Technische und Organisatorische Maßnahmen

i.S.d. Art. 32 DSGVO

der Organisation

Feuer Software GmbH

Stand: Juli 2022

Folgende Dienstleistungen werden mit diesem Subunternehmer zusammen erbracht:

Anbieter	**Produkte**
Microsoft Azure Global DE	Gesamte Feuersoftware Connect Plattform inklusive → EinsatzAPP → EinsatzMonitor → EinsatzTablet → EinsatzManager → Cobra4Agent
Netcup GmbH	OpenStreetMap Kartenmaterial OpenStreetMap Geocoding OpenStreetMap Routenberechnung Email Server (Systempostfächer Connect) Nextcloud
Amazon AWS	Amazon Simple Email Service zum Versand von Connect Mails

Informationen der Subunternehmer

Anbieter	***Weitere Informationen***
Microsoft Azure Global DE	Compliance / Zertifizierungen https://docs.microsoft.com/de-de/azure/compliance/ Product Offerings https://www.microsoft.com/licensing/terms/productoffering Datenschutz DPA https://www.microsoft.com/en-us/licensing/product-licensing/products#OST
Netcup GmbH	https://www.netcup-wiki.de/wiki/Zusatzvereinbarung_zur_Auftragsverarbeitung
Amazon AWS	https://aws.amazon.com/de/compliance/gdpr-center/

Maßnahmenforderung	***Umsetzung in der Praxis***
<u>Vertraulichkeit (gem. Art. 32 Abs. 1 lit. DSGVO)</u>	
Zutrittskontrolle	Eigene: • Alle Zugriffsberechtigten Geräte werden stets verschlossen und sicher aufbewahrt. Microsoft Azure Global DE Cloud: • Microsoft beschränkte Zugang zu Einrichtungen, in denen ihr Informationssysteme, die Kundendaten verarbeiten, sich befinden, auf benannte autorisierte Personen. • Microsoft führt Unterlagen über die eingehenden und ausgehenden Medien, die Kundendaten enthalten, einschließlich Art des Mediums, autorisierter Absender Empfänger, Datum und Uhrzeit, Anzahl der Medien und Arten von Kundendaten, die Sie enthalten. • Microsoft verwendet unterschiedliche Systeme nach Branchen Standard, um den Verlust von Daten aufgrund von Stromversorgungsausfällen oder Leitungsstörungen zu verhindern. • Microsoft verwendet Verfahren nach Branchen Standard, um Kundendaten zu löschen wenn sie nicht mehr benötigt werden. Netcup GmbH • Zugänge zu den Büroräumen grundsätzlich verschlossen • Zentrales Schließsystem mit Sicherheitsschlössern • Öffnen der Zugangstüren nur mit Schlüssel • Besucherregelung: Abholung von Besuchern (nach Klingeln) am Eingang zum Bürotrakt • Dokumentierte Verfahrensweise für Ausgabe und Rückgabe der Zugangsmittel • Dokumentierte Verfahrensweise für die Meldung des Verlusts eines Zugangsmittels • Alarmanlage (manuelle Scharfschaltung) • Videoüberwachung der Büro Eingangsbereiche im 1. und 2. OG • Videoüberwachung der angemieteten Bereiche in den Rechenzentren • Spezielle Räume abschließbar. • Regelung über Arbeitsanweisung • Alle Räume befinden sich im 1. und 2. OG
Zugangskontrolle	• Es bestehen ausschließlich personenbezogene Benutzerprofile. • Es besteht eine branchenübliche Passwortrichtlinie. Netcup GmbH • Nur benutzte Netzwerkdosen gepatched • Keine W-LANs im Einsatz • Firewall, Intrusion Detection System • Zugang zu DV-Geräten mit persönlicher Benutzer-ID und Kennwort

Maßnahmenforderung	***Umsetzung in der Praxis***
	• Dokumentierte Vergabe-Richtlinie für Benutzer-IDs und Kennworte • Zusätzliche Share-Berechtigungen • Zusätzliches Login für spezielle Applikationen • Kennwort: > 8 Zeichen, bestehend aus Sonderzeichen, Groß- und Kleinbuchstaben sowie Zahlen (3 aus 4) • Bei Bedarf zeitgesteuerte Kennwort-Erneuerung • Protokollierung der Logins und Kennwortfehleingaben • Home Partition der Arbeitsplatzrechner verschlüsselt • Verbindung zur Applikation im Rechenzentrum nur über VPN • Whitelist für zugelassene IP-Adressen • Für Kundensysteme bei Bedarf Zwei-Faktor-Authentifizierung
Zugriffskontrolle	• Es besteht eine personenbezogene Berechtigungstruktur gemäß der “Need-to-Know"-Prinzipien • Alle Endgeräte sind verschlüsselt. • Passwörter werden so gespeichert, dass sie während ihres Geltungszeitraums nicht lesbar sind. • Administrative Zugänge besitzten MFA. Netcup GmbH • Benutzerrollen-/Gruppenkonzept • Erteilung und Verwaltung von Benutzerechten voneinander getrennt • Überprüfung/Aktualisierung der Berechtigungen • Zentrales Virenschutzprogramm mit automatischer Aktualisierung • Zeitgesteuerte Bildschirmsperre mit Wiederanmeldung • Bildschirme so aufgestellt, dass ein unbefugtes Lesen verhindert wird • Papier-Shredder für Dokumentenvernichtung • Keine externen EDV-Dienstleister
<u>Integrität (Art. 32 Abs. 1 lit. b DSGVO)</u>	
Verschlüsselung	- Alle Anwendung bedürfen mindestens einer Verschlüsselung mittels TLS 1.2 - Datenbanken sind grundsätzlich verschlüsselt - Passwortspeicher nach dem aktuellen Stand der Technik verschlüsselt und gesichert. - Bereitstellung der Dienste nur über verschlüsselte Verbindungen (https etc.)
Signaturverfahren	- Veröffentlichte Anwendungen sind grundsätzlich signiert
Protokollierung	- Zugriffe werden entsprechend der gesetzlichen Vorgaben protokolliert -
Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)	

Maßnahmenforderung	***Umsetzung in der Praxis***
Verfügbarkeitskontrolle / Belastbarkeitskontrolle	• Alle System unterliegen regelmäßigen System- und Datensicherungen • Virenscanner und Firewalls im Einsatz • Technische Verfahren zur Lastverteilung werden angewendet. • Monitoring unter status.feuersoftware.com öffentlich einsehbar. • Alle Server stehen in Rechenzentren in Deutschland • Rechenzentren sind DIN ISO 27001-zertifiziert • Schutzmaßnahmen: o Geeignete Zutrittskotrollsysteme o Videoüberwachung Redundante o unterbrechungsfreie Stromversorgung o Überspannungsschutz Schutz gegen Feuer und Wassereintritt o Monitoring der Leitungskapazitäten o Intrusion Detection System (DoS/DDoS-Angriffe) • Redundante IT-Infrastruktur (z.B. durch Virtualisierung) • RAID-Festplattenspeicher • Ersatz- und Austauschkomponenten vor Ort vorhanden • Datensicherungskonzept vorhanden • Prüfung der Rücksicherung/Wiederherstellung • Einheitliche Beschaffungsstrategie für Soft- und Hardware • Virenscanner und Firewalls im Einsatz (zentrale Aktualisierung)
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung **(Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)**	
	- Alle Verfahren werden in regelmäßigen Abständen (mindestens 1 Mal im Jahr) durch interne Prozesse überprüft.