Contract

for Order Processing

in accordance with Art. 28 General Data Protection Regulation (GDPR)

between

we empower you GmbH

Altrottstraße 31

D-69190 Walldorf

–Contractor (Hereinafter **Processor**)–

und

Name und Contact Info of Client

–Client (Hereinafter **Controller**)–

Section 1 – General Provisions

1. Subject of the Contract

The Contract Processor provides services for the Controller in the following areas:

☐ Creating, editing, and organizing job profiles

☐ Organizing and processing of internal HR topics

based on the order / (and) the AGB / (and) the Framework Agreement executed on DATE

The Processor and its employees or persons commissioned by the processor have access to personal data and process it exclusively on behalf of and in accordance with the instructions of the Controller. The scope and purpose of data processing by the Processor are set out in the Main Contract (Framework Agreement) and in **Annex 1** to this contract. The Controller is responsible for assessing the permissibility of the data processing.

2. Contract Duration

The term of this contract shall be based on the term of the Main Contract (Framework Agreement) unless the following provisions result in obligations extending beyond the term of the main contract. Any termination rights arising from this contract shall remain unaffected by the above provision.

3. Type of Data Processed, Group of Affected Persons

As part of the performance of the services agreed in the Main Contract (Framework Agreement), the processor shall have access to the personal data specific in **Annex 1** of the affected Persons (data subjects) also specified in **Annex 1**.

4. Miscellaneous Provisions

4.1. The parties conclude this agreement to specify the mutual rights and obligations under data protection law. In case of doubt, the provisions of this agreement shall take precedence over the provisions of the main agreement.

4.2. Should the fulfillment of the subject matter of the order in accordance with Clause 1 of this Agreement be jeopardized by seizure or confiscation, by insolvency or composition proceedings or by other events or measures of third parties, the Processor shall inform the Controller immediately. The Processor shall immediately inform all parties involved in this context that the Controller has exclusive authority to dispose of the data.

4.3. Should individual parts of this Agreement be invalid, this shall not affect the validity of the remainder of this Agreement.

4.4. Any amendment to this agreement, including its termination and this clause, must be made in writing, which may also be in an electronic format.

5. Processing According to Instructions and Duty to Demonstrate

5.1. The Processor may only process personal data according to the documented instructions of the Controller – including with regard to the transfer of personal data to a third country or an international organization – unless the Processor is obliged to do so by Union or Member State law to which the Processor is subject; in such a case, the Processor shall notify the Controller of these

legal requirements prior to processing, unless the law in question prohibits such notification on grounds of important public interest.

5.2. Instructions shall generally be issued by the Controller in written form (e.g. by email). If, in exceptional cases, an instruction is given verbally, it shall be confirmed by the Processor accordingly in written form (e.g. by email).

5.3. The Processor shall inform the Controller immediately if, in its opinion, compliance with an instruction issued by the Controller violates the GDPR or another data protection regulation (obligation to remonstrate). The Processor is entitled to suspend the implementation of the instruction in question until it is confirmed or amended by the Controller. The Processor may refuse to carry out an obviously unlawful instruction.

6. Confidentiality / Secrecy Obligation

The persons employed by the Processor for data processing are prohibited from processing personal data without authorization. The Processor shall obligate all persons entrusted by it with the processing and fulfillment of this contract (hereinafter "Employees") accordingly (obligation of confidentiality, Art. 28 para. 3 subpara. 1 sentence 2 lit. b GDPR), instruct them about the special data protection obligations arising from this contract as well as existing instruction or purpose limitation and ensure compliance with the aforementioned obligation with due care. These obligations must be formulated in such way that they remain in force even after termination of this contract or the employment relationship between the employee and the Processor. Upon request, the Controller must be provided with suitable evidence of the employee's obligations.

7. Processing Security / Technical and Organizational Measures Pursuant to Art. 32 DSGVO

7.1. The Processor shall take all necessary technical and organizational measures in accordance with Article 32 GDPR. These are specified in **Annex 2**.

7.2. Technical and organizational measures are subject to technical progress and further development. During the term of this contract, the Processor shall continuously adapt them to the requirements of this contract and further develop them in line with technical progress. The security level of the technical and organizational measures specified here and in **Annex 2** may not be undercut.

7.3. The Processor undertakes to document changes to the technical and organizational measures that have a significant impact on the guaranteed security level in writing as a supplement to **Annex 2**, which may also be in an electronic format, and to notify the Controller thereof.

