Unterstützung bei der Durchführung einer Datenschutz-Folgenabschätzung

Es obliegt dem Verantwortlichen zu prüfen, ob die Voraussetzungen für die Durchführung einer Datenschutz-Folgenabschätzung gegeben sind. Diese Voraussetzungen ergeben sich aus Art. 35 DSGVO.

Viele unserer Kunden gehen davon aus, dass eine Datenschutz-Folgenabschätzung im Zusammenhang mit unseren Dienstleistungen notwendig ist. Als Auftragsverarbeiter von personenbezogenen Daten dürfen wir keine Datenschutz-Folgenabschätzung für unsere Kunden durchführen.

Dieses Dokument stellt keine Rechtsberatung dar. Wir erfüllen unsere Pflicht unter Berücksichtigung der Art der Verarbeitung und der uns zur Verfügung stehenden Informationen den Verantwortlichen bei der Durchführung einer Datenschutz-Folgenabschätzung zu unterstützen.

Wenn Sie weitere konkrete Fragen im Zusammenhang mit der Datenschutz-Folgenabschätzung haben, wenden Sie sich gerne an uns.

1. Beschreibung der Verarbeitung

Die cloudbasierte SaaS-Plattform MONA AI wird im Fachbereich Recruiting und HR eingesetzt, um den gesamten Bewerbungsprozess technologisch zu unterstützen und effizienter zu strukturieren. Der Zweck der Verarbeitung umfasst die automatisierte Vorqualifizierung von Bewerbern, die Durchführung strukturierter Interviews inklusive der Transkription von Antworten sowie die Koordination von Terminen und die interne Prozesssteuerung. Dabei werden insbesondere Stammdaten, Bewerbungsunterlagen sowie Kommunikations- und Prozessdaten von Bewerbern, Interessenten und in Form von Logdaten auch von internen Mitarbeitern verarbeitet. Wichtig hierbei ist, dass das System lediglich zur Aufbereitung von Informationen und zur Standardisierung dient; eine finale Einstellungsentscheidung oder eine automatisierte Entscheidungsfindung im Sinne des Art. 22 DSGVO findet nicht statt, da alle entscheidungsrelevanten Schritte durch einen menschlichen Entscheider freigegeben werden.

2. Welche Daten werden verarbeitet?

- **Stammdaten**: Hierzu gehören insbesondere der Name sowie die Kontaktdaten der Bewerber.

- **Bewerbungsunterlagen**: Sämtliche eingereichten Dokumente im Rahmen des Rekrutierungsprozesses.
- **Interviewantworten**: Die während des Auswahlprozesses gegebenen Antworten in Textform.
- **Kommunikationsdaten**: Informationen aus dem Austausch zwischen dem Unternehmen und den Bewerbern.
- **Prozess- und Statusdaten**: Daten zur Steuerung und zum aktuellen Stand des jeweiligen Bewerbungsverfahrens.
- **Besondere Kategorien**: Sofern Bewerber diese freiwillig in ihren Unterlagen angeben, können auch sensible Daten wie beispielsweise Gesundheitsangaben enthalten sein.
- **Logdaten**: Daten interner Mitarbeiter (z. B. Recruiter), die im Rahmen der Systemnutzung anfallen.

3. Welche Kategorie von Personen ist betroffen?

- **Bewerber:** Personen, die sich aktiv auf eine Stelle beworben haben und deren Unterlagen sowie Interviewantworten verarbeitet werden.
- **Interessenten:** Personen, die Interesse an Karrieremöglichkeiten gezeigt haben, aber gegebenenfalls noch keinen vollständigen Bewerbungsprozess durchlaufen.
- **Interne Mitarbeiter:** Hierzu zählen insbesondere Recruiter und HR-Verantwortliche, deren Aktivitäten im System (z. B. in Logdaten) erfasst werden.

4. Welche Zuständigkeiten bestehen für die Verarbeitung?

Datenverarbeiter, die für die oben unter 1. genannte Verarbeitungstätigkeit relevant sind, welches Tool/Service sie betreiben, und welche Aufgabe der Dienstleister übernimmt:

Dienstleister	Aufgabe	Serverstandort
Google Cloud EMEA Limited	Hosting- und Infrastrukturleistungen	Dublin, Irland (EU)

Strato AG	Telefonie- und Kommunikationsdienste	Berlin, Deutschland (EU)
IONOS SE	E-Mail-Dienste	Montabaur, Deutschland (EU)

5. **Welche Löschungsfristen gelten für die Daten?**

Die Löschung von personenbezogenen Daten erfolgt nur auf Anweisung des Auftraggebers. Die Löschungsfristen werden daher vom Augtraggeber festgelegt.

