|  |
| --- |
| **Technical and Organizational Measures in  Accordance With Art. 32 of the General Data  Protection Regulation** |

The technical and organizational measures described in Art. 32 GDPR are not intended for the public. This information is only accessible to the company data protection officer, to the respective supervisory authorities for data protection and to their own authorized employees of the respective data processing unit.

# Abbreviations

* DC: Datacenter
* B: softgarden Office Berlin
* SB: softgarden Office Saarbrücken

# Confidentiality

## Entrance Control

softgarden ensures that unauthorized persons have no access to the office, server and archive rooms.

This is done by:

|  |
| --- |
| **Medidas Técnicas y Organizativas de conformidad  con el artículo 32 del Reglamento General de  Protección de Datos** |

Las medidas técnicas y organizativas descritas en el art. 32 del RGPD no están destinadas al público. Solo podrán acceder a esta información el responsable de protección de datos de la empresa, las autoridades supervisoras correspondientes de la protección de datos y sus propios empleados autorizados de la correspondiente unidad de tratamiento de datos.

# Abreviaturas

* DC: Centro de datos
* B: Oficina de softgarden en Berlín
* SB: Oficina de softgarden en Saarbrücken

# Confidencialidad

## Control de entrada

softgarden asegura que ninguna persona no autorizada tendrá acceso a la oficina, servidor y salas de archivo.

Esto es realizado por:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Measure** | **Medida** | **DC** | **B** | **SB** | **Remarks** |
| Central reception area | Área de recepción central | X | X | - |  |
| Access through an alarm system with activated guard | Acceso a través del sistema de alarma con protección activada | X | - | - |  |
| Access with coded keys and key issue only to authorized persons | Acceso con llaves codificadas y clave emitida solo para las personas autorizadas | X | X | X |  |
| Logging of locks | Registro de bloqueos | X | X | X |  |
| Definition and documentation of the authorized persons | Definición y documentación de las personas autorizadas | X | X | X |  |
| Documentation of visit of non-employees (e.g. maintenance staff, customers, service providers, partners, visitors ...) | Documentación de las visitas de personas no empleadas (p. ej. personal de mantenimiento, clientes, proveedores de servicio, socios, visitantes....) | X | X | - | Visitors list at the reception in office Berlin  Lista de visitantes en la recepción de la oficina de Berlín |
| Foreign companies, maintenance personnel and visitors may only enter the premises accompanied by an employee | Las empresas extranjeras, el personal de mantenimiento y los visitantes solo podrán entrar en las instalaciones acompañados de un empleado | X | X | X |  |
| Legitimation of the authorized persons (key, PinCode) | Legitimación de las personas autorizadas (llave, Código Pin) | X | X | X |  |
| 2-factor authentication access | Acceso con autentificación de 2 factores | X | - | - |  |
| Withdrawal of access permissions after expiry of the authorization | Retirada de permisos de acceso después de expirar la autorización | X | X | X |  |
| There are security areas with different access authorizations | Existen áreas de seguridad con distintas autorizaciones de acceso | X | X | X |  |

## 

## Admission Control

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

## Control de admisión

softgarden evita que los sistemas informáticos sean usados por personas no autorizadas. Esto es realizado por:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Measure** | **Medida** | **DC** | **B** | **SB** | **Remarks** |
| Creation of a user account per user | Creación de una cuenta de usuario para cada usuario | X | X | X | Use of non-personal support accounts for access to customer systems, access data are only accessible to authorized employees  Uso de cuentas de soporte no personales para acceder a los sistemas de clientes, los datos de acceso solo son accesibles a los empleados autorizados |
| Authentication of persons authorized to process data by means of a password procedure (with special characters, minimum length 8 characters, regular password change) | La autentificación de personas autorizadas para tratar los datos mediante un procedimiento de contraseña (con caracteres especiales, longitud mínima de 8 caracteres, cambio regular de contraseña) | X | X | X |  |
| Passwords are stored encrypted | Las contraseñas se guardan cifradas | X | X | X |  |
| Automatic blocking of the user account in case of multiple incorrect entry of access data | Bloqueo automático de la cuenta del usuario en caso de múltiples entradas incorrectas de datos de acceso | X | X | X |  |
| Automatic locking of the workplace during inactivity | Bloqueo automático del puesto de trabajo durante la inactividad | X | X | X |  |
| Immediate blocking of authorizations when leaving employees (directive / work instruction) | Bloqueo inmediato de las autorizaciones cuando se despida a los empleados (directriz / instrucción de trabajo) | X | X | X |  |
| Regular control of the validity of permissions | Control regular de la validez de los permisos | X | X | X |  |
| The use of lockable cabinets for storing paper files | El uso de armarios con cerraduras para guardar los archivos en papel | X | X | - | no file storage at office Saarbrücken  no hay almacenamiento de archivos en la oficina de Saarbrücken |
| Secure transmission of authentication secrets (credentials) in the network via TLS / HTTPS, SSH, VPN (IPSec, openVPN) | Transmisión segura de secretos de autentificación (credenciales) en la red mediante TLS/HTTPS, SSH, VNP (IPSec, openVPN) | X | X | X |  |
| Access IDs to workstations are manually locked during extended absence of the respective employee (30 days) and must be manually unlocked by the IT administration after return. | Las ID de acceso a las estaciones de trabajo se bloquean manualmente durante una ausencia prolongada del empleado correspondiente (30 días) y la administración de TI debe desbloquearlo manualmente después de su regreso. | X | X | X |  |

