Annex 1: Data Processing Agreement pursuant to Art. 28 GDPR

between the controller	and the processor
CLIENT (Company)	softgarden e-recruiting GmbH Tauentzienstraße 14 10789 Berlin
- hereinafter referred to as "**Client**"	- hereinafter referred to as "**Contractor**" -

hereinafter jointly referred to as the **Contracting Parties.**

The contractor offers the client services relating to the electronic administration and processing of applications via an applicant management system (software as a service) and hosts the applicant data stored in the applicant management system on behalf of the client for this purpose.

§ 1 General

1. Within the scope of the existing service contract between the Parties (hereinafter referred to as "Main Contract"), it is necessary that the Contractor, as a processor within the meaning of Article 4 No. 8 of the Data Protection Regulation, processes personal data for which the Client is the controller within the meaning of Article 4 No. 7 of the Data Protection Regulation (hereinafter referred to as "**Client Data**"). This agreement specifies the rights and obligations of the parties under data protection law in connection with the Contractor's processing of Client Data for the performance of the main contract. In the event of any contradictions, the provisions of this agreement with all its components shall take precedence over the provisions of the associated main contract.
2. Insofar as the term "data processing" is used in this Agreement, this shall be based on the definition of "processing" within the meaning of Art. 4 No. 2 of the GDPR.

§ 2 Subject matter and duration of processing

1. The subject matter of this Agreement is the processing of personal Client Data by the Contractor in connection with the use of the Recruiting and Applicant Management System as Software as a Service (SaaS) by the Client.
2. The Contractor shall process the personal Client Data on behalf of and only in accordance with the Client's instructions for the duration of the Main Contract. The nature and purpose of the processing as well as the type of personal data and the categories of data subjects are set out in **Appendix 1.**
3. The term of this agreement on data processing on behalf is based on the term of the associated main contract (service agreements).

§ 3 Rights of the Client to issue instructions

1. The Client has the right to issue instructions to the Contractor regarding the type, scope and procedure of data processing. Verbal instructions shall be confirmed by the Client in text form (at least by e-mail/ticket) without undue delay.

2. The Contractor shall be obliged to carry out the Client's instructions without undue delay or, if applicable, within a reasonable period of time determined by the Client. Doing so, the Contractor shall in particular correct, delete or block personal data without undue delay upon the Client's instructions and confirm this in writing upon request.
3. The Contractor shall inform the Client without undue delay if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions. The Contractor shall be entitled, without acknowledging any obligation to check whether an unlawful instruction exists, to reject or suspend an instruction which it considers to be unlawful until it is confirmed or amended by the Client or to reject obviously unlawful instructions at any time or to suspend processing operations relating thereto.
4. To the extent that the Contractor is required by Union or Member State law to which the Contractor is subject to process the personal data even without instructions from the Client, the Contractor shall inform the Client of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.
5. The Client undertakes to give instructions only to persons authorised to give instructions. The Contractor shall be entitled to assume a corresponding authorisation to issue instructions in the case of instructions issued by the Client.
6. The Contractor shall designate the Client Service and Support department as the authorised recipient of instructions, contact: support@softgarden.de. Employees of the department as well as department managers of the Contractor are authorised to receive instructions.

§ 4 Obligations of the Client

1. As the controller within the meaning of Article 4 No. 7 of the GDPR, the client is responsible for the lawfulness of the processing of Client Data as well as for the protection of the rights of the data subjects resulting from Articles 12 to 23 of the GDPR.
2. The Client is responsible as the controller, in the context of the processing carried out by the Contractor on behalf of the Client, for the notification and communication in the event of a personal data breach, Art. 33 and 34 GDPR.
3. The Client is obliged to treat all knowledge of the Contractor's trade and business secrets (in particular with regard to technical and organisational data security measures) obtained within the framework of the contractual relationship as strictly confidential. This obligation shall remain in force even after termination of this contract.

§ 5 Obligations of the Contractor

1. Insofar as a data subject directly contacts the Contractor in exercising its rights under Chapter 3 of the GDPR (Art. 12 to 23 GDPR), taking into account Part 2, Chapter 2 of the Federal Data Protection Act (Sections 32 to 37 ‘BDSG’), the Contractor shall immediately forward this request to the Client. The Contractor shall support the Client in the fulfilment of data subject rights to the best of its ability, in particular in accordance with the Client's instructions and by means of suitable technical and organisational measures.
2. The Contractor shall support the Client in complying with the obligations set out in Articles 32 to 36 of the GDPR, taking into account the nature of the processing and the information available to the Contractor.
3. If the Contractor becomes aware of a personal data breach within the meaning of Art. 4 No. 12 of the GDPR ("data protection incident") with regard to the processed Client Data, it shall report this to the Controller without undue delay. Within the scope of the notification pursuant to Art. 33 (2) GDPR, the Contractor shall inform the Client, if possible, of the time, type and extent of the incident, the IT system affected, the affected data subjects, the time of discovery, all conceivable adverse consequences of the data security incident and the measures taken as a result.
4. The Contractor shall inform the Client without undue delay if a supervisory authority takes action against the Contractor pursuant to Art. 58 of the GDPR concerning a processing operation that the Contractor performs on behalf of the Client.

