

Rahmenvereinbarung zur Auftragsverarbeitung

gemäß Art. 28 Abs. 3 DSGVO · Version 1.0 · Stand 28.10.2026

Zwischen

smartline Digitalagentur, Inhaber Frank Kirsch, Friedrich-Ebert-Straße 4, 64732 Bad König,
kontakt@smartline.info – nachfolgend „Auftragsverarbeiter“ oder „smartline“ –

und

Firma / Rechtsform

Anschrift

Vertreten durch

E-Mail

Datenschutzkontakt (falls abweichend)

– nachfolgend „Verantwortlicher“ –

§ 1 Gegenstand und Anwendungsbereich

1. Diese Rahmenvereinbarung gilt für alle gegenwärtigen und zukünftigen Einzelverträge, Bestellungen und Leistungsabrufe der Parteien, soweit smartline dabei personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Erfasst sind insbesondere Website-Erstellung, Hosting, Wartung, CMS- und Shopbetrieb, Smart-CMS, Smartlinecard, Werbebildschirme, direktgefragt (Online-Sprechstunde) sowie individuelle Softwareleistungen. Eine Auftragsverarbeitung liegt nur vor, soweit der Verantwortliche Zwecke und wesentliche Mittel der Verarbeitung bestimmt. Eigenverantwortliche Verarbeitungen von smartline, insbesondere die eigene Vertragsverwaltung und Rechnungsstellung, sind nicht Gegenstand dieser Vereinbarung.
2. Gegenstand, Art, Zweck, Dauer, Datenarten und Kategorien betroffener Personen ergeben sich je tatsächlich beauftragter Leistung aus Anlage 1 und gegebenenfalls aus dem Produktblatt (Anlage 4). Neue Verarbeitungszwecke oder besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) bedürfen vor Aufnahme einer ergänzten Dokumentation und Prüfung.

§ 2 Laufzeit und Rangfolge

1. Diese Vereinbarung gilt ab Unterzeichnung bzw. dokumentierter elektronischer Annahme für die Dauer sämtlicher erfasster Auftragsverarbeitungen. Sie endet, sobald keine erfasste Verarbeitung mehr stattfindet und die Rückgabe- und Löschpflichten nach § 11 erfüllt sind. Das Ende eines Einzelauftrags lässt andere Aufträge unberührt.

2. Bei Widersprüchen gehen zwingende datenschutzrechtliche Bestimmungen und diese Vereinbarung hinsichtlich der Auftragsverarbeitung allgemeinen Leistungs- und Geschäftsbedingungen vor.

§ 3 Verantwortlichkeit und Weisungen

1. Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere für Rechtsgrundlagen, Informationspflichten, Zweckfestlegung, die Wahrung der Betroffenenrechte und die Rechtmäßigkeit seiner Weisungen.
2. smartline verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf Übermittlungen in Drittländer –, sofern smartline nicht durch Unionsrecht oder das Recht eines Mitgliedstaats zur Verarbeitung verpflichtet ist. In diesem Fall teilt smartline dem Verantwortlichen diese Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht verbietet.
3. Der Einzelauftrag und die dokumentierte Konfiguration der Leistung gelten als Erstweisung. Weitere Weisungen erteilt der Verantwortliche per E-Mail an kontakt@smartline.info oder in Textform. Mündliche Weisungen werden von smartline unverzüglich in Textform dokumentiert.
4. Hält smartline eine Weisung für rechtswidrig, informiert smartline den Verantwortlichen unverzüglich. smartline kann die Ausführung bis zur Klärung aussetzen, soweit dies rechtlich zulässig ist.

§ 4 Vertraulichkeit und Personal

smartline stellt sicher, dass alle Personen, die Zugang zu Auftragsdaten haben, vor Aufnahme der Tätigkeit schriftlich zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und Daten ausschließlich auf Weisung verarbeiten. Zugriffe werden auf die für die jeweilige Aufgabe erforderlichen Projekte begrenzt. Diese Pflichten bestehen auch nach Ende der Tätigkeit fort.

§ 5 Technische und organisatorische Maßnahmen

1. smartline trifft die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO zur Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme sowie zur raschen Wiederherstellung nach einem Zwischenfall, und überprüft deren Wirksamkeit regelmäßig.
2. Die Maßnahmen unterliegen dem technischen Fortschritt. smartline darf sie durch gleichwertige oder bessere Maßnahmen ersetzen. Änderungen, die das Schutzniveau mindern können, bedürfen der vorherigen Abstimmung mit dem Verantwortlichen.
3. Mobiles Arbeiten ist zulässig, soweit die in Anlage 2 dokumentierten Maßnahmen eingehalten werden. Daraus folgt kein Betretungsrecht privater Wohnräume. Gesetzlich erforderliche Prüfungen werden durch geeignete Nachweise ermöglicht.