8. Utilization of the Services of other Data Processors

8.1. The Processor shall have the Controller's general authorization to engage sub-processors included in an agreed list. The Processor shall expressly inform the Controller in writing at least 21 days in advance of any intended changes to this list by adding or replacing sub-processors, thereby giving the Controller sufficient time to object to such changes before engaging the relevant sub-processor(s). The Processor shall provide the controller with the necessary information to enable the controller to exercise its right to object.

8.2. The Controller may only raise an objection for good cause to be proven to the Processor. If the Controller does not raise an objection within 14 days of receipt of the notification, its right of objection to the corresponding assignment shall expire. If the Controller raises an objection, the

Processor shall be entitled to terminate the Service Agreement and this Agreement as soon as possible or with at least 3 months' notice.

8.3. In general, contractual relationships with service providers that relate to the testing or maintenance of data processing procedures or systems by other bodies or other ancillary services are not subject to approval, even if access to Controller data cannot be ruled out, so long as the Processor makes appropriate arrangements to protect the confidentiality of the Controller data.

8.4. If the Processor engages a sub-processor to carry out certain processing activities (on behalf of the Controller), such engagement shall be by way of a contract which imposes on the sub-processor substantially the same data protection obligations as those applicable to the Processor under these Clauses. The Processor shall ensure that the Sub-Processor complies with the obligations to which the Processor is subject under this Agreement and Art 28 DSGVO.

9. Information/Cooperation/Support Obligations of the Processor

9.1. In the event of disruptions in the processing activities, suspected data protection violations or breaches of contractual obligations of the Processor or suspected other security-relevant incidents at the Processor, at persons employed by the Processor within the scope of the order or by third parties, the Processor shall inform the controller immediately in writing or text form. The same applies to audits of the Processor by the data protection supervisory authority that concern processing operations or circumstances relevant to the controller. The notification of a personal data breach shall contain, as far as possible, the following information:

a) A description of the nature of the personal data breach, including, where possible, the categories and number of data subject concerned, the categories concerned and the number of personal data records concerned
b) A description of the likely consequences of the breach
c) A description of the measures taken or proposed to be taken by the Processor to address the breach and, where appropriate, measures to mitigate its possible adverse effects.

9.2. The Processor shall immediately take the necessary measures to secure the data concerned and to mitigate possible adverse consequences for the data subject(s), inform the Controller thereof, request further instructions from the Controller and provide the Controller with further information at any time, insofar as the Controller's data is affected by a breach pursuant to para. 1.

9.3. If the Controller's data is jeopardized by seizure or confiscation, by insolvency or composition proceedings or by other events or measures of third parties, the Processor shall inform the Controller immediately, unless prohibited from doing so by court or official order. In this context, the Processor shall immediately inform all competent bodies that the Controller has exclusive decision-making authority over the data.

9.4. The Processor shall inform the Controller immediately of any significant changes to the security measures pursuant to **Section 7.2**.

9.5. The Processor shall keep a record of all categories of processing activities carried out on behalf of the Controller, which shall contain all information pursuant to Art. 30 para. 2 DSGVO. The list shall be made available to the Controller upon request.

9.6. The Processor shall cooperate to an appropriate extent in the preparation of the list of procedures by the controller and in the preparation of a data protection impact assessment

pursuant to Art. 35 DSGVO and, if applicable, in the prior consultation of the data protection supervisory authorities pursuant to Art. 36 DSGVO. It must provide the Controller with the necessary information in an appropriate manner.

9.7. Costs incurred by the Processor because of its support activities shall be reimbursed to the Processor to a reasonable extent.

10. Control Rights of the Controller

10.1. The Controller shall verify the technical and organizational measures of the Processor before commencing data processing and thereafter on a regular basis. For this purpose, the Controller may, for example, obtain information from the Processor, obtain existing certificates from experts, certification or internal audits or, if possible, personally inspect the Processor's technical and organizational measures or have them inspected by a competent third party during normal business hours after timely consultation, at least 14 days in advance, provided that the third party is not in a competitive relationship with the Processor. The Controller shall only carry out the checks to the extent necessary and shall not disproportionately disrupt the Processor's business operations.

10.2. If the Controller commissions a third party to carry out the review, the Controller shall oblige the third party in writing in the same way as the Controller is obliged to the Processor under **Clause 6** of this Agreement. In addition, the Controller shall oblige the third party to maintain confidentiality and secrecy, unless the third party is subject to a professional obligation of confidentiality. At the request of the Processor, the Controller must immediately submit the obligation agreements with the third party to the Processor. The Controller may not commission a competitor of the Processor to carry out the inspection.

