|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  | | --- | | **Technical and Organizational Measures in Accordance**  **With Art. 32 of the General Data Protection Regulation** |   **If the Contractor has a computer center, the technical and organizational measures must be stated separately for the computer center and for the Contractor's offices.**  Please state and provide proof of the **specific** technical and organizational measures you implemented to guarantee data protection and data security.  The technical and organizational measures in accordance with Art. 32 of the General Data Protection Regulation and described hereafter are not designated for the public. Only company data protection officers, competent data protection supervisory authorities and authorized employees of the respective data processing office may access to this information.  **Following a review by the Principal**,the technical and organizational measures described hereafter will be binding—as a part of this Data Protection Contract: They are specified between the Contractor and the Principal as follows: Abbreviations  * DC: Datacenter * B: softgarden Office Berlin * SB: softgarden Office Saarbrücken  ConfidentialityEntrance Control softgarden ensures that unauthorized persons have no access to the office, server and archive rooms. This is done by:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Measure** | **DC** | **B** | **SB** | **Remarks** | | Central reception area | X | X | - |  | | Access through an alarm system with activated guard | X | - | - |  | | Access with coded keys and key issue only to authorized persons | X | X | X |  | | Logging of locks | X | X | X |  | | Definition of the authorized persons including their documentation for employees and non-employees (maintenance staff, visitors) / gatekeepers, plant protection | X | X | - | Lead a list of visitors at the reception in Berlin | | Foreign companies, maintenance personnel and visitors may only enter the premises accompanied by an employee | X | X | X |  | | Legitimation of the authorized persons (key, PinCode) | X | X | X |  | | 2-factor authentication access | X | - | - |  | | Withdrawal of access permissions after expiry of the authorization | X | X | X |  | | There are security areas with different access authorizations | X | X | X |  |  Admission Control softgarden prevents IT systems from being used by unauthorized persons. This is done by:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Measure** | **DC** | **B** | **SB** | **Remarks** | | Creation of a user account per user | X | X | X | Use of non-personal support accounts for access to customer systems, access data are only accessible to authorized employees | | Authentication of persons authorized to process data by means of a password procedure (with special characters, minimum length 8 characters, regular password change) | X | X | X |  | | Automatic blocking of the user account in case of multiple incorrect entry of access data | X | X | X |  | | Automatic locking of the workplace during inactivity | X | X | X |  | | Immediate blocking of authorizations when leaving employees (directive / work instruction) | X | X | X |  | | Regular control of the validity of permissions | X | X | X |  | | The use of lockable cabinets for storing paper files | X | X | - | no file storage at office Saarbrücken | | Secure transmission of authentication secrets (credentials) in the network via TLS / HTTPS, SSH, VPN (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. | 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:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Measure** | **DC** | **B** | **SB** | **Remarks** | | Definition of access authorizations for the access to data (creation of an authorization concept) | 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 | X | X | X |  | | Regular control of access, input, modification and deletion | X | - | - |  | | Disposal of unwanted data carriers (directive / work instruction) | X | X | X |  | | Written rule for copying data (IT security guideline / work