

Technische und organisatorische Maßnahmen —

Stand 1. Oktober 2026

Gültig ab 1. Oktober 2026

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Anlage 4 zur Vereinbarung zur Auftragsverarbeitung (Ziffer 4.2)

Stand 1. Oktober 2026

Auftragsverarbeiter: Andreas Schäfer, handelnd unter der Geschäftsbezeichnung SW-Sales, Am Bergle 12A, 77793 Gutach (Schwarzwaldbahn), Kontakt: info@sw-sales.de

1 Geltungsbereich und Schutzbedarf

1.1 Diese Anlage beschreibt die Maßnahmen, die SW-Sales bei der Verarbeitung personenbezogener Daten im Auftrag seiner Geschäftskunden über das Kundenportal unter sw-sales.de tatsächlich umsetzt. Sie berücksichtigt den Stand der Technik, die Implementierungskosten sowie Art, Umfang, Umstände und Zwecke der Verarbeitung und das Risiko für die Rechte und Freiheiten der betroffenen Personen (Art. 32 Abs. 1 DSGVO).

1.2 Verarbeitet werden insbesondere Steuergerätedateien (ECU/TCU), Fahrzeug- und Softwaredaten, Diagnose- und CSV-Protokolle, Ticketinhalte und, soweit der Auftraggeber sie angibt, Fahrzeug-Identifizierungsnummern (FIN). Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO und Daten über strafrechtliche Verurteilungen nach Art. 10 DSGVO sind nicht vorgesehen.

1.3 Den höchsten Schutzbedarf haben die FIN wegen ihres möglichen Bezugs zum Fahrzeughalter, die hochgeladenen Dateien und die Zugangsdaten der Konten. Die Maßnahmen sind darauf ausgerichtet.

1.4 SW-Sales ist ein Ein-Personen-Betrieb ohne Beschäftigte. Der Inhaber ist alleiniger Administrator und Bearbeiter und trägt die Verantwortung für alle Maßnahmen dieser Anlage. Eine zweite befugte Person besteht nicht. Werden künftig Beschäftigte oder externe Dienstleister mit Zugriff auf Auftragsdaten eingesetzt, werden sie vorab schriftlich zur Vertraulichkeit verpflichtet und diese Anlage wird angepasst.

2 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Zutrittskontrolle

- Server und Sicherungen werden vom Hoster noxtec GmbH ausschließlich in Deutschland betrieben, im Rechenzentrum maincubes FRA-01 in Offenbach am Main (u. a. ISO 27001 zertifiziert) in einem verschlossenen Rack mit mehrstufiger Zutrittskontrolle des

Rechenzentrums.

- Der Arbeitsplatz des Betreibers befindet sich in dessen Geschäftsräumen und ist nur ihm zugänglich. Bildschirme werden bei Abwesenheit gesperrt, mobile Geräte werden verschlossen aufbewahrt.

2.2 Zugangskontrolle

- Jede Person erhält ein eigenes Benutzerkonto; gemeinsam genutzte Konten gibt es nicht. Kundenkonten werden erst nach Prüfung der Unternehmereigenschaft freigeschaltet.
- Passwörter werden nur als Hash gespeichert (Argon2id, soweit von der Serverumgebung bereitgestellt, sonst bcrypt), nie im Klartext und für niemanden einsehbar.
- Anmeldeschutz: Nach fünf Fehlversuchen je Konto oder zwanzig je IP-Adresse innerhalb von 15 Minuten wird die Anmeldung vorübergehend gesperrt. Dieselben Grenzen gelten für das Zurücksetzen von Passwörtern und das erneute Anfordern von Bestätigungsmails. Links zum Zurücksetzen sind eine Stunde gültig und nur einmal verwendbar.
- Administratorzugänge des Portals sind ohne Zwei-Faktor-Anmeldung technisch gesperrt.
- Mehr-Faktor-Anmeldung ist für alle Dienstleisterzugänge des Betreibers eingerichtet: Domain- und E-Mail-Verwaltung, E-Mail-Postfächer, Rechnungsprogramm, Zahlungsdienst, Quellcodeverwaltung und Passwortmanager. Der Dateizugang zum Webserver erfolgt ausschließlich verschlüsselt über FTPS mit einem langen, nur dort verwendeten Passwort; einen Zugang zur Serververwaltung hat der Betreiber nicht.
- Zugangsdaten werden ausschließlich in einem durch Mehr-Faktor-Anmeldung geschützten Passwortmanager verwahrt.

2.3 Zugriffskontrolle

- Rollen nach dem Prinzip der geringsten Berechtigung: Geschäftskunden sehen ausschließlich Aufträge, Dateien, Tickets und Belege ihres eigenen Unternehmens. Die Zugehörigkeit wird bei jedem Abruf serverseitig geprüft, auch bei Dateidownloads.
- Die Verwaltung des Portals ist an eine eigene Berechtigung gebunden, die ausschließlich der Betreiber besitzt.
- Dateien werden nur über einen berechtigungsgeprüften Download ausgeliefert, nie über öffentliche Verzeichnisse oder erratbare Adressen. Jeder Download wird protokolliert.
- Die Berechtigungen werden mindestens jährlich überprüft (Rezertifizierung); nicht mehr benötigte Zugänge werden sofort entzogen.