§ 6 Unterauftragsverarbeiter

1. Der Verantwortliche erteilt eine allgemeine schriftliche Genehmigung für den Einsatz der in Anlage 3 aufgeführten Unterauftragsverarbeiter. smartline informiert den Verantwortlichen mindestens 30 Kalendertage vor einer beabsichtigten Hinzuziehung oder Ersetzung in Textform, soweit nicht ein dringender, sicherheitsbedingter Wechsel erforderlich ist. Der Verantwortliche kann aus datenschutzrechtlich begründeten Gründen vor Wirksamwerden widersprechen. Die Parteien suchen dann eine geeignete Alternative. Bis zur Klärung findet die betroffene neue Verarbeitung nicht statt.
2. smartline verpflichtet Unterauftragsverarbeiter vertraglich auf im Wesentlichen dieselben Datenschutzpflichten (Art. 28 Abs. 4 DSGVO) und haftet gegenüber dem Verantwortlichen für deren Einhaltung. Dienstleister ohne Zugriff auf Auftragsdaten sind keine Unterauftragsverarbeiter.

§ 7 Drittlandübermittlungen

Verarbeitungen und Zugriffe außerhalb der EU bzw. des EWR erfolgen nur, soweit sie in Anlage 3 ausgewiesen sind oder der Verantwortliche sie anweist, und nur bei Erfüllung der Voraussetzungen der Art. 44 ff. DSGVO (insbesondere Angemessenheitsbeschluss oder EU-Standardvertragsklauseln).

§ 8 Unterstützung des Verantwortlichen

smartline unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen bei der Erfüllung von Betroffenenrechten (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch) sowie bei den Pflichten nach Art. 32 bis 36 DSGVO. Bei smartline direkt eingehende Anfragen Betroffener werden unverzüglich an den Verantwortlichen weitergeleitet.

§ 9 Meldung von Datenschutzverletzungen

smartline meldet Verletzungen des Schutzes personenbezogener Daten dem Verantwortlichen unverzüglich nach Bekanntwerden, möglichst innerhalb von 24 Stunden, per E-Mail an die vom Verantwortlichen benannte Adresse sowie bei hoher Dringlichkeit zusätzlich telefonisch. Die Meldung enthält, soweit bekannt, Art der Verletzung, betroffene Datenkategorien und Personen, wahrscheinliche Folgen und ergriffene Gegenmaßnahmen. Fehlende Informationen werden nachgereicht. Kontakt bei smartline: frank.kirsch@smartline.info, 06063 5770 890.

§ 10 Nachweise und Kontrollen

smartline stellt dem Verantwortlichen alle zum Nachweis der Pflichten aus Art. 28 DSGVO erforderlichen Informationen zur Verfügung und ermöglicht Überprüfungen einschließlich Inspektionen durch den Verantwortlichen oder einen von ihm beauftragten, zur Verschwiegenheit verpflichteten Prüfer. Prüfungen erfolgen grundsätzlich nach angemessener Vorankündigung zu üblichen Geschäftszeiten und unter Wahrung der Vertraulichkeit anderer Kunden; bei konkretem Anlass auch kurzfristig. Vorrangig werden Dokumentenprüfungen und Nachweise genutzt, ohne gesetzliche Prüfrechte einzuschränken.

§ 11 Rückgabe und Löschung

1. Nach Ende der jeweiligen Leistung übergibt smartline nach Wahl des Verantwortlichen alle zugehörigen personenbezogenen Daten in einem gängigen Format (Datenbank-Export und Dateien) oder löscht sie, und löscht vorhandene Kopien, sofern keine gesetzliche Aufbewahrungspflicht besteht. smartline fragt die Wahl vor Beendigung ab. Bleibt eine Rückmeldung aus, erinnert smartline erneut und hält die Daten bis zur Entscheidung geschützt vor.
2. Daten in Sicherungskopien werden nicht mehr genutzt und mit Ablauf des Rotationszyklus der Sicherungen (Anlage 2) überschrieben. Wird eine Sicherung zurückgespielt, gelten die Löschanweisungen erneut.

§ 12 Haftung und Vergütung

Die gesetzliche Haftung, einschließlich Art. 82 DSGVO, bleibt unberührt. Die Vergütung der Hauptleistungen ergibt sich aus dem jeweiligen Einzelvertrag. Ein Aufwandsersatz für zusätzliche Unterstützungsleistungen kann gesondert vereinbart werden. Er darf gesetzliche Mitwirkungs- und Kontrollrechte nicht vereiteln.

