|  |
| --- |
| **Technisch-organisatorische Maßnahmen gemäß Art. 32 DSGVO** |

Die nachfolgend beschriebenen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO sind nicht für die Öffentlichkeit bestimmt. Zugriff auf diese Informationen haben nur der betriebliche Datenschutzbeauftragte, die jeweils zuständigen Aufsichtsbehörden zum Datenschutz und die eigenen die dazu befugten Mitarbeiter der jeweiligen datenverarbeitenden Stelle.

**Nach Prüfung durch den Auftraggeber** werden die nachfolgend beschriebenen technischen und organisatorischen Maßnahmen – als Bestandteil des vorliegenden Datenschutzvertrags – verbindlich: Sie sind wie folgt zwischen Auftragnehmer und Auftraggeber festgelegt:

Die nachfolgend beschriebenen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO sind nicht für die Öffentlichkeit bestimmt. Zugriff auf diese Informationen haben nur der betriebliche Datenschutzbeauftragte, die jeweils zuständigen Aufsichtsbehörden zum Datenschutz und die eigenen die dazu befugten Mitarbeiter der jeweiligen datenverarbeitenden Stelle.

# Abkürzungen

* RZ: Rechenzentren
* B: softgarden Büro Berlin
* SB: softgarden Büro Saarbrücken

# Vertraulichkeit

## Zutrittskontrolle

softgarden stellt sicher, dass Unbefugte keinen Zutritt zu den Büro-, Server- und Archivräumen haben. Dies geschieht durch:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Maßnahmen** | RZ | B | SB | Anmerkungen |
| Zentraler Empfangsbereich (Empfang) | X | X | - |  |
| Zugang durch eine Alarmanalage mit aufgeschaltetem Wachschutz | X | - | - |  |
| Zugang mit codierten Schlüsseln und Schlüsselausgabe nur an Befugte | X | X | X |  |
| Protokollierung der Schließungen | X | X | X |  |
| Festlegung der Zutrittsberechtigten einschließlich ihrer Dokumentation für Mitarbeiter und Firmenfremde (Wartungspersonal, Besucher) / Pförtner, Werkschutz) | X | X | - | Führen einer Besucherliste am Empfang in Berlin |
| Firmenfremde, Wartungspersonal und Besucher dürfen nur in Begleitung eines Mitarbeiters die Räumlichkeiten betreten | X | X | X |  |
| Legitimation der Zutrittsberechtigten (Schlüssel, PinCode) | X | X | X |  |
| 2-Faktor Authentifizierung Zutritt | X | - | - |  |
| Rücknahme von Zugangsmitteln nach Ablauf der Berechtigung | X | X | X |  |
| Es existieren Sicherheitsbereiche mit unterschiedlichen Zutrittsberechtigungen | X | X | X |  |

## 

## Zugangskontrolle

softgarden verhindert, dass EDV-Systeme von Unbefugten genutzt werden können. Dies geschieht durch:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Maßnahmen** | RZ | B | SB | Anmerkungen |
| Einrichtung eines Benutzerkontos pro Nutzer | X | X | X | Nutzung von personen-ungebundenen Support-Accounts für Zugriff auf Kundensysteme, Zugangsdaten sind nur berechtigten Mitarbeitern zugänglich |
| Authentifikation der mit der Datenverarbeitung befugten Personen durch ein Kennwortverfahren (mit Sonderzeichen, Mindestlänge 8 Zeichen, regelmäßiger Wechsel des Kennworts | X | X | X |  |
| Automatische Sperrung des Benutzerkontos bei mehrfacher fehlerhafter Eingabe der Zugangsdaten | X | X | X |  |
| Automatische Sperrung des Arbeitsplatzes bei Inaktivität | X | X | X |  |
| Umgehende Sperrung von Berechtigungen beim Ausscheiden von Mitarbeitern (Richtlinie/Arbeitsanweisung) | X | X | X |  |
| Regelmäßige Kontrolle der Gültigkeit von Berechtigungen | X | X | X |  |
| Die Nutzung von abschließbaren Schränken zur Aufbewahrung von Papierakten | X | X | - | keine Papieraktenlagerung im Büro Saarbrücken |
| Gesicherte Übertragung von Authentisierungsgeheimnissen (Credentials) im Netzwerk mittels TLS/HTTPS, SSH, VPN (IPSec, openVPN) | X | X | X |  |
| Zugangskennungen zu Arbeitsplatzrechnern werden bei längerer Abwesenheit des entsprechenden Mitarbeiters (30 Tage) manuell gesperrt und müssen nach Rückkehr wieder manuelle durch die IT-Administration entsperrt werden. | X | X | X |  |

