Technisch Organisatorische Maßnahmen (Art. 32 DSGVO)

Die folgenden technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit sind implementiert:

1.) Anonymisierung / Pseudonymisierung

a) Definitionen

Anonymisierung

„das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können."

Pseudonymisierung

„das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren."

b) Verarbeitung durch LogOn Recruiting Technologie

Im Zuge der Verarbeitung personenbezogener Daten durch LogOn eRecruiting Tools, werden diese pseudonymisiert bzw. teilweise anonymisiert.

c) Nutzerverwaltung/Kundendaten

Kundendaten bzw. Nutzerdaten, die für die Nutzung der Tools eingegeben werden bzw. durch den Geschäftsverkehr entstehen, werden auf LogOn Systemen gespeichert.

2.) Verschlüsselung

Alle mobilen Datenträger werden nach dem Stand der Technik verschlüsselt. Die internen IT-Richtlinien regeln den Umgang mit Daten sowie deren Speicherung.

3.) Sicherstellung der Vertraulichkeit

Zutrittskontrolle

Maßnahmen die Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden verwehren:

Bei dem durch die Firma LogOn Tech GmbH genutzten Gebäude handelt es sich um ein Bürogebäude welches durch mehrere Firmen genutzt wird.
Die Eingangstür wird durch ein codiertes Schloss gesichert. Die Gebäudeeingangstür ist nach außen mit einem starren Türknauf anstatt einer Klinke ausgestattet. Ferner ist das Gebäude durch ein Zutrittskontrollsystem ausgestattet.

Die Büroräume sind ebenfalls durch ein codiertes Schloss gesichert und nach außen nur mit einem starren Türknauf anstatt einer Klinke ausgestattet. Des Weiteren sind die Räume durch ein elektronisches Zutrittskontrollsystem ausgestattet und sind während der Geschäftszeiten außer zum Betreten und Verlassen geschlossen. Außerhalb der Geschäftszeiten sind die Büroräume abgeschlossen.

Die Räume der Personalverwaltung sind durch ein codiertes Schloss gesichert.
Ferner sind die Räume mit einem elektronischen Zutrittskontrollsystem ausgestattet und außerhalb der Geschäftszeiten fest abgesperrt. Zutritt zum Büro der Personalverwaltung wird nur gestattet, solange die Personalverwaltung oder der Geschäftsführer im Büro ist.

Der Serverraum wird ebenfalls durch ein codiertes Schloss gesichert. Zudem ist der Raum mit einem elektronischen Zutrittskontrollsystem ausgestattet und während der Geschäftszeiten außer zum Betreten und Verlassen abgeschlossen. Außerhalb der Geschäftszeiten ist der Raum fest abgeschlossen.

In der Tiefgarage ist noch ein weiterer Zu- und Ausgang vorhanden. Dieser Eingang ist durch eine normale Tür mit einem Türöffner-Chip gesichert.

Schlüssel und sonstige Zutrittsmittel werden ausschließlich an Berechtigte ausgegeben und sofort eingezogen, sollte die Berechtigung erlöschen. Die Berechtigung zum Betreten wird durch geeignete Maßnahmen protokolliert und dokumentiert.
Bei Verlust eines Zutrittsmittels oder wenn ein ehemals Berechtigter ein Zutrittsmittel nicht freiwillig zurückgibt wird das Zutrittsmittel gesperrt oder, sollte dies nicht möglich sein, wird das Schlosssystem ausgetauscht. Es existiert ein Berechtigungskonzept zur Feststellung der Kopierberechtigung der Zugangsschlüssel. Bei Chipkartengesicherten Türschlössern können die letzten 2000 Bedienungen abgerufen werden.

Die Fenster des Bürogebäudes bestehen aus Isolierverglasung. Weiter sind die Fenster nicht gesichert, da sich das Büro um 2. Stock befindet.

Zu- und Abgänge von Mitarbeitern werden über Chipkarten bzw. Transponder festgestellt und protokolliert.

Fremden Personen ist der Aufenthalt im gesamten Unternehmensgebäude sowie in den Büroräumen nur in Anwesenheit von Mitarbeitern gestattet. Hilfspersonen werden stets sorgfältig ausgewählt.

