# Vertrag über die Auftragsverarbeitung

**Die zwei R consulting & software GmbH, Klosengartenstr. 31, 50374 Erftstadt, („Auftragnehmer “) und der Kunde („Auftraggeber“) schließen einen Cloud-Vertrag über die Nutzung von Jana ab**

## § 1 Allgemeines

1.1. Der Auftragnehmer schließt mit seiner Registrierung für die Nutzung von Jana diesen Vertrag über die Auftragsverarbeitung (nachfolgend „**AVV**“) mit dem Auftraggeber, indem er im Registrierungsprozess die Geltung dieses AVV bestätigt.

1.2. Leistungen gegenüber Verbrauchern (§ 13 BGB) werden mit Jana nicht erbracht.

1.3. Alle vertragsrelevanten Dokumente sind bei Vertragsschluss auf der Website unter Jana-app.de („Website“) abrufbar und werden nicht separat von 2rSoftware für den Kunden gespeichert.

## § 2 Auftrag und Festlegungen zur Verarbeitung

2.1. Dieser Vertrag über die Auftragsverarbeitung (nachfolgend „**AVV**“) konkretisiert für alle Verarbeitungen die datenschutzrechtlichen Rechte und Pflichten der Parteien, welche sich aus den zwischen den Parteien bereits bestehenden oder künftig abzuschließenden Verträgen (nachfolgend „**Hauptvertrag**“) ergeben, unter denen es zu einer Verarbeitung personenbezogener Daten durch den Anbieter für den Auftraggeber kommt.

2.2. Dieser AVV kommt mit all seinen Bestandteilen zur Anwendung, wenn der Auftraggeber den Anbieter zur Verarbeitung personenbezogener Daten (nachfolgend „**Daten**“) im Auftrag gemäß Art. 28 DSGVO verpflichtet hat. Dabei bildet dieser AVV den Rahmen für eine Vielzahl unterschiedlicher Vorgänge der Auftragsverarbeitung.

2.3. Bei etwaigen Widersprüchen gehen die Regelungen dieses AVV mit all seinen Bestandteilen den Regelungen des zugehörigen Hauptvertrages vor.

2.4. Die für einzelne Verarbeitungen geltenden spezifischen datenschutzrechtlichen Festlegungen (nachfolgend „**Festlegungen**“) werden vor Beginn der Verarbeitung in Anlagen zum AVV (nachfolgend „**Anlagen**“) geregelt. Dies sind insbesondere Gegenstand und Dauer sowie Art und Zweck der Verarbeitung, die Kategorien von Daten und die Kategorien betroffener Personen sowie die technischen und organisatorischen Maßnahmen (nachfolgend „**TOM**“).

2.5. Die Anlagen sind Teil des AVV. Bei etwaigen Widersprüchen gehen die Anlagen der allgemeineren Regelung im AVV vor. Wird im Folgenden oder in den Anlagen auf den AVV Bezug genommen, so ist der AVV mit all seinen Bestandteilen gemeint.

## § 3 Verantwortlichkeit und Verarbeitung auf Weisung

3.1. Der Auftraggeber ist im Rahmen dieses AVV für die Einhaltung der anwendbaren gesetzlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Offenlegung gegenüber dem Anbieter sowie für die Rechtmäßigkeit der Verarbeitung allein verantwortlich („Verantwortlicher“ gemäß Art. 4 Nr. 7 DSGVO).

3.2. Der Anbieter handelt wegen der Verarbeitung der Daten ausschließlich weisungsgebunden, es sei denn es liegt ein Ausnahmefall gemäß Art. 28 Abs. 3 lit. a) DSGVO vor (anderweitige gesetzliche Verarbeitungspflicht). Mündliche Weisungen sind unverzüglich in Textform zu bestätigen. Wird der Auftraggeber als Auftragnehmer einer Auftragsverarbeitung für einen Dritten tätig, gelten die Verpflichtungen des Auftraggebers aus dieser Auftragsverarbeitung für den Dritten unmittelbar als Weisungen des Auftraggebers im Verhältnis zum Anbieter, sofern diese Verpflichtungen strenger sein sollten als diejenigen aus diesem AVV. Der Auftraggeber wird den Anbieter über solche Anforderungen Dritter an die Auftragsverarbeitung schriftlich in Kenntnis setzen.



zwei R software GmbH
Klosengartenstr. 31
50374 Erftstadt
Tel. : 02235 . 98 623
Fax : 02235 . 98 62 98
Mail : info@2rsoftware.de
Web : www.2rsoftware.de
Geschäftsführer:
Robert Schmitz
Robert Pyrzewski
AG : Köln
HRB : 50691
Bankverbindung: Sparkasse KölnBonn
IBAN : DE11 3705 0198 1024 7026 88
BIC : COLSDE33

3.3. Der Anbieter berichtigt oder löscht die vertragsgegenständlichen Daten oder schränkt deren Verarbeitung ein (nachfolgend „Sperrung“), wenn der Auftraggeber dies anweist und dies sonst vom Weisungsrahmen umfasst ist.