§ 6 Obligation to notify in the event of disclosure

1. The Contractor shall inform the Client without undue delay of any request or demand for disclosure of information of any kind by law enforcement agencies and other governmental authorities, insofar as such information is related to the agreements concluded between the Client and the Contractor ("**Duty of Notification**").

1. The Client shall be solely responsible for the decision on and the procedure for the disclosure of affected Client Data to governmental authorities and shall be supported by the Contractor in the disclosure to the best of its ability.

2. The Contractor shall only be exempt from the obligation to notify the Client if the Contractor itself is obliged to disclose to state authorities as well as to maintain secrecy towards the Client.

§ 7 Control rights of the Client

1. The Contractor shall grant the Client a right to control the data processing and compliance with this Agreement or the respective project order. In particular, the Contractor shall provide the Client with all information necessary to prove compliance with the obligations set out in this contract and shall enable the performance of audits, including inspections. The audits may also be carried out by a third party bound to secrecy, provided that the third party is not a competitor of the contractor.

2. The Parties agree that the Client shall conduct an audit pursuant to Paragraph 1 by instructing the Contractor to submit, at its option, a suitable attestation, report or report extracts from independent bodies (e.g. auditor, audit, data protection officer, information security officer, data protection auditor or quality auditor) or a suitable certification by an IT security or data protection audit - e.g. in accordance with ISO 27001 or “BSI-Grundschutz” - ("audit report"). In justified exceptions, the Client may conduct independent inspections.

3. The Contractor undertakes to support the performance of the audits. This includes the granting of all required access, information and inspection rights. The same applies to public inspections by the competent supervisory authority in accordance with the applicable data protection regulations.

4. In the event of independent inspections by the Client at the Contractor's premises, each party shall bear the costs incurred by the inspection, such as inspection, personnel and travel costs. Insofar as the Contractor's involvement in connection with inspections exceeds the required maximum of three (3) man-days and this is associated with a higher inspection effort or the commissioning of external service providers by the Contractor, the costs incurred for this may be invoiced to the Client in accordance with the hourly and daily rates customary in the industry.

§ 8 Subcontracting relationships

1. The Contractor may establish subcontracting relationships with further processors (subcontractors). The Contractor currently employs the subcontractors listed in **Appendix 1.** The Client agrees to their engagement.

2. The Contractor shall always inform the Client in text form or a suitable electronic form of any intended change with regard to the use or substitution of subcontractors, which shall give the Client the opportunity to object to such changes within 14 calendar days, whereby this may not be done without good cause under data protection law. In the event of a justified 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 not reasonable for the Contractor - stop the service towards the Client within two (2) weeks after receipt of the objection and terminate the main contract without notice and with immediate effect. This shall not affect the Client's extraordinary right of termination for good cause.

3. The contractor shall ensure that the data protection obligations agreed in this contract also apply to the subcontractor and, pursuant to Article 28 (4) of the GDPR, shall oblige the subcontractor accordingly by way of a contract or other legal instrument in accordance with Union law or the law of the Member State concerned prior to the start of the activities, whereby in particular sufficient guarantees must be provided that the appropriate technical and organisational measures are implemented in such a way that the processing is carried out in accordance with the requirements of the GDPR.

4. If the engagement of a subcontractor is associated with a transfer of the client data to a country outside the European Union (EU) or the European Economic Area (EEA) ("third country"), the provisions of Section 9 shall also apply.
5. Services of third-party providers that can be booked via the so-called Marketplace of the Contractor and - as far as possible - also individually booked and integrated into the system by the Contractor on behalf of the Client shall - unless otherwise agreed - not become subcontractors of the Contractor and shall not establish any duty of inspection of the Contractor under data protection law.

§ 9 Transfer of client data to third countries

1. The provision of the contractually agreed data processing within the scope of the provision of the recruiting and applicant management system generally takes place in member states of the European Union (EU) or the European Economic Area (EEA).
2. Any transfer of client data to a country outside the EU/EEA ("**third country**") may only take place if the special requirements of Art. 44 et seq. GDPR are fulfilled.