instruction) | X | X | X |  | | Assignment of minimum authorizations (Need-to-know principle) | X | X | X |  | | No assignment of generic or group IDs or passwords | X | - | - | Use of non-personal support accounts for access to customer systems, access data are only accessible to authorized employees | | Avoid concentration of functions - Separate functions of administrator activities to different qualified persons | X | X | X |  | | Maintain a history of administrative changes | 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 a physical separation; a logical separation of the data is sufficient. This is done by:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Measure** | **DC** | **B** | **SB** | **Remarks** | | Identification of the collected data (file number ID, customer / transaction number) | X | X | X |  | | Logical separation of data processed for different clients Separation of functions / production / test | X | X | X |  | | The personal data of the respective client are logically separated by assignment to the respective user account. | - | X | X |  |  IntegrityTransmission 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:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Measure** | **DC** | **B** | **SB** | **Remarks** | | Determining the persons authorized to transmit or transport (electronically, manually) | X | X | X |  | | Checking the data for completeness after data transport, transmission and data transmission or storage | X | X | X | Manual comparison with checksums | | Implementation of security gateways at the network transfer points | X | X | X |  | | Use of a recognized encryption method that encrypts all communications 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 |  | | As far as data carriers are transmitted by transport companies, the data carriers are only forwarded after prior authentication of the transport company. | X | X | X |  | | Paper and data media containing personal data are disposed of by a qualified disposal company in accordance with data protection laws. | 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. | 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:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Measure** | **DC** | **B** | **SB** | **Remarks** | | Management of a documentation of the access authorizations (work instruction access groups and access authorization) | X | X | X |  | | Recording of activities under the contract | X | X | X |  | | Random control and evaluation of the protocol data for abuse | 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. | - | X | X | Capture history in the Just Hire application |  Availability and ResilienceAvailability Control softgarden ensures the protection of personal data from random or intentional destruction or loss. This is achieved through:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Measure** | **DC** | **B** | **SB** | **Remarks** | | Uninterruptible power supply (UPS) | X | X | X |  | | Virus protection (on workstations) | X | X | X | Virus protection on windows workstations | | Virus protection (on servers) | X | X | X |  | | Firewall | X | X | X |  | | Emergency plan | X | X | X |  | | Georedundant datacenter | X | - | - |  | | Central fire alarm system | X | X | - |  | | Availability monitoring | X | X | X | All critical systems are monitored 24/7 through automated monitoring procedures |  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.   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Measure** | **DC** | **B** | **SB** | **Remarks** | | Backup procedure acc. Backup concept (daily, weekly, monthly) | X | X | X |  | | Storage of backup data in data cabinets, safes, in the other fire compartment | X | X | X |  |  Resilence 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:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Measure** | **DC** | **B** | **SB** | **Remarks** | | Virtualization and use of container infrastructures with load balancers | X | - | - |  | | Periodic penetration tests of the softgarden products to detect security leaks | X | - | - | The