Anlage 1

Technische und organisatorische Maßnahmen i.S.d. Art. 32 DSGVO

bAV Solutions GmbH | Winefeldstraße 14 | 77955 Ettenheim

Pseudonymisierung/Anonymisierung personenbezogener Daten

☐ Ersetzen personenbezogener Daten durch Zufallscodes

☒ Data Masking der Authentifizierungsdaten

☒ Personenbezogene Identifikationsmerkmale werden endgültig gelöscht

☐ Sonstige verwendete Methoden zur Pseudonymisierung:

☒ Sonstige verwendete Methoden zur Anonymisierung: Zuordnung einer anonymen bAV-ID

Zutrittskontrolle

☒ Abschließbarkeit der Räumlichkeiten

☒ Videoüberwachung

☒ Alarmanlage

☐ Pförtner/Wachschutz

☒ Schlüsselregelung

☒ Chipkarten/Transpondersysteme

☐ Besucherbuch/Protokoll der Besucher

☒ Abschließbarkeit des Serverraums

☒ Zutrittsbefugnis zum Serverraum

☐ Fenstersicherung im Serverraum

☐ Klimaanlage im Serverraum

☒ Brandschutz im Serverraum

Datenträgerkontrolle

☒ Aktenvernichter (mindestens Stufe 3)

☐ Abgeschlossene Lagerung von Datenträgern

☐ Verzeichnis für Datenträger

☐ Regelung zur Entsorgung von Datenträgern

☐ Zertifizierter Dienstleister zur Entsorgung von Datenträgern

☐ Überwachung von Fremdpersonal bei Kontakt mit personenbezogenen Daten

☒ Sonstige verwendete Methoden der Datenträgerkontrolle: Alle Daten werden cloudbasiert verarbeitet

Speicherkontrolle

☒ Clean Desk Policy

☒ Trennung des WLAN in privat und öffentlich

☒ Es wird ein Passwort zur Authentifizierung genutzt

☒ Passwort-Mindestlänge von 12 Zeichen

☒ Passwortkomplexität (Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen)

☒ Passwort-Wechselintervalle

☒ Richtlinie für den Umgang mit Passwörtern

☐ Gruppenweiter Auto-Logout

☐ Sperrung des Zugriffs nach mehreren Falschanmeldungen

☒ Zwei-Faktor-Authentifizierung

☒ Protokolle über Eingabe, Änderung und Löschung von Daten

☒ Auswertung von Protokollen hinsichtlich unberechtigter Zugriffe

☒ Verwendung von digitalen Signaturen

Zugriffskontrolle

☒ Ein Berechtigungskonzept ist vorhanden, um Benutzerrechte zu verwalten

☒ Unterschiedliche Zugriffsberechtigungen bzgl. Lesen, Schreiben und Löschen von Daten

☒ Betriebliche Anweisung zum Umgang mit mobilen Datenträgern

☒ Anzahl der Administratoren auf das "Notwendigste" reduziert

☒ Externe Wartung und Fernwartung - Regelungen und Kontrollen

☒ Sonstige verwendete Methoden der Zugriffskontrolle: Firewall schützt vor unberechtigten Zugriffen, extern und intern

Benutzerkontrolle

☒ Mitarbeiter-Schulungen zum Thema Datenschutz

☐ Sperren von Anschlüssen und Laufwerken

☒ Verschlüsselung von Datenträger

Transportkontrolle

☒ VPN-Tunnel

☒ Firewall

Eingabekontrolle

☒ Protokollierung bei fehlerhaften Zugriffsversuchen

☒ Protokollierung von Aktivitäten auf dem Server

Wiederherstellbarkeit

☒ Regelmäßige Backups

☐ Ein Disaster-Recovery-Plan ist definiert

☐ Test und Anpassung des Disaster-Recovery-Plans

Zuverlässigkeit

☐ RAID-System

☐ Test des Backupverfahrens

☐ Belastbarkeitstests

☒ Netzwerküberwachung/Intrusion Detection System

☒ Change-Management

☒ Sonstige verwendete Methoden zur Gewährleistung der Zuverlässigkeit: Regelmäßige Testläufe mit Serveranbieter

Weitergabekontrolle

☐ Transport von Datenträgern in sicheren Transportboxen mit Empfangsbestätigung

☒ Weitergabe von Informationen an Dritte nur nach schriftlicher Weisung

☒ Verschlüsselung der Datenübertragung

☒ Sonstige verwendete Methoden der Weitergabekontrolle: Empfängerprüfung über Faktorauthenifizierungscode, Einsatz von Verschlüsselungstechnologien für Dokumente, VPN-Technologie (SSL/TLS) zur Datenkommunikation

Auftragskontrolle

☒ Verpflichtung auf das Datengeheimnis

☒ Informationen werden nur, mit schriftlicher Anweisung, an Dritte weitergegeben.

