

Technischen und organisatorische Maßnahmen gem. Artt. 28 Abs. 3 lit. c und 32 DS-GVO

1. Vertraulichkeit (confidentiality)

- 1.1. Der körperliche Zutritt von Personen in Räumlichkeiten von SEO for Jobs ist nur nach vorheriger Legitimation möglich. Zum Einsatz kommen herkömmliche Sicherheitsschlösser, zu denen die Schlüssel ausschließlich an berechtigte Mitarbeiter ausgegeben werden.
- 1.2. Der Kreis der Zutrittsberechtigten ist festgelegt.
- 1.3. Besucher müssen an der Eingangstür klingeln und werden durch Mitarbeiter von SEO for Jobs eingelassen.
- 1.4. Besucher werden durchgehend begleitet.
- 1.5. Die Mitarbeiter sind schriftlich auf die Vertraulichkeit, bzw. das Datengeheimnis verpflichtet.
- 1.6. Der Zugang zu Workstations und Notebooks ist über individuelle Benutzerkonten geschützt.
- 1.7. Es wird unterschieden zwischen „normalen“ Benutzern und Administratoren.
- 1.8. Kein Einsatz von Sammelusern.
- 1.9. Die Anmeldung an Servern ist über gesonderte Administrator-Konten geschützt, die ausschließlich durch berechtigte Administratoren genutzt werden.
- 1.10. Die Vergabe jeglicher Benutzerkonten wird durch die Geschäftsleitung freigegeben.
- 1.11. Zugangsberechtigungen zu Rechnern werden personengebunden vergeben.
- 1.12. Zugangsberechtigungen werden auch für Netzwerklaufwerke personengebunden vergeben.

- 1.13. Der Kreis der jeweils befugten Personen ist auf das betriebsnotwendige Maß eingeschränkt.
- 1.14. Der Zugriff auf Administrations-Schnittstellen von Cloud-Diensten und kritischen Systemen ist zwingend durch eine Mehr-Faktor-Authentifizierung (MFA/2FA) geschützt.
- 1.15. Zugriffsberechtigungen werden in den Anwendungen rollenbasiert vergeben. Es wird nach dem Prinzip „need-to-know“ und „need-to-do“ verfahren.
- 1.16. Die Verwaltung der Rollen erfolgt in den Anwendungen.
- 1.17. Jeder Zugangsberechtigte kann nur auf Daten zugreifen, die er zur Ausübung der ihm übertragenen Aufgaben und Funktionen benötigt.
- 1.18. Mandantentrennung in den Anwendungen von SEO for Jobs.
- 1.19. Getrennte Datenbanken für unterschiedliche Anwendungen.
- 1.20. Personenbezogene Daten werden grundsätzlich zentral auf Servern bzw. bei eingesetzten Cloud-Dienstleistern gespeichert. Eine lokale Speicherung auf Endgeräten ist nur in begründeten Ausnahmefällen und unter Beachtung angemessener technischer und organisatorischer Schutzmaßnahmen vorgesehen.
- 1.21. Die Datenübertragung erfolgt verschlüsselt (TLS/SSL). Zudem werden personenbezogene Daten bei Cloud-Dienstleistern (z. B. AWS) im Ruhezustand (at Rest) mittels moderner Verschlüsselungsstandards (z. B. AES-256) gesichert.
- 1.22. Die Festplatten mobiler Rechner sind grundsätzlich verschlüsselt; etwaige Ausnahmen unterliegen einem gesonderten Freigabe- und Absicherungsprozess.
- 1.23. E-Mails können Ende-zu-Ende verschlüsselt (PGP) versandt und empfangen werden. Schlüssel werden pro E-Mailadresse erstellt.
- 1.24. Im Rahmen von Datenverarbeitungen im Auftrag verarbeitet SEO for Jobs die überlassenen personenbezogenen Daten ausschließlich aufgrund und anhand von vertraglichen vereinbarten Weisungen des Auftraggebers.
- 1.25. SEO for Jobs unterstützt die Auftraggeber bei der Ausübung ihrer Kontrollpflichten.
- 1.26. SEO for Jobs führt in unregelmäßigen Abständen stichprobenartige interne Auftragskontrollen durch.
- 1.27. Mit Dienstleistern und Subunternehmern werden Verträge zur Auftrags(daten)verarbeitung geschlossen, welche Regelungen enthalten, mit denen

die in dieser Bestätigung enthaltenen Maßnahmen auch den Dienstleistern auferlegt werden.

