Allgemeine Geschäftsbedingungen zur Nutzung der unentgeltlichen Basic-Version von gradar.com

§ 1. Vertragsgegenstand

(1) Während der Vertragslaufzeit (dazu § 2.) ist der Nutzer berechtigt, das von der QPM Quality Personnel Management GmbH [QPM oder Anbieter] entwickelte, internetbasierte analytische Stellenbewertungssystem „gradar the job evaluation engine“ in der Basic-Version zu nutzen.

(2) Das System wird darüber hinaus in den Versionen Starter Plus, Professional Plus und Enterprise gegen Entgelt angeboten.

(3) Funktionsumfang und Nutzungsvoraussetzungen ergeben sich aus **Anlagen 1** und **4** sowie der zum jeweiligen Zeitpunkt aktuellen Leistungsbeschreibung der Internetplattform.

§ 2. Vertragslaufzeit

(1) Der Vertrag beginnt mit dem Datum der Online-Registrierung auf www.gradar.com und hat eine Laufzeit von drei Monaten.

(2) Die Laufzeit verlängert sich jeweils um weitere drei Monate, wenn nicht 4 Wochen vor Ablauf gekündigt wird.

(3) Der Nutzer ist berechtigt, den Nutzungsvertrag mit dem Anbieter jederzeit ohne Angabe von Gründen und ohne Einhaltung einer Frist zu kündigen. Die Kündigung kann in Textform (z.B. per E-Mail) oder durch Löschung des Accounts durch den Nutzer erklärt werden.

(4) Wird die für die Anmeldung genutzte E-Mail Adresse nicht innerhalb von 10 Tagen bestätigt, oder vergehen 210 Tage ohne Anmeldung, wird der Account aus Gründen der Datensparsamkeit gelöscht.

(5) QPM ist neben der fristgebundenen Kündigung berechtigt, den Nutzungsvertrag ohne Einhaltung einer Frist außerordentlich zu kündigen, wenn ein wichtiger Grund vorliegt. Ein wichtiger Grund liegt insbesondere dann vor, wenn der Nutzer

- über das Kontaktformular Werbung oder andere unzulässige Inhalte versendet,
- versucht, die Software ganz oder teilweise zu ändern, zu modifizieren, anzupassen oder zu dekompilieren, soweit es jeweils über die Grenzen der §§ 69d Abs. 3, 69e UrhG hinausgeht,
- in sonstiger Weise schwerwiegend gegen seine vertraglichen Pflichten verstößt
- bei der Nutzung der Internetseite schuldhaft und schwerwiegend gegen sonstige gesetzliche Vorschriften verstößt.

(6) In diesen Fällen ist QPM auch berechtigt, das Benutzerkonto des Nutzers zeitlich befristet oder dauerhaft zu sperren oder zu löschen und die Einrichtung eines neuen Benutzerkontos zu verweigern.

§ 3. Preise, Fälligkeit, Zurückbehaltungsrecht

(7) Die vom Nutzer zu zahlende quartalsweise Nutzungsgebühr beträgt
für die **Basic-Version** mit einem Nutzer 0,- €
In der Nutzungsgebühr enthalten sind das Hosting der Software und technischer Support.

(8) Ein Upgrade auf eine entgeltpflichtige Version ist jederzeit möglich.

(9) In der Nutzungsgebühr nicht eingeschlossen sind Beratung und Schulung, über die bei Bedarf gesonderte Vereinbarungen zu treffen sind.

(10) Gerät der Nutzer mit der Bezahlung vereinbarter Zusatzleistungen mehr als 14 Tage in Verzug, kann QPM in Ausübung des Zurückbehaltungsrechts den Zugang zur Basic-Version sperren.

§ 4. Kontakt

Für Supportanfragen steht das QPM-Team telefonisch unter +49 (0) 211 9367 249-0 oder per E-Mail support@gradar.com zur Verfügung.

gradar the job evaluation engine (www.gradar.com) ist ein Produkt der
QPM Quality Personnel Management GmbH
Am Haferkamp 78
D-40589 Düsseldorf
https://qpm.de

Geschäftsführung: Philipp Schuch und Lisanne Metz
Sitz der Gesellschaft: Düsseldorf
Amtsgericht: Düsseldorf, HRB 73656
USt-IdNr.: DE297336053
St.-Nr.: 106/5722/0606

§ 5. Datenschutz und Datensicherheit

(1) Das internetbasierte Stellenbewertungsprogramm wird auf europäischen Servern gehostet. Die Internet-Verbindung ist durch SSL verschlüsselt.

