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 considered.

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. 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 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 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