3.4. Der Anbieter informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Vorschriften über den Datenschutz oder diese AVV verstößt. Der Anbieter darf die Umsetzung der Weisung solange aussetzen, bis diese vom Auftraggeber in Textform bestätigt oder abgeändert wurde. Die Ausführung offensichtlich datenschutzrechtswidriger Weisungen darf der Anbieter ablehnen.

3.5. Die Parteien benennen gegenseitig in Textform einen oder mehrere Ansprechpartner in datenschutzrechtlichen Angelegenheiten, einschließlich der bestellten Datenschutzbeauftragten. Ergeben sich bei den Ansprechpartnern Änderungen, haben sich die Parteien hierüber in Textform zu informieren.

3.6. Der Anbieter gewährleistet, dass die zur Verarbeitung der Daten befugten Personen (a) die Weisungen des Auftraggebers kennen und diese beachten, sowie (b) sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits- und Verschwiegenheitspflicht besteht auch nach Beendigung der Verarbeitung fort.

3.7. Wird der Auftraggeber als Auftragnehmer einer Auftragsverarbeitung für einen Dritten tätig, gelten die Verpflichtungen des Anbieters aus diesem AVV auch unmittelbar im Verhältnis zwischen dem Dritten und dem Anbieter. Dies gilt für alle Leistungen des Anbieters, welche dieser im Auftrag des Auftraggebers gegenüber dem Dritten erbringt. Insbesondere stehen dem Dritten die Kontroll- und Informationsrechte aus § 9 unmittelbar gegenüber dem Anbieter zu.

## § 4 Sicherheit der Verarbeitung

4.1. Die Parteien vereinbaren TOM gemäß Art. 32 DSGVO zum angemessenen Schutz der Daten (nachfolgend „**Anlage-TOM**“).

4.2. Änderung der Anlage-TOM bleiben dem Anbieter vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau insgesamt nicht unterschritten wird. Wesentliche Änderungen sind dem Auftraggeber in Textform mitzuteilen und bedürfen der vorherigen Zustimmung durch den Auftraggeber in Textform.

## § 5 Unterrichtung bei Datenschutzverletzungen und Fehlern der Verarbeitung

5.1. Der Anbieter unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes der ihm vom Auftraggeber anvertrauten Daten im Sinne des Art. 4 Nr. 12 DSGVO in seinem Organisationsbereich bekannt werden oder ein konkreter Verdacht einer solchen Datenschutzverletzung beim Anbieter besteht.

5.2. Stellt der Auftraggeber Fehler bei der Verarbeitung fest, hat er den Anbieter unverzüglich hierüber zu unterrichten.

5.3. Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Behebung der Datenschutzverletzung gemäß § 5.1 oder der Fehler gemäß § 5.2 sowie zur Minderung möglicher nachteiliger Folgen, insbesondere für die betroffenen Personen. Hierüber stimmt er sich mit dem Auftraggeber ab. Mündliche Unterrichtungen § 5.1 oder § 5.2 sind unverzüglich in Textform nachzureichen.

## § 6 Übermittlung von Daten an einen Empfänger in einem Drittland oder in einer internationalen Organisation

Die Übermittlung von Daten an einen Empfänger in einem Drittland außerhalb von EU und EWR ist unter Einhaltung der in Art. 44 ff. DSGVO festgelegten Bedingungen zulässig. Einzelheiten werden bei Bedarf in einer oder mehreren Anlagen geregelt.

## § 7 Unterbeauftragung weiterer Auftragsverarbeiter

7.1. Der Anbieter darf die Verarbeitung personenbezogener Daten ganz oder teilweise durch weitere Auftragsverarbeiter (nachfolgend „**Unterauftragnehmer**“) erbringen lassen.



zwei R software GmbH
Klosengartenstr. 31
50374 Erftstadt
Tel. : 02235 . 98 623
Fax : 02235 . 98 62 98
Mail : info@2rsoftware.de
Web : www.2rsoftware.de
Geschäftsführer:
Robert Schmitz
Robert Pyrzewski
AG : Köln
HRB : 50691
Bankverbindung: Sparkasse KölnBonn
IBAN : DE11 3705 0198 1024 7026 88
BIC : COLSDE33

7.2. Der Anbieter informiert den Auftraggeber in Textform rechtzeitig vorab über die Beauftragung von Unterauftragnehmern oder Änderungen in der Unterbeauftragung. Der Auftraggeber kann bei Vorliegen eines wichtigen Grundes der Unterbeauftragung innerhalb von vier Wochen nach Kenntnisnahme in Textform widersprechen. Ein wichtiger Grund liegt insbesondere vor, wenn ein begründeter Anlass zu Zweifeln besteht, dass der Unterauftragnehmer die vereinbarte Leistung entsprechend den anwendbaren gesetzlichen Bestimmungen zum Datenschutz oder gemäß dieser AVV erbringt. Im Fall eines begründeten Widerspruchs des Auftraggebers räumt dieser dem Anbieter eine angemessene Frist ein, um den vom Widerspruch betroffenen Unterauftragnehmer durch einen anderen Unterauftragnehmer zu ersetzen. Ist dem Anbieter dies nicht möglich oder dem Auftraggeber nicht zumutbar, ist die jeweilige Partei zur außerordentlichen Kündigung des Hauptvertrags aus wichtigem Grund berechtigt.