(2) Alle in der Zwischenablage gespeicherten Daten werden nach Beendigung der Verbindung/Abmeldung gelöscht.

(3) Die Software bewertet Stellen, so dass keine personenbezogenen Daten übertragen zu werden brauchen.

(4) Die datenschutzrechtlichen Verpflichtungen der Vertragsparteien sind in der **Anlage 2** zu diesem Vertrag geregelt.

(5) Eine Auflistung der getroffenen technisch-organisatorischen Maßnahmen zum Datenschutz findet sich in **Anlage 3** zu diesem Vertrag.

(6) Mit der Nutzung der Basic Version von gradar sowie der Bestätigung der E-Mail Adresse willigt der Nutzer ein, dass QPM ihn per E-Mail oder mit Hilfe von automatisierte Benachrichtigungen (E-Mail) kontaktieren darf. Dieser Einwilligung kann jederzeit formlos schriftlich oder per E-Mail widersprochen werden.

(7) QPM behält sich das Recht vor, die Kontaktdaten (Name und E-Mail Adresse) von neuregistrierten Nutzern der Basis Version zum Zwecke der vertrieblichen Nachverfolgung („Follow-Up“) durch einen lokalen Partner an einen solchen weiterzuleiten. Die Liste der Partner ist auf https://www.gradar.com/ veröffentlicht.

(8) Die Partner sind verpflichtet, die Kontaktdaten nur für individuelle, vertriebsorientierte Weiterverfolgung zu verwenden und nicht in CRM-Systemen zu speichern oder für Mailingaktionen zu verwenden.

§ 6. Gerichtsstand und anwendbares Recht

(9) Sofern der Nutzer Kaufmann ist, ist der Gerichtsstand Düsseldorf.

(10) Dieser Vertrag unterliegt dem Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Übereinkommens über Verträge über den internationalen Warenkauf vom 11.04.1980 (CISG) und des deutschen Internationalen Privatrechts.

Anlage 1: Nutzungsvoraussetzungen

§ 1. Technische Voraussetzungen

(1) gradar.com ist eine webbasierte Anwendung, die Nutzung setzt daher ein internetfähiges Endgerät sowie eine Internetanbindung seitens des Kunden voraus.

(2) Die Internetanbindung sollte hinsichtlich Stabilität und Bandbreite dem jeweils aktuellen Stand der Technik entsprechen.

(3) Um die Software nutzen zu können, werden ferner Kenntnisse in der Bedienung von Internetbrowsern, einfachen Webanwendungen und Office-Software sowie ein gültiger E-Mail Account benötigt.

(4) Der Kunde erwirbt eine befristete Nutzungslizenz (Starter, Professional oder Enterprise) und erhält von der QPM als Anbieter der Anwendung die Zugangsdaten. Zugriff und Nutzung erfolgen durch einen Internetbrowser.

§ 2. Zugang

Der Zugang erfolgt anhand einer individuellen Login-ID (E-Mail Adresse) und eines Passworts über eine mittels SSL-Verschlüsselung gesicherte Verbindung, die über www.gradar.com aufgerufen wird.

§ 3. Updatemanagement

(1) Bei technischer oder inhaltlicher Notwendigkeit werden Updates der gradar Applikation auf dem Server veröffentlicht.

(2) Die Ergebnisse der Stellenbewertung werden mit einer Versionsnummer gespeichert. So ist gewährleistet, dass bei einer späteren Neubewertung einer Stelle das Ergebnis der Stellenbewertung konsistent bleibt, auch wenn eine neue Version der Anwendung oder des Algorithmus der Stellenbewertung veröffentlicht wurde.

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.

Anlage 3: Technisch-organisatorische Maßnahmen nach Art. 32 DS-GVO

+++ Stand 10.11.2022 +++

Hosting-Partner:

Informationen zu den technischen und organisatorischen Maßnahmen unserer Hosting-Partner T-Systems International GmbH und der Strato AG finden Sie auf den folgenden Webseiten:

- **T-Systems International GmbH:**
  https://cloud.telekom.de/de/infrastruktur/open-telekom-cloud/mehr/compliance
- **Strato AG:**
  https://www.strato.de/sicherheit/

Beide Rechenzentren sind unter anderem nach ISO 27001 zertifiziert.

