JOINT-CONTROLLERSHIP-VEREINBARUNG TALENT.CLOUD

(gültig bis 30.06.2021)

I. Vertragsparteien

Zwischen der karriere.at GmbH, FN 256668d, mit Sitz in Österreich, 4020 Linz, Donaupromenade 1 – im Folgenden auch kurz als karriere.at oder Verantwortlicher1 bezeichnet – und «Firmenname», mit Sitz in «LandRegion», «Postleitzahl» «Ort», «StraßeNr» – im Folgenden auch kurz als Auftraggeber oder Verantwortlicher2 bezeichnet – wird der folgende Vertrag geschlossen:

II. Präambel

Der Auftraggeber nutzt die karriere.at talent.cloud zur Suche von Kandidaten. Bei der talent.cloud handelt es sich um eine Kandidatendatenbank, mittels der potentielle Arbeitgeber Zugriff auf Kandidatendaten erhalten. Dabei legen Kandidaten Accounts mit ihren Daten bei karriere.at an und können diese Accounts zur Suche für Arbeitgeber freischalten. Diese Daten können vom Kandidaten anonymisiert werden. Der Account und die dort hinterlegten personenbezogenen Daten können vom Kandidaten jederzeit oder auf Anfrage an karriere.at gelöscht werden.

karriere.at ist gemäß den Bestimmungen der DSGVO Verantwortlicher, da sie die Kandidatendaten gemäß ihren eigenen Strukturen zum Zwecke der Zusammenführung mit potentiellen Arbeitgebern verarbeitet. Sohin hat es einen rechtlichen und tatsächlichen Einfluss auf die Entscheidung, wie personenbezogene Daten verarbeitet werden. Ebenso ist der Auftraggeber gemäß den Bestimmungen der DSGVO Verantwortlicher, da die Kandidatendaten in dessen Unternehmen zum Zwecke der Kandidatensuche verarbeitet werden, ohne dass es zu einer Weisung durch karriere.at kommt oder kommen kann. Der Auftraggeber hat einen rechtlichen und tatsächlichen Einfluss auf die Entscheidung, wie personenbezogene Daten verarbeitet werden. Es handelt sich daher um eine gemeinsame Verantwortung.

Es handelt sich daher um die Übermittlung von einem Verantwortlichen (karriere.at) an einen anderen Verantwortlichen (Auftraggeber), wobei der Erlaubnistatbestand der Übermittlung an und Verarbeitung durch den Auftraggeber in der Handlung der zweckgebundenen freiwilligen Überlassung der Daten durch den Kandidaten an karriere.at sowie der informierten Einwilligung in die Überlassung an Dritte ist.

III. Vertragsgegenstand

Die Vertragsparteien planen bzw. unterhalten bereits eine Geschäftsbeziehung. Es handelt sich hierbei um nachstehend beschriebene Dienstleistung/Auftrag, die im Folgenden auch als Hauptvertrag bezeichnet wird. Auf den Hauptvertrag wird verwiesen:

talent.cloud: Zugriff auf die karriere.at Kandidatendatenbank, Suche nach geeigneten Kandidaten und gegebenenfalls Kontaktaufnahme mit Kandidaten aus der talent.cloud, sowie Kandidaten-Matching mit passenden Kandidaten.

Gegenstand, Dauer und Umfang richten sich ausschließlich nach dem Hauptvertrag, insofern nicht in diesem Vertrag aus rechtlichen Notwendigkeiten abweichende Erfordernisse getroffen werden mussten.

Im Rahmen des Hauptvertrages erbringt karriere.at an den Auftraggeber Dienstleistungen, die im Hauptvertrag näher beschrieben sind und die Kandidatendatenbank betreffen. Hierbei kommt es zur Übermittlung von personenbezogenen Daten der Kandidaten an den Auftraggeber aus der Kandidatendatenbank. Daher ist es erforderlich, dass die Vertragsparteien eine Vereinbarung zur gemeinsamen Datenverarbeitung gem. Art. 26 EU-DSGVO schließen. Diese Vereinbarung findet auf alle Tätigkeiten Anwendung, welche mit dem Hauptvertrag in Zusammenhang stehen und bei denen

Beschäftigte der Vertragsparteien oder durch diese Beauftragte personenbezogene Daten im Rahmen des Hauptvertrages verarbeiten.

Beide Vertragsparteien sind im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenverarbeitung verantwortlich („Verantwortliche“ im Sinne des Art. 4 Ziff. 7 DSGVO). Dabei legen beide Verantwortliche im Rahmen des Hauptvertrages und der gegenständlichen Joint-Controllership-Vereinbarung die Zwecke und Mittel der Verarbeitung eigenständig fest.

Beide Vertragsparteien führen für die Verarbeitung ein Verzeichnis der bei ihnen stattfindenden Verarbeitungstätigkeiten im Sinne des Art. 30 DSGVO. Auf wechselseitige Anforderung werden die für die Übersicht nach Art. 30 DSGVO notwendigen Angaben zur Verfügung gestellt.

IV. Definitionen

Personenbezogene Daten: Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Verantwortlicher: Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Drittland: Ein Land, das sich außerhalb der EU/EWR befindet.

