Data Processing Agreement
in accordance with Art. 28 of the General Data Protection Regulation ("GDPR")

between

Jobufo GmbH, Friedrichstr. 231, 10969 Berlin
- **Contractor**-

and the customer of Jobufo GmbH,
- **Client** (see offer)-

1. Technical-organizational measures

(1) The Contractor shall document the implementation of the technical and organizational measures required under the GDPR before the start of processing, in particular with regard to the specific execution of the order. These measures are the foundation of the order. As far as the examination/audit of the customer reveals a need for adaptation, this shall be implemented by mutual agreement.

(2) The precautions to be taken are data security measures and measures to ensure a level of protection appropriate to the risk with regard to confidentiality, integrity, availability and the resilience of the systems. In this context, the state of the art, the implementation costs and the nature, scope and purposes of the processing as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 (1) of the GDPR shall be taken into account.

(3) The technical and organizational measures are subject to technical progress and further development. In this respect, the contractor is permitted to implement alternative adequate measures. In doing so, the security level of the specified measures may not be undercut. Significant changes shall be documented.

(4) The Contractor undertakes to implement and further comply with all technical and organizational measures required for this order in accordance with Art. 28 Para. 3 Sentence 2 lit. c, 32 DSGVO [details in Annex 1]. The examination of the technical and organizational measures taken by the Customer shall be carried out within the scope of its control powers pursuant to Section 6 of this Agreement.

2. Correction, restriction and deletion of data

(1) The Contractor may not correct, delete or restrict the processing of the data processed under the order on its own authority, but only in accordance with documented instructions from the Customer. Insofar as a data subject contacts the Contractor directly in this regard or with regard to other data subject rights, the Contractor shall forward this request to the Customer without delay.

(2) To the extent that the Parties have agreed separately in a contract, the deletion concept, right to be forgotten, correction, data portability and information shall be ensured directly by the Contractor in accordance with the Customer's documented instructions.

3. Further obligations of the contractor

In addition to compliance with the provisions of this contract, the Contractor shall fulfill its statutory obligations under Articles 28 to 33 of the GDPR; in this respect, the Contractor shall in particular ensure compliance with the following requirements:

a) A data protection officer has been appointed who performs his duties in accordance with Art. 38 and 39 of the GDPR. This officer actively works towards compliance with all regulations relating to data protection and their fulfillment within the meaning of Art. 39 of the GDPR. In addition, he supports the further development of all topics relevant to data protection (e.g. updating of data protection training for employees). The contact details of the Contractor's data protection officer can be found in item 10 of this Agreement. The Customer shall be informed immediately of any change of data protection officer.

b) The Contractor undertakes to maintain confidentiality during processing in accordance with Art. 28 Para. 3 Sentence 2 lit. b, 29, 32 Para. 4 GDPR. When carrying out the work, the Contractor shall only use employees who have been obligated to maintain confidentiality and who have previously been familiarized with the data protection provisions relevant to them. The Contractor and any person subordinate to the Contractor who has access to personal data may process such data exclusively in accordance with the Customer's instructions, including the powers granted in this Agreement, unless they are legally obliged to process such data by EU law or the national law of the Processor.

c) The Customer and the Contractor shall cooperate with the supervisory authority in the performance of its duties upon request.

d) The Contractor shall inform the Customer without undue delay about control actions and measures of the supervisory authority, insofar as they relate to this Order. This shall also apply insofar as a competent authority investigates in the context of administrative offence or criminal proceedings with regard to the processing of personal data in the case of commissioned processing at the Contractor.

e) Insofar as the Customer, for its part, is subject to an inspection by the supervisory authority, administrative offense or criminal proceedings, the liability claim of a data subject or a third party or any other claim in connection with the commissioned processing at the Contractor, the Contractor shall support it to the best of its ability.

f) The Contractor shall regularly monitor the internal processes as well as the technical and organizational measures to ensure that the Processing in its area of responsibility is carried out in compliance with the requirements of applicable data protection law and that the protection of the rights of the data subject is ensured.

4. Subcontracting relationships

(1) Subcontracting relationships within the meaning of this regulation shall be understood to be those services which relate directly to the provision of the main service. This does not include ancillary services which the Contractor uses e.g. as telecommunications services, postal/transport services. However, the Contractor shall be obligated to enter into appropriate and legally compliant contractual agreements as well as control measures to ensure data protection and data security of the Customer's data also in the case of outsourced ancillary services.