Unsere technisch-organisatorischen Maßnahmen gliedern sich nach

a) Maßnahmen im Geschäftsbetrieb der QPM GmbH und
b) Maßnahmen für den Betrieb der Plattform gradar.com.

Technisch-organisatorische Maßnahmen für den Geschäftsbetrieb der QPM Quality Personnel Management GmbH

Zutrittskontrolle

"Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren"

- Kein Publikumsverkehr
- Sicherheitsschlösser und -türen (RC4)
- Fenster mit 3-Fach-Verglasung und zeitgesteuerten elektrischen Rollladen

Zugangskontrolle

"zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können"

Technische Maßnahmen:

- Authentifikation mit individuellem, lokalen Benutzerkonto + Passwort
- Separates Administratorkonto
- Verwendung von 2FA wo möglich
- Regelmäßige Aktualisierung aller Betriebssysteme und lokal installierter Softwarekomponenten
- Einsatz und regelmäßige Aktualisierung von Anti-Viren-Software
- Einsatz von Firewalls am Übergang LAN / WAN
- Verschlüsselung aller Datenträger in Laptops / Desktops
- Lokal installierter TeamDrive Client zur AES256 verschlüsselten Datensynchronisation
- Zugriff nur auf relevante TeamDrive Spaces für einzelne Nutzer
- Sperrung der Auto-Installation fremder / neuer Hardware
- Sperrung mobiler Datenträger an Laptops / Desktops
- Verschlüsselung von Smartphones
- Regelmäßige Kontrolle aller Zugriffe
- Regelmäßige interne Informationssicherheitsaudits
- IT-Monitoring und Antivirenschutz über ESET - Clients
- Einsatz von Intrusion-Prevention-System (kurz: IPS) und Intrusion-Detection-System (kurz: IDS) - Server

Organisatorische Maßnahmen:

- Verwaltung und Dokumentation der Benutzerberechtigungen gemäß Berechtigungskonzept zu Vergabe und Entzug von Zugriffsrechten
- Clean Desk Policy
- Passwortvergabe / Passwortregeln
- Bereitstellung von unternehmenseigener Hardware und Software
- Bereitstellung von Hardware-Token für 2FA
- Installation neuer Hardware (z.B. via Bluetooth oder USB) nur durch IT-Support
- Verzicht auf mobile Datenträger an Laptops / Desktops
- Schutzniveau Ermittlung durch ein Informationssicherheitsmanagementsystem (ISMS)

Zugriffskontrolle

"zu 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"

Technische Maßnahmen:

- Einsatz von Aktenvernichtern
- Kein Einsatz von und Sperrung mobiler Datenträger an Laptops / Desktops
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten

Organisatorische Maßnahmen:

- Anzahl der Administratoren auf das Notwendigste reduzieren
- Passwortrichtlinie inkl. Länge und Wechsel
- Verwaltung der Benutzerrechte durch Systemadministratoren
- Verzicht auf mobile Datenträger
- Regelmäßige Datenschutzschulung aller Mitarbeitenden

Weitergabekontrolle

"zu 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"

Technische Maßnahmen:

- Verschlüsselung und Passwortschutz einzelner Dokumente beim Datenaustausch mit Kunden, z.B. via idgard.de
- Verschlüsseltes TeamDrive für administrative Kundendaten mit gesonderten Zugriffsrechten
- Verschlüsseltes TeamDrive für projektbezogene Kundendaten mit gesonderten Zugriffsrechten

Sperrung mobiler Datenträger an Laptops / Desktops

Organisatorische Maßnahmen:

- Austausch von Kundendaten ausschließlich über verschlüsselte Verbindungen
- Anonymisierung bzw. Pseudonymisierung von Kundendaten z.B. bei Vergütungsanalysen
- Verzicht auf Nutzung mobiler Datenträger
- Mitarbeitersensibilisierung durch regelmäßige Schulungen zum Datenschutz

Eingabekontrolle

"zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind"

Technische Maßnahmen:

- Protokollierung der Eingabe, Änderung und Löschung von Daten

Organisatorische Maßnahmen:

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen

Auftragskontrolle

"zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können"

Organisatorische Maßnahmen:

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit und technischer Kompetenz)
- Abschluss von Auftragsverarbeitungsverträgen mit den Auftragnehmern
- Übersicht und Auflistung aller Auftragsverarbeitungsverträge
- Laufende Überprüfung der Auftragnehmer und ihrer Tätigkeiten auf Änderungen der verarbeiteten Daten und Schutzmaßnahmen
- Schriftliche Weisungen an den Auftragnehmer
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Verpflichtung der Mitarbeiter des Auftragnehmers auf die datenschutzrechtliche Vertraulichkeit