Dies vorausgeschickt, vereinbaren die Vertragsparteien zum Schutz der obigen Informationen und personenbezogenen Daten, welche zum Zweck der Verarbeitung von karriere.at an den Auftraggeber übermittelt werden, im Sinne der DSGVO und der Vertraulichkeit Nachstehendes:

V. Datenschutz

1. Datenverarbeitung Auftraggeber: Der Auftraggeber verarbeitet im Einzelnen folgende personenbezogene Daten:

- Kandidaten in der talent.cloud-Kandidatendatenbank innerhalb des Recruitingprozesses: Name, Vorname, Kontaktdaten und weitere personenbezogene Daten, die aus dem Bewerbungsschreiben und dem Lebenslauf hervorgehen im Rahmen des Bewerbungsprozesses und Kandidatenmanagements sowie zum Support und zur Wartung des Systems.
- Mitarbeiter von karriere.at: Name, Vorname, Kontaktdaten im Rahmen der vertraglichen Zusammenarbeit sowie zum Support und zur Wartung des Systems.

2. Datenverarbeitung karriere.at: karriere.at verarbeitet im Einzelnen folgende personenbezogene Daten:

- Kandidatendaten in der talent.cloud-Kandidatendatenbank aufgrund deren freiwilliger Bekanntgabe bzw. Registrierung: Name, Vorname, Kontaktdaten und weitere personenbezogene Daten, die aus dem Lebenslauf hervorgehen im Rahmen der talent.cloud sowie zum Support und zur Wartung des Systems.
- Mitarbeiter des Auftraggebers: Name, Vorname, Kontaktdaten im Rahmen der vertraglichen Zusammenarbeit sowie zum Support und zur Wartung des Systems.

3. Datenverwendung Auftraggeber: Der Auftraggeber verpflichtet sich, personenbezogene Daten und Verarbeitungsergebnisse ausschließlich im Rahmen des Hauptvertrages, der Joint-Controllership-Vereinbarung, der Allgemeinen Geschäftsbedingungen von karriere.at sowie der geltenden datenschutzrechtlichen Bestimmungen zu den unter Punkt V.1. genannten Zwecken zu verarbeiten. Die

Vervielfältigung der erhaltenen personenbezogenen Daten, Unterlagen und Informationen durch den Auftraggeber bedarf ausdrücklich der vorherigen schriftlichen Zustimmung von karriere.at. Desgleichen bedarf eine Verwendung der überlassenen Daten für andere Zwecke des Auftraggebers der vorherigen schriftlichen Zustimmung von karriere.at. Der Auftraggeber verpflichtet sich zur Dokumentation der Datenverarbeitung von Kandidatendaten und Offenlegung gegenüber karriere.at auf Anfrage. Der Auftraggeber bestätigt und garantiert mit der Einwilligung in diese Vereinbarung, dass sämtliche ihn betreffenden datenschutzrechtlichen Bestimmungen eingehalten werden.

4. Datenverwendung karriere.at: karriere.at verpflichtet sich, Kandidaten vor der Anlage eines Accounts die notwendigen Datenschutzinformationen in rechtlich ausreichender Form zur Verfügung zu stellen, damit Kandidaten informiert, freiwillig und vorab darüber entscheiden können, ob und in welchem Ausmaße ihre personenbezogenen Daten im Account potentiellen Arbeitgebern zur Verfügung gestellt werden. karriere.at verpflichtet sich zur Dokumentation der Rechtmäßigkeit der Datenverarbeitung von Kandidatendaten. Weiters verpflichtet sich karriere.at Kandidatendaten nur Unternehmen zur Verfügung zu stellen, die der gegenständlichen Vereinbarung zustimmen und personenbezogene Daten gemäß den geltenden datenschutzrechtlichen Standards verarbeiten.

5. Verpflichtung zur Verschwiegenheit: Die Vertragsparteien erklären, dass alle mit der Datenverarbeitung beauftragten Personen, insbesondere die Mitarbeiter, vor Aufnahme der Tätigkeit zur Wahrung des Datengeheimnisses im Sinne der DSGVO verpflichtet wurden. Dies gilt insbesondere für sämtliche Erhebungen, Verarbeitungen und Nutzungen von personen- und firmenbezogenen Daten, die die Vertragsparteien im Zusammenhang mit dem von Auftraggeber beauftragten Leistungen durchführen. Insbesondere bleibt die Verschwiegenheitsverpflichtung, der mit dem Datenverkehr beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragsverarbeiter aufrecht. Die Verpflichtung zur Verschwiegenheit ist auch für Daten von juristischen Personen und handelsrechtlichen Personengesellschaften einzuhalten.

6. Verschwiegenheitserklärung der Mitarbeiter: Die Vertragsparteien setzen im Rahmen der Vertragsbeziehung nur solche Mitarbeiter ein, die bei der Aufnahme ihrer Tätigkeit gemäß der DSGVO auf das Datengeheimnis und die in dieser Vereinbarung geregelten Voraussetzungen mit schriftlicher Bestätigung verpflichtet worden sind. Vertrauliche Informationen werden nur an berechtigte Personen weitergegeben, die sie aufgrund ihrer Tätigkeit zur Erreichung des Zwecks dieser Vereinbarung erhalten müssen.