(2) The Customer grants the Contractor general permission to use additional subcontractors, if

- a contractual agreement is made with the subcontractor in accordance with Article 28 (2-4) of the GDPR or
- the Contractor informs the Customer in text form - for example by e-mail/newsletter or via a link - if it intends to use additional subcontractors or replace subcontractors.

The Customer may object to such changes, whereby this may not be done without an important reason under data protection law. The objection to the intended change shall be raised in text form within 14 days of the provision of the information on the change to the Contractor to the contact details of the data protection officer stated below under item 10. In the event of an objection, the Contractor may, at its own discretion, provide the service without the intended change or - if the provision of the service without the intended change is unreasonable for the Contractor - discontinue the service to the Customer within 4 weeks after receipt of the objection and terminate the service agreement without notice and with immediate effect.

(3) The transfer of personal data of the Customer to the subcontractor and its initial activity shall only be permitted once all requirements for subcontracting have been met.

(4) If the subcontractor provides the agreed service outside the EU/EEA, the Contractor shall ensure the permissibility under data protection law by taking appropriate measures. The same shall apply if service providers within the meaning of Paragraph 1 Sentence 2 are to be used.

(5) Any further outsourcing by the subcontractor shall require the express consent of the Contractor (at least in text form) or a general approval of the Contractor analogous to Paragraph 2. All contractual provisions in the contractual chain shall also be imposed on the further subcontractor.

5. Data processing outside the EU/EEA

The Contractor may also transfer personal data to third parties or processors outside the EU. In this case, the contractor shall ensure on its own responsibility prior to the transfer that either an adequate level of data protection exists at the recipient (e.g. based on an adequacy decision of the EU Commission for the respective country or by agreeing on so-called EU standard contractual clauses) or that sufficient consent has been obtained from the data subjects.

6. Control rights of the customer

(1) The Customer shall have the right to carry out inspections in consultation with the Contractor or to have them carried out by inspectors to be named in individual cases. The Customer shall have the right to satisfy itself of the Contractor's compliance with this Agreement in its business operations by means of spot checks, which must generally be notified in good time (in principle at least two weeks in advance). Company and business secrets of the Contractor which become known to the Customer during an inspection shall be treated as strictly confidential by the Customer. No records of such secrets may be made unless absolutely necessary to exercise the right of inspection on the part of the Customer.

(2) The Contractor shall ensure that the Customer can satisfy itself of the Contractor's compliance with its obligations pursuant to Art. 28 GDPR. The Contractor undertakes to provide the Customer with the necessary information upon request and, in particular, to provide evidence of the implementation of the technical and organizational measures.

(3) Proof of such measures, which do not only concern the specific order, can be provided by current test certificates, reports or report excerpts from independent bodies (e.g. data protection officer, auditor, audit, IT security department, data protection auditors, quality auditors).

(4) Access to the Contractor's premises shall only be granted in the permanent presence of a representative of the Contractor. This representative shall be authorized to decide how the inspection is to proceed to the extent necessary to avoid disruptions to the Contractor's business operations and to maintain the Contractor's confidentiality obligations towards third parties.

(5) Regular on-site inspections by the customer are permitted a maximum of once per calendar year. Additional inspections by the Customer may only be carried out for an important reason to be proven by the Customer.

7. Notification of violations by the Contractor

If necessary, in particular because the relevant information is not otherwise available to the Customer, and taking into account the nature of the Processing, the Contractor shall assist the Customer in complying with the personal data security obligations set out in Articles 32 to 36 of the GDPR, data breach notification obligations, data protection impact assessments and prior consultations. This includes, but is not limited to the following:

a) Ensuring an adequate level of protection through technical and organizational measures that take into account the circumstances and purposes of the processing, as well as the predicted likelihood and severity of a potential security breach, and allow for the immediate detection of relevant breach events.

b) The obligation to report personal data breaches to the customer without undue delay.

c) The obligation to support the customer within the scope of its duty to inform the data subject and, in this context, to provide the customer with all relevant information without delay.

d) The support of the customer for its data protection impact assessment.

e) The support of the customer in the context of prior consultations with the supervisory authority.

8. Authority of the Customer to issue instructions

(1) The Customer shall confirm verbal instructions without delay (at least in text form).

(2) The Contractor shall inform the Customer without undue delay if it believes that it has identified a breach of data protection regulations. The Contractor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Customer.