11. International Data Transfer

11.1. Processing of Controller Data shall take place exclusively within the Federal Republic of Germany or within the EEA.

11.2. The Processor shall nevertheless be permitted to process Controller Data outside the EEA in compliance with the provisions of this Agreement if it informs the Controller in advance of the place of data processing and the requirements of Art. 44 – 48 DSGVO are met or an exception pursuant to Art. 49 DSGVO applies.

An adequate level of data protection exists, for example, with companies that are certified in accordance with the EU-US Data Privacy Framework or with companies that conclude the EU standard contractual clauses.

12. Liability

12.1. The Controller and Processor shall be liable to data subjects in accordance with the provisions of Art. 82 DSGVO.

12.2. Unless otherwise stipulated above, liability under this Agreement shall correspond to that of the Main Agreement (Framework Agreement).

13. Extraordinary Termination Rights

The Controller may terminate the main contract in whole or in part without notice if the Processor does not fulfill its obligations under this contract, intentionally or grossly negligently violates provisions of the

DSGVO or is unable or unwilling to carry out an instruction of the Controller. In the case of simple – i.e. neither intentional nor grossly negligent – violations, the Controller shall set the Processor a reasonable deadline within which the Processor can remedy the violation.

14. Deletion and Return of Personal Data

14.1. The Processor shall delete or return the Controller Data to the Controller after termination of this Agreement unless the Processor is legally obliged to continue storing the Controller Data.

14.2. The Processor may retain documentation that serves as proof of the proper processing of Controller Data in accordance with the order even after the end of the contract.

[**Place**], the [**Date**] [**Place**], the [**Date**].

_____ _____

- Contractor / Processor - *- Client / Controller -*

Annex List:

Annex 1 Scope and Purpose of Processing / Categories of Data Subjects

Annex 2 Technical and Organizational Measures According to Art. 32 DSGVO

Annex 3 Approved Subcontractor Relationships

Annex 1 – Scope and Purpose of Processing / Categories of Data Subjects

1. Types of Data Covered by the Order

In the normal course of performing the services, the Contractor receives access to personal data. Among other things, this includes:

☒ Address

☐ Billing and Payment data

☒ Age

☐ Working Time

☐ Audio Data

☐ Bank Account Details

☒ Applicant Data

☐ Image Data

☒ E-Mail-Address

☐ Health Data

☐ Hobbies

☐ Credit Card Data

☐ Customer Behavior Data

☐ Communication Data

☐ Customer History

☒ Wage and Salary Data

☐ Employee Evaluations

☒ Employee Qualifications and Characteristics

☒ Names

☐ User ID's

☐ Passwords

☒ Personal Master Data

☒ Planning and Control Data

☒ Personnel and Identification Numbers

☐ Travel Booking and Billing Data

☐ Telecommunications Billing Data

☐ Telecommunications Connection Data

☒ Telephone Numbers

☒ Contract Data

☐ Video Data

☐ Access Data

☐ Miscellaneous: [**Bitte ausführen**]

2. Categories of Data Subjects

A complete list of the categories of data subjects shall be drawn up by the client. Among others, the following categories are affected:

- ☒ Employees
- ☒ Apprentices & Interns
- ☒ Applicants
- ☒ Former Employees
- ☒ Freelance Employees
- ☐ Shareholders
- ☐ Relatives of Employees
- ☐ Customers/Clients
- ☐ Interested Potential Candidates
- ☐ Suppliers and Service Providers
- ☐ Tenants
- ☐ Business Partners
- ☐ Consultants
- ☐ Visitors
- ☐ Press Representatives
- ☐ Subscribers
- ☐ Sales Representatives
- ☐ Contact Persons
- ☐ Other: [**Bitte ausführen**]

Annex 2 –Technical and Organizational Measures

The Contractor uses the services of various professional providers specializing in the provision of servers and similar services for secure data processing. The following technical and organizational measures of the Contractor therefore consist of two sub-areas. A distinction is made between the measures taken by (contractor name) and the respective subcontractors. Both the specifications determined by the service providers and the contractually agreed measures for securing personal data are taken into account.