## Zugriffskontrolle

softgarden gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Dies geschieht durch:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Maßnahmen** | RZ | B | SB | Anmerkungen |
| Festlegung der Zugriffsberechtigungen für den Zugriff auf Daten (Erstellung eines Berechtigungskonzeptes) | X | X | X |  |
| Festlegung der Befugnisse zur Kenntnis, Eingabe, Veränderung und Löschung von Daten, die im Rahmen der Auftragserfüllung durch den Auftragnehmer verarbeitet werden | X | X | X |  |
| Regelmäßige Kontrolle des Zugriffs, Eingabe, Veränderung und Löschung | X | - | - |  |
| Entsorgung nicht mehr benötigter Datenträger (Richtlinie / Arbeitsanweisung) | X | X | X |  |
| Schriftliche Regelung zum Kopieren von Daten (IT Sicherheitsrichtlinie / Arbeitsanweisung) | X | X | X |  |
| Vergabe minimaler Berechtigungen (Need-to-know -Prinzip) | X | X | X |  |
| Keine Vergabe von generischen oder Gruppenkennungen oder Passwörtern | X | - | - | Nutzung von personen-ungebundenen Support-Accounts für Zugriff auf Kundensysteme, Zugangsdaten sind nur berechtigten Mitarbeitern zugänglich |
| Vermeidung der Konzentration von Funktionen - Funktionstrennung von Administratorentätigkeiten auf unterschiedliche qualifizierte Personen | X | X | X |  |
| Führen einer Historie durchgeführter administrativer Änderungen | X | X | X |  |
| Zugriff auf die Produktionsinfrastruktur über VPN | - | X | X |  |

## Trennungskontrolle

softgarden gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Es besteht keine Notwendigkeit zu einer physischen Trennung; eine logische Trennung der Daten ist ausreichend. Dies geschieht durch:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Maßnahmen** | RZ | B | SB | Anmerkungen |
| Kennzeichnung der erfassten Daten (Aktenzeichen. ID, Kunden/Vorgangsnummer) | X | X | X |  |
| Logische Trennung der für unterschiedliche Auftraggeber verarbeiteten Daten Funktionstrennung /Produktion/ Test | X | X | X |  |
| Die personenbezogenen Daten der jeweiligen Auftraggeber werden durch Zuordnung zu den jeweiligen Benutzeraccounts logisch voneinander getrennt. | - | X | X |  |

# Integrität

## Weitergabekontrolle

softgarden gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtung zur Datenübertragung vorgesehen ist. Dies geschieht durch:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Maßnahmen** | RZ | B | SB | Anmerkungen |
| Festlegung der zur Übermittlung bzw. den Transport (elektronisch, manuell) befugten Personen | X | X | X |  |
| Prüfung der Daten auf Vollständigkeit nach Datentransport, -übertragung und Datenübermittlung oder -speicherung | X | X | X | Manueller Abgleich mit Checksummen |
| Implementation von Sicherheitsgateways an den Netzübergabepunkten | X | X | X |  |
| Einsatz eines anerkannten Verschlüsselungsverfahrens, welches sämtliche Kommunikation zwischen dem Bewerber und den Servern des Auftragnehmers verschlüsselt. | X | X | X |  |
| Ein- und ausgehende Datenströme werden durch eine moderne, kaskadiert aufgebaute Firewall-Lösung gefiltert | X | X | X |  |
| Soweit Datenträger durch Transportunternehmen übermittelt werden, werden die Datenträger nur nach vorheriger Authentisierung des Transportunternehmens weitergegeben. | X | X | X |  |
| Papier- und Datenträger mit personenbezogenen Daten werden durch ein qualifiziertes Entsorgungsunternehmen datenschutzgerecht entsorgt. | X | X | X |  |
| Die vollständige, datenschutzgerechte und dauerhafte Löschung von Datenträgern mit personenbezogenen Daten wird protokolliert. Die Protokolle werden mindestens 12 Monate revisionssicher aufbewahrt. | X | X | X |  |