## 

## Access Control

The Contractor ensures that the persons authorized to use data processing systems can only access the data that is subject to their access authorization and that personal data may not be read, copied, edited or deleted without authorization during processing, use or storage.   
This is achieved through:

## Control de acceso

El contratista garantizará que las personas autorizadas para usar los sistemas de tratamiento de datos solo puedan acceder a los datos que estén sujetos a su autorización de acceso y que los datos personales no se pueden leer, copiar, editar ni borrar sin autorización durante el tratamiento, uso o almacenamiento.   
Esto se consigue mediante:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Measure** | **Medida** | **DC** | **B** | **SB** | **Remarks** |
| Definition of access authorizations for the access to data (creation of an authorization concept) | La definición de las autorizaciones de acceso para el acceso a los datos (creación de un concepto de autorización) | X | X | X |  |
| Defining the powers to note, input, alteration and deletion of data processed as part of the contractor's fulfillment of the contract | Definición de los poderes para anotar, introducir, alterar y borrar los datos tratados como parte del cumplimiento del contrato por parte del contratista | X | X | X |  |
| Regular control of access, input, modification and deletion | Control regular de acceso, introducción, modificación y supresión | X | - | - |  |
| Disposal of unwanted data carriers (directive / work instruction) | Eliminación de portadores de datos no deseados (directriz / instrucción de trabajo) | X | X | X |  |
| Written rule for copying data (IT security guideline / work instruction) | Norma escrita para la copia de datos (guía de seguridad de TI / instrucción de trabajo) | X | X | X |  |
| Assignment of minimum authorizations (Need-to-know principle) | La definición de las autorizaciones de acceso para el acceso a los datos (creación de un concepto de autorización) | X | X | X |  |
| No assignment of generic or group IDs or passwords | Definición de los poderes para anotar, introducir, alterar y borrar los datos tratados como parte del cumplimiento del contrato por parte del contratista | X | - | - | Use of non-personal support accounts for access to customer systems, access data are only accessible to authorized employees  Uso de cuentas de soporte no personales para acceder a los sistemas de clientes, solo los empleados autorizados pueden acceder a los datos de acceso |
| Avoid concentration of functions - Separate functions of administrator activities to different qualified persons | Control regular de acceso, introducción, modificación y supresión | X | X | X |  |
| Maintain a history of administrative changes | Eliminación de portadores de datos no deseados (directriz / instrucción de trabajo) | X | X | X |  |
| Access to the production infrastructure via VPN | Norma escrita para la copia de datos (guía de seguridad de TI / instrucción de trabajo) | - | X | X |  |

## 

## Separation control

softgarden ensures that data collected for different purposes can be processed separately. There is no need for a physical separation; a logical separation of the data is sufficient.

This is done by:

## Control de separación

softgarden garantiza que los datos recopilados para distintos fines se podrán tratar por separado. No hay necesidad de separación física: es suficiente una separación lógica de los datos. Esto es realizado por:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Measure** | **Medida** | **DC** | **B** | **SB** | **Remarks** |
| Identification of the collected data (file number ID, customer / transaction number) | Identificación de los datos recopilados (ID número de archivo, número de cliente / transacción) | X | X | X |  |
| Logical separation of data processed for different clients Separation of functions / production / test | Separación lógica de datos tratados para distintos clientes Separación de funciones / producción / prueba | X | X | X |  |
| The personal data of the respective client are logically separated by assignment to the respective user account. | Los datos personales de los clientes correspondientes se separan lógicamente mediante asignación a la cuenta de usuario correspondiente. | - | X | X |  |