7. Sperre: Der Auftraggeber darf Daten von betroffenen Personen (Kandidaten) nur im Rahmen dieses Vertrages zu den hierin genannten Zwecken verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 lit. a DSGVO vor. Der Auftraggeber informiert karriere.at unverzüglich, wenn er der Auffassung ist, dass ein Verstoß gegen datenschutzrechtliche Bestimmungen vorliegt oder ein Data Breach. Für den Fall, dass der Auftraggeber personenbezogene Daten, die im Rahmen dieses Vertragsverhältnisses übermittelt wurden, rechtswidrig, zweckwidrig oder in sonstiger unzulässiger Weise behandelt oder diese Daten nicht mit der gebotenen Sorgfalt verarbeitet, ist karriere.at berechtigt, den Account des Auftraggebers zu sperren und die Löschung oder Vernichtung der übermittelten Daten zu verlangen. Dies beeinträchtigt den vereinbarten Entgeltsanspruch von karriere.at in keiner Weise.

8. Zugriffsberechtigte Personen des Auftraggebers: Der Auftraggeber gibt im Zuge des Eingehens des Vertragsverhältnisses jene Personen bekannt, die Zugriff auf die Kandidatendaten haben.

9. Sicherheitsmaßnahmen: Die Vertragsparteien erklären, dass ausreichende Sicherheitsmaßnahmen im Sinne der DSGVO ergriffen wurden, um zu verhindern, dass Daten ordnungswidrig verwendet oder Dritten unbefugt zugänglich werden. Insofern eine Vertragspartei Unregelmäßigkeiten bezüglich der Datenschutzanwendungen feststellt, wird dies umgehend dem Vertragspartner mitgeteilt.

10. Technische und organisatorische Maßnahmen: Die Vertragsparteien gestalten in ihrem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Es werden technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten getroffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DSGVO) genügen. Die Vertragsparteien haben technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dies beinhaltet beispielsweise folgende Maßnahmen, die vor Missbrauch und Verlust der Daten schützen, wie beispielsweise:

- Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren (Zutrittskontrolle),
- zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
- dafür Sorge zu tragen, 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 (Zugriffskontrolle),
- dafür Sorge zu tragen, 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 (Weitergabekontrolle),
- dafür Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
- dafür Sorge zu tragen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
- dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
- dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungskontrolle).

Maßnahme ist beispielsweise die Verwendung eines dem Stand der Technik entsprechenden Verschlüsselungsverfahrens. Eine Darstellung dieser technischen und organisatorischen Maßnahmen seitens karriere.at ist im Business Account verfügbar. Bei Änderung der getroffenen Sicherheitsmaßnahmen muss sichergestellt sein, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

11. Auftragsverarbeiter: Die Vertragsparteien können ein anderes Unternehmen auch ohne Zustimmung zur Durchführung von Verarbeitungen heranziehen. Hierbei ist jede Vertragspartei verpflichtet, dass ein Vertrag im Sinne der DSGVO geschlossen wird. In diesem Vertrag stellt der Verantwortliche sicher, dass der Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Verantwortlichen auf Grund dieser Vereinbarung obliegen.

12. Rechte von betroffenen Personen: Die Vertragsparteien sind verpflichtet, alle technischen und organisatorischen Voraussetzungen zu treffen, damit den Rechten von Betroffenen, insbesondere der Art. 15 (Auskunftsrecht), Art. 16 (Recht auf Berichtigung, Art. 17 (Recht auf Löschung/Recht auf Vergessenwerden), Art. 18 (Recht auf Vergessenwerden), Art. 19 (Recht auf Mitteilung von Änderungen), Art. 20 (Recht auf Datenübertragbarkeit), und Art. 21 (Recht auf Widerspruch) DSGVO gegenüber Betroffenen innerhalb der gesetzlichen Fristen entsprochen werden kann. Dabei vereinbaren die Vertragsparteien, dass sie sich wechselseitig unterstützen. karriere.at ist berechtigt Art und Umfang der Unterstützung selbst zu bestimmen und hierfür dem Auftraggeber ein angemessenes Entgelt zu verrechnen. Der Auftraggeber verpflichtet sich hinsichtlich der personenbezogenen Daten entsprechend

den vertraglichen Bestimmungen zu handeln und diese auf Anforderung von karriere.at oder von Betroffenen zu löschen, zu sperren, zu berichtigen, zu übertragen oder hierüber Auskunft zu geben. Soweit ein Betroffener sich unmittelbar an eine Vertragspartei zwecks Berichtigung, Löschung oder Sperrung seiner Daten wenden sollte, wird diese Vertragspartei dieses Ersuchen unverzüglich an den Vertragspartner weiterleiten. Die Betroffenen sind berechtigt sich an beide Verantwortliche zu wenden. Sollte zwischen den Vertragsparteien kein Einvernehmen über die Bearbeitung von Anfragen von Betroffenen und Betroffenenrechte erzielt werden, so haben beide Verantwortliche die Bearbeitung in ihrer eigenen Sphäre durchzuführen.

