Technische & organisatorische Maßnahmen der eRecruiter GmbH

Kategorie	Bereich	Maßnahme(n)	technisch (T) / organisatorisch (O)	Gilt nicht bei eigenem Hosting der Software
Zutrittskontrolle				
Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.				
	Rechenzentrumzugang	Lagerung aller Daten bei NextLayer, einem ISO 27001 zertifizierten Rechenzentrum mit Sitz in Wien (Österreich). Siehe Annex ./1a	TO	X
	Bürozugang	Der Zutritt zu den Büroräumlichkeiten ist durch Schüssel bzw. Fingerprint gesichert.	TO	
	Bereiche im Büro	Weiters sind in Büroräumlichkeiten Sicherheitszonen eingerichtet (Serverraum, HR/Finance) sind gesondert abgegrenzt.	TO	
	Videoüberwachung	Es erfolgt zudem am Hauptstandort eine Videoüberwachung der öffentlichen Räume (Eingangsbereich, Treppenhaus) durch eine externe Sicherheitsfirma.	T	
	Biometrische Zugangskontrolle	Am Hauptstandort wird der Zugang durch einen Fingerabdruckscan gewährt.	T	
	Bürozugang	Das Büro wird während der Abwesenheit aller Mitarbeiter abgesperrt und auch die Fenster werden geschlossen.	O	
	Bürozugang	Closed-Shop-Betrieb; Es gibt bei uns keinen Publikumsverkehr.	O	
	Besucher	Es werden keine Besucher empfangen.	O	
	Instandhaltungsarbeiten / Wartungsarbeiten an Büromobiliar	Wenn Instandhaltungs- und oder Wartungsarbeiten stattfinden durch Arbeiter ist immer mindestens ein Mitarbeiter ebenfalls im Büro.	O	

	Büro für Finance, Lagerraum	Sind nur für die jeweiligen Mitarbeiter via biometrischer Zutrittskontrolle (Fingerprintscan) zugänglich.	T	
	Büromöbel für Finance	Büromöbel sind zusätzlich verschließbar.	T	

Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.				
	Rechenzentrum	Lagerung aller Daten verschlüsselt bei NextLayer, einem ISO 27001 zertifizierten Rechenzentrum mit Sitz in Wien (Österreich). Siehe Annex ./1a	TO	X
	Passworte für Firmenlaptops	Es wird eine Passwortrichtlinie (min. 7 Zeichen, kein Name, min. 1 Kleinbuchstabe, min. 1 Großbuchstabe, min. 1 Zahl/Sonderzeichen, Wechsel alle 6 Montate und keine Wiederverwendung) eingesetzt, die für alle Passwörter von Domain-Accounts eingesetzt wird.	T	
	Notebooks	Die Laptops aller Mitarbeiter sind mit Bitlocker gesichert und verschlüsselt.	T	
	Telearbeit / Home Office	Bei Remote Arbeit (unterwegs oder zu Hause) ist die Verbindung via VPN nötig um Zugriff auf seine E-Mails und sein Laufwerk zu haben.	T	
	Differenzierter Zugang zu Daten und Systemen	Gewisse Datenbereiche sind nur für bestimmte Personen (abhängig von ihre Rolle und ihren Aufgaben im Unternehmen) einseh- oder bearbeiterbar.	TO	
	eRecruiter	Der Zugriff auf den eRecruiter erfolgt über Benutzer mit Passwörtern, die sich an eine, dem Kunden angepasste, Passwortrichtlinie halten müssen.	TO	
	Firmenhandys	Firmenhandys müssen bei "find my iphone" aktiviert sein um im Falle eines Verlusts gelöscht werden zu können.	TO	

Zugriffskontrolle

Maßnahmen, die gewährleisten, 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.				
	eRecruiter	eRecruiter protokolliert das Login aller Benutzer, inkl. dem Administratorzugang, der nur für Support verwendet wird.	T	
	eRecruiter - Zugang zu Kunden	Die Logindaten für den Administratorzugang sind in einem abgegrenzten Bereich gespeichert zu dem nur Mitarbeiter die im Support arbeiten, zugriff haben.	T	
	eRecruiter - Einsicht in Passwörter	Im eRecruiter sind Passwörter von Benutzern, Bewerbern und auch Ansprechpartnern für NIEMANDEN ersichtlich. Passwörter können nur neu gesetzt werden - nicht aber eingesehen.	T	
	eRecruiter - Rollen und Rechte	Vergabe von Benutzerrechten erfolgt aufgrund der mit dem Kunden definierten Regeln.	TO	
	eRecruiter - Löschung von Daten	Es werden keine Benutzer, Ansprechpartner, Jobs oder Bewerber im eRecruiter unserer Kunden gelöscht - außer auf ausdrückliche schriftliche Weisung des Kunden.	O	
	eRecruiter - Near Shoring Entwicklerteam	Das Near Shoring Entwicklerteam arbeitet nur am Quellcode des eRecruiters und testet auf einem eigenen System, dass keinerlei Echtdaten beinhaltet. Zugriff auf echte personenbezogene Daten ist daher nicht möglich.	T	
	intern eingesetzte Datenverarbeitende Systeme	Nicht jeder hat Zugriff zu allen Systemen. Zugriffe werden nach Tätigkeitsbereich auf das notwendige beschränkt.	TO	
	physische Dokumente	Es wird nach Möglichkeit ohne physische Ausdrucken / Papieren gearbeitet.	O	