7.3. Der Anbieter wird mit dem Unterauftragnehmer die in diesem AVV getroffenen Regelungen inhaltsgleich vereinbaren. Insbesondere müssen die mit dem Unterauftragnehmer zu vereinbarenden TOM ein gleichwertiges Schutzniveau aufweisen.

7.4. Keine Unterbeauftragungen im Sinne dieser Regelung sind Leistungen, die der Anbieter als reine Nebenleistung zur Unterstützung seiner geschäftlichen Tätigkeit außerhalb der Auftragsverarbeitung in Anspruch nimmt. Der Anbieter ist jedoch verpflichtet, zur Gewährleistung des Schutzes der Daten auch für solche Nebenleistungen angemessene Vorkehrungen zu ergreifen.

## § 8 Rechte betroffener Personen und Unterstützung des Auftraggebers

Macht eine betroffene Personen Ansprüche gemäß Kapitel III der DSGVO bei einer der Parteien geltend, so informiert sie die jeweils andere Partei darüber unverzüglich. Der Anbieter unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Bearbeitung solcher Anträge sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.

## § 9 Kontroll- und Informationsrechte des Auftraggebers

9.1. Der Anbieter weist dem Auftraggeber die Einhaltung seiner Pflichten mit geeigneten Mitteln nach. Der Auftraggeber überprüft die Geeignetheit.

9.2. Für die Einhaltung der vereinbarten Schutzmaßnahmen und deren geprüfter Wirksamkeit kann der Anbieter auf angemessene Zertifizierungen oder andere geeignete Prüfungsnachweise verweisen. Angemessen sind insbesondere Zertifizierungen nach Art. 40 DSGVO oder Nachweise nach Art. 42 DSGVO. Daneben kommen unter anderem in Betracht: eine Zertifizierung nach ISO 27001 oder ISO 27017, eine ISO 27001-Zertifizierung auf Basis von IT-Grundschutz, eine Zertifizierung nach anerkannten und geeigneten Branchenstandards oder ein Prüfungsnachweis gemäß SOC / PS 951. Die Zertifizierungs- und Prüfungsverfahren sind von einem anerkannten unabhängigen Dritten durchzuführen. Der Anbieter hat seine Zertifikate oder Prüfungsnachweise zur Verfügung zu stellen. Weitere geeignete Mittel (z.B. Tätigkeitsberichte des Datenschutzbeauftragten oder Auszüge aus Berichten der Wirtschaftsprüfer) können zum Nachweis der Einhaltung der vereinbarten Schutzmaßnahmen dem Auftraggeber zur Verfügung gestellt werden. Das Inspektionsrecht des Auftraggebers aus § 9.3 bleibt hiervon unberührt.

9.3. Der Auftraggeber ist berechtigt, zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs, regelmäßig nach vorheriger Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit, Inspektionen beim Anbieter zur Prüfung der Einhaltung der datenschutzrechtlichen Bestimmungen durchzuführen. Der Anbieter darf die Inspektion von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der von ihm getroffenen TOM abhängig machen.

9.4. Zur Behebung der bei einer Inspektion getroffenen Feststellungen stimmen die Parteien die umzusetzenden Maßnahmen ab.

9.5. Macht eine Aufsichtsbehörde von Befugnissen nach Art. 58 DSGVO Gebrauch, so informieren sich die Parteien hierüber unverzüglich. Sie unterstützen sich in ihrem jeweiligen Verantwortungsbereich bei Erfüllung der gegenüber der jeweiligen Aufsichtsbehörde bestehenden Verpflichtungen.



zwei R software GmbH
Klosengartenstr. 31
50374 Erftstadt
Tel. : 02235 . 98 623
Fax : 02235 . 98 62 98
Mail : info@2rsoftware.de
Web : www.2rsoftware.de
Geschäftsführer:
Robert Schmitz
Robert Pyrzewski
AG : Köln
HRB : 50691
Bankverbindung: Sparkasse KölnBonn
IBAN : DE11 3705 0198 1024 7026 88
BIC : COLSDE33

## § 10 Verarbeitung von Sozialdaten im Auftrag

Werden unter dem AVV Sozialdaten i.S.d. § 67 Abs. 2 SGB X (neu) im Auftrag verarbeitet, gilt dieser AVV mit folgenden vorrangigen Regelungen, wobei Daten neben personenbezogenen Daten i.S.v. Art. 4 Nr. 1 DSGVO auch Sozialdaten i.S.d. § 67 Abs. 2 SGB X (neu) umfassen:

10.1. Bei der Übermittlung von Sozialdaten an einen Empfänger in einem Drittland oder in einer internationalen Organisation sind neben § 6 ergänzend § 77 SGB X (neu) und § 80 Abs. 2 SGB X (neu) zu beachten.

