Anlage 2: Datenschutzrechtliche Verpflichtungen der Vertragsparteien

Zwischen

Nutzer

- Nutzer -

und

QPM Quality Personnel Management GmbH
Am Haferkamp 78
D-40589 Düsseldorf,

vertreten durch die Geschäftsführung Philipp Schuch oder Lisanne Metz

- Auftragnehmer -

über Auftragsverarbeitung i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO).

§0. Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Vertrag in ihren Einzelheiten beschriebenen Auftragsdatenverarbeitung ergeben.
Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten (>>Daten<<) des Nutzers verarbeiten.

§ 1. Gegenstand, Dauer und Spezifizierung der Auftragsdatenverarbeitung

Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

Art der Daten	**Zweck der Datenerhebung, -verarbeitung oder -nutzung**	**Kreis der Betroffenen**
Für die generelle Nutzung von gradar u.a. zur Stellenbewertung / Management einer Stellenarchitektur		
Vorname, Name, geschäftliche E-Mail-Adresse, IP-Adresse	Zugang zur *Software as a Service* auf *.gradar.com, Kommunikation mit den Nutzern (z.B. Release Notes, technische Hilfeleistung)	Ausgewählte Beschäftigte und ehemalige Beschäftigte des Nutzers, die das gradar System nutzen
Zeitstempel „Letzte Anmeldung“ **Zeitstempel** „Stellendaten: „angelegt, zuletzt geändert“ **Zähler** „Anzahl Logins“ **Benutzerprofil** mit Sprach-, Land und Zeitzoneneinstellung	Nutzung der gradar Software, Dokumentation von Änderungen, Vermeidung von Versionskonflikten	Ausgewählte Beschäftigte und ehemalige Beschäftigte des Nutzers, die das gradar System nutzen

Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüberhinausgehende Verpflichtungen ergeben.

§ 2. Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Nutzers. Dies umfasst die im Vertrag und im Leistungsumfang aufgeführten und näher bezeichneten Tätigkeiten. Im Rahmen des Vertrages ist der Nutzer allein für die Einhaltung der gesetzlichen Datenschutzbestimmungen verantwortlich, insbesondere für die Rechtmäßigkeit der

Übermittlung an den Auftragnehmer und die Rechtmäßigkeit der Verarbeitung; der Nutzer ist "Verantwortlicher" im Sinne von Artikel 4 Nr. 7 DSGVO.

(2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Nutzer danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

(3) Der Nutzer legt den oder die Weisungsberechtigten fest.
Falls nicht anders definiert sind dies die Unternehmensadministratoren. Der Auftragnehmer legt support@gradar.com als Weisungsempfänger fest. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und in schriftlicher oder elektronischer Form die Nachfolger oder Vertreter mitzuteilen.

§ 3. Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Nutzers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor. Der Auftragnehmer informiert den Nutzer unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung so lange aussetzen, bis sie vom Nutzer bestätigt oder abgeändert wurde.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Nutzers treffen, die den Anforderungen der Datenschutzgrundverordnung (Art. 32 DSGVO) genügen. Der Auftragnehmer 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 Nutzer sind diese technischen und organisatorischen Maßnahmen (Anlage 3) bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Der Auftragnehmer unterstützt den Nutzer im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten.

(4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Nutzers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(5) Mit Bezug auf die gegenständliche Auftragsverarbeitung unterrichtet der Auftragnehmer den Nutzer unverzüglich, über Störungen, Verdacht auf Datenschutzverletzungen oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten. Es gilt Art. 33 DSGVO zur Mitteilungspflicht.
Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und unterstützt den Nutzer in angemessenem Umfang.

(6) Kontaktdaten des Datenschutzbeauftragten des Auftragnehmers:
PROLIANCE GmbH
Herr Dominik Fünkner
www.datenschutzexperte.de
Leopoldstr. 21
80802 München
datenschutzbeauftragter@datenschutzexperte.de

(7) Ansprechpartner des Auftragnehmers i.S. der DSGVO:
QPM Quality Personnel Management GmbH
Geschäftsführung
Am Haferkamp 78
40589 Düsseldorf
support@gradar.com

(8) Der Auftragnehmer nutzt ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen um seinen Pflichten nach Art. 32 Abs. 1 lit. d) DSGVO nachzukommen.

(9) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Nutzer dies anweist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Nutzer oder gibt diese Datenträger an den Nutzer zurück, sofern nicht im Vertrag bereits vereinbart.
Eine über die Auftragsverarbeitung hinausgehende Verarbeitung (und damit auch eine

Aufbewahrung) erfolgt lediglich im Rahmen der gesetzlich vorgeschriebenen Aufbewahrungsfristen, denen der Auftragnehmer unterliegt.
In besonderen, vom Nutzer zu bestimmenden Fällen, kann eine Aufbewahrung über das Ende der Vertragslaufzeit hinaus erfolgen. Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

(10) Daten, Datenträger sowie sämtliche sonstige Materialien sind unter Berücksichtigung der gegenseitigen Vereinbarung von unter § 1 Abs. (2) I-III fallenden Daten und Datensätzen nach Auftragsende auf Verlangen des Nutzers entweder herauszugeben oder zu löschen.

(11) Macht eine betroffene Person Ansprüche gegen den Nutzer gemäß Artikel 82 DSGVO geltend, so unterstützt der Auftragnehmer den Nutzer bei der Abwehr dieser Ansprüche, soweit dies möglich ist.