§ 13 Schlussbestimmungen

Änderungen und Ergänzungen bedürfen der Textform. Die Anlagen sind Bestandteil dieser Vereinbarung. Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen unberührt. Es gilt deutsches Recht.

Verantwortlicher	smartline Digitalagentur
Ort, Datum:	Bad König,
Name, Unterschrift	Frank Kirsch, Inhaber

Bei elektronischem Abschluss über smartline.info ersetzt der Abschlussnachweis (Zeitpunkt, Vertragsversion, bestätigende Person) die Unterschrift.

Anlage 1 – Leistungsarten, Datenarten und Betroffene

Erfasst sind nur die tatsächlich beauftragten Leistungen. Die Auswahl ergibt sich aus Angebot, Auftrag, Leistungsabruf oder Produktblatt (Anlage 4).

Leistung	Zweck / Dauer	Datenarten	Betroffene
Website, Hosting, Wartung	Bereitstellung, Fehlerbehebung, Updates, Sicherung; Vertragsdauer zzgl. Löschphase	IP-Adressen, Logdaten, Formulareingaben, CMS-Benutzerkonten, ggf. Kunden-, Bewerber- oder Bestelldaten	Websitebesucher, Beschäftigte, Kunden, Bewerber
Smart-CMS, Shops	CMS-Betrieb, Benutzerverwaltung, Bestellabwicklung im Auftrag, Support	Konten, Kontaktdaten, Inhalte, Bestellungen, Transaktionsmetadaten (keine Zahlungskartendaten)	Redakteure, Käufer, Besucher
Smartlinecard	Bereitstellung digitaler Visitenkarten, Kontakt- und QR-Funktionen	Name, geschäftliche Kontaktdaten, Profilbilder, technische Zugriffsdaten; Statistiken nur wenn aktiviert	Karteninhaber, Besucher
Werbebildschirm	Ausspielung von Inhalten auf Bildschirmen, Inhaltspflege	Inhalte inkl. Personenabbildungen, Benutzerkonten, Zugriffsdaten	Abgebildete Personen, Redakteure
direktgefragt	Veranstaltungsbetrieb, Wortmeldungen, Fragen, Audio-/Videoübertragung	Name, E-Mail, Fragen, Stimme bei Wortmeldung, Bild und Ton der Vortragenden, IP- und Verbindungsdaten	Teilnehmer, Moderatoren, Vortragende
SEO, individuelle Entwicklung	Analyse, Fehlersuche, Implementierung, Migration, soweit Zugriff auf Personendaten besteht	Logdaten, Analyse-Kennungen, Daten gemäß Einzelauftrag	Besucher, Nutzer, Kunden, Beschäftigte

Einschränkung direktgefragt: In dieser Fassung nicht freigegeben für Gesundheitsdaten, Berufsgeheimnisse und vertrauliche Einzelgespräche. Eine Aufzeichnung findet nicht statt, solange sie nicht gesondert vereinbart ist.

Anlage 2 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Systemlandschaft: Kundenwebsites, Smart-CMS, Smartlinecard und Odenwaldclick werden bei der Nodeeps (Rechenzentrum Ettenheim, Deutschland) betrieben. Werbebildschirm-Anwendungen und Testsysteme laufen auf einem eigenen Server in den Geschäftsräumen von smartline. Der Produktivbetrieb von direktgefragt erfolgt bei der Hetzner Online GmbH (Rechenzentrum Frankfurt am Main), die Audio-/Videoübertragung über LiveKit Cloud (Serverregion EU/Frankfurt).

1. Vertraulichkeit

- **Zutrittskontrolle:** Der eigene Server steht in einem abgeschlossenen Raum der Geschäftsräume von smartline. Der Schlüssel liegt ausschließlich beim Inhaber. Für die Rechenzentren der Unterauftragsverarbeiter gelten deren zertifizierte Zutrittskontrollen.
- **Zugangskontrolle:**
 - Zugangsdaten werden ausschließlich in einem verschlüsselten Passwortmanager (Bitwarden) verwaltet, nicht in Dateien oder E-Mails.
 - Mehr-Faktor-Authentifizierung ist aktiv für Passwortmanager, Server-Administration (Synology DSM) und kaufmännische Software, sowie überall dort, wo Anbieter sie bereitstellen.
 - Kundenportale nutzen passwortlose Anmeldung über zeitlich begrenzte Einmal-Links bzw. -Codes mit Begrenzung der Anmeldeversuche.
- **Zugriffskontrolle:**
 - Jeder Mitarbeitende erhält Zugriff nur auf die ihm zugewiesenen Projekte.
 - Zugänge werden nach Projektende bzw. Ausscheiden entzogen.
 - Administrative Bereiche sind gesondert geschützt und von Suchmaschinen ausgeschlossen.
- **Trennungskontrolle:** Kundensysteme sind je Kunde getrennt (eigene Webspaces, Datenbanken bzw. Mandanten). Test- und Produktivsysteme sind getrennt.
- **Verschlüsselung:**
 - Übertragungen erfolgen verschlüsselt (HTTPS/TLS, SMTP über SSL, SFTP wo vom Hoster angeboten).
 - Zugangsdaten in Webanwendungen liegen in gesonderten, vor Web-Zugriff gesperrten Konfigurationsdateien.
 - Externe Sicherungen sind clientseitig verschlüsselt.