§ 10 Confidentiality obligation

1. When processing personal data on behalf of the Client, the Contractor is obliged to maintain the confidentiality of personal data that it processes and/or comes to know in connection with the Service Agreements.
2. The Contractor shall ensure that the persons authorised to process the personal Client Data have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality.

§ 11 Technical and organisational measures

1. The Contractor commits itself towards the Client to guarantee technical and organisational measures that are necessary to comply with the applicable data protection regulations. This includes, in particular, the requirements of Article 32 of the GDPR. The contractor shall regularly review, assess and evaluate the effectiveness of the technical and organisational measures to ensure the security of the processing and document the results.
2. The implemented technical and organisational measures at the time of the conclusion of the contract can be found in **Appendix 2** to this agreement. The contracting parties agree that changes to the technical and organisational measures may be necessary in order to adapt to technical and legal circumstances. Changes to the technical and organisational measures must not lead to a lowering of the existing level of protection. The contractor shall document significant changes to the measures taken.
3. The Contractor shall publish and regularly update the current technical and organisational measures as well as the evidence of compliance with technical and organisational measures on its website, insofar as these are designated for publication at its reasonable discretion and/or due to another obligation of the Contractor.

§ 12 Obligations of the contractor after termination

1. After termination of the service agreements or earlier upon request by the Client - but at the latest upon termination of the service agreements - the Contractor shall, at the Client's discretion and on the Client's instructions, delete or return to the Client all documents, data and created processing or utilisation results as well as data files related to the contractual relationship that have come into its possession and delete existing copies, unless there is an obligation to store the personal data under Union law or the law of the Member States. The same applies to test and committee material.
2. Documentation and protocols that serve as proof of orderly and proper data processing or legal retention periods shall be retained beyond the end of the contract in accordance with the respective retention periods.

§ 13 Special provisions for entities of the church

1. Insofar as the Client is an entity of the church subject to the provisions of the “Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland” (EKD Data Protection Act), the Contractor submits to the church data protection supervision in addition to the provisions of this Data Processing Agreement pursuant to Section 30 (5) sentence 3 EKD-Datenschutzgesetz. The submission extends to the tasks and powers of the Church's data protection supervision pursuant to Sections 43, 44 EKD Data Protection Act.
2. Insofar as the Client is an entity of the church subject to the provisions of the “Gesetz über den Kirchlichen Datenschutz” (KDG), the Parties expressly include the application of the KDG, in particular Sections 29 and 31 KDG, as well as compliance with the provisions made therein in this Agreement.

§ 14 Term and termination

The term and termination of this contract are governed by the provisions on the term and termination of the main contract. Termination of the main contract automatically results in termination of this contract. An isolated termination of this contract is excluded.

§ 15 Liability and compensation

1. The client and the contractor shall be liable towards data subjects in accordance with the provision set out in Article 82 of the GDPR.
2. If a data subject asserts claims for damages against one of the contracting parties due to a breach of data protection provisions, the party subject to the claim shall inform the other party thereof without delay.
3. The parties shall support each other in the defence of claims for damages by data subjects unless this would endanger the legal position of one party in relation to the other party or the supervisory authority.

§ 16 Final provisions

1. This Data Processing Agreement is valid without a separate signature upon conclusion of the main contract.
2. This Data Processing Agreement supersedes any prior agreements, contracts or notices between the Client and the Contractor in relation to the processing of Personal Data on behalf of the Client.
3. In the event of any contradictions, the provisions of this contract with all its components shall take precedence over the provisions of the associated main contract.
4. In the event of conflicts between different language versions of this Agreement, the German version shall prevail.
5. If any provision of this agreement should be or become invalid, this shall not affect the validity of the remainder of the agreement.
6. The Appendices 1 and 2 attached to this commissioned processing agreement form an integral part thereof.
7. The contractual relationship and its performance shall be governed exclusively by the laws of the Federal Republic of Germany. For all disputes arising from or in connection with this contract, the agreement on the place of jurisdiction of the main contract shall apply - as far as permissible.

Appendix 1: Specification of the data processing

Appendix 2: Technical and organisational measures

	27.03.2026
Place, date	Place, date
	Christian Heuermann Sophia Jenkner
Client Name / Signature / company	Contractors softgarden e-recruiting GmbH softgarden e-recruiting GmbH

Appendix 1 to the Data Processing Agreement

Specification of the data processing

1. Subject of the processing:

The subject of the agreement is the processing of personal data by the recruiting and applicant management software, including the booked product components and ancillary processing in the broadest sense, which are processed on behalf of the client.

