Informationsblatt zur Erhebung von personenbezogenen Daten (Art. 12 und 13 DSGVO)

Verfahren: KommSafe

Verarbeitungstätigkeit: KommSafe ist eine Cloudspeicherlösung zum sicheren Austausch und zur Ablage von Dateien über das Internet.

1. Name und Kontaktdaten des Verantwortlichen

<Bitte nutzen Sie den RTF Download und tragen dort Ihre Daten ein, bevor Sie dieses Informationsblatt weitergeben>

2. Kontaktdaten des Datenschutzbeauftragten

<Bitte nutzen Sie den RTF Download und tragen dort Ihre Daten ein, bevor Sie dieses Informationsblatt weitergeben>

3. Zweck und Rechtsgrundlagen der Datenverarbeitung

Ihre Daten werden zu folgendem Zweck erhoben:
KommSafe ist eine Cloudspeicherlösung zum sicheren Austausch und zur Ablage von Dateien über das Internet.

Funktionen:
- Bereitstellung einer Plattform zum Austausch und zur Ablage von Dateien über das Internet
- Up- /Download, Verschieben und Löschen von Dateien, Datenverwaltung sowie Zugriff per App und Outlook
- Abbildung der Organisationsstruktur des Kunden über Data Rooms
- Eigene Rechteverwaltung für Benutzer und Data Rooms
- Ablaufdatum für Dateien, Benutzeraccounts und Up- / Download-Links zur einfachen Vermeidung von redundanten Daten
- Kommentarfunktion für Dateien
- Sortierung nach Benutzer, Datum, Typ, Größe, Name etc.
- Dateiaustausch mit Dritten über temporäre Up- / Downloadlinks (optional passwortgeschützt, zeitlich limitiert)
- Dateien werden nicht erst auf dem Server, sondern schon vor der Übertragung verschlüsselt
- Datenübertragung erfolgt verschlüsselt mit HTTPS
- Mehrstufiges Berechtigungssystem für den Austausch von Dateien
- Protokollierung von erfolgreichen und fehlgeschlagenen Zugriffsversuchen, Up- und Downloads sowie deren Dateinamen

Die Rechtsgrundlage, auf der Ihre Daten erhoben werden, ist:
Art. 6 Abs. 1 lit. a und f DSGVO, Art. 4 BayDSG in Verbindung mit Kundenverträgen
EU-U.S. Data Privacy Framework

4. Empfänger oder Kategorien von Empfängern der personenbezogenen Daten

Ihre personenbezogenen Daten werden weitergegeben an: Datenübermittlung erfolgt im Rahmen der Zweckerfüllung (Dateiaustausch) zwischen Sender und Empfänger der zu übertragenden Dateien

1. Kommunikationspartner (Einladungs- bzw. Bestätigungsmails zum Up- bzw. Download)
2. Kommunikationspartner (Up- bzw. Download der zu übermittelnden Dateien)

Die Kommunikation mit Partnern aus einem Drittland ist grundsätzlich nicht vorgesehen. Die Verantwortung für die Einhaltung obliegt aber den Kommunikationspartnern selbst.

5. Übermittlung von personenbezogenen Daten an ein Drittland

Ihre personenbezogenen Daten werden weitergegeben an:
Durch die Einbindung des weiteren Auftragsverarbeiters AWS (Anbieter mit Hauptsitz in den USA) ist aus Datenschutzsicht ein Drittlandsbezug gegeben. Dieser ist datenschutzrechtlich vertretbar aufgrund Vorliegen der Bestimmungen des Kapitels V der DSGVO.

Gemäß dem EU-U.S. Data Privacy Framework ist AWS für den Bereich der Non-HR Data zertifiziert (zum Zeitpunkt der Erstellung dieses Dokuments bis 01.07.2025). Zudem werden die durch die Anwender für das Hosting bereitgestellten Daten vor dem Upload durch ein asymmetrischen Verfahren clientseitig verschlüsselt, so dass weder Dracoon noch AWS Zugriff auf die verarbeiteten Klartextdaten besitzen.

Gemäß vorliegendem Supplementary Addendum wird AWS den Kunden (Verantwortlichen i. S. v. Art. 4 Ziffer 7 DSGVO) im Falle von behördlichen Anfragen bezüglich einer Offenlegung der verarbeiteten Daten unverzüglich informieren und bei Vorliegen eines Verbots der Offenlegung dieser Daten nach europäischem Gesetz gegen diese Anfragen Rechtsmittel einlegen. Zudem könnten den anfragenden Behörden ohnehin nur verschlüsselte Daten übermittelt werden, da den eingebundenen Auftragnehmern ein Zugriff auf die zur Entschlüsselung notwendigen Schlüssel nicht eingeräumt wird. Somit wird die Verarbeitung aus datenschutzrechtlicher Sicht vertretbar angesehen, gemessen an dem mit dieser Verarbeitung verbundenem Risiko für die Personen, deren Daten verarbeitet werden.

Die Aspekte der Datensicherheit und Verfügbarkeit sind durch die Erfüllung der Anforderungen des BSI C5-Katalogs und entsprechender ISO-Normen sowie der KRITIS-Kompatibilität gem. § 8a Abs. 3 BSIG seitens Dracoon und des BSI-C5-Testats sowie der Zertifizierungen gem. ISO 27001, SOC 1, SOC 2 und SOC 3 seitens AWS gut abgedeckt. Der Aspekt der Georedundanz wird durch drei Availability-Zonen und 3 Edge-Standorte in der AWS-Region Frankfurt abgedeckt und umfasst sowohl die verarbeiteten Daten als auch Backups.

6. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien

Ihre Daten werden in dem Verfahren mit folgenden Fristen gelöscht:
1. Protokolldaten werden nach 10 Tagen gelöscht

2. Nach Beendigung des Vertragsverhältnisses werden die Daten gelöscht (eventuell noch benötigte Dateien muss der Kunde vor Vertragsende selbst herunterladen)
3. Die Löschung von Benutzer-Daten nach Wegfall des Speichergrunds obliegt dem Administrator des Kunden
4. Die Löschung der Dateien liegt in der Verantwortung der Kommunikationspartner (Ablauf-Datum für Dateien festlegen oder manuelles Löschen der Dateien nach Wegfall des Speichergrunds)

7. Betroffenenrechte

Nach der Datenschutz-Grundverordnung stehen Ihnen die Rechte aus Art. 15-18,20,21 zu:

- Recht auf Auskunft über die zu Ihrer Person gespeicherten Daten, Recht auf Berichtigung, Löschung, Einschränkung der Verarbeitung oder Widerspruch gegen die Verarbeitung, wenn die gesetzlichen Voraussetzungen dafür vorliegen,
- Beschwerderecht beim Bayerischen Landesbeauftragten für den Datenschutz, Wagmüller-Straße 18, 80538 München,
- Recht auf Datenübertragbarkeit, wenn die gesetzlichen Voraussetzungen dafür vorliegen.

8. Widerrufsrecht bei Einwilligung

Wenn Sie in die Datenerhebung durch den Verantwortlichen (siehe 1. Name und Kontaktdaten des Verantwortlichen) durch eine entsprechende Erklärung eingewilligt haben, können Sie die Einwilligung jederzeit für die Zukunft widerrufen.

9. Pflicht zur Bereitstellung der Daten

Wenn Sie die erforderlichen Daten nicht bereitstellen, hat dies folgende Konsequenzen:
Daten müssen auf anderen Wegen (z.B. per USB-Stick) ausgetauscht werden mit den sich daraus ergebenden erheblichen Sicherheitsrisiken.