

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 shall be regarded 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 "processing", "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 in connection with the performance of the Agreement, unless a Union or Member State law to which the Processor is subject 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 grounds of public interest.
- 2.3 The Processor does not determine the purposes or the essential means of the processing of Personal Data. Nothing in this Data Processing Agreement is intended in

any way to transfer 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 the Personal Data for purposes other than, or going beyond, those reasonably necessary for the performance of the Agreement;
 - 2.4.3 provide the Personal Data to third parties unless permitted under the Agreement and/or the Data Processing Agreement, 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 The Parties shall comply with the provisions of the GDPR as in force from time to time and future (European) legislation regarding the processing of Personal Data. If future legislation requires adjustment of the Data Processing Agreement, the Parties shall enter into consultation to agree new arrangements 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, to the extent possible, taking into account the nature of the processing and the information available to the Processor. The reasonable costs that this obligation entails 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, upon the Controller's first request, 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 authorised to process the Personal Data have committed themselves to confidentiality.
- 4.2 This confidentiality obligation shall survive 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 organisational measures to ensure a level of security appropriate to the risk, which include, among other things, 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 natural 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 unauthorised disclosure of or unauthorised 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 this

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, upon its request, with all information necessary to assess the Processor's compliance 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 safeguards implemented by the Processor do not adequately meet the requirements of 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 undue delay after becoming aware of a Personal Data Breach. The notification shall contain sufficient information to enable the Controller to comply with Articles 33 and 34 GDPR.
- 7.2 The Processor shall keep the Controller fully informed about the progress of the remediation efforts 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 remedy or mitigate the adverse consequences of the breach referred to in Article 7.1 where applicable.

- 7.3 The Processor is not permitted to communicate with any Data Subject or supervisory authority in the context of a breach as referred to in Article 7.1 other than on instruction from the Controller, or with its express authorisation.

8. SUB-PROCESSORS

- 8.1 The Controller hereby grants the Processor general written authorisation to engage other processors (Sub-processors) in the processing of Personal Data 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 within 30 days.
- 8.3 The Processor shall ensure that all Sub-processors engaged by it that play a role in the performance of the Agreement will comply with the obligations contained in this Data Processing Agreement, particularly the obligation to provide sufficient guarantees with regard to applying appropriate technical and organisational 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 erasure of Personal Data. The Processor shall - if possible - assist the Controller in fulfilling

those obligations. 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 substantively to the request and shall notify the Controller without undue delay.

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 performance of the Agreement shall take place within the European Economic Area (EEA). Any transfer outside the EEA shall comply with Chapter V GDPR.
- 10.2 Without the prior written consent of the Controller, the Processor may therefore not transfer Personal Data to, or store Personal Data in, a country or organisation outside the EEA or make Personal Data accessible from a non-EEA country, unless the transfer complies with Chapter V GDPR, 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 in any event that the Controller warrants that it is entitled to collect and process such data, or to have such data collected and processed.
- 11.2 The Controller indemnifies the Processor against all losses, damages and costs resulting from any claims by third parties,

explicitly including Data Subjects and supervisory authorities (such as the Dutch Data Protection Authority), relating to or arising from unlawful processing or other breach of the GDPR or the Data Processing Agreement that can be attributed to the Controller.

12. LIABILITY

- 12.1 The Processor warrants the proper performance of its obligations under this 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 otherwise expires, 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 The Controller shall notify the Processor no later than one (1) month prior to termination of the Agreement whether the Personal Data shall be returned or deleted.
- 13.4 The Processor is entitled to delete the Personal Data thirty (30) calendar days after termination of the Agreement.
- 13.5 The Processor shall ensure that the Personal Data has been deleted no later than three (3) months after termination of the Agreement.
- 13.6 The Processor shall retain a copy of the Personal Data only if 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 the Parties.
- 14.2 This Data Processing Agreement is governed exclusively by the laws of the Netherlands.