9. Deletion and return of personal data

(1) Copies or duplicates of the data will not be made without the knowledge of the customer. Excluded from this are security copies, insofar as they are necessary to ensure proper data processing, as well as data required with regard to compliance with statutory retention obligations.

(2) After completion of the contractually agreed work or earlier upon request by the Customer - at the latest upon termination of the service agreement - the Contractor shall hand over to the Customer all documents, created processing and utilization results as well as data files related to the contractual relationship that have come into its possession or, after prior consent, destroy them in a manner that complies with data protection requirements, unless the legal provisions of the EU or national law require the storage of personal data.

(3) Documentation that serves as proof of orderly and proper data processing shall be kept by the Contractor beyond the end of the contract in accordance with the respective retention periods. The Contractor may hand them over to the Customer at the end of the contract to relieve the Contractor.

10. Specification of the order content, subcontractor and data protection officer

(1) Recruiting Assistant

Insofar as the Recruiting Assistant is the subject matter of the contract in the cooperation agreement on the technology partnership, the following shall apply:

Subject of the order	The subject matter of the Data Handling Order is the performance of the following tasks by the Contractor: the subject matter of the Data Handling Order Agreement (the "Order") results from the concluded Technology Partnership Cooperation Agreement between the Controller and the Processor (the "Service Agreement"). In particular, it concerns: ○ Collection and transmission of applicant data ○ Integration of this data into the existing HR systems or provision via e-mail if no HR system is available ○ Integration of the application assistant functionality (e.g., audio, video and telephone interview application) into the website of the responsible party ○ Use of a messaging tool (e.g., GutscheinUFO) to send brief messages to applicants and employees
Order duration	The duration of this order corresponds to the term of the service agreement.
Nature and purpose of the intended processing of data	The nature and purpose of the processing of personal data by the Processor for the Controller are described in the Technology Partnership Cooperation Agreement. In particular, the following applies: How does the data get to the Processor? The Client links from its website / job advertisement to the Recruiting Assistant of the Contractor. The applicant then enters his or her data (form) in the process managed by the Recruiting Assistant and is supported via various channels (phone, messenger). What does the processor do with the data? The data is processed by the contractor, stored and enriched with the information necessary for the application. Once the application is complete, the data is transferred to the customer. What do any subcontractors do? How does the data get to and from them? Essentially, only hosting providers are used as subcontractors, who only process the data as part of making the technical infrastructure available. How does the data get back to the controller after processing? The data is transferred electronically to the customer's HR systems. If there is no HR system, the data is transmitted by e-mail.

Categories of affected persons	The categories of data subjects affected by the processing include: ○ Applicants ○ Contact persons of the customer ○ Other contact persons (e.g. service providers of the customer) ○ Employees of the contractor
Type of data	The subject of the processing of personal data are the following types/categories of data: ○ General personal data of applicants: name, gender, age, address, e-mail, phone number ○ Candidate data: Curriculum vitae, references, assessment of the candidate, audio and/or video application of the applicants ○ Contact person/employee : name, professional e-mail and phone number
Subcontractors used	1. Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA, Provision of the server structure, exclusive server location: Netherlands (as a safeguard, however, additionally conclusion of standard contractual clauses & as additional mitigation: encryption of all data on the servers with AES-256, RSA-2048) 2. SendGrid, 1801 California St, Denver, CO, USA, Sending applications by e-mail in the absence of an Applicant Tracking System (third-country transfer: conclusion of standard contractual clauses) 3. When using WhatsApp for Business: Smooch Technologies ULC, Level 12, 5333 Avenue Casgrain, Montreal, Canada H2T 1X3 (Third-country transfer: Adequacy decision for Canada)

(2) Mega-Apply.ai

To the extent that Mega-Apply.ai is the subject matter of the contract in the Technology Partnership Cooperation Agreement, the following shall apply:

Subject of the order	The subject matter of the Commissioned Processing Agreement (the "Order") is derived from the Technology Partnership Cooperation Agreement between the Customer and the Contractor (the "Service Agreement"). In particular, it concerns: ○ Receipt from job advertisements of the Customer in online application platforms and transmission of data of applicants* to the Customer (surname, first name, date of birth, gender, contact data such as e-mail/telephone number, cover letter, CV, attachments and other data relevant to the application) ○ Integration of this data into existing HR systems or provision by e-mail if no HR system is available