§ 4. Pflichten des Nutzers

(1) Der Nutzer hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Macht eine betroffene Person Ansprüche gegen den Auftragnehmer gemäß Artikel 82 DSGVO geltend, gilt §3 Abs. 11 entsprechend.

§ 5. Anfragen Betroffener

(1) Macht eine betroffene Person, gegenüber dem Auftragnehmer, Ansprüche gemäß den in Kapitel III §15-22 der DSGVO aufgeführten Rechten:

a) Berichtigung
b) Löschung
c) Einschränkung der Verarbeitung
d) Datenübertragbarkeit

geltend und der Auftragnehmer ist in der Lage, die betroffene Person auf der Grundlage der von der betroffenen Person bereitgestellten Informationen mit dem Nutzer in Verbindung zu bringen, verweist der Auftragnehmer die betroffene Person an den Nutzer.

(2) Der direkte Kontakt mit der betroffenen Person beschränkt sich auf diese Antwort.

(3) Der Auftragnehmer leitet die Forderung der betroffenen Person unverzüglich an den Nutzer weiter. Der Auftragnehmer unterstützt den Nutzer nach Möglichkeit und auf dessen Weisung hin, soweit dies vereinbart ist. Der Auftragnehmer haftet nicht, wenn der Nutzer nicht vollständig, nicht richtig oder nicht rechtzeitig auf die Anfrage der betroffenen Person reagiert.

(4) Der Nutzer und der Auftragnehmer haften gegenüber der betroffenen Person gemäß Artikel 82 der Datenschutz-Grundverordnung.

§ 6. Nachweismöglichkeiten

(1) Der Auftragnehmer stellt dem Nutzer auf dessen Anfrage alle erforderlichen Informationen zum Nachweis der in diesem Vertrag und Art. 28 DSGVO geregelten Pflichten zur Verfügung. Insbesondere erteilt der Auftragnehmer dem Nutzer Auskünfte über die gespeicherten Daten und die Datenverarbeitungsprogramme.

(2) Der Auftragnehmer hat dem Nutzer auf Anforderung geeigneten Nachweis über die Einhaltungen der Verpflichtungen gemäß Art. 28 Abs. 1 und Abs. 4 DSGVO zu erbringen. Dieser Nachweis kann durch die Bereitstellung von Dokumenten und Zertifikaten, die genehmigte Verhaltensregeln i. S. v. Art. 40 DSGVO oder genehmigte Zertifizierungsverfahren i. S. v. Art. 42 DSGVO abbilden, erbracht werden.

(3) Sollten im Einzelfall Inspektionen durch den Nutzer oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Nutzer beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.
Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung i.H. eines Beratertagessatzes verlangen. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

(4) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Nutzers eine Inspektion vornehmen, gilt grundsätzlich Absatz 3 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7. Subunternehmer (weitere Auftragsverarbeiter)

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice wie IT-Helpdesk (ohne Zugang zur gradar-Plattform) oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, auch bei ausgelagerten Nebenleistungen

angemessene und gesetzeskonforme Kontrollmaßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Nutzers zu ergreifen.

(2) Der Nutzer stimmt zu, dass der Auftragnehmer Unterauftragnehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung der Unterauftragnehmer informiert der Auftragnehmer den Nutzer in Textform (bspw. per E-Mail). Der Nutzer kann der Änderung innerhalb von 3 Wochen ab Erhalt der Information durch den Auftragnehmer in schriftlicher Form oder in Textform (bspw. per E-Mail) begründet widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben.

(3) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird vertraglich sicherstellen, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber Unterauftragnehmern gelten. Der Vertrag des Auftragnehmers mit dem Subunternehmer wird schriftlich oder in elektronischem Format abgeschlossen werden.

(4) Eine Beauftragung von Subunternehmern in Drittstaaten erfolgt nur, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(5) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgender Subunternehmer durchgeführt:

Name und Anschrift des Subunternehmers	**Beschreibung der Teilleistungen**
Telekom Deutschland GmbH, Landgrabenweg 151, 53227 Bonn, Deutschland (betrieben durch T-Systems)	Webhosting der internetbasierten Software „gradar the job evaluation engine“ unter *.gradar.com
STRATO AG, Pascalstraße 10, D-10587 Berlin, Deutschland	Webhosting der Unternehmenswebsites wie www.gradar.com, www.qpm.de und des E-Mail Servers (für qpm.de)
Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521	Bereitstellung von Microsoft 365 Applikationen wie z.B. Exchange (E-Mail für gradar.com), Office, Teams, OneDrive auf Server in Europa / Deutschland, mit Betreuung durch Diensteanbieter / Lösungspartner STRATO AG.
Uniscon universal identity control GmbH. Ridlerstrasse 57 (Newton), D-80339 München, Deutschland	Hosting der versiegelten Cloud- Plattform zum sicheren Datenaustausch https://www.idgard.de/

Mailjet SAS, 13-13 bis, rue de l'Aubrac, 75012 Paris, Frankreich	E-Mail- und SMS-Versandlösung und zugehörige Dienstleistungen
TeamDrive Systems GmbH, Max-Brauer-Allee 50, D-22765 Hamburg, Deutschland	Server-Laufwerk zur Speicherung und Synchronisation aller Dateien der QPM GmbH mit Ende-zu-Ende-Verschlüsselung auf Servern in Europa.

(6) Kern- und unterstützende Prozesse sind ferner im Verarbeitungsverzeichnis dokumentiert.

§ 8. Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Nutzer unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Nutzer als »Verantwortlicher « im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

(4) Es gilt deutsches Recht.