E-Mail: info@dataroomX.de **Web:** www.dataroomX.de
Telefon: +49 651 / 84 03 1-0 **Telefax:** +49 651 / 84 03 1-122

Hausanschrift: rdts AG, Am Wissenschaftspark 7, 54296 Trier

dataroom
individuell . sicher . günstig

Vertrag über die Auftragsdatenverarbeitung (ADV)

zwischen

- Auftragnehmer -

rdts AG / datroomX®
vertreten durch den Vorstand Thomas Stiren
Am Wissenschaftspark 7
54296 Trier

und

- Auftraggeber -

_____
_____
_____
_____
_____

über Auftragsdatenverarbeitung i. S. d. §11 Abs. 2 Bundesdatenschutzgesetz (BDSG)

E-Mail: info@dataroomX.de **Web:** www.dataroomX.de
Telefon: +49 651 / 84 03 1-0 **Telefax:** +49 651 / 84 03 1-122

Hausanschrift: rdts AG, Am Wissenschaftspark 7, 54296 Trier

dataroom
individuell . sicher . günstig

Regelung zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Auftrag gemäß § 11 Bundesdatenschutzgesetz

§ 1 Regelungsgegenstand

Im Rahmen der Leistungserbringung zur Bereitstellung von Datenräumen ist es erforderlich, dass die rdts mit personenbezogenen Daten umgeht, für die der Auftraggeber als verantwortliche Stelle im Sinne der datenschutzrechtlichen Vorschriften fungiert (nachfolgend „Auftraggeber-Daten“ genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang der rdts mit „Auftraggeber-Daten“ zur Durchführung des „Vertrags“.

§ 2 Art, Umfang, Zweck und Laufzeit der Auftragsdatenverarbeitung

1) Die rdts erhebt, verarbeitet und nutzt die „Auftraggeber-Daten“ im Auftrag und nach Weisung des Auftraggebers i.S.v. § 11 BDSG (Auftragsdatenverarbeitung). Der Auftraggeber bleibt im datenschutzrechtlichen Sinn verantwortliche Stelle.

2) Die Erhebung, Verarbeitung und Nutzung der „Auftraggeber-Daten“ im Rahmen der Auftragsdatenverarbeitung erfolgt entsprechend der Beauftragung des dataroomX-Datenraumes.

3) Die rdts darf die „Auftraggeber-Daten“ im Rahmen des datenschutzrechtlich Zulässigen für eigene Zwecke auf eigene Verantwortung verarbeiten und nutzen. Die rdts darf zudem die „Auftraggeber-Daten“ anonymisieren und in anonymisierter Form für eigene Zwecke verarbeiten und nutzen.

4) Die Erhebung, Verarbeitung und Nutzung der „Auftraggeber-Daten“ findet im Gebiet der Bundesrepublik Deutschland.

5) Die Laufzeit und Kündigung dieses Vertrags richtet sich nach den Bestimmungen zur Laufzeit und Kündigung des „Vertrags“. Eine Kündigung des „Vertrags“ bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

§ 3 Weisungsbefugnisse des Auftraggebers

1) Die rdts verwendet die „Auftraggeber-Daten“ ausschließlich in Übereinstimmung mit den

E-Mail: info@dataroomX.de **Web:** www.dataroomX.de
Telefon: +49 651 / 84 03 1-0 **Telefax:** +49 651 / 84 03 1-122

Hausanschrift: rdts AG, Am Wissenschaftspark 7, 54296 Trier

Weisungen des Auftraggebers. Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung der rdts und erfolgen durch die Übernahme etwa dadurch bedingter Mehrkosten der rdts durch den Auftraggebe.

2) Ist die rdts der Ansicht, dass eine zulässige Einzelweisung gegen geltendes Datenschutzrecht verstößt, wird er den Auftraggeber möglichst zeitnah darauf hinweisen. Außerdem ist die rdts berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen.

§ 4 Pflichten des Auftraggebers

1) Der Auftraggeber ist für die Rechtmäßigkeit der Erhebung, Verarbeitung und Nutzung der „Auftraggeber-Daten“ sowie für die Wahrung der Rechte der Betroffenen verantwortlich. Sollten Dritte gegen die rdts aufgrund der Erhebung, Verarbeitung oder Nutzung von „Auftraggeber-Daten“ Ansprüche geltend machen, wird der Auftraggeber die rdts von allen solchen Ansprüchen auf erstes Anfordern freistellen.

2) Der Auftraggeber ist Eigentümer der „Auftraggeber-Daten“ und Inhaber aller etwaigen Rechte, die die „Auftraggeber-Daten“ betreffen.