Order duration	The duration of this order corresponds to the term of the service agreement.
Nature and purpose of the intended processing of data	The type and purpose of the processing of personal data by the processor for the controller are specifically described in the service agreement. How does the data get to the processor? The contractor extracts the data of applicants* from job advertisements of the customer in online application platforms. What does the processor do with the data? The contractor transfers the data to the customer. What do any subcontractors do? How does the data get to them and back? Only hosting providers are used as subcontractors, who only process the data in the context of providing the technical infrastructure. How does the data get back to the responsible party after processing? The data is transferred electronically to the customer's HR systems.
Categories of affected persons	The categories of data subjects affected by the processing include: ○ Applicants
Type of data	The subject of the processing of personal data are the following types/categories of data: ○ General personal data of applicants: name, gender, age, address, e-mail, phone number ○ Applicant data: Curriculum vitae, certificates, assessment of the candidate, audio and/or video application of the applicants
Subcontractors used	1. Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA, Provision of the server structure, exclusive server location: Netherlands (as a safeguard, however, additionally conclusion of standard contractual clauses & as additional mitigation: encryption of all data on the servers with AES-256, RSA-2048) 2. SendGrid, 1801 California St, Denver, CO, USA, Sending applications by e-mail in the absence of an Applicant Tracking System (third-country transfer: conclusion of standard contractual clauses)

The Contractor's **data protection officer** is Mr. **Asmus Eggert**, **lawyer**, mip Consult GmbH, Wilhelm-Kabus-Str. 9, 10829 Berlin, 030-2088999-0, a.eggert@mip-consult.de

Place, Date: see offer
Client

See Offer_____________________
(Signature of the person responsible)

See Offer_____________________
(Name in capital letters)

Place, Date: Berlin, 27. Oktober 2021
Contractor

Th. Paucker
____
(Signature of the processor)

Thomas Paucker_______________
(Name in capital letters)

Annex to the Data Processing Agreement - Technical-organizational measures

- Description of the Contractor's technical and organizational measures for the adequate protection of the Customer's data in accordance with Art. 32 GDPR -

The technical and organizational measures shall ensure the resilience, integrity pseudonymization, availability, encryption, confidentiality and recoverability of the systems and services of Jobufo and its subcontractors in connection with this DP Agreement.

In addition to this, the customer is responsible for the development and implementation of its own suitable measures in accordance with Art. 24 GDPR. Corresponding guidelines, such as ISO 27002, should be requested from the Federal Office for Information Security by the customer and adhered to.

1. Confidentiality (Art. 32 para. 1 lit. b GDPR)

1.1 Entry control

Measures to prevent unauthorized persons from accessing data processing systems with which the personal data are processed and used.

- Security zones and their physical protection are defined and documented in a security zone concept for all relevant sites and can be presented on request. Content-related points of the concept are, for example: supervision of external persons within the security zones, controlled access allocation, use of GDPR-compliant server structures according to ISO 27001, etc.).
- The defined safety zone concept is implemented for all relevant sites.
- The security zone concept is reviewed at least 1x per year.
- The security zones for all relevant sites are protected by physical barriers (fence, solid walls, doors, access control system, intrusion alarm system, etc.) to ensure access for authorized persons only. Visitors to security zones are escorted by authorized personnel.
- There is a documented and effective procedure for granting, changing and withdrawing access rights, including the return of access equipment. This assignment is carried out according to the "need-to-know" principle.

1.2 Admission control

Measures to prevent data processing systems from being used by unauthorized persons.

- There is a documented and effective access control concept, including network security zones and network segmentation.
- The access control concept defines the assignment, modification and revocation of access rights as well as their release for internal and external employees.
- Every connection is established exclusively via encrypted protocols such as HTTPS, SSL/TLS, SSH or protocols of a similar or higher security standard.

- The processes for granting, changing, and revoking access rights, as well as their release, are logged in a traceable manner.

- The access control concept is reviewed at least twice a year by the Contractor's data protection officer.

- Each user ID is clearly assigned to a natural person at all times and may not be passed on or shared.

- Secure passwords are used. Structure and handling are carried out in accordance with a documented password guideline, which provides exclusively for 2-factor authentication for all employees for all systems. The self-selected password must comply with the recommendations of the German Federal Office for Information Security (min. 8 characters, use of all available characters including upper and lower case, digits and special characters).

- Default passwords of systems and applications (e.g. Oracle, SAP) are always changed.

- It is ensured that initial passwords become unusable for users after a short period of time if they have not been changed immediately.