6. **Welche Sicherheitsmaßnahmen setzen Sie im Zusammenhang mit dieser Verarbeitungstätigkeit ein? Bitte beschreiben Sie im Detail, wie die Sicherheitsmaßnahmen umgesetzt werden.**

Die vom Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen sind in der Übersicht der technischen und organisatorischen Maßnahmen beschrieben, die dem Auftragsverarbeitungsvertrag beigefügt ist. Hier werden weitere, detailliertere Sicherheitsmaßnahmen beschrieben, die bei der Durchführung der Datenschutz-Folgenabschätzung helfen können:

- **Verschlüsselung**

Maßnahmen, die für die Gewährleistung der Vertraulichkeit der gespeicherten Daten (in der Datenbank, in unstrukturierten Dateien, Backups usw.) sowie das Verfahren zur Verwaltung der verwendeten kryptografischen Schlüssel (Erstellung, Speicherung, Änderung bei Verdacht auf Datengefährdung, Zugriffsschutz usw.) implementiert sind.

Umsetzung: Die Übertragung von Daten erfolgt über verschlüsselte Transportkanäle wie TLS/HTTPS. Soweit relevant, erfolgt der Zugriff aus dem Remote-Kontext über abgesicherte Verfahren wie VPN oder gesicherte

Authentifizierung. Zudem werden firmeneigene Endgeräte durch Verschlüsselungsmechanismen geschützt.

- **Netzwerksicherheit**

Je nach Art des Netzwerks, auf dem die Verarbeitung ausgeführt wird (isoliert, privat oder Internet), muss der Verantwortliche angemessene Schutzsysteme installieren: Firewalls, Intrusion Detection Systeme oder andere aktive oder passive Geräte, die für die Sicherstellung der Netzwerksicherheit verwendet werden.

Umsetzung: Die Verarbeitung erfolgt in einem Cloud-Betrieb über externe Provider, wobei die Primärverarbeitung in der Google Cloud Region Frankfurt (europe-west3) stattfindet. Zum Schutz werden Cloud-basierte Mechanismen sowie eine geografische Redundanz im EU-Raum eingesetzt. Die Systeme werden kontinuierlich überwacht, um Störungen oder unbefugte Zugriffe frühzeitig zu erkennen

- **Anonymisierung**

Der Zweck einer Anonymisierungslösung besteht darin, dass personenbezogene Daten ihren identifizierenden Charakter verlieren. Eine Anonymisierungslösung muss von Fall zu Fall erstellt und an die beabsichtigten Verwendungszwecke angepasst werden. Eine Hilfe für die Bewertung einer guten Lösung bietet die Art.29-Gruppe. Sie nennt drei Kriterien:

- die Individualisierung: es ist noch immer möglich, eine individuelle Person zu isolieren
- die Korrelation: es ist möglich, getrennte Datensätze für dasselbe Individuum miteinander zu verknüpfen
- die Schlussfolgerung: hier ist es möglich, aus den Informationen über eine Person auf deren Identität zu schließen.

Eine Gruppe von Daten, für die es unmöglich ist, zu individualisieren oder zu korrelieren oder abzuleiten, ist a priori anonym.

Wird eines der drei Kriterien nicht eingehalten, kann nur nach einer erneuten eingehenden Analyse der Risiken einer Einordnung als anonym vorgenommen werden.

Umsetzung: Falls die Nutzung von Echtdaten in Test- oder Entwicklungszusammenhängen zwingend erforderlich ist, erfolgt dies ausschließlich in anonymisierter Form. Damit wird sichergestellt, dass kein Personenbezug in diesen Umgebungen hergestellt werden kann.

- **Datentrennung**

Methoden zur Reduzierung der Möglichkeiten, personenbezogene Daten zu korrelieren und eine Kompromittierung aller gespeicherten Daten zu verhindern, indem beispielsweise die spezifischen Daten der jeweiligen Geschäftsprozesse identifiziert und logisch getrennt werden.