10.2. Die Anzeigepflicht nach § 80 Abs. 1 S. 1 SGB X (neu) vor Erteilung des Auftrags ist durch den Auftraggeber erfüllt worden. Handelt es sich beim Anbieter um eine öffentliche Stelle, hat dieser die Anzeigepflicht nach § 80 Abs. 1 S. 1 SGB X (neu) vor Erteilung des Auftrags erfüllt.

10.3. Handelt es sich beim Anbieter um eine nicht-öffentliche Stelle, stellt der Auftraggeber sicher, dass die besonderen Voraussetzungen für die Erteilung des Auftrags gemäß § 80 Abs. 3 SGB X (neu) gegeben sind, sofern sich die Verarbeitung im Auftrag nicht auf die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen bezieht, bei denen ein Zugriff auf Sozialdaten nicht ausgeschlossen werden kann.

10.4. Liegen zu erwartende oder bereits eingetretene Störungen im Betriebsablauf bei Verarbeitungen im Auftrag vor, die sich auf die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen beziehen, bei denen ein Zugriff auf Sozialdaten nicht ausgeschlossen werden kann, wird der Auftraggeber diese unverzüglich gemäß § 80 Abs. 5 S. 2 SGB X (neu) der Rechts- oder Fachaufsichtsbehörde mitteilen.

## § 11 Bankgeheimnis

Der Anbieter hat bei der Verarbeitung im Auftrag das Bankgeheimnis zu wahren, soweit der Auftraggeber dem Bankgeheimnis unterworfen ist. Hierauf wird der Auftraggeber den Anbieter hinweisen, sofern dies für den Anbieter aus dem Hauptvertrag oder der Stellung des Auftraggebers nicht ersichtlich ist. Das Bankgeheimnis erstreckt sich auf alle personenbezogenen Daten und anderen Informationen, die dem Auftraggeber über seine Kunden, Interessenten oder über Dritte aus der Geschäftsbeziehung zu diesen bekannt werden. Unter das Bankgeheimnis fällt auch die Angabe, ob der Auftraggeber überhaupt eine Geschäftsbeziehung zu einem Kunden unterhält.

## § 12 Haftung und Schadenersatz

12.1. Macht eine betroffene Person gegenüber einer Partei Schadenersatzansprüche wegen eines Verstoßes gegen datenschutzrechtliche Bestimmungen geltend, so hat die beanspruchte Partei die andere Partei hierüber unverzüglich zu informieren.

12.2. Auftraggeber und Anbieter haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

12.3. Die Parteien unterstützen sich wechselseitig bei der Abwehr von Schadenersatzansprüchen betroffener Personen, es sei denn, dies würde die Rechtsposition der einen Partei im Verhältnis zur anderen Partei, zur Aufsichtsbehörde oder gegenüber Dritten gefährden.

## § 13 Kosten

Die durch Maßnahmen des Auftraggebers beim Anbieter anfallenden Kosten sind vom Auftraggeber zu tragen, soweit diese nicht mit der Vergütung nach dem Hauptvertrag abgegolten sind. Dies gilt insbesondere für durch Kontrollen und Inspektionen des Auftraggebers nach § 9 dem Anbieter anfallende Kosten.

## § 14 Laufzeit

14.1. Der AVV wird auf unbestimmte Zeit geschlossen. Die Laufzeit einer Anlage wird in der jeweiligen Anlage geregelt; ohne eine solche Regelung läuft die Anlage auf unbestimmte Zeit.

14.2. Der AVV kann mit einer Frist von drei Monaten zum Quartalsende gekündigt werden, wenn gleichzeitig oder zuvor alle Anlagen beendet wurden.



zwei R software GmbH
Klosengartenstr. 31
50374 Erftstadt
Tel. : 02235 . 98 623
Fax : 02235 . 98 62 98
Mail : info@2rsoftware.de
Web : www.2rsoftware.de
Geschäftsführer:
Robert Schmitz
Robert Pyrzewski
AG : Köln
HRB : 50691
Bankverbindung: Sparkasse KölnBonn
IBAN : DE11 3705 0198 1024 7026 88
BIC : COLSDE33

14.3. Eine Anlage endet mit Beendigung des zugehörigen Hauptvertrags, ohne dass es einer gesonderten Kündigung dieser Anlage bedarf. Der Anbieter hat in diesem Fall nach Wahl des Auftraggebers unverzüglich die nach der Anlage verarbeiteten Daten herauszugeben oder datenschutzkonform zu löschen und dies dem Auftraggeber in Textform zu bestätigen. Sofern der Anbieter eine eigene gesetzliche Pflicht zur Speicherung dieser Daten hat, hat er dies dem Auftraggeber in Textform anzuzeigen.

## § 15 Fortgeltung und Überleitung von Altverträgen

Der AVV ersetzt mit Wirkung ab seiner Unterzeichnung die bestehenden Verträge nach § 11 BDSG. Haben die Parteien vor Abschluss dieses AVV Festlegungen nach § 1 vereinbart, so gelten diese sinngemäß unter dem AVV fort, es sei denn sie werden durch Anlagen ersetzt, denen derselbe Verarbeitungsgegenstand zu Grunde liegt.