2. Integrität

- **Weitergabekontrolle:** Daten werden nur verschlüsselt übertragen. Zugriffe von außen auf den eigenen Server erfolgen ausschließlich über einen Reverse Proxy mit TLS. Keine Weitergabe an Dritte außer an Unterauftragsverarbeiter nach Anlage 3.
- **Eingabekontrolle:** Änderungen an Kundensystemen werden im Rahmen der Wartung je Kunde protokolliert (Wartungsberichte, Kundenprotokoll). Webanwendungen von smartline führen Anmelde- und Änderungsprotokolle, soweit vorgesehen.

3. Verfügbarkeit und Belastbarkeit

- **Datensicherung:**

- Doppelte Sicherung des eigenen Servers: auf ein räumlich getrenntes zweites System sowie verschlüsselt in Synology C2 (Speicherort Frankfurt am Main).
- Websites werden im Rahmen der Wartung zusätzlich gesichert.
- Die Sicherung läuft täglich und inkrementell, mit Versionierung. Ältere Versionen werden nach dem eingestellten Rotationsschema überschrieben.
- Die Wiederherstellung wurde erfolgreich getestet.
- **Updates und Überwachung:**
 - CMS-, Plugin- und Systemupdates im Rahmen der Wartung.
 - Malware-Prüfung bei WordPress-Wartungen.
 - Überwachung der Erreichbarkeit und Inhalte von Wartungskunden-Websites mit automatischer Alarmierung.
- **Wiederherstellung:** Dokumentierter Ablauf zur Bereinigung kompromittierter Websites (Analyse, Bereinigung, Prüfung, Rotation von Schlüsseln).

4. Verfahren zur regelmäßigen Überprüfung

- Überprüfung dieser Maßnahmen mindestens jährlich sowie bei jeder Änderung der Systemlandschaft oder der Unterauftragsverarbeiter.
- Mitarbeitende werden vor Aufnahme der Tätigkeit schriftlich auf Vertraulichkeit und Datenschutz verpflichtet.
- Datenschutzvorfälle werden dokumentiert und nach § 9 gemeldet.

Anlage 3 – Unterauftragsverarbeiter

Unterauftragsverarbeiter	Leistung	Verarbeitungsort	Drittlandgrundlage
Nodeeps, Ettenheim	Webhosting, Datenbanken, E-Mail für Kundenwebsites, Smart-CMS, Smartlinecard	Deutschland (Ettenheim)	–
Synology Inc., Taipeh (Taiwan) – Dienst Synology C2	Verschlüsselte externe Datensicherung	Deutschland (Frankfurt am Main)	Daten werden vor der Übertragung verschlüsselt, der Schlüssel liegt ausschließlich bei smartline
Hetzner Online GmbH, Gunzenhausen	Serverbetrieb direktgefragt (ab Produktivstart)	Deutschland (Frankfurt am Main)	–
LiveKit, Inc. (USA)	Audio-/Videoübertragung direktgefragt	EU (Frankfurt am Main)	EU-Standardvertragsklauseln (Data Processing Addendum von LiveKit)
Freie Mitarbeiter (Kategorie)	Projektmitarbeit Web und Grafik, Zugriff nur auf zugewiesene Projekte	Deutschland	–

Nur für die jeweils beauftragten Leistungen relevant: Hetzner und LiveKit ausschließlich bei direktgefragt.

Anlage 4 – Produktblatt / Leistungsabruf

Kunde / Auftragsnummer / Datum

Beauftragte Leistungen und Module (Anlage 1)

Besondere Weisungen

Abweichende Datenarten / Betroffene

Aufzeichnung (nur direktgefragt): ja / nein,
Speicherfrist

Beginn, Laufzeit, gewünschtes Rückgabeformat

Datenschutz- und Notfallkontakt des
Verantwortlichen

Freigabe durch Verantwortlichen: _____ Datum: _____