2. Nature and purpose of the processing:

The Contractor shall make the recruiting and applicant management software available to the Client and shall have access to the personal data processed by the Client within the scope of this.

Within the scope of the recruiting and applicant management software, the following data processing takes place in particular:

- Structured recording and collection of applicant data,
- Structured presentation of applicant data,
- Communication of applicants, recruiters and HR managers,
- Implementation and communication of and with third parties and cooperation partners,
- Evaluation of applicant data in the form of reporting,
- Provision of application status information to connected job boards,
- Provision of a talent pool,
- Processing of employee data as part of the onboarding process (applies if the Onboarding Software is used)
- Request feedback from applicants and employees recruited via the software.
- If contractually agreed with the job board portal, forwarding of the quality signal of the application

The Client itself determines which additional service modules are used via the Marketplace or the Contractor's optional services. Depending on the scope of services, data processing may therefore take place for purposes other than those mentioned above.

Categories of data subjects

The Client determines which data are processed of which groups of data subjects.

Usually, the following groups of data subjects are affected by the data processing:

- Applicants of the Client
- Recruiters, employees and personnel managers of the Client
- Jobseekers and prospective job applicants

Categories of personal data

The Client determines which data are processed of which groups of data subjects.

Typically, the following categories of personal data of applicants may be processed:

- Personal details:

  Salutation, academic degree, first name, last name, nationality, date of birth

- Contact and address details:
  Street, house number, postcode, city, country, state, telephone number, fax, e-mail address
- Application data:
  Application photo, cover letter, CV, work experience/work references, (university) certificates and other qualifications, driving licence class, willingness to travel
- Account and log data:
  Applicant account, user ID, IP address, log files, status of application
- Usage data, if personal:
  Email content, invitations, feedbacks, ratings
- Special categories of personal data within the meaning of Art. 9 GDPR:
  Insofar as stated/consented, an inference is possible or necessary for factual reasons: ethnic origin, political opinion/party affiliation, trade union membership, religious or ideological conviction, genetic/biometric data (e.g. application photo), health data (e.g. information on pregnancy, information on a disability or health restrictions), information on sexual orientation (e.g. sex/gender, homosexuality)

Typically, the following categories of personal data may be processed by recruiters, employees and HR managers:

- Personal details:
  Salutation, academic degree, first name, last name, function level, company
- Contact and address data:
  Company headquarters, telephone number, fax, e-mail address
- Account and log data:
  User ID, IP address, log files, role, logging of processing within the system
- Usage data:
  Comments, email content, invitations, feedbacks, ratings

Data processing locations

Processing on behalf takes place at the following locations:

softgarden e-recruiting GmbH (business premises of the Contractor)

Location Berlin: Tauentzienstraße 14, 10789 Berlin

Location Saarbrücken: Europaallee 29, 66113 Saarbrücken

WIIT AG (formerly myLoc managed IT AG), Am Gatherhof 44 40472 Düsseldorf (headquarter)

Locations of the service provider: Am Gatherhof 44 40472 Düsseldorf (data center D1)

Equinix Germany GmbH, Rebstöcker Straße 33, 60326 Frankfurt (headquarter)

Kruppstraße, 60388 Frankfurt am Main (data centre)

Location of the service provider: Kruppstraße 121-127, 60388 Frankfurt am Main (data center FR2)

Location of the service provider: Albertstr. 27, 40233 Düsseldorf (data center DU1)

Persons of the Contractor receiving instructions

The following persons of the Contractor are authorised to accept instructions from the Client: Client Service Team: support@softgarden.de

Data Protection Officer of the Contractor

Die Datenschutzkanzlei, Herr David Oberbeck, Hallerstraße 76, 20146 Hamburg;
Tel.: +49 40 226 34 56 0; E-Mail: datenschutzbeauftragter@softgarden.de.

Appointed subcontractors

The confirmation of the use of subcontractors, or of optional and/or free services, is usually carried out via the recruiting system by means of a so-called "opt-in procedure" of the user. In order not to make the provision and use of the software dependent on third-party services, the Contractor will also offer the Client the option of implementing third-party services in the system on behalf of the Client, which can be booked in particular via the Contractor's *Marketplace* and - where possible - also individually.