2. Integrität (integrity)

- 2.1. Zugriffsberechtigungen werden in den Anwendungen rollenbasiert vergeben. Es wird nach dem Prinzip „need-to-know“ und „need-to-do“ verfahren.
- 2.2. Die Mitarbeiter sind schriftlich auf die Vertraulichkeit, bzw. das Datengeheimnis verpflichtet.
- 2.3. SEO for Jobs sichert seine Systeme über Virensoftware und Firewall ab.
- 2.4. Personenbezogene Daten werden nach definierten Löschkzyklen oder unmittelbar nach Zweckwegfall gelöscht, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen.
- 2.5. Sachbearbeiter und Zeitpunkt von Verarbeitungen werden automatisch protokolliert.
- 2.6. Die Protokolle sind vor unbefugtem Zugriff geschützt.
- 2.7. Im Rahmen von Datenverarbeitungen im Auftrag verarbeitet SEO for Jobs die überlassenen personenbezogenen Daten ausschließlich aufgrund und anhand von vertraglichen vereinbarten Weisungen des Auftraggebers.
- 2.8. Jeder Zugangsberechtigte kann nur auf Daten zugreifen, die er zur Ausübung der ihm übertragenen Funktionen benötigt.
- 2.9. Mandantentrennung in den Anwendungen von SEO for Jobs.
- 2.10. Getrennte Datenbanken für unterschiedliche Anwendungen.
- 2.11. Die Datenübertragung mit und zwischen den Systemen von SEO for Jobs erfolgt verschlüsselt.
- 2.12. E-Mails können Ende-zu-Ende verschlüsselt (PGP) versandt und empfangen werden. Schlüssel werden pro E-Mailadresse erstellt.
- 2.13. Im Rahmen von Datenverarbeitungen im Auftrag verarbeitet SEO for Jobs die überlassenen personenbezogenen Daten ausschließlich aufgrund und anhand von vertraglichen vereinbarten Weisungen des Auftraggebers.
- 2.14. SEO for Jobs führt in unregelmäßigen Abständen stichprobenartige interne Auftragskontrollen durch.

3. Verfügbarkeit (availability)

- 3.1. Die Anmeldung an Servern ist über gesonderte Administrator-Konten geschützt, die ausschließlich durch berechtigte Administratoren genutzt werden.
- 3.2. Die Vergabe jeglicher Benutzerkonten wird durch die Geschäftsleitung freigegeben.
- 3.3. Zugangsberechtigungen zur Rechnern werden personengebunden vergeben.
- 3.4. Zugangsberechtigungen werden auch für Netzwerklauferke personengebunden vergeben.
- 3.5. Der Kreis der jeweils befugten Personen ist auf das betriebsnotwendige Maß eingeschränkt.
- 3.6. Zugriffsberechtigungen werden in den Anwendungen rollenbasiert vergeben. Es wird nach dem Prinzip „need-to-know“ und „need-to-do“ verfahren.
- 3.7. Die Verwaltung der Rollen erfolgt in den Anwendungen.
- 3.8. Jeder Zugangsberechtigte kann nur auf Daten zugreifen, die er zur Ausübung der ihm übertragenen Funktionen benötigt.
- 3.9. Sachbearbeiter und Zeitpunkt von Verarbeitungen werden automatisch protokolliert, die Protokolle sind vor unbefugtem Zugriff geschützt.
- 3.10. SEO for Jobs sichert seine Systeme über Virensoftware und Firewall ab.
- 3.11. Eine lokale Datenhaltung auf Workstations ist grundsätzlich nicht vorgesehen. Soweit sie in begründeten Ausnahmefällen erforderlich ist, erfolgt sie nur unter Einhaltung angemessener technischer und organisatorischer Schutzmaßnahmen.
- 3.12. Backups der Datenbanken und Server werden regelmäßig, in der Regel täglich sowie anlassbezogen vor wesentlichen Deployments oder Änderungen, erstellt.
- 3.13. Backups werden räumlich getrennt von den Betriebsräumen bzw. in geeigneten externen Infrastrukturen gespeichert.
- 3.14. SEO for Jobs führt in unregelmäßigen Abständen stichprobenartige interne Auftragskontrollen durch.
- 3.15. Mit Dienstleistern und Subunternehmern werden Verträge zur Auftrags(daten)verarbeitung geschlossen, welche Regelungen enthalten, mit denen

die in dieser Bestätigung enthaltenen Maßnahmen auch den Dienstleistern auferlegt werden.

4. Belastbarkeit (resilience)

- 4.1. SEO for Jobs sichert seine Systeme über Virensoftware und Firewall ab.
- 4.2. Eine lokale Datenhaltung auf Workstations ist grundsätzlich nicht vorgesehen. Soweit im Einzelfall eine lokale Verarbeitung oder Zwischenspeicherung erforderlich ist, erfolgt diese nur unter Einhaltung angemessener technischer und organisatorischer Schutzmaßnahmen.
- 4.3. Es existieren verteilte Systeme und Rechenzentren an unterschiedlichen Standorten. Die Verarbeitung findet in ISO 27001-zertifizierten Rechenzentren (z. B. AWS Region Frankfurt) statt. Die physische Sicherheit wird durch die strengen Kontrollen der Infrastruktur-Anbieter gewährleistet
- 4.4. Backups der Datenbanken und Server werden regelmäßig, in der Regel täglich sowie anlassbezogen vor wesentlichen Deployments oder Änderungen, erstellt.