## § 16 Schlussbestimmungen

16.1. Sollten die Daten des Auftraggebers beim Anbieter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Anbieter den Auftraggeber unverzüglich darüber in Textform zu informieren. Der Anbieter wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Verantwortung für die Daten ausschließlich beim Auftraggeber liegt.

16.2. Mündliche Nebenabreden wurden nicht getroffen. Änderungen und Ergänzungen des AVV bedürfen zu ihrer Wirksamkeit der Textform und der ausdrücklichen Bezugnahme auf die AVV. Abweichende mündliche Abreden der Parteien sind unwirksam. Dies gilt auch für Änderungen dieser Klausel.

16.3. Sollte nur eine Bestimmung dieses AVV ganz oder teilweise rechtsunwirksam oder nichtig sein oder werden, bleibt dieser AVV im Übrigen unberührt. An Stelle der rechtsunwirksamen oder nichtigen Bestimmung gilt das Gesetz, sofern die hierdurch entstandene Lücke nicht durch ergänzende Vertragsauslegung gemäß §§ 133, 157 BGB geschlossen werden kann. Beide Parteien sind jedoch verpflichtet, unverzüglich Verhandlungen aufzunehmen mit dem Ziel einer Vereinbarung an Stelle der rechtsunwirksamen oder nichtigen Bestimmung, die deren Sinn und Zweck in rechtlicher und wirtschaftlicher Hinsicht am Nächsten kommt, insbesondere dem Charakter der Vereinbarung als Dauerschuldverhältnis zur Regelung datenschutzrechtlicher Belange gerecht wird.

16.4. Es gilt deutsches Recht unter Ausschluss des Kollisionsrechts; Art. 3 Abs. 3, Abs. 4 ROM-I-VO bleiben unberührt.



zwei R software GmbH
Klosengartenstr. 31
50374 Erftstadt
Tel. : 02235 . 98 623
Fax : 02235 . 98 62 98
Mail : info@2rsoftware.de
Web : www.2rsoftware.de
Geschäftsführer:
Robert Schmitz
Robert Pyrzewski
AG : Köln
HRB : 50691
Bankverbindung: Sparkasse KölnBonn
IBAN : DE11 3705 0198 1024 7026 88
BIC : COLSDE33

# Anlage: Festlegungen zur Auftragsverarbeitung (Cloud)

Die Parteien treffen zum Vertrag über die Auftragsverarbeitung ergänzend folgende Festlegungen:

## § 1 Gegenstand der Verarbeitung

Gegenstand der Verarbeitung ist die Bereitstellung der im Hauptvertrag „Allgemeine Nutzungsbedingungen“ (nachfolgend „**Hauptvertrag**“) bezeichneten Cloud Services einschließlich der zugehörigen Wartungs-, Pflege- und Supportleistungen durch den Anbieter für den Auftraggeber. Soweit im Hauptvertrag vereinbart gehört hierzu auch die vorherige Migration von Daten aus einem beim Auftraggeber vorhandenen System in die vom Anbieter bereitgestellten Cloud Services.

## § 2 Dauer des Auftrags

Die Dauer der Verarbeitung ergibt sich aus dem Hauptvertrag.

## § 3 Zweck der Verarbeitung

Die Verarbeitung erfolgt fortlaufend über die Laufzeit des Hauptvertrags.

Ausschließlich zur Erfüllung der Pflichten des Anbieters aus dem Hauptvertrag im Zusammenhang mit der Bereitstellung der Cloud Services und ggf. der Migration vorhandener Daten werden personenbezogene Daten aus dem Herrschaftsbereich des Auftraggebers durch den Auftragnehmer vollumfänglich i.S.d. Art. 4 Nr. 2 DSGVO verarbeitet, insbesondere erhoben, gespeichert, verändert, ausgelesen, abgefragt, verwendet, offengelegt, abgeglichen, verknüpft und gelöscht.

## § 4 Kategorien von Daten (Zutreffendes bitte ankreuzen)

Die von der Verarbeitung betroffenen Kategorien von Daten hängen von der Nutzung der Cloud Services durch den Auftraggeber ab. Als Gegenstand der Verarbeitung in Betracht kommende Kategorien von Daten sind:

| | | |
|---|---|---|
| ☒ Stammdaten (Adressen) | ☐ Gesundheitsdaten | ☐ Personal- und Identifikationsnummern |
| ☐ Alter | ☐ Kreditkartendaten | ☐ Reisebuchungs- und Reiseabrechnungsdaten |
| ☐ Arbeitszeitdaten | ☐ Kundenverhaltensdaten | ☐ Telekommunikations-abrechnungsdaten |
| ☐ Audiodaten | ☐ Lohn- und Gehaltsdaten | ☐ Telekommunikations-verbindungsdaten |
| ☐ Bankverbindung inkl. Zahlungsverkehr | ☐ Mitarbeiter-bewertungen | ☒ Telefonnummern |
| ☐ Bewerberdaten | ☐ Beschäftigte (Qualifikationen) | ☐ Vertragsdaten |
| ☐ Bilddaten | ☒ Namen | ☐ Videodaten |
| ☐ Hobbys | ☒ Nutzerkennungen | ☒ Zahlungsdaten |
| ☒ E-Mails | ☒ Passwörter | ☐ Zugangsdaten |
| ☐ sonstige: | | |