Verfügbarkeitskontrolle/Integrität

"zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind"

Technische Maßnahmen:

- Feuerlöschgeräte
- Rauchmeldeanlage
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Geschäftsräumen
- Schutzsteckdosenleisten in Geschäftsräumen
- Unterbrechungsfreie Stromversorgung (USV) für lokales Serversystem in Geschäftsräumen
- IT-Monitoring und Antivirenschutz über ESET - Clients
- Einsatz von Intrusion-Prevention-System (kurz: IPS) und Intrusion-Detection-System (kurz: IDS) - Server

Organisatorische Maßnahmen:

- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Testen von Datenwiederherstellung
- Lokale Serversysteme nicht unter sanitären Anlagen

Trennungskontrolle

"zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können"

Technische Maßnahmen:

- Trennung der Unternehmensdaten von administrativen Kundendaten und projektbezogenen Daten in separaten TeamDrive Spaces

Organisatorische Maßnahmen:

- Festlegung und Dokumentation von Zugriffsrechten

Technisch-organisatorische Maßnahmen für den Betrieb von gradar.com

Zutrittskontrolle

"Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren"

- Hier verweisen wir auf die Maßnahmen unseres Hosting-Partners T-Systems International GmbH: „Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;“
- Zur zusätzlichen Sicherheit ist ein Intrusion-Prevention-System (kurz: IPS) und Intrusion-Detection-System (kurz: IDS) im Einsatz

Zugangskontrolle

"zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können"

Technische Maßnahmen:

- Authentifikation der Systemadministratoren mit E-Mail + Passwort + OTP (2FA)
- Optionale Zwei-Faktor-Authentifizierung (2FA) für Unternehmensanwender
- Optionaler Single Sign-On (SSO) mit Google Workspace, Micosoft Azure oder Okta für Unternehmensanwender
- Einsatz von Firewalls
- Verschlüsselung des Datenträgers des (*stateless*) Applikationsservers
- Verschlüsselung der Datenbanken
- Verschlüsselte Kommunikation zwischen Applikationsserver und Datenbank
- Verschlüsselte Kommunikation zwischen Applikationsserver und Endnutzer-Client

Organisatorische Maßnahmen:

- Getrennte Benutzerkonten für Systemadministration, Sachbearbeitung, persönliche Nutzung
- Verwaltung der Benutzerberechtigungen durch Unternehmensadministratoren

Zugriffskontrolle

"zu 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"

Technische Maßnahmen:

- Zugriff auf Server-Systemen nur via VPN
- Port-Freigaben auf das Notwendigste reduziert,
- Getrennte Systeme für Applikationsserver und Datenbank
- Verschlüsselung der Passwörter mit Bcrypt Algorithmus
- Mandantentrennung in allen relevanten Datenbanktabellen
- Verschlüsselung der Datenbank
- Verschlüsselung der Kommunikation zwischen Applikationsserver und Datenbank
- Verschlüsselung der Kommunikation zwischen Applikationsserver und Endnutzer-Client

Organisatorische Maßnahmen:

- Anzahl der Administratoren auf das Notwendigste reduziert
- Verwaltung der Benutzerrechte durch Systemadministratoren
- Zwei-Faktor-Authentifizierung (2FA) für Systemadministratoren
- Verwaltung der unternehmensspezifischen Zugriffsrechte auf Ergebnisse der Stellenbewertung durch Unternehmensadministratoren
- Abbildung einer unternehmensspezifischen Organisationsstruktur (als Basis für die Zugriffsverwaltung auf Stelleninformationen)
- Abbildung von unternehmensspezifischen Standorten / Populationen (als Basis für die Zugriffsverwaltung auf Vergütungsinformationen)
- Regelmäßige Kontrolle und Dokumentation der Zugriffsverwaltung

Weitergabekontrolle

"zu 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"

Technische Maßnahmen:

- Logische, softwareseitige Mandantentrennung der mit dedizierten Subdomains angelegten Unternehmensaccounts
- Verschlüsselung von Datenträgern und Datenbanken sowie Backups
- Abbildung einer unternehmensspezifischen Organisationsstruktur (als Basis für die Zugriffsverwaltung auf Stelleninformationen)
- Abbildung von unternehmensspezifischen Standorten / Populationen (als Basis für die Zugriffsverwaltung auf Vergütungsinformationen)

Organisatorische Maßnahmen:

- Sensibilisierung und aktive Unterstützung der Unternehmensadministratoren für Möglichkeiten der Benutzerverwaltung und Management der Zugriffsmöglichkeiten

Eingabekontrolle

"zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind"

Mit der Applikation werden Stellen bewertet, so dass keine personenbezogenen Daten von Stelleninhabern übertragen zu werden brauchen. Es ist möglich (aber nicht erforderlich), personenbezogene Daten serverseitig in Kommentarfeldern oder Stellenbeschreibungen zu speichern.