3) Dem Auftraggeber obliegt es, der rdts die „Auftraggeber-Daten“ rechtzeitig zur Leistungserbringung zur Verfügung zu stellen, und er ist verantwortlich für die Qualität der „Auftraggeber-Daten“. Der Auftraggeber hat der rdts unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse der rdts Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

§ 5 Pflichten der rdts

1) Die rdts stellt sicher und kontrolliert regelmäßig, dass die Datenverarbeitung und -nutzung im Rahmen der Leistungserbringung in seinem Verantwortungsbereich, der Unterauftragnehmer einschließt, in Übereinstimmung mit den Bestimmungen dieses Vertrags erfolgt. Sie wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen des Bundesdatenschutzgesetzes (Anlage zu § 9 BDSG) genügen. Diese Maßnahmen werden im

E-Mail: info@dataroomX.de **Web:** www.dataroomX.de
Telefon: +49 651 / 84 03 1-0 **Telefax:** +49 651 / 84 03 1-122

Hausanschrift: rdts AG, Am Wissenschaftspark 7, 54296 Trier

Anhang 1 festgestellt.

2) Die rdts darf ohne vorherige Zustimmung durch den Auftraggeber im Rahmen der Auftragsdatenverarbeitung keine Kopien oder Duplikate der „Auftraggeber-Daten“ anfertigen. Hiervon ausgenommen sind jedoch Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung und zur ordnungsgemäßen Erbringung der Leistungen (einschließlich der Datensicherung) erforderlich sind, sowie Kopien, die zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind. Diese Kopien erfolgen in einem räumlich getrennten Backup-Rechenzentrum für die ersten sieben Tage rückwirkend täglich, für die weiteren drei Wochen mindestens eines pro Woche.

3) Die rdts unterstützt den Auftraggeber bei Kontrollen durch die Aufsichtsbehörde im Rahmen des Zumutbaren und Erforderlichen, soweit diese Kontrollen die Datenverarbeitung durch die rdts betreffen.

4) Die rdts hat dem Auftraggeber auf Anforderung eine Übersicht über die in § 4e Satz 1 BDSG genannten Angaben sowie über die zugriffsberechtigten Personen zur Verfügung zu stellen (§ 4g Abs. 2 Satz 1 BDSG)

5) Die rdts hat die bei der Verarbeitung von „Auftraggeber-Daten“ beschäftigten Personen gemäß § 5 BDSG schriftlich auf das Datengeheimnis zu verpflichten.

6) Die rdts ist verpflichtet, einen fachkundigen und zuverlässigen betrieblichen Datenschutzbeauftragten nach § 4f BDSG zu bestellen, sofern und solange die gesetzlichen Voraussetzungen für eine Bestellpflicht gegeben sind.

§ 6 Mitzuteilende Verstöße der rdts

1) Die rdts informiert den Auftraggeber zeitnah, wenn er feststellt, dass er oder ein Mitarbeiter bei der Verarbeitung von „Auftraggeber-Daten“ gegen datenschutzrechtliche Vorschriften oder gegen Festlegungen aus diesem Vertrag verstoßen haben, sofern deshalb die Gefahr besteht, dass „Auftraggeber-Daten“ unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind.

2) Soweit den Auftraggeber aufgrund eines Vorkommnisses nach § 7 Abs. 1 gesetzliche Informationspflichten wegen einer unrechtmäßigen

E-Mail: info@dataroomX.de **Web:** www.dataroomX.de
Telefon: +49 651 / 84 03 1-0 **Telefax:** +49 651 / 84 03 1-122

Hausanschrift: rdts AG, Am Wissenschaftspark 7, 54296 Trier

Kenntniserlangung von „Auftraggeber-Daten“ (insbesondere nach § 42a BDSG) treffen, hat die rdts den Auftraggeber bei der Erfüllung der Informationspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der rdts hierdurch entstehenden, nachzuweisenden Aufwände und Kosten zu unterstützen.

§ 7 Rückgabe und Löschung überlassener Daten und Datenträger

1) Die rdts hat sämtliche „Auftraggeber-Daten“ nach Beendigung der vertragsgegenständlichen Leistungserbringung (insbesondere bei Kündigung oder sonstiger Beendigung des „Vertrags“) zu löschen und von dem Auftraggeber erhaltene Datenträger, die zu diesem Zeitpunkt noch „Auftraggeber-Daten“ enthalten, an den Auftraggeber zurückzugeben.

2) Über eine Löschung bzw. Vernichtung von „Auftraggeber-Daten“ hat die rdts ein Protokoll zu erstellen, das dem Auftraggeber auf Anforderung vorzulegen ist.

3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung oder gesetzlichen Aufbewahrungsfristen dienen, sind durch die rdts entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

§ 8 Verhältnis zu sonstigen Vereinbarungen

Soweit in diesen Bedingungen keine Sonderregelungen enthalten sind, gelten die Bestimmungen zur Auftragsdatenverarbeitung. Im Fall von Widersprüchen aus sonstigen Vereinbarungen, gehen die Regelungen aus dieser Auftragsdatenverarbeitung vor.