Zugangskontrolle
Maßnahmen die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können

Für den Zugriff auf die Datenverarbeitungssysteme ist ein Passwortsystem eingerichtet, für dieses System gibt es eine entsprechende Passwortrichtlinie. Jeder Berechtigte erhält eine individuelle Benutzerkennung und ein persönliches, geheim zu haltendes Passwort, welches nicht an Dritte weitergegeben werden darf. Für den Fall der Abwesenheit besteht eine entsprechende Regelung.
Berechtigungen werden in regelmäßigen Abständen kontrolliert. Sobald eine Berechtigung erlischt wird das Passwort gesperrt.
Das Passwort besteht aus wenigstens 8 Zeichen (zufällig ausgewählten Großbuchstaben, Kleinbuchstaben Sonderzeichen und Zahlen). Das vergebene Passwort muss spätestens alle drei Monate vom Berechtigten selbst geändert werden.
Nach 1 Stunde Inaktivität wird ein Berechtigter automatisch vom System abgemeldet.
Beim Verlassen des Arbeitsplatzes ist der Bildschirm zu sperren. Während der Mittagspause werden alle User abgemeldet und die Laptops im persönlichen Spind eingeschlossen.

Die internen Netze werden nach dem Stand der Technik gegen Zugriffe von außen durch eine vollständige physische Trennung interner und externer Netzwerke abgeschottet. Zudem wird die Software der Firewall wenigstens täglich aktualisiert. Die internen Netzte werden verschlüsselt.

Verbindungswege werden von außen durch ein Virtual Private Network abgesichert.

Zugriffskontrolle
Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die Ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

Zugriffe der Benutzer werden bei An- und Abmeldung sowie bei Programmausführung protokolliert. Shell-Zugriffe werden ebenfalls protokolliert. Versuchte Richtlinienverstöße sowie der generelle Internetzugriff werden protokolliert.

Organisatorische Voraussetzungen wie zum Beispiel Organigramme, Stellenbeschreibungen und Aufgabenbeschreibungen sind vorhanden. Diese werden regelmäßig aktualisiert und in Rollendefinitionen umgesetzt, die Rollenzuordnung wird regelmäßig überprüft. Es existiert ein entsprechendes Berechtigungskonzept.
Innerhalb des Zugriffsberechtigungskonzepts sind abgestufte Zugriffsberechtigungen aufgebaut, die das Eingeben, Lesen, Kopieren, Verändern oder Entfernen von Auftraggeberdaten bei Verarbeitung, Nutzung und nach der Speicherung nur in dem für die jeweilige Aufgabe erforderlichen Umfang erlauben und ansonsten verhindern. Dieses Zugriffsberechtigungskonzept umfasst die Verwaltung der Zugriffsrechte durch Systemadministratoren.
Die einzelnen Datenbanken sind verschlüsselt, die Verschlüsselung folgt dem AES-Standard mit einer Schlüssellänge von 256 Bit sowie mit einem Hash Algorithmus.
Die Zugriffsmöglichkeiten sind zeitlich begrenzt. Zudem erfolgt eine Trennung von Test- und Produktionsbetrieb.
Die E-Mail- und Internetnutzung erfolgt kontrolliert und organisiert. Die private E-Mail- und Internetnutzung ist im Unternehmen geregelt.
Nicht mehr benötigte Datenträger und Fehldrucke werden datenschutzgerecht entsorgt.

Trennungskontrolle
Maßnahmen die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

Für die Datenerhebung- und Verarbeitung gibt es ein entsprechendes Konzept.
Des Weiteren besteht eine Dokumentation der Archivierung und Recherche.
Datenerhebungszwecke werden immer genau dokumentiert. Sofern Daten für mehr als eine verantwortliche Stelle gespeichert werden erfolgt dies in einer mandantenfähigen Datenbank und unter Dokumentation der Zwecke, für welche die jeweiligen Daten verarbeitet und genutzt werden sollen. Zudem sind die Zugriffsreche klar festgelegt.

Die Produktions- und Testnetze sind durch geeignete Maßnahmen physikalisch getrennt. Das Sicherheitsniveau der Testsysteme ist dabei ebenso hoch wie das der Produktionssysteme. Es ist gewährleistet, dass nur nach Rücksprache mit dem Auftraggeber Produktionsdaten als Testdaten verwendet werden.

4.) Sicherstellung der Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle
Maßnahmen die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Der Auftragnehmer gewährleistet einen hinreichenden Softwareschutz gegen die Verletzung der Systemintegrität durch speicherresidente Scanner gegen Viren, Trojaner, Würmer und sonstige Malware.

Die Ausführung arbeitsplatzfremder Software wird durch vertragliche Verbote der Nutzer, technische Maßnahmen und Spamfilter verhindert. Zudem wird die Ausführung arbeitsplatzfremder Software durch eine wenigstens tägliche Aktualisierung des Betriebssystems, der vorhandenen Betriebs- und Sicherheitssoftware verhindert. Ferner findet eine Lizenzüberwachung statt.