	Vernichtung von physischen Dokumenten	Ein Aktenvernichter (Cross Shredder) wird verwendet.	TO	

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, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.				
	Speichermedien	Es besteht eine Weisung, dass Daten nicht auf mobilen Datenträgern gespeichert werden.	O	
	Notebooks	Es besteht eine Weisung, dass Notebooks nur von befugten Personen verwendet und transportiert werden dürfen.	O	
	eRecruiter - Weitergabe an Partner	Es werden nur Daten unserer Kunden weitergegeben, wenn Partnerfeatures explizit vom Kunden gekauft wurden. Außerhalb dieser verträglichen Vereinbarungen werden keine Daten weitergegeben aus dem eRecruiter, außer wir erhalten eine schriftliche Weisung des Kunden oder haben eine gesetzliche Verpflichtung diesbezüglich.	O	
	Telearbeit	Zugriff außerhalb des Firmennetzwerks nur auf Dateien oder E-Mails nur über VPN möglich.	T	
	Verschwiegenheit	Mitarbeiter unterschreiben eine Verschwiegenheitserklärung.	O	
	Schulung Datenschutz	Mitarbeiter werden darauf geschult sorgfältig mit Daten umzugehen.	O	

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.				
	eRecruiter	Im Rahmen der Änderung von Daten werden im eRecruiter die Änderungen in Form von menschenlesbaren Protokollen (History) und andererseits im Form von Audit Logs gespeichert. Es wird im Rahmen von Audit Logs protokolliert welcher Benutzer, wann auf personenbezogene Daten zugegriffen hat.	T	

Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.				
	Weisungsgebundenheit im Support	Änderungen in eRecruiter unserer Kunden werden nur vorgenommen, wenn diese von weisungsbefugten Personen beauftragt wurden. Eine Liste von Weisungsbefugten Personen wird der Auftragsdatenverarbeitervereinbarung angehängt.	O	
	Dokumentation der Supportanfragen	Supportanfragen werden in Form von Tickets pro Kunde dokumentiert, inkl. zuständigen Bearbeiter.	TO	

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.				
	Anwendungsserver-Backup	Anwendungsserver (Betrieb der eRecruiter-Anwendungen) werden einer täglichen Sicherung unterzogen. Diese Sicherungen erstellen ein Backup der virtuellen Festplatten im Form von Snapshots. Es ist möglich diese Snapshots in Echtzeit auf die Anwendungsserver wiederherzustellen.	T	X
	Datenspeicher-Backup	Ein Backup von Dateien am Datenspeicher (Dokumente, Lebensläufe, andere Dokumente, die von eRecruiter Kunden hochgeladen werden) wird einerseits in Form der Windows Dateiarchivierung durchgeführt. Dateien werden dadurch bei jeder Änderung versioniert und diese Versionen werden für 30 Tage behalten für eine Wiederherstellung. Versionen, die älter als 30 Tage sind, werden automatisch entfernt. Der Datenspeicher wird neben dem Echtzeitbackup einmal täglich als Vollbackup gesichert. Dieses Vollbackup erfolgt zunächst als Snapshot der virtuellen Festplatte und diese Backups werden, danach auf Magnetbänder gesichert und für 3 Monate aufbewahrt bevor sie gelöscht werden.	T	X
	Datenbank-Backup	Das Backup des Datenbankservers erfolgt einerseits stündlich in Form von Transaction Logs und anderseits täglich als Vollbackup der einzelnen Datenbanken. Die Transaction Logs und Vollbackups werden täglich auf Magnetbänder gesichert und für 3 Monate aufbewahrt.	T	X
	Firewall	ISO27001 Zertifikat von Nextlayer.	T	X

	Virenschutz (Rechenzentrum)	Im Rahmen der Speicherung der Daten auf den Datenspeicher erfolgt eine Virenprüfung (ClamAV).	T	X
	Virenschutz (Notebooks, Büro)	Es sind alle IT-Systeme, die von Mitarbeitern verwendet werden, oder Server in den Büroräumlichkeiten mit einem Virenschutz ausgestattet (TrendMicro).	T	
	Brandmelder	In den Büroräumlichkeiten sind Brandmelder vorhanden.	T	
	Feuerlöscher	Feuerlöscher sind in allen Büros vorhanden.	O	

Aufbewahrungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.				
	eRecruiter - Miete (SaaS)	Im eRecruiter wird eine strenge technische Mandantentrennung durchgeführt bei der Verwendung einer gemeinsamen Datenbank und eines gemeinsamen Fileservers. Es ist Benutzern nicht möglich auf Daten eines anderen Mandanten zuzugreifen.	T	X
	eRecruiter - Hosting / Mietkauf (Private SaaS)	In diesem Fall wird ein gemeinsamer Datenbankserver verwendet, eine Trennung der Daten in unterschiedliche Datenbanken ist aber gegeben, diese sind also aufgrund der Rechenzentruminfrastruktur von einander abgeschirmt.	T	X