Vereinbarung

über eine

gemeinsame Verarbeitung von Personenbezogenen Daten nach Art 26

Im folgenden Verantwortlicher 1

*** Firmennamen ***
*** Straße + Hausnummer ***
*** PLZ + Ort ***

Im folgenden Verantwortlicher 2

*** Firmennamen ***
*** Straße + Hausnummer ***
*** PLZ + Ort ***

1 Inhalt

2 Management Summary

- Dieses Dokument regelt die Rechte und Pflichten der beiden Verantwortlichen (in Folge auch „Parteien“ genannt) in Bezug auf die gemeinsame Verarbeitung personenbezogener Daten.
- Diese Vereinbarung findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter der Parteien oder durch sie beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.
- In dieser Vereinbarung verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

3 Dauer der Vereinbarung

Die Verarbeitung beginnt am [DATUM] und endet am [DATUM].

ODER

Die Verarbeitung beginnt am [DATUM] und erfolgt auf unbestimmte Zeit bis zur Kündigung dieses Vertrags oder des Hauptvertrags durch eine Partei.

ODER

Die Verarbeitung beginnt am [DATUM] und endet nach einmaliger Ausführung.

4 Gegenstand der Vereinbarung

4.1 Verpflichtung zur Information der Betroffenen gemäß Art 13 und 14 DSGVO

Verantwortlicher 1 verpflichtet sich, den Betroffenen, die gem. gemäß Art 13 und 14 DSGVO verpflichtenden Informationen zukommen zu lassen.

oder

Verantwortlicher 2 verpflichtet sich, den Betroffenen, die gem. gemäß Art 13 und 14 DSGVO verpflichtenden Informationen zukommen zu lassen.

4.2 Verpflichtung zur Wahrung der Betroffenenrechte

Beide Parteien ergreifen die technischen und organisatorischen Maßnahmen, damit die Rechte der betroffenen Personen nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllt werden können.

4.3 Verpflichtung zur Information der Betroffenen gemäß Art 26 Abs 2 DSGVO

Verantwortlicher 1 verpflichtet sich, den Betroffenen die gem. gemäß Art 26 Abs 2 DSGVO verpflichtenden Informationen zukommen zu lassen.

oder

Verantwortlicher 2 verpflichtet sich, den Betroffenen die gem. gemäß Art 26 Abs 2 DSGVO verpflichtenden Informationen zukommen zu lassen.

4.4 Vertraulichkeit

Beide Parteien erklären rechtsverbindlich, dass alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet wurden, oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

4.5 Verarbeitung nach Art 32 DSGVO

Beide Parteien erklären rechtsverbindlich, dass alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen wurden.

4.6 Verpflichtung nach Art 32 bis 36 DSGVO

Beide Parteien verpflichten sich zur Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).

4.7 Technisch-organisatorische Maßnahmen

Vertraulichkeit

- **Zutrittskontrolle:** Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, z.B.: Schlüssel, Magnet- oder Chipkarten, elektrische Türöffner, Portier, Sicherheitspersonal, Alarmanlagen, Videoanlagen.
- **Zugangskontrolle**: Schutz vor unbefugter Systembenutzung, z.B.: Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern.
- **Zugriffskontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Standard-Berechtigungsprofile auf „need to know-Basis“, Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insb von administrativen Benutzerkonten.
- **Pseudonymisierung**: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.
- **Klassifikationsschema für Daten:** Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

Integrität

- **Weitergabekontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur.
- **Eingabekontrolle**: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement.

Verfügbarkeit und Belastbarkeit

- **Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline. on-site/off-site), unterbrechungsfreie Stromversorgung (USV, Dieselaggregat), Virenschutz, Firewall, Meldewege und Notfallpläne. Security Checks auf Infrastruktur- und Applikationsebene, Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern.
- Rasche **Wiederherstellbarkeit**.
- **Löschungsfristen**: Sowohl für Daten selbst als auch Metadaten wie Logfiles, udgl.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen.
- Incident-Response-Management.
- Datenschutzfreundliche Voreinstellungen.
- **Auftragskontrolle:** Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes

Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters (ISO-Zertifizierung, ISMS), Vorabüberzeugungspflicht, Nachkontrollen.

4.8 Subunternehmer

{Verbot der Hinzuziehung eines Sub-Auftragsverarbeiters} Verantwortlicher 1/ Verantwortlicher 2 / Beide Parteien ist/sind nicht berechtigt, Sub-Unternehmer heranzuziehen.

{Zulässigkeit der Hinzuziehung von Sub-Auftragsverarbeitern} Verantwortlicher 1/ Verantwortlicher 2 / Beide Parteien ist/sind kann Sub-Unternehmer [*Tätigkeiten*] hinzuziehen.

4.9 Regelungen zur Berichtigung, Löschung und Sperrung von Daten

Im Rahmen dieser Vereinbarung verarbeitete Daten werden nur entsprechend der getroffenen vertraglichen Vereinbarung berichtigt, gelöscht oder gesperrt.

4.10 Vertragsstrafe

- Bei Verstoß gegen die Abmachungen dieses Vertrages wird eine verschuldensunabhängige Vertragsstrafe von € 50.000,- je Einzelfall vereinbart. Die Vertragsstrafe wird insbesondere bei Mängeln in der Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen verwirkt. Bei dauerhaften Verstößen gilt jeder Kalendermonat, in dem der Verstoß ganz oder teilweise vorliegt, als Einzelfall. Die Einrede des Fortsetzungszusammenhangs ist ausgeschlossen.

- Die Vertragsstrafe hat keinen Einfluss auf andere Ansprüche der Parteien.

4.11 Sonderkündigungsrecht

- Beide Parteien können den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß der anderen Partei gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt. Ein schwerwiegender Verstoß liegt insbesondere vor, wenn eine Partei die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.

- Bei unerheblichen Verstößen durch eine Partei setzt die andere Partei eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist sie zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

- Bei außerordentlicher Kündigung hat die daran schuldige Partei der anderen alle Kosten zu erstatten, die durch die verfrühte Beendigung des Hauptvertrages oder dieses Vertrages entstehen.

4.12 Sonstiges

- Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.
- Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

5 Unterschriften inkl. Funktion

Ort, Datum	Ort, Datum
Verantwortlicher	Verantwortlicher