Ob die Cloud Services des Anbieters für die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO geeignet ist, bedarf einer Risikobewertung durch den Auftraggeber.



zwei R software GmbH
Klosengartenstr. 31
50374 Erftstadt
Tel. : 02235 . 98 623
Fax : 02235 . 98 62 98
Mail : info@2rsoftware.de
Web : www.2rsoftware.de
Geschäftsführer:
Robert Schmitz
Robert Pyrzewski
AG : Köln
HRB : 50691
Bankverbindung: Sparkasse KölnBonn
IBAN : DE11 3705 0198 1024 7026 88
BIC : COLSDE33

## § 5 Kategorien betroffener Personen (Zutreffendes bitte ankreuzen)

Die von der Verarbeitung betroffenen Kategorien betroffener Personen hängen von der Nutzung der Cloud Services durch den Auftraggeber ab. Als Kategorien betroffener Personen kommen dabei in Betracht:

☒ Beschäftigte

☒ Auszubildende und Praktikanten

☐ Bewerber

☒ ehemalige Arbeitnehmer

☐ freie Mitarbeiter

☐ Gesellschafter, Organe der Gesellschaft

☐ Angehörige von Beschäftigten

☒ Kunden

☒ Interessenten

☒ Lieferanten und Dienstleister

☐ Mieter

☒ Geschäftspartner

☐ externe Berater

☐ Besucher

☐ Pressevertreter

☐ andere Kategorien:

## § 6 Unterauftragnehmer (Zutreffendes bitte ankreuzen)

☐ Der Anbieter setzt für die Verarbeitung keine Unterauftragnehmer ein.

☒ Der Anbieter setzt für die Verarbeitung folgende Unterauftragnehmer ein:

1&1 IONOS Cloud GmbH, Greifswalder Str. 207, 10405 Berlin

## § 7 Offenlegung von Daten an Empfänger in Drittländern oder internationalen Organisationen (Zutreffendes bitte ankreuzen)

☒ Eine Offenlegung von Daten an Empfänger in Drittländern erfolgt nicht.

☐ Der Anbieter legt Daten gemäß Ziff. 4 gegenüber folgenden Kategorien von Empfängern in Drittländern offen und hat dafür die folgenden Bedingungen i.S.d. Art. 44 ff. DSGVO getroffen:



zwei R software GmbH
Klosengartenstr. 31
50374 Erftstadt
Tel. : 02235 . 98 623
Fax : 02235 . 98 62 98
Mail : info@2rsoftware.de
Web : www.2rsoftware.de
Geschäftsführer:
Robert Schmitz
Robert Pyrzewski
AG : Köln
HRB : 50691
Bankverbindung: Sparkasse KölnBonn
IBAN : DE11 3705 0198 1024 7026 88
BIC : COLSDE33

# Anlage: Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

## § 1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

### 1.1. Zutrittskontrolle

Folgende Maßnahmen verhindern, dass unbefugte Personen Zutritt zu Datenverarbeitungsanlagen haben:

☐ Zutrittskontrollsystem, Ausweisleser (Magnet-/Chipkarte)

☐ Türsicherungen (elektrische Türöffner, Zahlenschloss, etc.)

☐ Sicherheitstüren / -fenster

☐ Gitter vor Fenstern/Türen

☐ Zaunanlagen

☒ Schlüsselverwaltung/Dokumentation der Schlüsselvergabe

☐ Werkschutz, Pförtner

☐ Alarmanlage

☐ Videoüberwachung

☐ Spezielle Schutzvorkehrungen des Serverraums

☐ Spezielle Schutzvorkehrungen für die Aufbewahrung von Backups und anderen Datenträgern

☐ Nicht-reversible Vernichtung von Datenträgern

☐ Mitarbeiter- und Berechtigungsausweise

☐ Sperrbereiche

☒ Besucherregelung (z.B. Abholung am Empfang, Dokumentation von Besuchszeiten, Besucherausweis, Begleitung nach dem Besuch bis zum Ausgang)

☐ Andere Maßnahmen:

### 1.2. Zugangskontrolle

Folgende Maßnahmen verhindern, dass unbefugte Dritte Zugang zu Datenverarbeitungsanlagen haben:

☒ Persönlicher und individueller Login bei Anmeldung am System/Netzwerk

☐ Autorisierungsprozess für Zugangsberechtigungen

☒ Begrenzung der befugten Benutzer

☐ Single Sign-On

☐ BIOS-Passwörter

☒ Elektronische Dokumentation von Passwörtern und Schutz dieser Dokumentation vor unbefugtem Zugriff

☐ Personalisierte Chipkarten, Token, PIN-/TAN, etc.