Der Auftragnehmer gewährleistet durch eine unterbrechungsfreie Stromversorgung und die Einhaltung der einschlägigen Brandschutzvorschriften einen hinreichenden Hardwareschutz. Der Serverraum wird klimatisiert bzw. gekühlt.

Der Datenbestand wird wenigstens einmal täglich inkrementell und einmal monatlich vollständig auf externen Speichermedien verschlüsselt gesichert.

Auftragskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

Für jede Auftragsdatenverarbeitung existiert ein schriftlicher Vertrag. Die zu erfüllenden technischen und organisatorischen Maßnahmen sind Bestandteil dieses Vertrags.
Vor Beginn und danach finden regelmäßig Überprüfungen beim Auftragnehmer statt, ob dieser die vertraglichen Vereinbarungen einhalten kann und einhält. Bei der Aushändigung lesbarer Datenträger wird sichergestellt, dass sich darauf keine Restdaten, etwa von anderen Verarbeitungen befinden. Es werden schriftliche Regelungen getroffen, wie der Auftragnehmer nicht mehr benötigte Unterlagen zu behandeln hat.

5.) Sicherstellung der Integrität

Weitergabekontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Alle Beteiligten werden identifiziert und authentifiziert. Die Authentifizierung erfolgt über Eingabe eines Passworts und ein Auth-Verfahren. Übertragene Daten, wie auch E-Mail Anhänge werden verschlüsselt.
Mobile Datenträger mit Auftraggeberdaten, mobile Endgeräte mit Auftraggeberdaten und USB Ports dürfen nur von speziell zur Datenweitergabe und – Sicherung befugten Mitarbeitern ausschließlich für Vertrags- und Sicherungszwecke eingesetzt werden. Auftraggeberdaten werden auf mobilen Datenträgern, auf Datenträgern in mobilen Endgeräten und zur elektronischen Weitergabe stets verschlüsselt.

Das Passwort der Verschlüsselung besteht aus wenigstens 8 Zeichen (zufällig ausgewählten Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen), generische Begriffe und Eigennamen dürfen nicht verwendet werden. Die einzelnen Datenbanken sind verschlüsselt. Für die elektronische Weitergabe besteht eine besonders gesicherte Leitung.
Bei den zur Erhebung, Verarbeitung und Nutzung von Auftraggeber-Daten eingesetzten Systeme sind Bildschirme und andere Ausgabegeräte so angeordnet, dass unbeteiligte Mitarbeiter und sonstige Dritte keinen Einblick in diese Daten nehmen können.

Datenempfänger und Transport – und Übermittlungswege werden stets dokumentiert. Die zur Weitergabe von Daten befugten Personen und die zu übermittelnden Daten werden ebenfalls dokumentiert. Selbiges gilt für die eingesetzten Abruf- und Übermittlungsprogramme.

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Unbefugte eingaben, Veränderungen und Löschungen werden durch ein Passwortsystem verhindert. Die Anwendungen Office, Datev und Basecamp, Trello und Slack haben eine zweite Zugangskontrolle. Die Eingabe, Veränderung oder Löschung von personenbezogenen Daten wird revisionssicher protokolliert. Zudem werden Eingangsberechtigungen revisionssicher geführt und schriftlich erteilt. Alle Mitarbeiter sind auf die Vertraulichkeit verpflichtet.

6.) Wiederherstellung der Daten

Es besteht ein eigenes umfangreiches Backup-Konzept, ein Notfallhandbuch. Hierbei wird auf das mehrstufige Sicherheitskonzept im DIN ISO 27001 zertifizierten Rechenzentrumsbetrieb der IDKOM Networks GmbH und Oracle Deutschland B.V. & Co. KG zurückgegriffen.

7.) Laufende Bewertung und Evaluierung

Eine Datenschutzleitlinie ist implementiert.
Ein Datenschutzbeauftragter ist bestellt und wird regelmäßig im Datenschutz geschult.
Die Mitarbeiter-/innen werden regelmäßig in Datenschutzangelegenheiten unterwiesen.
Ein Meldeprozess für eine Datenschutzverletzung ist implementiert.

Die technischen und organisatorischen Maßnahmen werden jährlich durch den Datenschutzbeauftragten sowie den Geschäftsführer auditiert. Im Rahmen des Audits werden die Maßnahmen in Bezug auf den Stand der Technik, sowie die notwendigen technischen und rechtlichen Anforderungen geprüft und ggf. angepasst. Das Ergebnis des Audits wird entsprechend dokumentiert.