description of service: Cloud services (Personnel administration, time processing, financial and salary administration)

Name: **Spotler Nederland BV**

Address: Boris Pasternaklaan 16 2719 DA Zoetermeer

Description of service: Email processing, recruitment and selection, relationship management, customer and contract administration

Name: **Textkernel BV**

Address: Nieuwendammerkade 26A-5 1022 AB Amsterdam

Description of service: Processing CV data, recruitment and selection

Name: **Snowflake Computing Netherlands B.V.**

Address: Gustav Mahlerlaan 300 1022 AB Amsterdam

Description of service: Data lake, data warehouse, processing of metadata and telemetry

Name: **NIXZ**

Address: Binckhorstlaan 36 - C0.28, 2516 BE Den Haag, the Netherlands

Description of service: Plugin to create and manage a connection between LinkedIn and candidates.

V. Duration of processing

For the duration of the data processing agreement

APPENDIX 2 SECURITY SPECIFICATION

Technical and organizational security measures

A. General information about security measures taken:

- An information security policy has been established, which includes best practices regarding information security
- Employees of the Processor have signed an employment contract with confidentiality agreement
- Personal data is exclusively processed by approved sub-processors with whom a processing agreement has been concluded, providing at least the same level of protection of personal data as Mysolution
- Should the Processor receive personal data in the form of a backup for solving a software incident or for converting data, these are stored in a protected network segment where only those directly involved have access. The data is immediately destroyed if it is no longer necessary to retain the data.
- Microsoft BV has guidelines regarding GDPR compliance: https://www.microsoft.com/en-us/TrustCenter/CloudServices/Azure/GDPR
- Salesforce.org has guidelines regarding GDPR compliance: https://help.salesforce.com/articleView?id=data_protection_and_privacy.htm
- Snowflake Computing Netherlands B.V. has guidelines regarding GDPR compliance: https://www.snowflake.com/legal/

B. Measures to ensure that only authorized personnel has access to Personal Data:

- The Processor has an authorization and rights structure based on user roles. Only employees with the correct user role have access to personal data
- Access to the data center is only granted to authorized personnel.

C. Measures to protect Personal Data against loss or modification and against unauthorized or unlawful processing, access or disclosure:

- Data storage takes place in a European data center, which is ISO 27001 certified. The data center has 24/7 surveillance, both electronic and physical
- Employees of the Processor and its Sub-processors only have remote access to the servers using 2-factor authentication
- All traffic to and from the servers takes place using a secure SSL connection.

D. Measures for detecting vulnerabilities and incident management:

- Security investigations and penetration tests are periodically conducted by external parties on the hosted web applications. Any findings are implemented in the application.