☐ Protokollierung des Zugangs

☐ Zusätzlicher Login für bestimmte Anwendungen

☐ Automatische Sperrung der Clients nach Zeitablauf ohne Useraktivität



zwei R software GmbH
Klosengartenstr. 31
50374 Erftstadt
Tel. : 02235 . 98 623
Fax : 02235 . 98 62 98
Mail : info@2rsoftware.de
Web : www.2rsoftware.de
Geschäftsführer:
Robert Schmitz
Robert Pyrzewski
AG : Köln
HRB : 50691
Bankverbindung: Sparkasse KölnBonn
IBAN : DE11 3705 0198 1024 7026 88
BIC : COLSDE33

☒ Firewall

### 1.3. Zugriffskontrolle

Folgende Maßnahmen stellen sicher, dass unbefugte Dritte keinen Zugriff auf Daten haben:

☒ Verwaltung und Dokumentation von differenzierten Berechtigungen

☒ Abschluss von Verträgen zur Auftragsverarbeitung für die externe Pflege, Wartung und Reparatur von Datenverarbeitungsanlagen, sofern bei der Fernwartung die Verarbeitung von Daten Gegenstand der Leistung des Auftragnehmers ist.

☐ Auswertungen/Protokollierungen von Datenverarbeitungen

☐ Autorisierungsprozess für Berechtigungen

☐ Genehmigungsroutinen

☐ Profile/Rollen

☐ Verschlüsselung von Datenträgern

☐ Maßnahmen zur Verhinderung unbefugten Überspielens von Daten auf mobile Datenträger (z.B. Kopierschutz, Sperrung von USB-Ports, Data Loss Prevention System/DLP)

☐ Mobile Device Management (MDM)

☐ Vier-Augen-Prinzip

☐ Funktionstrennung (Segregation of Duties)

☐ Fachkundige Akten- und Datenträgervernichtung gemäß DIN 66399

☐ Nicht-reversible Löschung von Datenträgern

☐ Sichtschutzfolien für mobile Datenverarbeitungsanlagen

### 1.4. Trennungskontrolle

Folgende stellen sicher, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

☐ Speicherung der Datensätze in physikalisch getrennten Datenbanken

☐ Verarbeitung auf mindestens logisch getrennten Systemen

☒ Zugriffsberechtigungen nach funktioneller Zuständigkeit

☐ Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen

☒ Mandantenfähigkeit von IT-Systemen

☐ Verwendung von Testdaten

☒ Trennung von Entwicklungs- und Produktionsumgebung

## § 2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

### 2.1. Weitergabekontrolle

Es ist sichergestellt, dass Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert, entfernt oder sonst verarbeitet werden können und überprüft werden kann, welche Personen oder Stellen Zugriff auf Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:

☐ Verschlüsselung von E-Mail oder E-Mail-Anhängen

☐ Verschlüsselung von Datenträgern


zwei R software GmbH
Klosengartenstr. 31
50374 Erftstadt
Tel. : 02235 . 98 623
Fax : 02235 . 98 62 98
Mail : info@2rsoftware.de
Web : www.2rsoftware.de
Geschäftsführer:
Robert Schmitz
Robert Pyrzewski
AG : Köln
HRB : 50691
Bankverbindung: Sparkasse KölnBonn
IBAN : DE11 3705 0198 1024 7026 88
BIC : COLSDE33

☒ Gesicherter File Transfer oder sonstiger Datentransport

☐ Physikalische Transportsicherung

☐ Verpackungs- und Versandvorschriften

☐ Qualifizierte elektronische Signatur

☒ Verschlüsseltes WLAN

☐ Fernwartungskonzept (z.B. Verschlüsselung, Ereignisauslösung durch Auftraggeber, Challenge-Response, Rückrufautomatik, Einmal-Passwort)

☐ Mobile Device Management (MDM)

☐ Data Loss Prevention System (DLP)

☐ Regelung zum Umgang mit mobilen Datenträgern (z.B. Laptop, USB-Stick, Mobiltelefon)

☐ Protokollierung von Datenübertragung oder Datentransport

☐ Protokollierung von lesenden Zugriffen

☐ Protokollierung des Kopierens, Veränderns oder Entfernens von Daten

### 2.2. Eingabekontrolle

Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat:

☒ Zugriffsrechte

☐ Systemseitige Protokollierungen

☐ Dokumenten Management System (DMS) / Enterprise Content Management System (ECMS) mit Änderungshistorie

☐ Sicherheits-/Protokollierungssoftware

☒ Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten

☐ Vieraugenprinzip

☐ Data Loss Prevention System (DLP)

## § 3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Durch folgende Maßnahmen ist sichergestellt, dass Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Auftraggeber stets verfügbar sind:

☒ Sicherheitskonzept für Software- und IT-Anwendungen

☒ Backup Verfahren

☒ Aufbewahrungsprozess für Backups (z.B. brandgeschützter Safe, getrennter Brandabschnitt)