2.4 Trennungskontrolle

- Beim Hoster läuft das Portal in einem eigenen Hosting-Abonnement mit eigenem Systembenutzer, eigenem Verzeichnis und eigener Datenbank, logisch getrennt von anderen

Kunden des Hosters.

- Die Daten der Geschäftskunden sind über eindeutige Vorgangs- und Unternehmenskennungen voneinander getrennt; es gibt keine gemeinsamen Ablageverzeichnisse.
- Entwicklung und Test erfolgen in getrennten lokalen Umgebungen mit synthetischen Testdaten, ohne echte FIN oder Kundendaten. Echte Daten gelangen nur für einen Wiederherstellungstest vorübergehend in eine isolierte Testumgebung, die danach gelöscht wird.

2.5 Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

- Übertragungen zum und vom Portal erfolgen ausschließlich verschlüsselt über HTTPS (TLS).
- Besonders schutzbedürftige Felder – FIN, USt-IdNr. und Telefonnummer – werden in der Datenbank mit authentifizierter Verschlüsselung (libsodium) gespeichert. Der Schlüssel liegt getrennt vom Quellcode in der geschützten Serverkonfiguration. Die Felder sind deshalb auch in Sicherungen verschlüsselt.
- Die Angabe der FIN ist freiwillig und nur vorgesehen, wenn sie für die Bearbeitung erforderlich ist.
- Der Analysearbeitsplatz ist mit BitLocker vollständig verschlüsselt.
- Zugangsdaten und Schlüssel stehen nicht im Quellcode und nicht in Protokollen.

3 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Weitergabekontrolle

- Dateien werden nicht per E-Mail versendet. Benachrichtigungen enthalten nur Text und Links ins Portal; Dateien stehen ausschließlich im Portal zum geschützten Download bereit.
- Das Portal schützt Formulare gegen Cross-Site Request Forgery und setzt Sicherheitsheader (unter anderem Content-Security-Policy, X-Frame-Options, Referrer-Policy).
- Es werden keine Tracking-, Werbe- oder Analysedienste eingebunden. An Zahlungs- und Rechnungsdienste werden keine Steuergerätedateien, Protokolle oder FIN übermittelt.

3.2 Eingabekontrolle

- Ein manipulationsgeschütztes Auditprotokoll hält sicherheitsrelevante Vorgänge mit Zeitpunkt und handelnder Person fest, unter anderem Anmeldesperren, Passwortänderungen, Freischaltungen und Sperren von Konten, Auftragseingang und Bearbeitungsschritte, Guthabenbuchungen, Änderungen der Unterauftragsverarbeiter, Datenexporte und Löschläufe. Jeder Eintrag ist mit dem vorherigen über eine HMAC-SHA256-Prüfsumme verkettet; nachträgliche Änderungen werden bei der Kettenprüfung erkannt.

- Zustimmungen zu AGB und dieser Vereinbarung werden mit Fassung, Konto und Zeitpunkt gespeichert. Jede Dateiversion eines Auftrags wird mit Prüfsumme, Versionsnummer und Änderungsnotiz abgelegt.
- Auf das Auditprotokoll hat nur der Betreiber Zugriff.

3.3 Dateisicherheit

- Hochgeladene Dateien werden auf ihre Größe geprüft (Hauptdatei höchstens 12 MB, CSV-Protokolle und PDF-Analysen höchstens 5 MB), CSV-Protokolle zusätzlich auf ihr Format; Dateien mit ausführbarer Endung werden abgewiesen. Sie werden zunächst in einem Quarantänebereich außerhalb des öffentlich erreichbaren Webverzeichnisses gespeichert.
- Gespeichert wird jede Datei unter einem zufälligen Namen ohne Dateiendung; der Originalname steht nur in der Datenbank und wird nie als Speicherpfad verwendet. Hochgeladene Inhalte werden auf dem Server nie ausgeführt und nur als Download ausgeliefert.
- Die fachliche Analyse erfolgt ausschließlich an einem isolierten Arbeitsplatz ohne Portalzugangsdaten, mit Virenschutz (Microsoft Defender) und vollständiger Datenträgerverschlüsselung. Lokale Arbeitskopien werden nach Abschluss des Auftrags gelöscht.