test includes softgarden products in the datacenter environment. This is not applicable to softgarden offices. |  Procedures for periodic review, evaluation and evaluationDataprivacy management softgarden ensures a process of periodic review and evaluation of the effectiveness of technical and organizational safeguards. This is done by:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Measure** | **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) | X | X | X |  | | Regular rating of the privacy level by the privacy group | X | X | X |  | | Third parties must submit a confidentiality statement | X | X | X |  | | If functional overlaps exist for organizational reasons, the four-eyes principle is applied and documented. | - | X | X |  | | Defined rules of representation within functional groups | - | 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:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Measure** | **DC** | **B** | **SB** | **Remarks** | | Carry out a risk analysis for the processing of personal data | X | X | X |  | | Creation of protection requirement categories | X | X | X |  | | Alignment of processes according to "Privacy by Design & Default" | - | X | X |  | | If necessary, the implementation of a Data protection impact assessment | 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:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Measure** | **DC** | **B** | **SB** | **Remarks** | | Clear contract design with subcontractors | X | X | X |  | | Formalization of the order | X | X | X |  | | Regular control of activities | X | X | X | Monitoring of softgarden processes through internal audits | | 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. | 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. | 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. | 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.   |  |  |  | | --- | --- | --- | |  |  |  | | Place, Date |  | Mathias Heese / Managing Director  Martin Behrend / VP Finance  Name of the Contractor / Signature / Company Stamp | | |  | | --- | | **Środki techniczno-organizacyjne zgodnie z art. 32 RODO** |   Opisane poniżej środki techniczne i organizacyjne zgodnie z art. 32 RODO nie są przeznaczone do wiadomości publicznej. Dostęp do tych informacji mają wyłącznie zakładowi inspektorzy ochrony danych, właściwe organy nadzorcze ochrony danych i wewnętrzni, upoważnieni pracownicy danej jednostki przetwarzającej dane.  **Po sprawdzeniu przez Zleceniodawcę** poniżej opisane środki techniczne i organizacyjne są wiążące jako część składowa przedłożonej umowy o ochronę danych osobowych: Zleceniobiorca i Zleceniodawca ustalają następujące środki: Skróty  * CD: Centra danych * B: softgarden biuro w Berlinie * SB: softgarden biuro w Saarbrücken  PoufnośćKontrola dostępu (fizycznego) softgarden zapewnia, że osoby nieupoważnione nie mają dostępu do pomieszczeń biurowych, serwerowni i archiwum. Następuje to poprzez:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Środki** | CD | B | SB | Uwagi | | Recepcja centralna (recepcja) | X | X | - |  | | Dostęp za pośrednictwem systemu alarmowego z podłączoną ochroną | X | - | - |  | | Dostęp z kodowanymi kluczami, a klucz wydany jest wyłącznie osobie upoważnionej | X | X | X |  | | Protokołowanie zamknięć | X | X | X |  | | Określenie osób upoważnionych do dostępu wraz z ich dokumentacją dla pracowników i firm zewnętrznych (serwis, odwiedzający) / (portier, ochrona zakładu) | X | X | - | Prowadzenie spisu odwiedzających na recepcji w Berlinie | | Firmy zewnętrzne, serwis i odwiedzający mogą wchodzić na teren zakładu wyłącznie w towarzystwie pracownika | X | X | X |  | | Legitymowanie osób upoważnionych do dostępu (klucz, kod pin) | X | X | X |  | | Dostęp z 2-etapową identyfikacją | X | - | - |  | | Odbiór dostępu po wygaśnięciu upoważnienia | X | X | X |  | | Istnieją obszary bezpieczeństwa z różnymi prawami dostępu | X | X | X |  |  Kontrola dostępu (do systemu) softgarden zabezpiecza systemy IT przed korzystaniem przez osoby nieupoważnione Następuje to