## Eingabekontrolle

softgarden gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Dies geschieht durch:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Maßnahmen** | RZ | B | SB | Anmerkungen |
| Führung einer Dokumentation der Zugriffsberechtigungen (Arbeitsanweisung Zugriffsgruppen und Zugriffsberechtigung) | X | X | X |  |
| Erfassung der Tätigkeiten im Rahmen des Auftrags | X | X | X |  |
| Stichprobenartige Kontrolle und Auswertung der Protokolldaten auf Missbrauch | X | - | X |  |
| Für alle Nutzer, die die entsprechenden Anwendungsprogramme zur Verarbeitung der personenbezogenen Daten nutzen, wird eine Historie vorgehalten, die erfasst, welcher Nutzer wann welche Aktion ausgeführt hat, sofern diese Aktion persönliche Daten modifiziert. | - | X | X | Erfassung der Historie in der Anwendung Just Hire |

# Verfügbarkeit und Belastbarkeit

## Verfügbarkeitskontrolle

softgarden gewährleistet, dass personenbezogene Daten gegen zufällige oder vorsätzliche Zerstörung oder Verlust geschützt sind. Dies geschieht durch:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Maßnahmen** | RZ | B | SB | Anmerkungen |
| Unterbrechungsfreie Stromversorgung (USV) | X | X | X |  |
| Virenschutz (auf den Arbeitsplätzen) | X | X | X | Virenschutz auf Windows Arbeitsplätzen |
| Virenschutz (auf den Servern) | X | X | X |  |
| Firewall | X | X | X |  |
| Es existiert ein Notfallplan | X | X | X |  |
| Georedundante Rechenzentren | X | - | - |  |
| Zentrale Brandmeldeanlage | X | X | - |  |
| Verfügbarkeitsüberwachung (Monitoring) | X | X | X | Alle kritischen Systeme werden 24/7 durch automatisierte Monitoring Verfahren überwacht |

## Wiederherstellbarkeit

softgarden gewährleistet die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu diesen bei einem physischen oder technischen Zwischenfall durch die folgenden Maßnahmen rasch wiederherzustellen:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Maßnahmen** | RZ | B | SB | Anmerkungen |
| Backup-Verfahren gem. Backupkonzept (täglich, wöchentlich, monatlich) | X | X | X |  |
| Aufbewahrung der Backup-Daten in Datensicherungsschränken, Tresoren, im anderen Brandabschnitt | X | X | X |  |

## 

## Belastbarkeit

softgarden gewährleistet Verfügbarkeit und Belastbarkeit geschäftskritischer Systeme und der Systeme zur Verarbeitung personenbezogener Daten durch folgende technischen und organisatorischen Maßnahmen:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Maßnahmen** | RZ | B | SB | Anmerkungen |
| Virtualisierung und Betrieb in Containerinfrastruktur mit Loadbalancern | X | - | - |  |
| regelmäßige Penetrationstests der softgarden Produkte auf Sicherheitsschwachstellen | X | - | - | Getestet werden die softgarden Produkte in der Umgebung der Rechenzentren. Nicht anwendbar in der Umgebung der Büroräume. |

# Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

## Datenschutzmanagement

softgarden gewährleistet einen Prozess zur regelmäßigen Überprüfung und Bewertung der Wirksamkeit der technischen und organisatorischen Schutzmaßnahmen. Dies geschieht durch:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Maßnahmen** | RZ | B | SB | Anmerkungen |
| Alle Mitarbeiter wurden schriftlich auf das Datengeheimnis (Art. 28 Abs.3 lit.b)) verpflichtet und unterwiesen. | X | X | X |  |
| Regelmäßige Bewertung des Datenschutz-Niveaus durch die Datenschutz-Gruppe | X | X | X |  |
| Dritte müssen eine Verschwiegenheitserklärung abgeben | X | X | X |  |
| Wenn aus organisatorischen Gründen Funktionsüberschneidungen bestehen, wird das Vier-Augen-Prinzip angewendet und dokumentiert. | - | X | X |  |
| Es existiert eine definierte Vertreterregelung innerhalb der Funktionsgruppen | - | X | X |  |

## Beurteilung des angemessenen Schutzniveaus (Art. 32 Abs. 2 DS-GVO)

softgarden gewährleistet eine dokumentierte Beurteilung eines angemessenen Schutzniveaus, bezüglich der Risiken, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust, Veränderung, unbefugter Offenlegung oder unbefugtem Zugang - der im Auftrag verarbeiteten personenbezogenen Daten. Dies geschieht durch:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Maßnahmen** | RZ | B | SB | Anmerkungen |
| Durchführung einer Risikoanalyse für die Verarbeitungen personenbezogener Daten | X | X | X |  |
| Erstellung von Schutzbedarfskategorien | X | X | X |  |
| Ausrichtung der Prozesse nach „Privacy by Design & Default“. | - | X | X |  |
| Bei Bedarf die Durchführung einer Datenschutz-Folgenabschätzung (DSFA) | X | X | X |  |

## Auftragskontrolle (Art. 32 Abs. 3 und 4 DS-GVO)

softgarden gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers und zur Erfüllung des vertraglich definierten Verwendungszweckes verarbeitet werden. Der Auftraggeber kann dies durch ein gemäß Art. 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Art. 42 DSGVO nachweisen. Sollte keine Zertifizierung vorliegen geschieht der Nachweis durch:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Maßnahmen** | RZ | B | SB | Anmerkungen |
| Eindeutige Vertragsgestaltung mit Unterauftragnehmern | X | X | X |  |
| Formalisierung der Auftragserteilung (Formularwesen) | X | X | X |  |
| Regelmäßige Kontrolle der Tätigkeiten | X | X | X | Überwachung der softgarden Prozesse durch interne Audits |
| Die Weisungsberechtigten des Auftraggebers und die zur Entgegennahme von Weisungen befugten Personen sind vertraglich definiert, Weisungen erfolgen immer schriftlich. | X | X | X |  |
| softgarden informiert den Auftraggeber unverzüglich über Fälle von schwerwiegenden Betriebsstörungen, bei Verdacht auf Datenschutzverletzungen, wenn Fehler festgestellt werden oder anderen Unregelmäßigkeiten beim Umgang mit Daten des Auftraggebers. | X | X | X |  |
| Aufträge werden als Support-Ticket (Mindestangaben: Auftraggeber/Kunde, Aktion/Teilauftrag, genaue Spezifikation der Verarbeitungsschritte/-parameter, Bearbeiter, Termine, ggf. Empfänger) erfasst, dort werden die durchgeführten Arbeiten dokumentiert. Es gibt eine eindeutige Zuordnung zwischen Support-Ticketnummer und Kundenauftrag. | X | X | X |  |

|  |
| --- |
| **Verpflichtungserklärung zur Umsetzung der  technischen und organisatorischen Maßnahmen** |

Der Auftragnehmer bestätigt, dass er die technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten des Auftraggebers – wie in **Anlage 2** beschrieben – vor Beginn der Datenverarbeitung umgesetzt hat. Der Auftragnehmer verpflichtet sich, die Erfüllung dieser Anforderungen für die Dauer der Zusammenarbeit sicherzustellen, regelmäßig zu kontrollieren, zu dokumentieren und auf Nachfrage des Auftraggebers zur Verfügung zu stellen.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insofern ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber unverzüglich mitzuteilen.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Ort, Datum |  | Mathias Heese / Geschäftsführer  Martin Behrend / VP Finance  Name des Auftragnehmers/ Unterschrift / Firmenstempel |