4 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

- Der Hoster sichert den gesamten Webserver täglich automatisiert auf einen vom Produktivsystem getrennten Sicherungsserver in Deutschland und bewahrt die Sicherungen sieben Tage auf. Ein Datenverlust ist damit auf höchstens einen Tag begrenzt.
- Die Wiederherstellung aus einer Sicherung wird mindestens vierteljährlich in einer isolierten Testumgebung geprüft und mit Datum, Alter der Sicherung und Dauer bis zur Betriebsbereitschaft dokumentiert.
- Rechenzentrum mit redundanter Strom- und Klimaversorgung, unterbrechungsfreier Stromversorgung, Netzersatzanlage sowie Brandfrüherkennung; der Hoster überwacht den Server, hält Betriebssystem und Hosting-Plattform aktuell und strebt eine Verfügbarkeit von 99,9 % im Jahr an.
- Ein Mail- oder Übertragungsfehler macht einen gespeicherten Auftrag oder eine Buchung nie rückgängig; fehlgeschlagene Benachrichtigungen werden erneut versucht und im Verwaltungsbereich angezeigt.
- Sicherheitsupdates für WordPress, Plugins und das Portal spielt der Betreiber zeitnah ein; der Stand wird monatlich geprüft und dokumentiert.

5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

- Automatisierte Tests prüfen bei jeder Änderung des Portals unter anderem Berechtigungen, Upload-Grenzen, Anmeldeschutz, Verschlüsselung und die Auditkette.
- Monatlich: Prüfung und Dokumentation des Update-Stands.
- Vierteljährlich: Wiederherstellungstest.
- Jährlich: Überprüfung dieser Anlage, Rezertifizierung der Berechtigungen, Überprüfung der Mehr-Faktor-Anmeldungen und der Unterauftragsverarbeiter sowie eine externe Sicherheitsprüfung der öffentlich erreichbaren Anwendung.
- Wesentliche Änderungen der Maßnahmen werden dokumentiert. Nachteilige Änderungen teilt SW-Sales dem Auftraggeber mit (Ziffer 4.2 der Vereinbarung).

6 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO)

- Es werden nur die für den Auftrag erforderlichen Angaben abgefragt; freiwillige Angaben wie die FIN sind als solche gekennzeichnet.
- Das Portal setzt nur technisch notwendige Cookies.
- Nicht abgeschickte Auftragsentwürfe und deren Dateien werden spätestens 24 Stunden nach der letzten Bearbeitung gelöscht.

7 Löschung und Aufbewahrung

- Löschfristen werden automatisiert und protokolliert umgesetzt, unter anderem:
- Uploads abgelehnter Aufträge: 7 Tage nach der Ablehnung
- CSV-Protokolle: 90 Tage nach Abschluss der Logprüfung beziehungsweise nach Fertigstellung des Auftrags
- technische Auftragsdateien und Nachweise: 3 Jahre nach Ende des Jahres der Fertigstellung
- Protokolle fehlgeschlagener Anmeldungen: 14 Tage
- versendete Benachrichtigungen: 30 Tage
- Rechnungen und Buchungsunterlagen: nach den gesetzlichen Aufbewahrungsfristen; sie werden nie automatisch gelöscht
- Eine Löschsperre (Legal Hold) wird nur fallbezogen gesetzt und dokumentiert.
- Sicherungen werden im Sicherheitszyklus des Hosters nach sieben Tagen überschrieben. Nach Vertragsende löscht der Hoster alle Daten binnen 30 Tagen.
- Das Löschprotokoll enthält keine unnötigen Inhaltsdaten.

8 Auftragskontrolle und Unterauftragsverarbeiter

- Daten werden ausschließlich auf dokumentierte Weisung des Auftraggebers verarbeitet;

Weisungen werden über das Ticketsystem des Portals oder in Textform erteilt und dokumentiert.

- Unterauftragsverarbeiter werden nur mit einem Vertrag nach Art. 28 DSGVO eingesetzt, der sie auf gleichwertige Pflichten verpflichtet. Ihre Liste steht in Anlage 3 und im Kundenkonto. Neue oder geänderte Unterauftragsverarbeiter werden mindestens 14 Tage vorher angekündigt.
- Verträge, Maßnahmen und Datenorte der Unterauftragsverarbeiter werden jährlich überprüft.

9 Umgang mit Datenschutzvorfällen (Art. 33 und 34 DSGVO)

- Ein dokumentierter Ablauf regelt Erkennung, Eindämmung, Beweissicherung, Risikobewertung und Wiederherstellung.
- Verletzungen des Schutzes personenbezogener Daten, die Auftragsdaten betreffen, meldet SW-Sales dem Auftraggeber unverzüglich; internes Ziel sind 24 Stunden nach Bekanntwerden, damit der Auftraggeber die Frist von 72 Stunden nach Art. 33 DSGVO einhalten kann. Der Hoster ist vertraglich verpflichtet, Vorfälle spätestens 48 Stunden nach Kenntnis an SW-Sales zu melden.
- Mindestinhalt einer Meldung an den Auftraggeber:
 - Zeitpunkt der Feststellung und bekannte Dauer
 - betroffene Systeme, Kunden, Datenarten und ungefähre Zahl der Datensätze
 - wahrscheinliche Folgen für betroffene Personen
 - bereits ergriffene Eindämmungs- und Wiederherstellungsmaßnahmen
 - Kontakt für Rückfragen und Zeitpunkt der nächsten Aktualisierung
 - Kennzeichnung, welche Angaben bestätigt und welche noch vorläufig sind