☒ Auswahl der Auftragnehmer unter Sorgfalt-Gesichtspunkten (Zertifizierung, Referenzen, usw.)

☒ Sonstige verwendete Methoden der Auftragskontrolle: Eindeutige Vertragsgestaltung. Kontrolle der Vertragsausführung. Klare Anweisungen an den Auftragnehmer hinsichtlich des Umfangs der Verarbeitung personenbezogener Daten. Soweit eine Datenverarbeitung im Auftrag durchgeführt wird, wird der Auftragnehmer vor Aufnahme der Datenverarbeitung nach den Vorschriften der DSGVO auf die Einhaltung der erforderlichen technischen und organisatorischen Maßnahmen überprüft. Über jeden Auftrag wird ein Vertrag nach den Vorschriften der Datenschutz-Grundverordnung abgeschlossen. Dies gilt auch für Verträge über Wartungsarbeiten an den Datenverarbeitungssystemen und Softwarepflege je nach Bedarf und sonstige IT Service-Unterstützung, wenn dabei ein Zugriff auf personenbezogenen Daten nicht ausgeschlossen werden kann. Bei der Überprüfung der Auftragnehmer und der Vergabe von Aufträgen im Rahmen einer Datenverarbeitung im Auftrag wird unser Datenschutzbeauftragte hinzugezogen.

Datenintegrität

☒ Regelmäßige Software-Aktualisierungen

☒ Virenschutz des Netzwerkes und der IT-Systeme

☒ Datenschutz-Managementsystem

Verfügbarkeitskontrolle

☒ Ausarbeitung eines Datensicherungskonzepts

☐ Getrennte Partitionen für Betriebssysteme und Daten

☐ Sichere Aufbewahrung der Backups an einem sicheren, ausgelagerten Ort

☐ Unterbrechungsfreie Stromversorgung

☐ Softwareüberwachung vom Server

☐ Verwendung von Schutzsteckdosen

☒ Redundante Auslegung sämtlicher wichtigen Systeme

Trennbarkeit

☒ Verschiedene Arbeitsplätze für verschiedene Daten

☐ Trennung der Datensätze durch Speicherung in physikalisch getrennte Datenbanken

☐ Mandantenfähigkeit relevanter Anwendungen

☒ Trennung in Test-, Produktions- und Entwicklungsebene

Anlage 2

Subdienstleister

Firma	Anschrift	Auftragsinhalt
Microsoft Corporation	One Microsoft Way. Redmond, WA 98052-6399, USA	E-Mail-Provider, Cloud-Dienstleister zur Verwaltung und Verarbeitung von Daten und Dokumenten.
Serverprofis GmbH	Mondstr. 2-4 85622 Feldkirchen	Webhosting
dWERK GmbH & Co. KG	Darmstädter Str. 170, 64625 Bensheim	Setup und Bereitstellung eines interaktiven Videoplayers für die Beratung der Mitarbeiter/innen des Auftraggebers
cPanel, L.L.C	2550 North Loop W., Suite 4006 Houston, TX 77092	Web-basiertes Konfigurationstool für Webhosting
Automattic Inc.	San Francisco, CA, USA	Content-Management-System

Anlage 3

Weisungsberechtigte Personen, Adresse zur Meldung von Datenschutzverletzungen

Folgende Personen sind zur Erteilung von Weisungen befugt:

Marc Robin Karkossa | marc.karkossa@bavsolutions.de

Ferdinand Weide | ferdinand.weide@bavsolutions.de

Luis Weber | luis.weber@bavsolutions.de

Kontakt zur Meldungen über die Verletzung personenbezogener Daten:

info@bavsolutions.de