The following subcontractors will be used at the time of the conclusion of the contract:

Name and address of the subcontractor	Order content
WIIT AG (formerly myLoc managed IT AG) Am Gatherhof 44 40472 Düsseldorf	Colocation and Managed Services Rack rental and provision of • Redundant firewalls and load balancers • Redundant power supply by means of emergency generator, UPS (n+1 redundancy) and A/B feed in the server racks • Multiple redundant IP connections and redundant network infrastructure • Separate backup and administration networks • redundant, energy-efficient cooling (n+1 redundancy) • dedicated servers • SSL certificates • Replacement of defective server hardware • Other support activities for all server systems (e.g. within the framework of proactive monitoring)
Equinix (Germany) GmbH Rebstücker Street 33 60326 Frankfurt am Main	See above: Additional colocation and managed services as described above. Server location is Kruppstraße, Frankfurt, Germany
Cloudflare Inc., 101 Townsend St, San Francisco, CA 94107, USA; Cloudflare Germany GmbH, Rosenthal 7, c/o Mindspace, 80331 Munich, Germany	DDoS-protection/WAF. • Data Localisation Suite with "Regional Services" and "Metadata Boundary for Customers" to ensure data localization in Germany. • "Regional Services" ensure that end customer content traffic is securely transmitted to Cloudflare PoPs within the

	region selected by softgarden and inspected within a Point of Presence (‚PoP') in that defined region (decrypting that content for inspection and then re-encrypting it). softgarden has chosen Germany as the selected region, therefore all end customer traffic is inspected exclusively on servers in Germany and end customer traffic is not inspected outside of Germany. Metadata Boundary ensures that Cloudflare does not transmit customer logs originating from covered services outside the European Union.

The following subcontractors will be used at the time of the conclusion of the contract, provided that **optional** additional products are activated:

Textkernel B.V. Nieuwendammerkade 26a5 NL-1022 AB Amsterdam (Server location Germany)	CV parsing (optional opt-in) • Convert uploaded CVs into structured form • Maintenance and support services for the CV parsing service
Cronofy B.V. Mr. Treublaan 7, 1097 DP Amsterdam, The Netherlands (Server location Germany)	Calendar integration (optional opt-in) • to arrange meetings, appointments and tasks • Processing of calendar structures and events
360 Dialog GmbH Tölzer Straße 1 82031 Grünwald Germany (Server location Frankfurt, Germany and Dublin, Ireland)	Product 'Recruiting via text message' by using the product 'Unified Messaging API' from MessengerPeople GmbH. Sending an application to WhatsApp, Telegram or Facebook Messenger, if this has been booked (optional module); use of messenger communication. MessengerPeople processes the personal data stored by applicants with the respective messenger service, in particular first and last name, end device, profile picture, in order to provide the service. In addition, the messages transmitted via the messenger service are transferred to the recruiting system via the API.

If you have ordered our products and services via direct purchase on our website, the above-mentioned optional additional products are **activated by default**. You have the option to deactivate selected additional options at any time. Please contact our support team for assistance.

For customers who purchase our services through our sales department, the optional additional services are still **deactivated by default** and are only activated on request.

Appendix 2 to the Data Processing Agreement

Technical and organisational measures

The technical and organisational measures described below describe the status at the time of the conclusion of the contract. Pursuant to Section 11 (2) of the contract, the contracting parties agree that changes to the technical and organisational measures may become necessary in order to adapt to technical and legal circumstances. Changes to the technical and organisational measures must not lead to a lowering of the existing level of protection. A current overview of the technical and organisational measures taken can be viewed at any time on our website at https://softgarden.com/en/data-protection/ .

Abbreviations

- DC: Data centers
- B: softgarden office Berlin
- SB: softgarden office Saarbrücken

Confidentiality

Entrance control

softgarden ensures that unauthorised persons have no access to the office, server and archive rooms. This is done by:

Measures	DC	B	SB	Notes
Central reception area	X	X	-	
Alarm system with connected security guard	X	X	-	
Coded keys and key issuance to authorised persons only	X	X	X	
Logging of closures	X	X	X	
Determination and documentation of access authorisations	X	X	X	
Documentation of access of external persons (e.g. maintenance personnel, customers, service providers, partners, visitors ...)	X	X	X	
Entrance to the premises by noncompany personnel only in the company of an employee	X	X	X	
Legitimation of the authorised persons (key, PinCode)	X	X	X	
Two-factor authentication for access	X	-	-	
Withdrawal of means of access after expiry of authorisation	X	X	X	
Security areas with different access authorisations	X	X	X	

Access control

softgarden prevents IT systems from being used by unauthorised persons. This is done by:

Measures	DC	B	SB	Notes
One user account per user	X	X	X	Use of person-independent support accounts and one admin-account for access to customer systems, login