13. Kontrolle: Die Vertragsparteien verpflichten sich, wechselseitig geeignete Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind. Dieser Nachweis kann beispielsweise aufgrund einer Selbstauskunft, eines Testats eines Sachverständigen, unternehmensinterner Verhaltensregeln, Zertifikaten oder genehmigter Verhaltensregeln erbracht werden.

14. Einsichtnahme: karriere.at wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht der Einsichtnahme und Kontrolle der Datenverarbeitungseinrichtungen beim Auftraggeber eingeräumt. Die Einsichtnahmen werden zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt.

15. Löschung von Daten: Nach Beendigung der Zusammenarbeit oder nach Aufforderung durch karriere.at, werden die Daten nach Wahl von karriere.at berichtigt oder gelöscht. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftraggeber die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch karriere.at oder gibt diese Datenträger an karriere.at zurück, sofern nicht im Vertrag bereits vereinbart. karriere.at ist jeweils hierüber seitens des Auftraggebers gegebenenfalls ein geeigneter Nachweis zu erbringen (Protokoll). Entstehen nach Vertragsbeendigung zusätzliche Kosten durch die Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

16. Unterstützung: Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftraggeber karriere.at bei der Erfüllung der Anfragen und Ansprüche oder Abwehr der Ansprüche Art. 12 -23 DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten im Rahmen seiner Möglichkeiten zu unterstützen.

17. Bestellung eines Datenschutzbeauftragten: Die Vertragsparteien werden einen Datenschutzbeauftragten benennen, soweit die Voraussetzungen des Art. 37 DSGVO vorliegen. Sofern kein Datenschutzbeauftragter benannt ist, benennen die Vertragsparteien einen Ansprechpartner. Die von karriere.at benannte Person ist auf der karriere.at Website angeführt. Seitens des Auftraggebers wir die Person separat genannt.

18. Data Breach Notification: Die Vertragsparteien verpflichten sich wechselseitig darüber unverzüglich zu informieren, wenn eine Vertragspartei, dessen Organe, Mitarbeiter oder Berater Kenntnis davon erlangen, dass personenbezogene Daten oder vertrauliche Informationen unter Verstoß gegen diese Vereinbarung weitergegeben wurden. Ebenso unterrichten sich die Vertragsparteien unverzüglich von schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf Datenschutzverletzungen oder anderen Unregelmäßigkeiten bei der Verarbeitung von Daten. Die Vertragsparteien treffen die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen und sprechen sich hierzu unverzüglich mit dem Vertragspartner ab.

19. Haftung: Auftraggeber und karriere.at haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

20. Regress: Im Innenverhältnis wird vereinbart, dass der jeweilige Vertragspartner nicht berechtigt ist, sich beim anderen Vertragspartner wegen eines in der eigenen Sphäre verursachten Fehlers oder Verstoßes gegen die Bestimmungen des Vertrages oder der DS-GVO oder sonstiger anzuwendender datenschutzrechtlicher Bestimmungen schad- und klaglos zu halten.

VI. Schriftform, Gerichtsstand, Verschiedenes

1. Form: Dieser Vertrag wird mit seiner Unterfertigung oder mit Zustimmung durch den Auftraggeber rechtskräftig. Die Zustimmung kann auch konkludent, beispielsweise durch die Annahme des Hauptvertrages erteilt werden. Änderungen und Ergänzungen dieser Vereinbarung und all seiner Bestandteile bedürfen der Schriftform und eines ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung des Vertrages handelt. Dies gilt auch für den Verzicht auf das Formerfordernis.

2. Rechtswahl: Es gilt österreichisches Recht.

3. Gerichtsstand: Gerichtsstand für sämtliche Streitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung ist das für karriere.at sachlich und örtlich zuständige Gericht. Dabei steht es karriere.at frei, etwaige Ansprüche aus dieser Vereinbarung auch bei dem für den Sitz des Auftraggebers sachlich und örtlich zuständigen Gericht geltend zu machen. Gesetzliche Regelungen über ausschließliche Zuständigkeiten bleiben unberührt.

4. Exekution/Insolvenz: Sollten die Daten von karriere.at beim Auftraggeber durch Pfändung oder Beschlagnahme, durch ein Konkurs-, Sanierungs- oder Insolvenzverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftraggeber unverzüglich darüber zu informieren. Der Auftraggeber wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich bei karriere.at im Sinne der DSGVO liegen.

5. Salvatorische Klausel: Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen des Hauptvertrages vor. Sollte eine Bestimmung dieser Vereinbarung ungültig sein oder werden, bleibt die Vereinbarung selbst, samt aller übrigen Bestimmungen gültig und aufrecht.

VEREINBARUNG ZUR AUFTRAGSDATENVERARBEITUNG

I. Vertragsparteien

Zwischen der karriere.at GmbH, FN 256668d, mit Sitz in Österreich, 4020 Linz, Donaupromenade 1 - im Folgenden auch kurz als Auftragsverarbeiter oder Auftragnehmer bezeichnet –

und

«Firmenname», mit Sitz in «LandRegion», «Postleitzahl» «Ort», «StraßeNr»– im Folgenden auch kurz als Auftraggeber bezeichnet – wird der folgende Vertrag geschlossen:

II. Vertragsgegenstand

Die Vertragsparteien planen bzw. unterhalten bereits eine Geschäftsbeziehung. Es handelt sich hierbei um nachstehend beschriebene Dienstleistung/Auftrag, die im Folgenden auch als Hauptvertrag bezeichnet wird:

Veröffentlichung von Inseraten und Arbeitgeberprofilen

Gegenstand, Dauer und Umfang richten sich ausschließlich nach dem Hauptvertrag, insofern nicht in diesem Vertrag aus rechtlichen Notwendigkeiten abweichende Erfordernisse getroffen werden mussten.