E-Mail: info@dataroomX.de **Web:** www.dataroomX.de
Telefon: +49 651 / 84 03 1-0 **Telefax:** +49 651 / 84 03 1-122

Hausanschrift: rdts AG, Am Wissenschaftspark 7, 54296 Trier

dataroom
individuell . sicher . günstig

Anlage 1 und 2

Anlage 1 – Technische und organisatorische Maßnahmen (TOM) gemäß § 9 BDSG

Die detaillierte Dokumentation wird dem Auftraggeber im Falle der Einreichung von erweiterten Fragenkatalogen zur Verfügung gestellt.

1. Zutrittskontrolle

– Verwaltung, Entwicklung und Kunden-Support sind vom Rechenzentrum getrennt.
– Schutzmaßnahmen des Gebäudes durch Einbruchsmeldeanlagen, Sicherheitstüren- und -fenster
– Schutzmaßnahmen des Rechenzentrums
– Besucherkontrolle
– Verpflichtung der Gebäudereinigung gemäß § 5 BDSG

2. Zugangskontrolle

– Benutzeridentifikation
– Verbindliche Passwortparameter
– Bildschirmsperre
– Keine Verarbeitung von Kundendaten auf mobilen Datenträgern
– Fernzugriffe nur für den Bereitschaftsdienst
– Getrenntes WPA2 verschlüsseltes WLAN
– Firewall-Monitoringsysteme

3. Zugriffskontrolle

– Verwaltung der Rechte durch Systemadministrator
– Anzahl der Administratoren auf das „Notwendigste“ reduziert
– Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
– Sichere Aufbewahrung von Datenträgern
– Protokollierung der Vernichtung
– Verschlüsselung von Datenträgern

4. Weitergabekontrolle

– Verwendung und Übertragung personenbezogener Daten ausschließlich elektronisch durch SSL-Verschlüsselung
– Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)

E-Mail: info@dataroomX.de **Web:** www.dataroomX.de
Telefon: +49 651 / 84 03 1-0 **Telefax:** +49 651 / 84 03 1-122

Hausanschrift: rdts AG, Am Wissenschaftspark 7, 54296 Trier

dataroom
individuell . sicher . günstig

5. Eingabekontrolle
– Der Auftraggeber trägt die Verantwortung für die Geheimhaltung der zugewiesenen Passwörter auf die ihm zur Verfügung gestellten Umgebungen.

6. Auftragskontrolle
– Verpflichtung aller Mitarbeiter auf das Datengeheimnis
– Datenschutzmanagement nach Art. 30 DSGVO durch eigenes Datenschutz-Team
– Vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen

7. Verfügbarkeitskontrolle
– Verfügbarkeitskontrollmaßnahmen für Rechenzentrum
– Einsatz unterbrechungsfreie Stromversorgung (USV).
– Notfallkonzepte (bspw. Notfallmaßnahmen bei Hardwaredefekte / Brand / Stromausfall, etc.).
– Kundenserver mit Hardware-RAID-Systemen (i.d.R. SSD-Festplatten)
– Sicherung Kundendaten auf externe Backupsysteme

8. Trennungsgebot
– Trennungskontrolle durch die Kapselung der einzelnen Kundenbereiche
– Festlegung von Datenbankrechten
– Trennung von Produktiv- und Testsystem

E-Mail: info@dataroomX.de **Web:** www.dataroomX.de
Telefon: +49 651 / 84 03 1-0 **Telefax:** +49 651 / 84 03 1-122

Hausanschrift: rdts AG, Am Wissenschaftspark 7, 54296 Trier

dataroom
individuell . sicher . günstig

Anlage 2 – Planung der Verarbeitungstätigkeiten nach Art. 30 DSGVO (Datenschutzmanagement)

1. Regelmäßige Audits eines Datenschutzmanagement-Teams
– Qualitätssicherung und Prozessdokumentation
– Projekt- und Aufgabenmanagement
– Schulungen & Sensibilisierung

2. Notfallplan/-umsetzung
– Umfang der Datenpanne
– Betroffene Daten
– Betroffene Kunden
– Informations-/Meldepflicht an zuständige Landesdatenschutzbeauftragten
– Sicherheitslücken schließen
– Schäden beheben

3. Nachhaltigkeitssicherung
– Schulungen & Gesetzesrecherche
– Umsetzung neuer Vorgaben
– Audit-Wiederholung 1 x jährlich

Ort, Datum

…….

- Auftraggeber -

…….

Vorname Name
Funktion

Trier, 30.01.2018

- Auftragnehmer –

Thomas Stiren
Vorstand