Measures	DC	B	SB	Notes
				data is only accessible to authorized employees
Authentication of persons authorised to process data by means of a password procedure (with special characters, minimum length eight characters, regular change of password)	X	X	X	
Encrypted storage of passwords	X	X	X	
Automatic blocking of the user account in case of multiple incorrect entry of the access data	X	X	X	
Automatic locking of the workplace in case of inactivity	X	X	X	
Immediate blocking of authorisations when employees leave (guideline/ work instruction)	X	X	X	
Regularly check the validity of authorisations	X	X	X	
Use of lockable cabinets for the storage of paper files	X	X	-	No paper file storage in the Saarbrücken office
Secure transmission of authentication secrets (credentials) in the network via TLS/HTTPS, SSH, VPN (IPSec, openVPN)	X	X	X	
Manual blocking of access IDs to computers in case of longer absence of the respective employee (30 days)	X	X	X	After returning, the access IDs must be manually unlocked again by the IT administration.
Access restriction to Office WLAN	-	-	X	
Operation of an office guest WLAN for mobile devices and visitors	-	X	X	

Access control

softgarden ensures that those authorised to use a data processing system can only access the data subject to their access authorisation and that personal data cannot be read, copied, modified or removed without authorisation during processing, use and after storage. This is done by:

Measures	DC	B	SB	Notes
Determination of access authorisations for access to data (creation of an authorisation concept)	X	X	X	
Storage of data on encrypted data carriers	X			
Determination of authorisations of knowledge, input, modification and deletion of data processed by the contractor in the context of the performance of the contract	X	X	X	
Regular control of accesses, entries, changes and deletions	X	-	-	
Disposal of data carriers no longer required (guideline/ work instruction)	X	X	X	
Written regulation on copying data (IT security guideline/ work instruction)	X	X	X	
Allocation of minimal authorisations (need-to-know principle)	X	X	X	
No assignment of generic passwords-group identifiers	X	-	-	Use of non-personal support accounts for access to customer

Measures	DC	B	SB	Notes
				systems, login data is only accessible to authorised employees
Avoiding the concentration of functions/separation of administrative tasks among different qualified persons	X	X	X	
Keeping a history of administrative changes made	X	X	X	
Access to the production infrastructure via VPN	-	X	X	

Separation control

softgarden ensures that data collected for different purposes can be processed separately. There is no need for physical separation; logical separation of data is sufficient. This is done by:

Measures	DC	B	SB	Notes
Identification of the recorded data (file number, ID, customer/ case number)	X	X	X	
Logical separation of data processed for different clients, separation of functions production/ test	X	X	X	
Logical separation of the personal data of the respective clients through assignment to the respective user accounts	X	X	X	Software separation of the clients

Integrity

Transfer control

softgarden ensures that personal data cannot be read, copied, altered or removed without authorisation during electronic transmission or during its transport or storage on data carriers, and that it is possible to check and determine to which entities personal data is intended to be transmitted by means of data transmission equipment. This shall be done by:

Measures	DC	B	SB	Notes
Determination of the persons authorised for transmission or transport (electronically, manually)	X	X	X	
Checking data for completeness after data transport, transmission and data transfer or storage	X	X	X	Manual adjustment with checksums
Implementation of safety gateways at the network transfer points	X	X	X	
Use of a recognised encryption procedure which encrypts all communication between the applicant and the contractor's servers.	X	X	X	
Incoming and outgoing data streams are filtered by a modern, cascaded firewall solution	X	X	X	
Insofar as data carriers are transmitted by transport companies, the data carriers shall only be passed on after prior authentication of the transport company.	X	X	X	
Paper and data carriers containing personal data are disposed by a qualified disposal company in accordance with data protection regulations.	X	X	X	
The complete, data protection-compliant and permanent deletion of data carriers with personal data is logged. The logs are stored in an audit-proof manner for at least 12 months.	X	X	X	

Input control

softgarden ensures that it is possible to subsequently check and determine whether and by whom personal data have been entered into, changed or removed from data processing systems. This is done by:

Measures	DC	B	SB	Notes
Documentation of access authorisations (work instruction access groups and access authorisation)	X	X	X	
Recording of the activities within the scope of the order	X	X	X	
Random control and evaluation of log data for misuse	X	-	X	Evaluation of log files via SysOps team in Saarbrücken
Maintaining a history for all users using the corresponding application programmes for processing personal data, that records which user has performed which action and when, provided that this action modifies personal data	X	X	X	Recording the history in the "Just Hire" application

Availability and resilience

Availability control

softgarden ensures that personal data is protected against accidental or intentional destruction or loss. This is done by:

Measures	DC	B	SB	Notes
Uninterruptible Power Supply (UPS)	X	X	X	
Virus protection (on the workplaces)	X	X	X	Virus protection on Windows workplaces
Virus protection (on the servers)	X	X	X	
Firewall	X	X	X	
Emergency plan	X	X	X	
DDoS-Protection/ WAF (Cloudflare)	X			SaaS
Geo-redundant data centres	X	-	-	
Central fire alarm system	X	X	-	
Availability monitoring	X	X	X	24/7 monitoring of all critical systems through automated monitoring procedures

Recoverability

softgarden guarantees the ability to quickly restore the availability of and access to personal data in the event of a physical or technical incident through the following measures:

Measures	DC	B	SB	Notes
Backup procedure according to backup concept (daily, weekly, monthly)	X	X	X	
Storage of backup data in data cabinets, safes, in other fire compartment	X	X	X	

Resilience

softgarden ensures availability and resilience of business-critical systems and the systems for processing personal data through the following technical and organisational measures:

Measures	DC	B	SB	Notes
Virtualisation and operation in container infrastructure with load balancers	X	-	-	
Regular penetration tests of softgarden products for security vulnerabilities	X	-	-	The softgarden products are tested in the environment of the raking centres. Not applicable in the office environment. Penetration tests by customers can be carried out on the staging environment after consultation with softgarden. Conducting them in the production environment is not permitted.
DDoS-Protection/ WAF (Cloudflare)	X	-	-	SaaS

Procedures for regular review, assessment and evaluation

To ensure the maintenance and continuous improvement of the level of data protection and information security, softgarden regularly (at least annually) undergoes internal and external audits.

softgarden is certified according to

- DIN EN ISO 9001:2015
- DIN EN ISO/IEC 27001:2017 including the requirements of the standards ISO/IEC 27017:2015 and ISO/IEC 27018:2019

Data protection and information security management

softgarden ensures a process for regular review and evaluation of the effectiveness of the technical and organisational protection measures. This is done by:

Measures	DC	B	SB	Notes
Informing and obliging employees to comply with the data protection legal requirements according to the GDPR	X	X	X	
Regular assessment of the level of data protection by a data protection team	X	X	X	
Third parties must sign a confidentiality agreement.	X	X	X	
If there are overlapping functions for organisational reasons, the dual control principle is applied and documented.	-	X	X	
There is a defined system of representatives within the functional groups.	-	X	X	
Regular review of the data protection and information security management system through internal and external audits	X	X	X	

Assessment of the adequate level of protection (Art. 32(2) GDPR)

softgarden ensures a documented assessment of an adequate level of protection, in relation to the risks associated with the processing - in particular through destruction, loss, alteration, unauthorised disclosure or access - of the personal data processed on behalf of it. This shall be done by:

Measures	DC	B	SB	Notes
Carrying out a risk analysis for the processing operations of personal data	X	X	X	
Creation of protection needs categories	X	X	X	
Alignment of processes according to Privacy by Design and Privacy by Default	-	X	X	
Carrying out data protection impact assessments (where required by law)	X	X	X	

Mandate control (Art. 32 (3) and (4) GDPR)

softgarden guarantees that personal data processed on behalf of the contractor will only be processed in accordance with the instructions of the client and for the fulfilment of the contractually defined purpose. The contractor can prove this by means of a certification pursuant to Art. 40 or an approved certification procedure pursuant to Art. 42 GDPR. If no certification is available, the proof shall be provided by:

Measures	DC	B	SB	Notes
Clear contract design with subcontractors	X	X	X	
Formalisation of order placement (forms system)	X	X	X	
Regular control of the activities	X	X	X	Monitoring the softgarden processes through internal audits
The persons authorised to give instructions to the client and the persons authorised to receive instructions are contractually defined; instructions are always given in text form (e.g. by e-mail or ticket system).	X	X	X	
softgarden will inform the client immediately about cases of serious operational disruptions, suspected data protection violations, if errors are detected or other irregularities in the handling of the client's data.	X	X	X	
Orders are recorded as a support ticket (minimum details: Client/customer, action/partial order, exact specification of processing steps/parameters, processor, deadlines, recipient if applicable), where the work performed is documented. There is a clear assignment between support ticket number and customer order.	X	X	X	

Data deletion/ anonymisation:

Data erasure:

Canceled and hired applications are initially set to the status "cancelled/hired" and, in the standard configuration, deleted or anonymised 6 months after cancellation or hiring, unless otherwise set by the client. The anonymisation of rejected applicants who do not wish to be included in the talent pool takes place automatically. Any further deletion/anonymisation of individual applicants (e.g. at the applicant's request) is carried out manually. Applicant data can also be deleted manually by users with the appropriate authorisation.