- Passwords may only be reset or changed by authorized persons in accordance with a defined process.

- Administrators use separate accesses for managing systems and their privileged activities are logged.

- The delegation of rights (substitution regulation) takes place exclusively in accordance with defined specifications.

- All employees are instructed to lock their workstations when they leave. By default, workstations are configured with automatic locking.

- All access to systems (applications, operating systems, BIOS, boot devices, etc.) is password protected or locked.

- Employee devices are automatically locked when inactive or unused for 10 minutes. All employees are instructed to lock all devices immediately when leaving the workplace. Further details can be found in the data protection training.

- External access (remote access) is secured via a firewall, using strong encryption and 2-factor authentication.

1.3 Access control

Measures to ensure that authorized persons can only access the data subject to their access authorization and that personal data cannot be read, copied, modified or removed without authorization during processing, use and storage.

- It is ensured that only those access rights are assigned that are required to fulfill the respective task.

- The allocation and release of access rights is documented in a comprehensible manner so that it can be determined who has access to the data.

- The allocation procedure and access rights are regularly checked and confirmed. Access rights are revoked immediately if they are no longer required.
- A responsible person is defined for all data, who decides who may have which access.
- Access rights are adjusted if the tasks in the business processes change.
- In the applications, it is ensured that the assigned access rights are technically implemented.
- Unauthorized access is excluded in all environments that contain production data (including development, testing, etc.).

1.4 Disconnection control
Measures to ensure that data collected for different purposes can be processed separately.

- Data collected for different purposes is separated (physically or logically) so that it is processed, stored and deleted separately according to the purpose (roles and authorization concept). This applies to all systems used by the Contractor.
- Development, test and production environments are separated.

1.5 Pseudonymization (Art. 32 Para. 1 lit. a GDPR; Art. 25 Para. 1 GDPR)

- Where appropriate, processing is carried out with pseudonymized data.
- Personal data is then processed in such a way that the data can no longer be attributed to a specific data subject without the use of additional information.

2. Integrity (Art. 32 para. 1 lit. b GDPR)

2.1 Transport and transfer control
Measures to ensure that personal data cannot be read, copied, altered, or removed without authorization during electronic transmission, its storage on data media, or during its transport, and that it is possible to determine to which entities personal data is intended to be transmitted by data transmission equipment.

- Data is secured during transport, storage, transmission and processing outside the protected area of the company using procedures such as strong encryption, two-factor authentication (e.g. hard disk encryption).
- Information handling instructions are established and employees are trained to prevent misuse of data (e.g., certified disposal of paper and media, selection of transmission methods, encryption of all media prior to official use). In particular, guidelines on telecommuting in the remote office and on the use of the Internet, IT and communication media in compliance with data protection requirements are provided here. The relevant instructions and training will be provided before the official start of work, but no later than on the first working day. The obligation to comply with all instructions is confirmed in writing by the employees. The same applies to cooperation with external employees (e.g. freelancers), who also sign a non-disclosure agreement.

- Cryptographic keys to protect data are securely managed in an appropriate management system.

- The contractor uses a REST API to implement an exchange of data. We secure all communication between the systems from our partners and us using two encryptions: RSA (2048 bit) and AES-256, where we assign different roles to always keep accesses to a minimum. This applies to the transmission of all data mentioned in this document.

2.2 Input control
Measures to ensure that it can be determined retrospectively whether and by whom personal data has been entered into systems, modified or removed.

- The following events are logged (system or otherwise):
    - General personal data: Last name, first name, gender, age, audio, video, resume, credentials, candidate assessment
    - Logging in and out
    - Configuration changes
    - Password changes
    - Creation, modification and deletion of accounts and groups
    - Protocol configuration changes
    - Activation and deactivation of security software such as virus scanner or local firewall
    - Changes to personal data in applications

- The degree of monitoring of system and network resources is determined according to the risk. Relevant legal aspects are taken into account.

- Log systems and logging information are protected from unauthorized access, modification, and deletion and are regularly evaluated.

- Clocks of all critical systems are synchronized with a reliable and agreed time server.

2.3 Order control
Measures to ensure that personal data processed on behalf of the customer can only be processed in accordance with the customer's instructions:
No commissioned data processing within the meaning of Art. 28 GDPR without corresponding instructions from the customer, e.g.: Clear contract design, formalized order management, strict selection of the service provider, prior conviction obligation, follow-up checks.