APPENDIX 1 OVERVIEW OF PERSONAL DATA AND SUB-PROCESSORS

I. Types of Personal Data

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

II. Categories of Data Subjects

- Candidates/Applicants/Assesseees
- 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 prospective customers
- Performance of the agreement or contract

IV. Sub-processors

Name: **Salesforce.org**

Address: Prins Bernhardplein 200 1097JB Amsterdam, the Netherlands

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, the Netherlands

Description of service: Cloud services (Personnel administration, timesheet processing, financial and payroll administration)

Name: **Google Netherlands B.V.**

Address: Claude Debussylaan 34 1082 MD Amsterdam, the Netherlands

Description of service: Cloud services, generative AI and language models

Name: **Anthropic Ireland, Limited / Anthropic PBC**

Address (EEA): 6th Floor South Bank House, Barrow Street, Dublin 4, Dublin, Ireland

Address (US): 548 Market Street, PMB 90375, San Francisco, California 94104, United States

Description of service: AI systems, generative AI and language models

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

Address: Gustav Mahlerlaan 300 1022 AB Amsterdam, the Netherlands

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

Name: **Spotler Nederland BV**

Address: Boris Pasternaklaan 16 2719 DA Zoetermeer, the Netherlands

Description of service: Email processing, customer and contract administration

Name: **Textkernel BV**

Address: Nieuwendammerkade 26A-5 1022 AB Amsterdam, the Netherlands

Description of service: Processing of CV data, recruitment and selection

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.

Name: **Supabase Inc.**

Address: A Delaware corporation with offices located at 65 Chulia Street #38-02/03, OCBC Centre, Singapore 049513

Description of service: Hirewithmaia authentication and database for the processing of chat messages, logs and usage data

Name: **Veeam Software B.V.**

Address (EEA): Reykjavikstraat 1, 3543 KB, Utrecht, the Netherlands

Address (US): 3000 Carillon Point, Suite 600, Kirkland (Seattle), WA 98033, United States

Description of service: Backup software and backup cloud services

V. Duration of processing

For the duration of the Data Processing Agreement.

APPENDIX 2 SECURITY SPECIFICATION

Technical and Organisational Security Measures

A. General Information on Implemented Security Measures:

- An information security policy has been established, incorporating best practices in information security. The information security programme applies to the entire IT infrastructure and includes strict password policies, firewalls, and antivirus protection.
- Processing activities are documented, responsibilities are clearly assigned, and periodic data protection reviews are conducted to ensure compliance.
- Systems are regularly updated and patched, with up-to-date virus protection and vulnerability scans to prevent misuse.
- Employees of the Processor have signed an employment agreement that includes a confidentiality clause. Regular training on GDPR requirements, data protection best practices, and information security is provided to all employees to promote a culture of compliance.
- Personal Data is processed only when strictly necessary for the provision of specific services, and no excessive or irrelevant data is collected.
- Personal Data is processed exclusively by approved Sub-processors with whom a data processing agreement has been concluded, ensuring a level of data protection at least equivalent to that of Mysolution.
 - Google has guidelines regarding GDPR compliance:
<https://cloud.google.com/privacy/gdpr>
 - Microsoft has guidelines regarding GDPR compliance:
<https://www.microsoft.com/en-us/TrustCenter/CloudServices/Azure/GDPR>
 - Salesforce has guidelines regarding GDPR compliance:
https://help.salesforce.com/articleView?id=data_protection_and_privacy.htm
 - Snowflake has guidelines regarding GDPR compliance:
<https://www.snowflake.com/legal/>
- Personal Data is only retained for as long as necessary for the defined purpose.
- If the Processor receives Personal Data in the form of a backup for the purpose of resolving a software incident or performing a data conversion, such data is stored in an isolated network segment with access restricted to directly involved personnel. The data is immediately destroyed once its retention is no longer necessary.
- Documented business continuity plans are in place, and their effectiveness is tested annually.

B. Measures to ensure that only authorised personnel have access to Personal Data:

- The Processor operates a role-based access control and authorisation model. Only employees with the appropriate user role have access to Personal Data.
- Access to the data centre is only granted to authorised personnel.

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

- Data is stored in a European data centre that is ISO 27001 certified. The data centre is secured 24/7, both electronically and physically.
- Employees of the Processor and its Sub-processors access servers exclusively remotely and only via mandatory two-factor authentication.
- Server access logs are maintained and regularly reviewed to detect unauthorised actions.
- A robust backup system ensures the integrity and availability of data, supported by a tested disaster recovery plan.

D. Measures for detecting vulnerabilities and incident management:

- Extended Detection and Response (XDR) in combination with a 24/7 Security Operations Centre (SOC) is used to detect suspicious activity and block unauthorised access.
- Regular penetration tests are performed by external parties on the hosted web applications. Any findings are addressed and resolved within the application.
- A defined protocol for responding to data breaches is in place. Incident response includes documented procedures for identifying, investigating, and resolving security incidents and data breaches.