poprzez:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Środki** | CD | B | SB | Uwagi | | Utworzenie konta użytkownika dla każdego użytkownika | X | X | X | Korzystanie z niepowiązanych personalnie kont wspierających dostęp do systemów klientów, danych dostępowych możliwe jest wyłącznie przez upoważnionych pracowników. | | Uwierzytelnianie osób upoważnionych do przetwarzania danych przy użyciu haseł (ze znakami specjalnymi, co najmniej 8 znaków, regularna zmiana hasła) | X | X | X |  | | Automatyczna blokada konta użytkownika w przypadku wielokrotnego wprowadzanie fałszywych danych dostępowych | X | X | X |  | | Automatyczna blokada miejsca pracy podczas braku aktywności | X | X | X |  | | Niezwłoczna blokada uprawnień w przypadku odejścia pracownika z pracy (wytyczne/instrukcja robocza) | X | X | X |  | | Regularna kontrola ważności uprawnień | X | X | X |  | | Korzystanie z zamykanych szaf do przechowywania dokumentacji papierowej | X | X | - | Niepozostawianie dokumentów papierowych w biurze Saarbrücken | | Zabezpieczone przenoszenie danych uwierzytelniających (uwierzytelnienie logowania) w sieci za pośrednictwem TLS/HTTPS, SSH, VPN (IPSec, openVPN) | X | X | X |  | | Hasła dostępu do komputerów w miejscu pracy są manualnie blokowane w przypadku dłuższej nieobecności danego pracownika (30 dni) i po powrocie muszą zostać ponownie manualnie przywrócone przez administratora IT. | X | X | X |  |  Kontrola dostępu (do danych) softgarden gwarantuje, że osoby upoważnione do korzystania z systemu przetwarzania danych mają dostęp wyłącznie do swojego uprawnienia dostępu oraz że podczas przetwarzania, korzystania lub przechowywania dane osobowe nie mogą być odczytywane, kopiowane, zmieniane lub usuwane przez osoby nieupoważnione. Następuje to poprzez:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Środki** | CD | B | SB | Uwagi | | Określenie uprawnień dostępowych do dostępu do danych (sporządzenie koncepcji uprawnień) | X | X | X |  | | Określenie pozwoleń na zapoznawanie się, wprowadzanie, zmianę i usuwanie danych, które są przetwarzane przez Zleceniobiorcę w ramach wykonywania zlecenia | X | X | X |  | | Regularna kontrola dostępu, wprowadzania, zmiany i usuwania | X | - | - |  | | Utylizacja niepotrzebnych nośników danych (wytyczne / instrukcja robocza) | X | X | X |  | | Regulacja pisemna w zakresie kopiowania danych (wytyczne bezpieczeństwa IT / instrukcja robocza) | X | X | X |  | | Przyznawanie uprawnień minimalnych (zasada need-to-know) | X | X | X |  | | Nieprzyznawanie identyfikatorów lub haseł generowanych i grupowych | X | - | - | Korzystanie z niepowiązanych personalnie kont wspierających dostęp do systemów klientów, danych dostępowych możliwe jest wyłącznie przez upoważnionych pracowników. | | Unikanie kumulowania funkcji – podział funkcji w zakresie czynności administracyjnych na różne, wyspecjalizowane osoby | X | X | X |  | | Prowadzenie historii przeprowadzonych zmian administracyjnych | X | X | X |  | | Dostęp do infrastruktury produkcyjnej za pośrednictwem VPN | - | X | X |  |  Kontrola podziału softgarden gwarantuje, że dane pobierane w różnych celach mogą być oddzielnie przetwarzane. Nie ma konieczności podziału fizycznego; podział logiczny danych jest wystarczający. Następuje to poprzez:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Środki** | CD | B | SB | Uwagi | | Oznaczenie pobranych danych (ID sygnatury, klient / numer sprawy) | X | X | X |  | | Logiczny podział różnych danych przetwarzanych dla Zleceniodawcy  Podział funkcji / produkcji / testu | X | X | X |  | | Dane osobowe poszczególnych pracowników oddzielane są logicznie od siebie poprzez przyporządkowanie do danego konta użytkownika. | - | X | X |  |  IntegralnośćKontrola przekazywania softgarden gwarantuje, że dane osobowe podczas ich przenoszenia drogą elektroniczną, transportowania lub zapisywania na nośnikach danych nie mogą być odczytywane, kopiowane, zmieniane lub usuwane oraz można sprawdzić i stwierdzić, w których miejscach przewidziana jest transmisja danych osobowych przez urządzenia do transmisji danych. Następuje to