# 

# Integrity

## Transmission control

softgarden  guarantees that personal data cannot be read, copied, edited or removed during electronic transmission, when being transported or when being saved and that where personal data transmissions via data transmission facilities are scheduled can be determined and reviewed. This is achieved through:

# Integridad

## Control de transmisión

softgarden garantiza que los datos personales no se podrán leer, copiar, editar ni eliminar durante la transmisión electrónica, cuando se transporten o cuando se guarden y que se podrán determinar y revisar en el caso de que se programen transmisiones de datos personales a través de centros de transmisión de datos. Esto se consigue mediante:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Measure** | **Medida** | **DC** | **B** | **SB** | **Remarks** |
| Determining the persons authorized to transmit or transport (electronically, manually) | Determinación de las personas autorizadas para transmitir o transportar (electrónicamente, manualmente) | X | X | X |  |
| Checking the data for completeness after data transport, transmission and data transmission or storage | Comprobación de la integridad de los datos después del transporte, transmisión y transmisión o almacenamiento de datos | X | X | X | Manual comparison with checksums  Comparación manual de las sumas de comprobación |
| Implementation of security gateways at the network transfer points | Implementación de pasarelas de seguridad en los puntos de transferencia de la red | X | X | X |  |
| Use of a recognized encryption method that encrypts all communications between the applicant and the contractor's servers. | Uso de un método reconocido de cifrado que cifre todas las comunicaciones entre el solicitante y los servidores del contratista. | X | X | X |  |
| Incoming and outgoing data streams are filtered by a modern, cascaded firewall solution | Los flujos de datos entrantes y salientes se filtrarán mediante una solución moderna de cortafuegos en cascada | X | X | X |  |
| As far as data carriers are transmitted by transport companies, the data carriers are only forwarded after prior authentication of the transport company. | En lo que respecta a portadores de datos transmitidos por empresas de transporte, los portadores de datos solo se envían después de una autentificación previa de la empresa de transporte. | X | X | X |  |
| Paper and data media containing personal data are disposed of by a qualified disposal company in accordance with data protection laws. | El papel y los soportes de datos que contienen datos personales son eliminados por una empresa de eliminación cualificada de acuerdo con las leyes de protección de datos. | X | X | X |  |
| The complete, privacy-adequate and permanent deletion of data carriers containing personal data is logged. The logs are kept audit-proof for at least 12 months. | Se registra la eliminación completa, confidencial y permanente de los portadores de datos que contienen datos personales. Los registros se guardan a prueba de auditorías durante al menos 12 meses. | X | X | X |  |

## Input Control

softgarden ensures that whether and by whom personal data is entered into, edited on or removed from data processing systems can be subsequently determined and reviewed. This is achieved through:

## Control de entrada

softgarden garantiza que se pueda determinar y revisar posteriormente si se introducen, editan o eliminan los datos personales de los sistemas de tratamiento de datos y quién lo ha hecho. Esto se consigue mediante:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Measure** | **Medida** | **DC** | **B** | **SB** | **Remarks** |
| Management of a documentation of the access authorizations (work instruction access groups and access authorization) | Gestión de una documentación de las autorizaciones de acceso (grupos de acceso a la instrucción de trabajo y autorización de acceso) | X | X | X |  |
| Recording of activities under the contract | Registro de actividades en virtud del contrato | X | X | X |  |
| Random control and evaluation of the protocol data for abuse | Control y evaluación aleatorios de los datos de protocolo para el uso indebido | X | - | X |  |
| For all users who use the respective application programs for the processing of personal data, a history is kept, which records which user when which action has been performed, if this action modifies personal data. | Se mantiene un historial de todos los usuarios que utilizan los programas de aplicación correspondientes para el tratamiento de datos personales, que registra qué usuario, cuándo y qué acción, si esta acción modifica los datos personales. | - | X | X | Capture history in the Just Hire application  Captar historia en la aplicación Just Hire |

# 

# Availability and Resilience

## Availability Control

softgarden ensures the protection of personal data from random or intentional destruction or loss. This is achieved through:

# Disponibilidad y resistencia

## Control de disponibilid ad

softgarden garantiza la protección de los datos personales de la destrucción o pérdida aleatoria o intencional. Esto se consigue mediante