1. Technical and Organizational Measures of Subcontractors

As a responsible contractor, we empower you GmbH works together with professional providers of server services. They use their own technical and organizational measures. In particular, reference is made to the measures ot ensure the availability, resilience and recoverability of personal data. The contractor's personal data is stored and processed in the cloud-based CRM system of the service provider Salesforce. The data is stored and processed on servers within the EU. However, as Salesforce's headquarters are located in the USA, the transfer of data to the US authorities cannot be completely ruled out. Salesforce is certified for non-HR data in accordance with the EU-US Data Privacy Framework, so that the data transfer in this area is based on this or the adequacy decision of the EU Commission. For HR data, the legal basis is the standard of contractual clauses adopted by the EU Commission, which are processed in the order processing contract with Salesforce.

The technical and organizational measures of Salesforce listed below correspond to the current status at the time of conclusion of the contract: MONTH, YEAR.

1.1	Is the client's personal data stored on servers operated by any service providers? ☐ yes ☐ no
1.2	Which service provider stores the personal data processed here? ☐ Amazon Webservices (AWS) ☐ Heroku (salesforce) ☐ Salesforce ☐ Microsoft Azure
1.3	The following links can be used to access the technical and organizational measures of the services used at the time the contract is concluded. - Microsoft Azure: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=14

The Login and access requirements to the servers of the service providers are administered by them as follows:

Authentication Towards the Server Providers	
2.1.	Do employees authenticate themselves to the central directory service using an individual ID? ☐ yes ☐ no
2.2	Are there binding password parameters for logging in to the project-related software applications? ☐ yes ☐ no Who specifies the parameters: please specify
2.3	Password Character Length: please specify Must the password contain special characters? ☐ yes ☐ no Minimum validity period in days: please specify
2.4	Does the IT system force users to comply with the above-mentioned password requirements? ☐ yes ☐ no
2.5	What measures are taken if a password is lost, forgotten, or spied on? ☐ Admin assigns a new initial password ☐ other, specifically:
2.6	Is there a limit on unsuccessful login attempts? ☐ yes, please enter the number of attempts ☐ no
2.7	How long will access be blocked once the maximum number of unsuccessful login attempts has been reached? ☐ The accesses remain blocked until the block is manually lifted. ☐ The accesses remain blocked for: please enter the value in minutes.

Secure data transmission when accessing the servers of the service providers is guaranteed as follows:

Measures for secure data transmission between the contractor's workstations and the servers used	
3.1	Is the transfer of personal data encrypted throughout? ☐ Not at all ☐ No, data transfer takes place via MPLS ☐ Only Occasionally ☐ Via encrypted file as an email attachment ☐ via PGP / S/MIME ☐ via encrypted data carrier ☐ via VPN ☐ via https/TLS ☐ via SFTP ☐ Other: please enter
3.2	Who manages the keys or certificates? ☐ Users Themselves ☐ our own IT ☐ External Service Provider
3.3	Are the transmission processes logged? ☐ yes ☐ no
3.4	How long is this log data stored? Please enter the value in days
3.5	Are the logs evaluated regularly? ☐ yes ☐ no, but an evaluation would be possible if necessary

2. Technical and Organizational Measures of the Contractor

As the Contractor, the Contractor shall take the necessary **measures to ensure the confidentiality and integrity** of the personal data entrusted to it as follows:

Access Control Measures to the Office Premises of (Contractor Name)	
1.1	The **Main Location** (Headquarters) of the contractor is located: (Address)
1.2	Access to the office floor is controlled and is always locked.
1.3	Access to the individual offices is only possible for managing directors and project managers. Personalized access authorizations are required for this purpose.
1.4	Access to the office floor is secured via an electronic locking system.
1.5	Employees need **their cell phone for authentication** and the locking system provider's app is installed on the phone.
1.6	Access rights are personalized for each employee. The electronic locks functionally follow the company organization.
1.7	Positive access attempts are logged in the access system.
1.8	Rejected access attempts are logged.
1.9	Access logs are stored for a period of > 30 days.
1.10	Evaluations of the logs are carried out as required.
1.11	**Mechanical locks** are installed for access to the office level and the individual offices, which have been supplemented by an **electronic access system**.
1.12	Mobile phone is required for authentication against the electronic access system. This must be unlocked for access by the owner of the mobile device. Possession of the device is therefore not sufficient.
1.13	Only the management has access to the authorized keys.
1.14	The issuing of keys is logged. Keys are issued exclusively by the management.
1.15	There is a documented process for issuing electronic access authorizations and for adjusting access authorizations as required
1.16	In principle, external persons are met at the entrance by the contact person and may only move around the building/office floor if accompanied.