Im Rahmen des Hauptvertrages erbringt der Auftragsverarbeiter an den Auftraggeber Dienstleistungen bei denen der Auftragsverarbeiter mit der Erstellung, Bearbeitung und Auswertung von Daten, Unterlagen und Informationen befasst ist, die der Auftragsverarbeiter von dem Auftraggeber sowie ggf. von einem von diesen beauftragten Dritten erhält. Es handelt sich hierbei um personenbezogene Daten, die eine Auftragsdatenverarbeitung darstellen. Daher ist es erforderlich, dass die Vertragsparteien eine Vereinbarung zur Auftragsdatenverarbeitung gem. Art. 28 EU-Datenschutzgrundverordnung (DSGVO) schließen.

Diese Vereinbarung findet auf alle Tätigkeiten Anwendung, welche mit dem Hauptvertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragsverarbeiters oder durch diesen Beauftragte personenbezogene Daten des Auftraggebers verarbeiten.

III. Voraussetzungen

Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenverarbeitung verantwortlich („Verantwortlicher" im Sinne des Art. 4 Ziff. 7 DSGVO). Der Auftragsverarbeiter selbst führt für die Verarbeitung ein Verzeichnis der bei ihm stattfindenden Verarbeitungstätigkeiten im Sinne des Art. 30 DSGVO. Er stellt auf Anforderung dem Auftraggeber die für die Übersicht nach Art. 30 DSGVO notwendigen Angaben zur Verfügung.

Soweit der Auftragsverarbeiter unter Verstoß gegen diese Vereinbarung und gegen die DSGVO die Zwecke und Mittel der Verarbeitung selbst bestimmt, gilt der Auftragsverarbeiter in Bezug auf diese Verarbeitung als Verantwortlicher i.S.d. Art. 4 Ziff. 7 DSGVO.

IV. Definitionen

Personenbezogene Daten: Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Auftragsverarbeiter: Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Datenverarbeitung im Auftrag: Eine Datenverarbeitung im Auftrag ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter (Auftragnehmer) nach Weisung und im Auftrag des Verantwortlichen (Auftraggeber).

Weisung: Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt; der Auftraggeber hat ein Weisungsrecht im Rahmen dieser vereinbarten Leistung.

Subunternehmer: Als Auftragnehmer des Auftragsverarbeiters im Sinne der DSGVO ist der Subunternehmer ein „weiterer Auftragsverarbeiter".

Dritter: Der Ausdruck „Dritter" bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

Drittland: Ein Land, das sich außerhalb der EU/EWR befindet. Dies vorausgeschickt, vereinbaren die Vertragsparteien zum Schutz der obigen Informationen und personenbezogenen Daten, welche zum Zweck der Verarbeitung an den Auftragsverarbeiter übermittelt wurden, im Sinne der DSGVO und der Vertraulichkeit Nachstehendes:

V. Datenschutz

1. Datenverarbeitung im Auftrag: Der Auftragsverarbeiter verarbeitet im Einzelnen folgende Daten des Auftraggebers:

- Mitarbeiter des Auftraggebers: Name, Vorname, Kontaktdaten und weitere personenbezogene Daten, im Rahmen der Geschäftsbeziehung und zur Erfüllung der gesetzlich vorgeschriebenen Aufgaben sowie zum Support und zur Wartung des Systems.

2. Kategorien von Personen: Die folgenden Kategorien von Personen sind von der Datenverarbeitung betroffen:

- Mitarbeiter des Auftraggebers

3. Ort der Verarbeitung: Der Auftragsverarbeiter führt die Verarbeitung personenbezogener Daten ausschließlich innerhalb der EU / des EWR durch.

4. Auftragsgemäße Verwendung: Der Auftragsverarbeiter verpflichtet sich, personenbezogene Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der Aufträge des Auftraggebers und nach dokumentierter Weisung zu verarbeiten und ausschließlich dem Auftraggeber zurückzugeben oder nur nach dessen schriftlichem Auftrag zu übermitteln. Die Vervielfältigung der erhaltenen Daten, Unterlagen und Informationen durch Auftragsverarbeiter bedarf ausdrücklich der vorherigen schriftlichen Zustimmung des Auftraggebers. Desgleichen bedarf eine Verwendung der überlassenen Daten für eigene Zwecke des Auftragsverarbeiters eines derartigen schriftlichen Auftrages.