poprzez:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Środki** | CD | B | SB | Uwagi | | Określenie osób upoważnionych do przesyłania lub transportu (drogą elektroniczną, manualnie) | X | X | X |  | | Kontrola danych pod kątem kompletności po transporcie, przeniesieniu, przekazaniu, zapisaniu danych | X | X | X | Manualne porównanie sum kontrolnych | | Wdrożenie zabezpieczających przejść w punktach podłączenia do sieci | X | X | X |  | | Stosowanie uznanej procedury szyfrowania, która szyfruje całą komunikację między kandydatem, a serwerem Zleceniobiorcy. | X | X | X |  | | Przychodzące i wychodzące strumienie danych filtrowane są przy użyciu nowoczesnego, kaskadowego rozwiązania zapory sieci. | X | X | X |  | | Jeżeli nośnik danych przenoszony jest za pośrednictwem przedsiębiorstwa transportowego, nośniki danych przekazywane są wyłącznie po uprzednim uwierzytelnieniu przedsiębiorstwa. | X | X | X |  | | Nośniki danych i dokumentów z danymi osobowymi utylizowane są za pośrednictwem wyspecjalizowanej firmy utylizacyjnej zgodnie z polityką prywatności. | X | X | X |  | | Kompletne, trwałe usuwanie nośników danych z danymi osobowymi zgodnie z polityką prywatności jest protokołowane. Protokoły przechowywane są w bezpieczny sposób przez co najmniej 12 miesięcy. | X | X | X |  |  Kontrola wprowadzania softgarden gwarantuje, że w późniejszym czasie można sprawdzić i stwierdzić, czy i kto wprowadził, zmienił lub usunął dane osobowe w systemach przetwarzania danych. Następuje to poprzez:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Środki** | CD | B | SB | Uwagi | | Prowadzenie dokumentacji z uprawnieniami dostępu (instrukcja robocza, grupy dostępowe i uprawnienie dostępu) | X | X | X |  | | Rejestracja czynności w ramach zlecenia | X | X | X |  | | Wyrywkowa kontrola i analiza danych rejestrowych pod kątem nadużycia | X | - | X |  | | Dla wszystkich użytkowników, którzy korzystają z odpowiednich aplikacji w celu przetwarzania danych osobowych, prowadzona jest historia, jaki użytkownik kiedy wykonał daną czynność, jeżeli czynność ta prowadziła do modyfikacji danych. | - | X | X | Rejestracja historii przy użyciu aplikacji Just Hire |  Dostępność i obciążenieKontrola dostępności softgarden gwarantuje, że dane osobowe są chronione przed przypadkowym lub zamierzonym zniszczeniem lub utratą. Następuje to poprzez:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Środki** | CD | B | SB | Uwagi | | Zasilacz bezprzewodowy (UPS) | X | X | X |  | | Ochrona antywirusowa (w miejscach pracy) | X | X | X | Ochrona antywirusowa w miejscach pracy z oprogramowaniem Windows | | Ochrona antywirusowa (na serwerach) | X | X | X |  | | Firewall | X | X | X |  | | Istnieje plan awaryjny | X | X | X |  | | Redundantne centra danych | X | - | - |  | | Centralny system przeciwpożarowy | X | X | - |  | | Kontrola dostępności (monitoring) | X | X | X | Wszystkie systemy są pod kontrolą automatycznego monitoringu 24/7 |  Odzyskiwanie softgarden gwarantuje przywracanie dostępności danych osobowych oraz dostępu do nich w przypadku zdarzenia fizycznego lub technicznego przy użyciu następujących środków:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Środki** | CD | B | SB | Uwagi | | Procedura kopii zapasowej zgodnie z planem kopii zapasowej (codziennie, co tydzień, co miesiąc) | X | X | X |  | | Przechowywanie danych kopii zapasowej w szafach zabezpieczających dane, sejfach, w innym segmencie ochrony przeciwpożarowej | X | X | X |  |  Obciążenie softgarden gwarantuje dostępność oraz obciążenie systemów istotnych dla wykonywania działalności oraz systemów przetwarzania danych osobowych przy użyciu następujących środków technicznych i organizacyjnych:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Środki** | CD | B | SB | Uwagi | | Wirtualizacja i praca w infrastrukturze kontenerowej i z równoważeniem obciążenia | X | - | - |  | | Regularne kontrole penetracji produktów softgarden pod kątem słabych punktów w zakresie bezpieczeństwa | X | - | - | Produkty softgarden testowane są w środowisku centrum danych Nie stosuje się w środowisku biurowym. |  Procedura regularnej