Anonymisation of deleted applicants:

After the deadline, the applications are completely anonymised in the softgarden system:

- All attachments of the application are overwritten with a dummy content. The file name, size and content are deleted. Only the fact that and how many attachments were available for an application is retained for reporting purposes.
- Correspondence data is anonymised. In the process

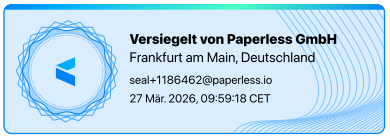
        - Attachments are anonymised
        - Subject, text and HTML, CC and BCC of the message are overwritten with a dummy text "deleted text".
        - the sender's address for incoming mails and the recipient's address for outgoing mails are overwritten with a random string.
- Master data of the application are anonymised
    - all application data specified by the client are overwritten with a random string in the process
- The application is removed from the application search index

If the application to be deleted was the last application of the applicant account, the following data is also overwritten with a random string:

- Login name
- Password
- First and last name
- E-mail address
- IP address from which the account was created
- IP address from which the privacy policy was confirmed
- In addition, all tags of the applicant are deleted

There is the possibility that quantitative evaluations are carried out on the participants to determine which applicants, at which location, had which interest. The anonymised data is used for this purpose. Anonymisation replaces all data with personal references with dummy texts, so that it is no longer possible to draw conclusions afterwards.

Paperless



AUDIT TRAIL

Dokument-Informationen

Vorgangsnummer:
686742

Name:
DPA_english_Rev 2_11

Eigentümer:
softgarden e-recruiting GmbH

Status: Abgeschlossen

Sprachvariante: de-DE

Zeitzone: UTC+01:00 (Berlin)

Ereignisübersicht

Dokument erstellt von **Sophia Jenkner** (sophia.jenkner@softgarden.de)	27. März 2026, 09:54:00 Uhr
Prozess gestartet von **Sophia Jenkner** (sophia.jenkner@softgarden.de)	27. März 2026, 09:56:25 Uhr
Prozess von allen Beteiligten abgeschlossen	27. März 2026, 09:59:15 Uhr
Dokument und Audit Trail versiegelt	27. März 2026, 09:59:17 Uhr

Beteiligte

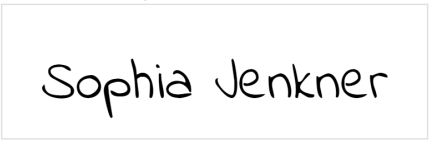
Sophia Jenkner (sophia.jenkner@softgarden.de)
Rolle: Versender

Sophia Jenkner (sophia.jenkner@softgarden.de)
Rolle: Empfänger (Ausfüllen & Unterschreiben)
Email Link gesendet am 27. März 2026 um 09:56:26 Uhr
Authentifizierung: Geheimer Link per Email an sophia.jenkner@softgarden.de
Geschäftsbedingungen akzeptiert am 27. März 2026 um 09:56:26 Uhr

Christian Heuermann (christian.heuermann@softgarden.de)
Rolle: Empfänger (Ausfüllen & Unterschreiben)
Email Link gesendet am 27. März 2026 um 09:56:28 Uhr, **zugestellt** am 27. März 2026 um 09:56:31 Uhr
Authentifizierung: Geheimer Link per Email an christian.heuermann@softgarden.de
Geschäftsbedingungen akzeptiert am 27. März 2026 um 09:58:50 Uhr

Sitzungen

Sophia Jenkner (sophia.jenkner@softgarden.de)
Zeitraum: 27. März 2026, 09:56:44 Uhr - 27. März 2026, 09:56:44 Uhr
IP Adresse: 78.46.93.69
Browser: Chrome 146.0.0.0

27. März 2026, 09:56:44 Uhr	**Daten erfasst**	**Unterschrift Sophia Jenkner:**  Unterschrieben am 27.03.2026 **Texteingabe:** softgarden e-recruiting GmbH
27. März 2026, 09:56:44 Uhr	**Abschluss**	Dokument vollständig ausgefüllt, Daten validiert und abgeschlossen

Christian Heuermann (christian.heuermann@softgarden.de)
Zeitraum: 27. März 2026, 09:59:14 Uhr - 27. März 2026, 09:59:14 Uhr
IP Adresse: 78.46.93.69
Browser: Edge 146.0.0.0

27. März 2026, 09:59:14 Uhr	**Daten erfasst**	**Unterschrift Christian Heuermann:**  Unterschrieben am 27.03.2026 **Datum:** 27.03.2026
27. März 2026, 09:59:14 Uhr	**Abschluss**	Dokument vollständig ausgefüllt, Daten validiert und abgeschlossen