5. Verpflichtung zur Verschwiegenheit: Der Auftragsverarbeiter erklärt, dass alle mit der Datenverarbeitung beauftragten Personen, insbesondere die Mitarbeiter, vor Aufnahme der Tätigkeit zur Wahrung des Datengeheimnisses im Sinne der DSGVO verpflichtet wurden. Dies gilt insbesondere für sämtliche Erhebungen, Verarbeitungen und Nutzungen von personen- und firmenbezogenen Daten, die der Auftragsverarbeiter im Zusammenhang mit dem von Auftraggeber beauftragten Leistungen durchführt. Insbesondere bleibt die Verschwiegenheitsverpflichtung, der mit dem Datenverkehr beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragsverarbeiter aufrecht. Die Verpflichtung zur Verschwiegenheit ist auch für Daten von juristischen Personen und handelsrechtlichen Personengesellschaften einzuhalten.

6. Verschwiegenheitserklärung der Mitarbeiter: Der Auftragsverarbeiter setzt im Rahmen der Auftragsdurchführung nur solche Mitarbeiter ein, die bei der Aufnahme ihrer Tätigkeit gemäß der DSGVO auf das Datengeheimnis und die in dieser Vereinbarung geregelten Voraussetzungen mit schriftlicher Bestätigung verpflichtet worden sind. Vertrauliche Informationen werden nur an berechtigte Personen weitergegeben, die sie aufgrund ihrer Tätigkeit zur Erreichung des Zwecks dieser Vereinbarung erhalten müssen.

7. Weisung: Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 lit. a DSGVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde. Die Weisungen werden durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in

schriftlicher an die vom Auftragsverarbeiter bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Hauptvertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Sämtliche Weisungen sind in Schriftform zu erteilen oder im Falle einer Dringlichkeit, in Schriftform nachzureichen. Rechtswidrigen Weisungen ist vom Auftragsverarbeiter nicht nachzukommen.

8. weisungsberechtigte Personen des Auftraggebers: Für den Fall, dass keine weisungsberechtigten Personen dem Auftragsverarbeiter genannt werden, ist ausschließlich die gesetzliche Vertretung des Auftraggebers zur Weisung berechtigt.

9. Sicherheitsmaßnahmen: Der Auftragsverarbeiter erklärt, dass ausreichende Sicherheitsmaßnahmen im Sinne der DSGVO ergriffen wurden, um zu verhindern, dass Daten ordnungswidrig verwendet oder Dritten unbefugt zugänglich werden. Insofern der Auftragsverarbeiter Unregelmäßigkeiten bezüglich der Datenschutzanwendungen feststellt, wird er dies umgehend dem Auftraggeber mitteilen.

10. Technische und organisatorische Maßnahmen: Der Auftragnehmer gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DSGVO) genügen. Der Auftragsverarbeiter hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Dies beinhaltet beispielsweise folgende Maßnahmen, die den Auftraggeber vor Missbrauch und Verlust seiner Daten schützen, wie beispielsweise:

- Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren (Zutrittskontrolle),
- zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
- dafür Sorge zu tragen, 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 (Zugriffskontrolle),
- dafür Sorge zu tragen, 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 (Weitergabekontrolle),
- dafür Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
- dafür Sorge zu tragen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
- dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
- dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungskontrolle).

Maßnahme ist beispielsweise die Verwendung eines dem Stand der Technik entsprechenden Verschlüsselungsverfahrens. Eine Darstellung dieser technischen und organisatorischen Maßnahmen ist im Business Account verfügbar. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem

Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

11. Subauftragsverarbeiter: Der Auftragsverarbeiter kann ein anderes Unternehmen auch ohne Zustimmung des Auftraggebers zur Durchführung von Verarbeitungen heranziehen. Der Auftragsverarbeiter hat jedoch den Auftraggeber von der beabsichtigten Heranziehung eines Subauftragsverarbeiters so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann. Außerdem muss ein Vertrag zwischen dem Auftragsverarbeiter und dem Subauftragsverarbeiter im Sinne der DSGVO geschlossen werden. In diesem Vertrag stellt der Auftragsverarbeiter sicher, dass der Subauftragsverarbeiter dieselben Verpflichtungen eingeht, die der Auftragsverarbeiter auf Grund dieser Vereinbarung obliegen. Ebenso wird der Auftragsverarbeiter die Einhaltung der vereinbarten Verpflichtungen regelmäßig kontrollieren. Zum Zeitpunkt des Abschlusses dieser Vereinbarung sind die im Business Account aufgeführten Unternehmen als Subauftragsverarbeiter für Teilleistungen für den Auftragsverarbeiter tätig und verarbeiten und/oder nutzen in diesem Zusammenhang auch unmittelbar die Daten des Auftraggebers. Für diese Subauftragsverarbeiter gilt die Einwilligung für das Tätigwerden als erteilt.