Company-Side Access and Access Control Measures for Project-Related Server Data	
2.1	Is there a process for assigning user IDs and access authorizations when new employees are hired and when employees leave the company or in the event of organizational changes?

	☐ Defined Approval Processes ☐ No Defined Approval Process, on Demand ☐ Other Allocation Methods: Please Specify
2.2	Are the assignment of or changes to access authorizations and project participations logged? ☐ yes ☐ no

Measures for Securing Paper Documents, Mobile Data Carriers	
3.1	Paper-based documents containing personal data are disposed of properly. Appropriate containers are available in which paper-based documents can be disposed of (data garbage cans). A specialized disposal service provider is used for this purpose.
3.2	Mobile and external data carriers used with personal data are disposed of professionally. Appropriate containers are available in which paper-based documents can be disposed of (data garbage cans). A disposal service provider specializing in this is used.
3.3	In principle, the use of USB sticks is not permitted. Only in absolutely exceptional cases and with the prior agreement and permission of the management is such use permitted. If personal data is stored on them, it must be deleted immediately after the data transfer. Only the company's own USB sticks are used. Storage is always encrypted.
3.4	Are employees allowed to use private data carriers (e.g. USB sticks)? ☐ generally, yes ☐ yes, but only after approval and verification of the storage medium by IT. ☐ no, all required storage media are provided by the company.
3.5	The storage of personal data on mobile devices is exclusively encrypted when switched off.
3.6	The processing of personal data on employee-owned devices is not permitted (bring your own device).
3.7	Inactivity on a screen for 10 minutes leads to automatic blocking of access and makes it necessary to log in again.

Administering Mobile Devices	
4.1	The mobile devices issued by the client are not administered by an MDM. Blocking and deletion access is therefore not possible.
4.2	The up-to-datedness and security of the operating systems installed on the mobile devices is not guaranteed via the MDM.

Procedure for Reviewing, Assessing, and Evaluating the Measures Taken	
5.1	A procedure is in place to regularly review, assess and evaluate the effectiveness of the technical and organizational measures to ensure the security of processing at the contractor.
5.2	Audits are carried out at regular intervals of 12 months.
5.3	The test results are documented.

The following contractual agreements have been made with the server service providers with regard to **pseudonymization and encryption**:

Agreed Requirements for the Server Providers, Contractually Defined by (Contractor Name)	
Use of Pseudonymization	
6.1	Is processed personal data pseudonymized? ☐ yes Please Specify Categories of Data ☐ no
6.2	Are Algorithms used for Pseudonymization? ☐ yes ☐ no
6.3	**If Yes:** Which Algorithm Pseudonymization? Click here to input text. .
6.4	Is the allocation data separated and stored in separate systems? ☐ yes ☐ no
6.5	How can pseudonymization be reversed if necessary? **Multiple Answers Possible!** ☐ According to a defined procedure ☐ According to the Multiple-Eye principle ☐ Direct access to non-pseudonymized raw data ☐ On the instruction of the line manager ☐ Other: please enter

Use of Encryption	
7.1	Is processed personal data encrypted in addition to the measures already described? ☐ yes Please specify categories of data. ☐ no
7.2	What types of encryption are used? **Multiple answers possible!** If multiple answers, please describe in the "other" field which type of encryption is used for which data. ☐ End-to-End Encryption ☐ Transport Encryption ☐ Data-at-Rest Encryption ☐ Other: please enter.
7.3	Which cryptographic algorithms are used for encryption or for encryption-like measures (e.g. hashing passwords)? ☐ AES ☐ SHA-256 ☐ RSA-2048 or higher ☐ Other: please enter
7.4	Who has access to the encrypted data? Employees from the departments: please enter. In total, # employees have access to the encrypted data.
Load Capacity	
8.1	Measures are in place to ensure the ability to ensure the resilience of the systems and services in connection with long term processing. ☐ no ☐ yes please enter the measures.
Recoverability	
9.1	Do emergency or recovery concepts and measures beyond B.2.11 exist that ensure the ability to quickly resotre the availability of and access to personal data in the event of a physical or technical incident? ☐ no ☐ yes please enter the measures

Annex 3 – Approved Subcontractor Relationships

Firm Sub-Contractor	Address / Country	Service
Salesforce	The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	CRM-System