☐ Gewährleistung der Datenspeicherung im gesicherten Netzwerk

☒ Bedarfsgerechtes Einspielen von Sicherheits-Updates

☒ Spiegeln von Festplatten

☒ Unterbrechungsfreie Stromversorgung (USV)

☐ Geeignete Archivierungsräumlichkeiten für Papierdokumente

☐ Brand- und/oder Löschwasserschutz des Serverraums

☐ Brand- und/oder Löschwasserschutz der Archivierungsräumlichkeiten

☐ Klimatisierter Serverraum



zwei R software GmbH
Klosengartenstr. 31
50374 Erftstadt
Tel. : 02235 . 98 623
Fax : 02235 . 98 62 98
Mail : info@2rsoftware.de
Web : www.2rsoftware.de
Geschäftsführer:
Robert Schmitz
Robert Pyrzewski
AG : Köln
HRB : 50691
Bankverbindung: Sparkasse KölnBonn
IBAN : DE11 3705 0198 1024 7026 88
BIC : COLSDE33

☒ Virenschutz

☒ Firewall

☐ Notfallplan

☐ Erfolgreiche Notfallübungen

☐ Redundante, örtlich getrennte Datenaufbewahrung (Offsite Storage)

## § 4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

### 4.1. Datenschutz-Management

Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

☒ Datenschutzleitbild des Anbieters

☒ Datenschutz-Richtlinie des Anbieters

☐ Richtlinien/Anweisungen zur Gewährleistung von technisch-organisatorischen Maßnahmen zur Datensicherheit (z.B.: UHB der Sparkasse)

☒ Benennung eines Datenschutzbeauftragten

☒ Verpflichtung der Mitarbeiter auf die Vertraulichkeit

☒ Hinreichende Schulungen der Mitarbeiter im Datenschutz

☒ Führen eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DSGVO)

☐ Durchführung von Datenschutzfolgenabschätzungen, soweit erforderlich (Art. 35 DSGVO)

☐ Externe Prüfung oder Auditierung

### 4.2. Management bei Datenschutzverletzungen

Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden:

☐ Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)

☐ Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber betroffenen Personen (Art. 34 DSGVO)

### 4.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Datenschutzfreundliche Voreinstellungen sind sowohl bei den standardisierten Voreinstellungen von Systemen und Apps als auch bei der Einrichtung der Verarbeitungen zu berücksichtigen. In dieser Phase werden Funktionen und Rechte konkret konfiguriert, wird im Hinblick auf Datenminimierung die Zulässigkeit bzw. Unzulässigkeit bestimmter Eingaben oder Eingabemöglichkeiten festgelegt und über die Verfügbarkeit von Nutzungsfunktionen entschieden. Ebenso werden die Art und der Umfang des Personenbezugs bzw. der Anonymisierung (z. B. bei Selektions-, Export- und Auswertungsfunktionen, die festgelegt und voreingestellt oder frei gestaltbar zur Verfügung gestellt werden) oder die Verfügbarkeit bestimmter Verarbeitungen, Funktionen oder Protokollierungen.

### 4.4. Auftragskontrolle

Durch folgende Maßnahmen ist sichergestellt, dass Daten nur nach Weisungen des Auftraggebers verarbeitet werden:



zwei R software GmbH
Klosengartenstr. 31
50374 Erftstadt
Tel. : 02235 . 98 623
Fax : 02235 . 98 62 98
Mail : info@2rsoftware.de
Web : www.2rsoftware.de
Geschäftsführer:
Robert Schmitz
Robert Pyrzewski
AG : Köln
HRB : 50691
Bankverbindung: Sparkasse KölnBonn
IBAN : DE11 3705 0198 1024 7026 88
BIC : COLSDE33

☒ Vereinbarung zur Auftragsverarbeitung mit Regelungen zu den Rechten und Pflichten der Parteien

☐ Prozess zur Erteilung und/oder Befolgung von Weisungen

☒ Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern

☐ Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung

☒ Schulungen/Einweisung aller zugriffsberechtigten Mitarbeiter beim Anbieter

☐ Unabhängige Auditierung der Weisungsgebundenheit

☒ Verpflichtung der Beschäftigten auf die Vertraulichkeit

☐ Vereinbarung von Vertragsstrafen für Verstöße gegen Weisungen

☐ formalisiertes Auftragsmanagement

☐ dokumentiertes Verfahren zur Auswahl von Unterauftragnehmern

☐ standardisiertes Vertragsmanagement zur Kontrolle von Unterauftragnehmern



zwei R software GmbH
Klosengartenstr. 31
50374 Erftstadt

Tel. : 02235 . 98 623
Fax : 02235 . 98 62 98

Mail : info@2rsoftware.de
Web : www.2rsoftware.de

Geschäftsführer:
Robert Schmitz
Robert Pyrzewski

AG : Köln
HRB : 50691

Bankverbindung: Sparkasse KölnBonn
IBAN : DE11 3705 0198 1024 7026 88
BIC : COLSDE33