12. Rechte von betroffenen Personen: Weiters verpflichtet sich der Auftragsverarbeiter, alle technischen und organisatorischen Voraussetzungen zu treffen, damit der Auftraggeber den Bestimmungen der § 15 (Auskunftsrecht), § 16 (Recht auf Berichtigung, § 17 (Recht auf Löschung/Recht auf Vergessenwerden), § 18 (Recht auf Vergessenwerden), § 19 (Recht auf Mitteilung von Änderungen), § 20 (Recht auf Datenübertragbarkeit), und § 21 (Recht auf Widerspruch) DSGVO gegenüber Betroffenen innerhalb der gesetzlichen Fristen erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Der Auftragsverarbeiter verpflichtet sich auch während der Vertragslaufzeit mit sämtlichen personenbezogene Daten nach genauer Anweisung des Auftraggebers zu handeln und diese auf Anforderung zu löschen, zu sperren, zu berichtigen, zu übertragen oder hierüber Auskunft zu geben. Soweit ein Betroffener sich unmittelbar an den Auftragsverarbeiter zwecks Berichtigung, Löschung oder Sperrung seiner Daten wenden sollte, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

13. Kontrolle: Der Auftragsverarbeiter verpflichtet sich, dem Auftraggeber geeignete Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind. Der Auftragsverarbeiter kann den Nachweis beispielsweise aufgrund einer Selbstauskunft, eines Testats eines Sachverständigen, unternehmensinterner Verhaltensregeln, Zertifikaten oder genehmigter Verhaltensregeln erbringen.

14. Einsichtnahme: Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht der Einsichtnahme und Kontrolle der Datenverarbeitungseinrichtungen eingeräumt. Die Einsichtnahmen werden zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt.

15. Löschung von Daten: Nach Beendigung der Zusammenarbeit oder nach Aufforderung durch den Auftraggeber, insofern dies vom Weisungsrecht umfasst ist, werden die Daten nach Wahl des Auftraggebers berichtigt oder gelöscht. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragsverarbeiter die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart. Dem Auftraggeber ist jeweils hierüber seitens des Auftragsverarbeiters gegebenenfalls ein geeigneter Nachweis zu erbringen (Protokoll). Entstehen nach Vertragsbeendigung zusätzliche Kosten durch die Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

16. Unterstützung: Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftragsverarbeiter den Auftraggeber bei der Erfüllung der Anfragen und Ansprüche oder Abwehr der Ansprüche Art. 12 -23 DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten im Rahmen seiner Möglichkeiten zu unterstützen.

17. Bestellung eines Datenschutzbeauftragten: Der Auftragsverarbeiter wird einen Datenschutzbeauftragten benennen, soweit die Voraussetzungen des Art. 37 DSGVO vorliegen. Sofern kein Datenschutzbeauftragter beim Auftragsverarbeiter benannt ist, benennt der Auftragsverarbeiter dem Auftraggeber einen Ansprechpartner. Die zu benennenden Personen werden auf der Website benannt.

18. Data Breach Notification: Der Auftragsverarbeiter verpflichtet sich, den Auftraggeber unverzüglich zu informieren, wenn der Auftragsverarbeiter, dessen Organe, Mitarbeiter oder Berater Kenntnis davon erlangen, dass personenbezogene Daten oder vertrauliche Informationen unter Verstoß gegen diese Vereinbarung weitergegeben wurden. Ebenso unterrichtet der Auftragsverarbeiter den Auftraggeber unverzüglich von schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf Datenschutzverletzungen oder anderen Unregelmäßigkeiten bei der Verarbeitung von Daten. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

19. Haftung: Auftraggeber und Auftragsverarbeiter haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

VI. Schriftform, Gerichtsstand, Verschiedenes

1. Form: Dieser Vertrag wird mit seiner Unterfertigung oder mit Zustimmung durch den Auftraggeber rechtskräftig. Die Zustimmung kann auch konkludent, beispielsweise durch die Annahme des Hauptvertrages erteilt werden. Änderungen und Ergänzungen dieser Vereinbarung und all seiner Bestandteile bedürfen der Schriftform und eines ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung des Vertrages handelt. Dies gilt auch für den Verzicht auf das Formerfordernis.

2. Rechtswahl: Es gilt österreichisches Recht.

3. Gerichtsstand: Gerichtsstand für sämtliche Streitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung ist das für den Auftragsverarbeiter sachlich und örtlich zuständige Gericht. Dabei steht es dem Auftragsverarbeiter frei, etwaige Ansprüche aus dieser Vereinbarung auch bei dem für den Sitz des Auftraggebers sachlich und örtlich zuständigen Gericht geltend zu machen. Gesetzliche Regelungen über ausschließliche Zuständigkeiten bleiben unberührt.

4. Exekution/Insolvenz: Sollten die Daten des Auftraggebers beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Konkurs-, Sanierungs- oder Insolvenzverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragsverarbeiter den Auftraggeber unverzüglich darüber zu informieren. Der Auftragsverarbeiter wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den ausschließlich beim Auftraggeber im Sinne der DSGVO liegen.

5. Salvatorische Klausel: Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen des Hauptvertrages vor. Sollte eine Bestimmung dieser Vereinbarung ungültig sein oder werden, bleibt die Vereinbarung selbst, samt aller übrigen Bestimmungen gültig und aufrecht.