Standardmäßig werden nur Name, E-Mail-Adresse und Telefonnummer der Anwender gespeichert.

Organisatorische Maßnahmen:

- Nachvollziehbarkeit von Eingabe und Änderung von Stellen sowie Ergebnissen der Stellenbewertung durch individuelle Benutzernamen

Auftragskontrolle

"zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können"

Organisatorische Maßnahmen:

- Auswahl der Auftragnehmer unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Regionalität, Datensicherheit und technischer Kompetenz)
- Abschluss von Auftragsverarbeitungsverträgen mit den Auftragnehmern
- Übersicht und Auflistung aller Auftragsverarbeitungsverträge
- Laufende Überprüfung der Auftragnehmer und ihrer Tätigkeiten auf Änderungen der verarbeiteten Daten und Schutzmaßnahmen
- Schriftliche Weisungen an die Auftragnehmer

Verfügbarkeitskontrolle/Integrität

"zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind"

Technische Maßnahmen:

- Hier verweisen wir auch auf die Maßnahmen unseres Hosting-Partners T-Systems Deutschland GmbH: „Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;
- Software Design Pattern zur automatischen Eingrenzung von Datenzugriffen
- Zustandslose Applikationsserver
- Trennung von Produktiv- und Testsystemen
- Pseudonymisierung von Testdaten

Organisatorische Maßnahmen:

- Festlegung und Dokumentation von Zugriffsrechten

Trennungskontrolle

"zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können"

Technische Maßnahmen:

- Trennung von Produktiv- und Testsystemen
- Pseudonymisierung von Testdaten

Organisatorische Maßnahmen:

- Festlegung und Dokumentation von Zugriffsrechten

QPM Quality Personnel Management

gradar the job evaluation engine

Anhang 4: gradar Funktionalitäten und Preise 2023

gradar Version	Basic	Starter Plus	Professional Plus	Enterprise
Jahreslizenz (SaaS)	0 €	2.000 €	4.000 €	6.000 €
Stellenbewertung	**nicht auf Server gespeichert**	**bis zu 75 Stellen**	**unbegrenzte Stellen**	**unbegrenzte Stellen**
20+ Sprachpakete	●	●	●	●
Drei gradar Karriefepfade: Fachlaufbahn, Führungslaufbahn, Projektmanagement	●	●	●	●
Detaillierte Faktorbeschreibungen	○	●	●	●
Globale Job-Familien mit detaillierten Definitionen und typischen Aktivitäten	○	●	●	●
Unternehmensspezifische Karriere-/Job-Level: Unternehmeseigene Level-Strukturen auf Basis von gradar Grades und konfigurierten Variablen	○	●	●	●
Ergebnisverwaltung / Dokumentation				
Kopieren und Einfügen: Kopie der Ergebnisse in Zwischenablage	●	●	●	●
Entwerfen, speichern und fortsetzen: Speicherung der Ergebnisse auf Server	○	●	●	●
Kommentarfunktion	○	●	●	●
Import von Stellen und benutzerdefinierten Variablen	○	●	●	●
Import von Stellenbeschreibungen und weiteren Dokumenten	○	●	●	●
Benutzer- / Zugriffsverwaltung				
Mehrnutzerlizenz (weitere Nutzerlizenzen 250 € p.a. je Nutzer)	○ **(1)**	● **(1)**	● **(3)**	● **(6)**
Standard Nutzertypen	○	●	●	●
Unbegrenzte Anzahl von Nur-Lese-Benutzern	○	○	●	●
Funktionales, rollenbasiertes Zugriffsmanagement auf Basis von Standardgruppen	○	●	●	●