Umsetzung: Es besteht eine strikte Trennung von Produktiv-, Test- und Entwicklungsumgebungen. Kundendaten werden technisch getrennt (z. B. durch getrennte Datenbanken oder gleichwertige Isolation) verarbeitet, um einen mandantenübergreifenden Zugriff zu verhindern.

- **Strenge technische Zugangskontrolle**

Der Zugang zu den Daten muss auf die Personen beschränkt werden, die ihn für die Erfüllung ihrer Aufgaben benötigen.

Umsetzung: Der Zugriff basiert auf einem rollenbasierten Berechtigungssystem (RBAC) nach dem Need-to-know-Prinzip. Die Rechte werden regelmäßig überprüft und der Zugriff auf Produktivdaten ist auf definierte Rollen stark beschränkt. Es gibt eine strikte Trennung zwischen Standard- und privilegierten Administrator-Konten.

- **Rückverfolgbarkeit (Protokollierung)**

Aufzeichnung von Aktionen, die auf dem IT-System ausgeführt werden, um betrügerischen Zugriff oder Missbrauch von persönlichen Daten zu erkennen sowie den Verursacher eines Vorfalls. Zu diesem Zweck muss ein Trace- und Incident-Management-System eingerichtet werden. Es sollte relevante Ereignisse aufzeichnen und sicherstellen, dass diese Datensätze nicht manipuliert werden können. In jedem Fall sollten Sie diese Datensätze nur für einen gewissen Zeitraum und nicht exzessiv lange aufbewahrt werden.

Umsetzung: Zugriffe und Änderungen an personenbezogenen Daten werden systemseitig automatisch protokolliert. Diese Protokolle sind einzelnen

Nutzerkonten zugeordnet, vor Manipulation geschützt und dienen der Fehleranalyse sowie der Nachweisführung bei Sicherheitsüberprüfungen.

- **Authentifizierung**

Die Authentifizierung ist eine Operation, durch die der Benutzer seine Identität beweist. Jeder berechtigte Benutzer sollte hierbei eindeutig identifiziert werden.

Umsetzung: Es werden ausschließlich personalisierte Benutzerkonten verwendet; Sammelkonten sind untersagt. Für den Zugang gelten verbindliche Passwortregeln. Für besonders schützenswerte Systeme wird eine Mehrfaktor-Authentifizierung (MFA) eingesetzt. Zudem verhindern automatische Sperrmechanismen (Session-Locks) die unbefugte Nutzung.

- **Bekämpfung von Malware**

Maßnahmen zum Schutz des Zugangs zu öffentlichen (Internet-) oder unkontrollierten (Partner-) Netzwerken sowie Arbeitsplatzrechnern und Servern gegen bösartigen Code, der die Sicherheit der personenbezogenen Daten beeinträchtigen könnte.

Umsetzung: Mitarbeitende nutzen ausschließlich firmeneigene Endgeräte, auf denen Sicherheitsmechanismen wie Endpoint-Schutz angewendet werden. Dies dient dem Schutz vor bösartigem Code beim Zugriff auf die Verarbeitungssysteme

- **Hardware-Sicherheit**

Maßnahmen, die ergriffen wurden, um die Möglichkeit zu verringern, dass die eingesetzten Systeme (Server, Workstations, Laptops, Peripheriegeräte, Kommunikationsgeräte, Wechselmedien usw.) zur Beschädigung personenbezogener Daten verwendet werden (Inventarisierung, Trennung, physische Redundanz, Zugangsbeschränkungen usw.).

Umsetzung: Es werden keine On-Premise-Server betrieben; die Infrastruktur liegt bei zertifizierten Cloud-Providern. Die eingesetzten firmeneigenen Endgeräte der Mitarbeitenden sind durch Verschlüsselung und Richtlinien zur sicheren Nutzung geschützt

- **Sensibilisierungsmaßnahmen**

Vorhandene Regelungen zur Schulung und Sensibilisierung von (neuen) Mitarbeitern bei Antritt ihrer (neuen) Funktion sowie für Personen, die Zugriff auf personenbezogene Daten hatten beim Ausscheiden aus der Organisation.

Umsetzung: Mitarbeitende erhalten mindestens jährlich Schulungen zu Datenschutz und Informationssicherheit, die durch den externen Datenschutzbeauftragten (heyData) durchgeführt werden. Zudem sind Verhaltens- und Sicherheitsregeln dokumentiert und werden bei Vertragsbeginn verbindlich zur Kenntnis gegeben