LISTE DER TECHNISCHEN / ORGANISATORISCHEN MASSNAHMEN

Typ	ID	Bereich	Zusammenfassung
Organisatorisch	TOM-37	Auftragskontrolle	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit und DSGVO-Compliance)
Organisatorisch	TOM-38	Auftragskontrolle	Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
Organisatorisch	TOM-39	Auftragskontrolle	Schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag)
Organisatorisch	TOM-40	Auftragskontrolle	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags (laut Auftragsdatenverarbeitungsvertrag)
Organisatorisch	TOM-41	Auftragskontrolle	Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags (laut Auftragsdatenverarbeitungsvertrag)
Organisatorisch	TOM-43	Auftragskontrolle	Vorherige Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen und entsprechender Dokumentation
Organisatorisch	TOM-44	Auftragskontrolle	Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbaren Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags (laut Auftragsdatenverarbeitungsvertrag)
Technisch	TOM-64	Auftragskontrolle	Dokumentation von technischen Support-Anfragen in einem zentralen System
Technisch	TOM-32	Eingabekontrolle	Systeme zur Protokollierung der Eingabe, Änderung und Löschung von Daten.
Organisatorisch	TOM-35	Eingabekontrolle	"Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)"
Organisatorisch	TOM-36	Eingabekontrolle	"Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts"
Technisch	TOM-57	Trennungsgebot	Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
Technisch	TOM-58	Trennungsgebot	Trennung von Produktiv- und Testsystem
Organisatorisch	TOM-60	Trennungsgebot	Berechtigungskonzept
Organisatorisch	TOM-61	Trennungsgebot	Festlegung von Datenbankrechten
Organisatorisch	TOM-62	Trennungsgebot	Logische Mandantentrennung (softwareseitig)
Technisch	TOM-45	Verfügbarkeitskontrolle	Feuerlöschgeräte in Serverräumen
Technisch	TOM-46	Verfügbarkeitskontrolle	Feuer- und Rauchmeldeanlagen
Technisch	TOM-47	Verfügbarkeitskontrolle	Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
Technisch	TOM-48	Verfügbarkeitskontrolle	Klimaanlage in Serverräumen

Technisch	TOM-49	Verfügbarkeitskontrolle	Schutzsteckdosenleisten in Serverräumen
Technisch	TOM-50	Verfügbarkeitskontrolle	Unterbrechungsfreie Stromversorgung (USV)
Organisatorisch	TOM-51	Verfügbarkeitskontrolle	"Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort"
Organisatorisch	TOM-52	Verfügbarkeitskontrolle	Backup- & Recoverykonzept
Organisatorisch	TOM-54	Verfügbarkeitskontrolle	Testen von Datenwiederherstellung
Organisatorisch	TOM-55	Verfügbarkeitskontrolle	Serverräume nicht unter sanitären Anlagen
Technisch	TOM-28	Weitergabekontrolle	Einrichtungen von VPN-Tunneln
Organisatorisch	TOM-65	Weitergabekontrolle	Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
Technisch	TOM-6	Zugangskontrolle	Authentifikation mit Benutzer + Passwort
Technisch	TOM-7	Zugangskontrolle	Einsatz von Anti-Viren-Software
Technisch	TOM-8	Zugangskontrolle	Einsatz von Firewalls
Technisch	TOM-9	Zugangskontrolle	Einsatz von VPN-Technologie
Technisch	TOM-10	Zugangskontrolle	Gehäuseverriegelungen
Technisch	TOM-11	Zugangskontrolle	Verschlüsselung von Datenträgern
Organisatorisch	TOM-12	Zugangskontrolle	Benutzerberechtigungen verwalten
Organisatorisch	TOM-13	Zugangskontrolle	Erstellen von Benutzerprofilen
Organisatorisch	TOM-14	Zugangskontrolle	Passwortvergabe / Passwortregeln
Organisatorisch	TOM-16	Zugangskontrolle	Sorgfältige Auswahl von Sicherheitspersonal
Technisch	TOM-17	Zugriffskontrolle	Einsatz von Aktenvernichtern
Technisch	TOM-18	Zugriffskontrolle	Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
Technisch	TOM-19	Zugriffskontrolle	Physische Löschung von Datenträgern vor deren Wiederverwendung
Organisatorisch	TOM-22	Zugriffskontrolle	Anzahl der Administratoren auf das „Notwendigste" reduzieren
Organisatorisch	TOM-23	Zugriffskontrolle	Einsatz von Dienstleistern zur Akten- und Datenvernichtung (nach Möglichkeit mit Zertifikat)
Organisatorisch	TOM-25	Zugriffskontrolle	Passwortrichtlinie inkl. Länge und Wechsel
Organisatorisch	TOM-26	Zugriffskontrolle	Sichere Aufbewahrung von Datenträgern
Organisatorisch	TOM-27	Zugriffskontrolle	Verwaltung der Benutzerrechte durch Systemadministratoren
Technisch	TOM-2	Zutrittskontrolle	Alarmanlage
Technisch	TOM-3	Zutrittskontrolle	Automatisches Zugangskontrollsystem
Technisch	TOM-4	Zutrittskontrolle	Sicherheitsschlösser

LISTE DER SUBAUFTRAGSVERARBEITER

- easyname GmbH, Hosting, 1100 Wien
- Emarsys, E-Mail, 1150 Wien
- eRecruiter, Bewerbungsverwaltung, 4020 Linz
- conova communications GmbH, Karolingerstraße 36A, 5020 Salzburg
- Jenseide OG, Videoproduktion, 1080 Wien
- ghostwood film GmbH, 1130 Wien