kontroli, analizy i ocenyZarządzanie ochroną danych softgarden gwarantuje proces regularnej kontroli i analizy skuteczności środków technicznych i organizacyjnych. Następuje to poprzez:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Środki** | CD | B | SB | Uwagi | | Wszyscy pracownicy zostali pisemnie zobowiązani do zachowania danych w tajemnicy (art. 28 ust. 3 lit. b)) oraz przeszkoleni w tym zakresie. | X | X | X |  | | Regularna analiza poziomu ochrony danych przez grupę ds. ochrony danych | X | X | X |  | | Osoby trzecie muszą złożyć oświadczenie o zachowaniu tajemnicy | X | X | X |  | | Jeżeli ze względów organizacyjnych dochodzi do nakładania się funkcji, stosowana i dokumentowana jest zasada dwóch par oczu. | - | X | X |  | | Istnieje określona regulacja reprezentacji w grupach funkcyjnych. | - | X | X |  |  Ocena prawidłowego poziomu bezpieczeństwa (art. 32 ust. 2 RODO) softgarden gwarantuje udokumentowaną ocenę prawidłowego poziomu ochrony w zakresie ryzyk, które są związane z przetwarzaniem danych osobowych zgodnie ze zleceniem, a przede wszystkim ryzyka zniszczenia, utraty, zmiany, nieupoważnionej publikacji lub nieupoważnionego dostępu. Następuje to poprzez:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Środki** | CD | B | SB | Uwagi | | Przeprowadzanie analizy ryzyka dla przetwarzania danych osobowych | X | X | X |  | | Sporządzenie kategorii wymagających ochrony | X | X | X |  | | Regulacja procesów zgodnie z „Privacy by Design & Default“. | - | X | X |  | | W razie konieczności przeprowadzanie oceny skutków ochrony danych (DSFA). | X | X | X |  |  Kontrola zlecenia (art. 32 ust. 3 i 4 RODO) softgarden gwarantuje, że dane osobowe, które są przetwarzane w ramach zlecenia, przetwarzane są wyłącznie zgodnie z poleceniami Zleceniodawcy oraz w celu spełnienia celu użytkowania określonego w umowie. Zleceniobiorca może to potwierdzić na podstawie procedury certyfikacji zgodnie z art. 40 lub 42 RODO. W przypadku braku certyfikacji, dowód przedkładany jest na podstawie:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Środki** | CD | B | SB | Uwagi | | Jednoznaczne sporządzenie umowy z podwykonawcami | X | X | X |  | | Formalizowanie udzielenia zlecenia (formularze) | X | X | X |  | | Regularna kontrola czynności | X | X | X | Kontrola procesów softgarden w ramach audytu wewnętrznego | | Osoby upoważnione do wydawania poleceń Zleceniodawcy oraz osoby upoważnione do przyjmowania poleceń są wyznaczone umownie, a polecenia wydawane pisemnie. | X | X | X |  | | softgarden niezwłocznie informuje Zleceniodawcę o wszelkich poważnych awariach w zakładzie, podejrzeniu naruszenia ochrony danych, gdy zostaną stwierdzone błędy lub inne nieścisłości w postępowaniu z danymi Zleceniodawcy. | X | X | X |  | | Zlecenia rejestrowane są w formie support-ticket (minimalne dane: Zleceniodawca/klient, czynność/zlecenie częściowe, dokładna specyfikacja etapów/parametrów przetwarzania, osoba przetwarzająca, terminy, ew. odbiorca), w nich dokumentowane są przeprowadzone dane. Numer support-ticket jest jednoznacznie przyporządkowany do zlecenia klienta. | X | X | X |  |  |  | | --- | | **Deklaracja zobowiązania do wdrażania środków technicznych i organizacyjnych** |   Zleceniobiorca potwierdza, że wdrożył środki techniczne i organizacyjne w zakresie ochrony danych osobowych Zleceniodawcy – jak opisano w **Załączniku 2** - przed rozpoczęciem przetwarzania danych. Zleceniobiorca zobowiązuje się do spełniania tych wymogów na czas współpracy oraz regularnej kontroli, dokumentowania, a na żądanie Zleceniodawcy, do ich udostępniania.  Środki techniczno-organizacyjne podlegają postępowi technicznemu oraz dalszemu rozwojowi. Zleceniobiorca może wdrażać odpowiednie środki alternatywne, o ile dostanie na to pozwolenie. Przy tym nie mogą one posiadać niższego poziomu bezpieczeństwa niż ustalone środki. Istotne zmiany należy dokumentować i niezwłocznie przekazać Zleceniodawcy.   |  |  |  | | --- | --- | --- | |  |  |  | | Miejscowość, data |  | Mathias Heese / Prezes  Martin Behrend / VP Finance  Nazwa Zleceniodawcy / podpis / pieczęć firmowa | |