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Measure** | **Medida** | **DC** | **B** | **SB** | **Remarks** |
| Uninterruptible power supply (UPS) | Suministro de alimentación ininterrumpido (SAI) | X | X | X |  |
| Virus protection (on workstations) | Protección antivirus (en estaciones de trabajo) | X | X | X | Virus protection on windows workstations  Protección antivirus en estaciones de trabajo de Windows |
| Virus protection (on servers) | Protección antivirus (en servidores) | X | X | X |  |
| Firewall | Cortafuegos | X | X | X |  |
| Emergency plan | Plan de emergencia | X | X | X |  |
| Georedundant datacenter | Centro de datos georedundante | X | - | - |  |
| Central fire alarm system | Sistema central de alarma contra incendios | X | X | - |  |
| Availability monitoring | Disponibilidad de monitorización | X | X | X | All critical systems are monitored 24/7 through automated monitoring procedures  Todos los sistemas críticos están monitorizados 24 h/7 días a la semana mediante procedimientos de monitorización automatizados |

## 

## Restorability

softgarden  guarantees that the availability of and access to personal data can be rapidly restored through the following measures in case of physical or technical incidents.

## Capacidad de recuperación

softgarden garantiza que la disponibilidad y el acceso a los datos personales se pueden recuperar rápidamente mediante las siguientes medidas en caso de incidentes físicos o técnicos.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Measure** | **Medida** | **DC** | **B** | **SB** | **Remarks** |
| Backup procedure acc. Backup concept (daily, weekly, monthly) | Acceso procedimiento de copia de seguridad Concepto de copia de seguridad (diario, semanal, mensual) | X | X | X |  |
| Storage of backup data in data cabinets, safes, in the other fire compartment | Almacenamiento de datos de copia de seguridad en armarios para datos, caja de seguridad, en la otra compartimentación contra incendios | X | X | X |  |

## 

## Resilience

softgarden guarantees availability and resilience of systems with critical business impact and impact on processing of personal data by the following technical and organizational measures:

## Resistencia

softgarden garantiza la disponibilidad y resistencia de los sistemas con impacto comercial crítico e impacto en el tratamiento de datos personales mediante las siguientes medidas técnicas y organizativas

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Measure** | **Medida** | **DC** | **B** | **SB** | **Remarks** |
| Virtualization and use of container infrastructures with load balancers | Acceso procedimiento de copia de seguridad Concepto de copia de seguridad (diario, semanal, mensual) | X | - | - |  |
| periodic penetration tests of the softgarden products to detect security leaks | Almacenamiento de datos de copia de seguridad en armarios para datos, caja de seguridad, en la otra compartimentación contra incendios | X | - | - | The test includes softgarden products in the datacenter environment. This is not applicable to softgarden offices.  La prueba incluye productos softgarden en el entorno de centro de datos. Esto no es aplicable a las oficinas softgarden. |

# 

# Procedures for periodic review, evaluation and evaluation

## Dataprivacy management

softgarden ensures a process of periodic review and evaluation of the effectiveness of technical and organizational safeguards. This is done by:

# Procedimientos para revisión, valoración y evaluación periódicos

## Gestión de la confidencialidad de los datos

softgarden asegura un proceso de revisión y evaluación periódicos de la eficacia de las protecciones técnicas y organizativas. Esto es realizado por:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Measure** | **Medida** | **DC** | **B** | **SB** | **Remarks** |
| Instructing all employees about and subjecting them to data protection secrecy obligations (Art. 28(3) Letter b of the General Data Protection Regulation) | Instruir a todos los empleados sobre las obligaciones del secreto de protección de datos y someterlos a ellas (art. 28(3) Letra b del Reglamento general de protección de datos). | X | X | X |  |
| Regular rating of the privacy level by the privacy team | Calificación regular del nivel de confidencialidad por parte del equipo de confidencialidad | X | X | X |  |
| Third parties must submit a confidentiality statement | Terceras partes deben enviar una declaración de confidencialidad | X | X | X |  |
| If functional overlaps exist for organizational reasons, the four-eyes principle is applied and documented. | Si existen superposiciones funcionales por motivos organizativos, se debe aplicar y documentar el principio de cuatro ojos. | - | X | X |  |
| Defined rules of representation within functional groups | Normas definidas de representación dentro de grupos funcionales | - | X | X |  |

## 

## Assessment of the appropriate level of protection (Art. 32 Sec. 2 GDPR)

softgarden guarantees a documented assessment of an appropriate level of protection, in terms of the risks associated with the processing - in particular by destruction, loss, alteration, unauthorized disclosure or access - of the personal data processed in the order. This is done by:

## Valoración del nivel de protección adecuado (Art. 32 apart. 2 RGPD)

softgarden garantiza una valoración documentada de un nivel de protección adecuado en cuanto a los riesgos asociados con el tratamiento: en especial por la destrucción, pérdida, alteración, divulgación o acceso no autorizados, de los datos personales tratados durante el encargo. Esto es realizado por:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Measure** | **Medida** | **DC** | **B** | **SB** | **Remarks** |
| Carry out a risk analysis for the processing of personal data | Realización de un análisis de riesgos para el tratamiento de datos personales | X | X | X |  |
| Creation of protection requirement categories | Creación de categorías de requisitos de protección | X | X | X |  |
| Alignment of processes according to "Privacy by Design & Default" | Armonización de procesos según "Confidencialidad por diseño y defecto" | - | X | X |  |
| If necessary, the implementation of a Data protection impact assessment | Si es necesario, la implementación de una evaluación de impacto de protección de datos | X | X | X |  |

## 

## Order Control (Art. 32 Sec. 3 and 4 GDPR)

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

## Control del encargo (Art. 32 apart. 3 y 4 RGPD)

softgarden garantiza que los datos personales tratados en el encargo solo serán tratados de acuerdo con las instrucciones del cliente y para el cumplimiento de la finalidad definida contractualmente. El contratista podrá demostrarlo mediante una homologación conforme al art. 40 o un procedimiento de certificación autorizado conforme al art. 42 del RGPD. Si no hay certificación, la prueba será proporcionada por:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Measure** | **Medida** | **DC** | **B** | **SB** | **Remarks** |
| Clear contract design with subcontractors | Diseño de contrato claro con subcontratistas | X | X | X |  |
| Formalization of the order | Formalización del encargo | X | X | X |  |
| Regular control of activities | Control regular de las actividades | X | X | X | Monitoring of softgarden processes through internal audits  Monitorización de los procesos de softgarden a través de auditorías internas |
| The authorized representatives of the client and the persons authorized to receive instructions are defined by contract, and instructions are always given in written form. | Los representantes autorizados del cliente y las personas autorizadas para recibir instrucciones serán definidos en el contrato y las instrucciones siempre se entregarán por escrito. | X | X | X |  |
| softgarden informs the client immediately about cases of data breaches, suspected violations of data protection, if errors are detected or other irregularities in the handling the clients data. | softgarden informará al cliente inmediatamente sobre casos de violaciones de datos, sospecha de violaciones de la protección de datos, si se detectan errores o irregularidades en la manipulación de los datos de los clientes. | X | X | X |  |
| Orders are recorded as a support ticket (minimum details: customer / customer, action / partial order, exact specification of the processing steps / parameters, processor, dates, recipients if necessary), where the work performed is documented. There is a clear assignment between support ticket number and sales order. | Los encargos se registran como una nota de soporte (datos mínimos: cliente / cliente, acción / encargo parcial, especificación exacta de los pasos del tratamiento / parámetros, encargado del tratamiento, fechas, destinatarios si es necesario), donde se documenta el rabajo realizado. Hay una asignación clara entre el número de la nota de soporte y el encargo de venta. | X | X | X |  |

|  |
| --- |
| **Declaration of Commitment for the Implementation of Technical and Organizational Measures** |

The Contractor confirms that he implemented the technical and organizational measures for the protection of the Principal's personal data—as described in **Annex 2**—before the commencement of data processing. The Contractor must ensure, regularly monitor and document the fulfillment of these requirements for the duration of the cooperation and must provide this documentation to the Principal on request.

The technical and organizational measures are subject to technical progress and developments. Therefore, the Contractor may implement adequate alternative measures. However, the security level of the specified measures must be maintained

Significant changes must be documented and provided to the Principal on request.

|  |
| --- |
| **Declaración de compromiso para la implementación de las medidas técnicas y organizativas** |

El contratista confirma que implementará las medidas técnicas y organizativas para la protección de los datos personales de la empresa principal, como se describe en el **Anexo 2**, antes de iniciar el tratamiento de datos. El contratista debe asegurar, monitorizar con regularidad y documentar el cumplimiento de estos requisitos durante la cooperación y debe proporcionar esta documentación a la empresa principal a demanda.

Las medidas técnicas y organizativas están sujetas a los avances y el progreso técnicos. Por tanto, el contratista puede implementar medidas alternativas adecuadas. Sin embargo, se debe mantener el nivel de seguridad de las medidas especificadas. Los cambios significativos se deben documentar y proporcionar a la empresa principal a demanda.

.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Place, Date |  | Mathias Heese / CEO  Martin Behrend / CFO  Name of the Contractor / Signature / Company Stamp |