- Formal agreements on the exchange of information between the above-mentioned contracting parties exist, which take into account the security of the data.

- Before commissioned processing is commenced, a legally binding agreement is concluded with each service provider on how information/data is to be handled.

- Before contracting external service providers, an assessment is made regarding their reputation, qualifications, software, hardware, human and financial resources and security aspects in relation to their future tasks.

- Compliance with contracts is monitored by regular checks on contract execution. In the event of deviations, the defined contacts for information security / data protection are involved and, if necessary, the contract or contract execution is adjusted.

- In the event of termination without notice, additional measures are taken to prevent intentional misuse of infrastructure or data by the external service provider (e.g., by blocking access).

- Instructors on the part of the customer or recipients of instructions on the part of the contractor are known by name (or as a role).

3. Availability, incl. resilience and recoverability (Art. 32 (1) lit. b+c GDPR)
Measures to ensure that personal data is protected against accidental destruction or loss.

- Protective measures (UPS, backup power supply, fire extinguishers, fire detection, etc.) against elementary hazards - especially fire, water, failure of supply networks, denial of service - are in place.

- Data is processed in physically protected areas, and the measures taken to secure the area are documented and regularly checked.

- Equipment to supply data processing systems is regularly maintained.

- Utilization of (system) resources is monitored and adjusted as necessary to ensure adequate system capacity.

- Up-to-date protection against malware, zero-day exploits or malicious behavior of software is installed on all information systems, centrally managed and kept up to date.

- Server systems are operated in secure environments (e.g., server rooms or data centers) and installation in offices is prevented.

- Data is backed up in such a way that it can be restored in a defined time, separated according to its purpose.

- When backing up data, the scope, frequency, type (full, differential, incremental), time frame, encryption and physically separate storage are taken into account and documented in a traceable manner.

- Whenever the backup procedure is changed, the recoverability of the data from the backup is verified.

- Redundancies that have been set up (e.g., RAID, clusters, load balancers) are regularly checked for functionality if they are not in continuous operation. Checks that have been performed are documented.

4. Procedures for periodic review, assessment and evaluation (Art. 32(1)(d) GDPR)
Measures to ensure that data protection requirements are implemented and that they are verifiable (data protection management).

- Relevant internal and external employees are instructed in and committed to data protection.
- Internal and external employees are trained for processing activities/applications and made aware of the consequences of data protection violations.
- Employee exit procedures ensure that security breaches are avoided and equipment provided is returned.
- Equipment is disposed of in a manner that prevents reconstruction of data.
- IT operating procedures (e.g., user management, backup, network management) are documented in a traceable manner, reviewed regularly, and modified as needed.
- All changes are handled as part of a comprehensibly documented change management process.
- The risk of data mishaps is reduced by separating responsibilities (e.g., system administration separate from data administration).
- Identification, provision and testing of updates are part of regular operations.
- Security functions of systems and applications are configured and activated.
- A set of rules for information security and data protection exists.
- The rules and regulations for information security and data protection and the security measures are regularly checked for compliance and effectiveness.
- There is a system and software development guideline that includes data protection aspects.

5. Incident-Response-Management
Measures to ensure that data breaches are quickly identified and reported.

- A process aligned to best practices (ITIL) is in place to ensure that security incidents are identified, assessed, and handled appropriately.
- Escalation procedures and organizational interfaces are defined with all relevant parties, and the data protection officer is involved without delay.
- All information security incidents that go beyond a typical minor disruption in day-to-day business are reported immediately to defined bodies without further review.
- Employees responsible for managing IT systems / applications are trained to recognize, classify and report security incidents.
- A process is established to ensure information security for all critical business processes even during a crisis or disaster..
- Processes and responsibilities are defined for an emergency / crisis and appropriate exercises are held.

6. Privacy-friendly technology design and default settings (Art. 25 GDPR)
Measures to ensure that privacy by design and by default are considered.

- Part of a new or to be changed data processing operation is an assessment of the risks of the data subjects and, depending on this, the identification and realization of technical and organizational security measures. Consideration is given at an early stage to ensuring compliance with data protection principles such as data minimization, integrity, accuracy of data processing, storage limitation, transparency, processing in good faith and purpose limitation.

- Before a new or modified data processing operation goes into production, an acceptance test is carried out to check whether data protection is ensured by means of appropriate default settings. This is carried out by the data protection officer and the technical manager.