● = enthalten ○ = nicht enthalten

gültig ab 1. Januar 2023, *Implementierung gegen Gebühr nach Aufwand

QPM Quality Personnel Management

gradar the job evaluation engine

gradar Version	Basic	Starter Plus	Professional Plus	Enterprise
Vollständig anpassbares, „Enterprise-Grade“ Zugriffsmanagement auf der Grundlage von Gruppenrichtlinien *Organisationsstrukturen* und *Standorten/Populationen*	○	○	○	●
Kompetenzmanagement (TMA Kompetenzbibliothek)				
Standardmodell basierend auf systemeigenen “globalen Job-Familien”	○	●	●	●
Anpassung stellenspezifischer Kompetenzen basierend auf dem globalen Modell	○	●	●	●
Unternehmensspezifisches Modell basierend auf eigenen Variablen und/oder Kompetenzen	○	○	○	● (*)
Arbeitsbedingungen				
Unternehmensspezifisches Modell	○	○	● (*)	● (*)
Job Matching				
Job Matching zu Vergütungsstudien basierend auf systemeigenen “globalen Job-Familien” und QPMs Übersicht “Compensation Survey Rosetta Stone”	○	●	●	●
Lokale Job Matches, um globale Job Matches auf Ebene von Standort / Population anzupassen	○	●	●	●
Unternehmensspezifische Matching-Matrizen zu Vergütungs-studien / Tarifverträgen etc.	○	○	○	● (*)
Vergütungsinformationen				
Import und Anzeige von Daten aus separat zu erwerbenden Drittanbieter Vergütungsstudien	○	●	●	●
Vergütungsstrukturierung, Modellierung und Anzeige von z.B. Gehaltsbändern	○	●	●	●
Vergütungsanalyse und Martkvergleich				
Upload und Verwaltung von Mitarbeiter(gehalts)daten	○	●	●	●
Statistische Analyse der Ist-Vergütung hinsichtlich z.B. Verteilung der Gehälter (Perzentile)	○	●	●	●

● = enthalten ○ = nicht enthalten

gültig ab 1. Januar 2023, *Implementierung gegen Gebühr nach Aufwand

gradar Version	Basic	Starter Plus	Professional Plus	Enterprise
Equal Pay Analyse zur Ermittlung von unbereinigter und bereinigter Entgeltlücke, z.B. nach Geschlecht	○	●	●	●
Compa-Ratio Analysen gegen interne Gehaltsbänder und externe Marktdaten	○	●	●	●
Erweiterte Möglichkeiten zur Vergütungsstrukturierung, z.B. analysegestützte Modellierung von Gehaltsbändern	○	●	●	●
Systemkonfiguration				
Eigene Subdomain	●	●	●	●
Eigenes Logo	○	●	●	●
Benutzerdefinierte Variablen (z.B. Job-Cluster, Job-Familien, Regionen etc.) mit detaillierten Beschreibungen	○	● **(3)**	● **(3)**	● **(6)**
Abbildung der unternehmens-spezifischen *Organisationsstruktur* und *Standorte / Populationen* (u.a. für Zugriffsrechte in Enterprise Version)	○	●	●	●
Unternehmensspezifischen Formulierungen der Grading-Faktoren	○	○	○	● (*)
Analysen & Berichte				
Quervergleich	○	●	●	●
Export der tabellarischen Berichte in CSV / XLSX	○	●	●	●
Export der stellenspezifischen Ergebnisse in DOCX	○	●	●	●
IT-Sicherheit und Datenschutz				
Hosting in Rechenzentrum der Telekom Deutschland, zertifiziert nach CSA Star Level 2, Trusted Cloud Data Protection Profile (TCDP) 1.0, ISO 9001, 14001, 22301, 20000, 27001, 27017, 27018, TÜV Trusted Cloud	●	●	●	●
Umfassender Überblick über die technischen und organisatorischen Maßnahmen zum Datenschutz gemäß Artikel 32 der GDPR	●	●	●	●

● = enthalten ○ = nicht enthalten

gültig ab 1. Januar 2023, *Implementierung gegen Gebühr nach Aufwand

gradar Version	Basic	Starter Plus	Professional Plus	Enterprise
Zwei-Faktor-Authentifizierung (2FA), die ein Benutzerkonto wirksam vor unberechtigtem Zugriff schützt.	○	●	●	●
Single Sign-On (SSO) mit Google Workspace, Micosoft Azure oder Okta. Verwenden Sie eines dieser IAM-Systeme (Identitäts- und Zugriffsmanagement (IAM)), um Benutzer in der App anzumelden.	○	○	●	●

● = enthalten ○ = nicht enthalten

gültig ab 1. Januar 2023, *Implementierung gegen Gebühr nach Aufwand