Vertrag zur Auftragsverarbeitung

Zwischen

der fodjan GmbH, Großenhainer Str. 101, 01127 Dresden

- Auftragnehmer -

und

der [Firmenbezeichnung, Straße Hausnummer, PLZ Ort]

- Auftraggeber -

Präambel

Der Auftraggeber möchte den Auftragnehmer mit den in § 3 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DS-GVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 Begriffsbestimmungen

Die Begriffsbestimmungen ergeben sich aus Art. 4 DS-GVO.

§ 2 Vertragsgegenstand

(1) Der Auftragnehmer erbringt für den Auftraggeber auf der Grundlage eines gesonderten Vertrages („Hauptvertrag“) Leistungen im Bereich Software as a Service über die Webplattform fodjan smart feeding. Die Software ermöglicht das Management verschiedener Daten der Kunden des Auftraggebers. Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers.

(2) Der konkrete Gegenstand der Verarbeitung, die Art und der Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in Anlage 1 zu diesem Vertrag festgelegt. Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

(3) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

(4) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag im Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

(5) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 3 Weisungsrecht

(1) Der Auftragnehmer darf personenbezogene Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden („Einzelweisung“). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von personenbezogenen Daten. Die weisungsberechtigten Personen ergeben sich aus Anlage 1. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.

(3) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(4) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 4 Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und personenbezogene Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der personenbezogenen Daten des Auftraggebers gem. Art. 32 DS-GVO, insbesondere mindestens die in Anlage 2 aufgeführten Maßnahmen der

a) Zutrittskontrolle
b) Zugangskontrolle
c) Zugriffskontrolle
d) Trennung
e) Pseudonymisierung und Verschlüsselung
f) Eingabekontrolle
g) Weitergabekontrolle
h) Verfügbarkeit und Belastbarkeit der Systeme und Dienste

i) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Beim Auftragnehmer ist als betrieblicher Ansprechpartner für den Datenschutz bestellt:

Alexander, Weidenhammer
DID Dresdner Institut für Datenschutz
Hospitalstraße 4
01097 Dresden

Tel.: (0)351 / 655 772-0
E-Mail: datenschutz@fodjan.de

(4) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im Folgenden „Mitarbeiter“ genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DS-GVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

§ 5 Informationspflichten des Auftragnehmers

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Textform informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
b) eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der personenbezogenen Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.

(3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen personenbezogene Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Sollten die personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder

Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die personenbezogenen Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DS-GVO liegt.

(5) Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 4 Abs. 2 hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

(6) Ein Wechsel in der Person des betrieblichen Ansprechpartners für den Datenschutz ist dem Auftraggeber unverzüglich mitzuteilen.

(7) Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DS-GVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

(8) An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

§ 6 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers. Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche (Textform ausreichend) Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

(3) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

(4) Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

(5) Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach § 4 Abs. 4 auf Verlangen nach.

§ 7 Einsatz von Subunternehmern

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in Anlage 3 genannten Subunternehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt, soweit er den Auftraggeber hiervon vorab in Kenntnis setzt und dieser der Beauftragung des Subunternehmers vorab in Textform zugestimmt hat. Eine Verweigerung der Zustimmung bedarf einer angemessenen Begründung des Auftraggebers (in Textform) aus datenschutzrechtlicher Sicht. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

(2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

§ 8 Anfragen und Rechte Betroffener

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12 bis 22 sowie 32 bis 36 DS-GVO.

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner personenbezogenen Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

§ 9 Haftung

(1) Sofern im Hauptvertrag Haftungsausschlüsse oder -erleichterungen zugunsten einer Partei oder beider Vertragspartner vereinbart sind, gelten diese nicht bezogen auf Schadensersatzansprüche, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung geltend macht.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

§ 10 Außerordentliches Kündigungsrecht

Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DS-GVO vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will. Bei einfachen - also weder vorsätzlichen noch grob fahrlässigen - Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

§ 11 Beendigung des Hauptvertrags

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, personenbezogene Daten und Datenträger zurückgeben oder - auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht - löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener personenbezogener Daten zu führen. Zu entsorgende Unterlagen sind mit einem Aktenvernichter nach DIN 66399 zu vernichten. Zu entsorgende Datenträger sind nach DIN 66399 zu vernichten.
(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der personenbezogenen Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.
(3) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen personenbezogenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

§ 12 Schlussbestimmungen

(1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden personenbezogenen Daten und der zugehörigen Datenträger ausgeschlossen ist.
(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.
(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.
(4) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist - soweit gesetzlich zulässig - der Sitz des Auftragnehmers.

(5) Vertragsgegenständliche Anlagen sind:

Anlage 1 – Gegenstand des Auftrags

Anlage 2 – Technische und organisatorische Maßnahmen des Auftragnehmers

Anlage 3 – Genehmigte Subunternehmer

-Auftragnehmer-

Dresden,	
Ort, Datum	fodjan GmbH Carsten Gieseler und Michael Schütze Geschäftsführer [Stempel und Unterschrift]

-Auftraggeber-

Ort, Datum	Firmenbezeichnung Vorname Nachname Position [Stempel und Unterschrift]

Anlage 1 - Gegenstand des Auftrags

1. Gegenstand und Zweck der Verarbeitung

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen: fodjan smart feeding ist ein Software as a Service-Angebot. Mit dem Angebot können Daten eines landwirtschaftlichen Betriebes verwaltet und ausgewertet werden. Basierend auf diesen Daten können die Prozesse des Betriebes optimiert werden. Der Futtermittelhandel wird unterstützt. CRM-Funktionalitäten sind ebenfalls in den Leistungen enthalten.

2. Art(en) der personenbezogenen Daten

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

- Name, Anschrift
- Zugriffszeiten und Benutzungsprofile
- Kommentare im Freitext
- Betriebsindividuelle Daten zum Produktionsprozess des Betriebes der Kunden des Auftraggebers
- wirtschaftliche Lage des Betriebes (Erträge, Kosten, Gewinn)

3. Kategorien betroffener Person

Kreis der von der Datenverarbeitung betroffenen Personen:

- Auftraggeber
- Kunden des Auftraggebers
- Mitarbeiter des Kunden des Auftraggebers
- Geschäftspartner des Kunden (Tierarzt, Berater…) des Auftraggebers

4. Weisungsberechtigte Personen des Auftraggebers

Name, Vorname: _____

Position: _____

Tel.:

E-Mail: _____

5. Weisungsempfangsberechtigte Personen des Auftragnehmers

Michael Schütze und Carsten Gieseler
Großenhainer Straße 101
01127 Dresden

Email: info@fodjan.de
Tel: +49 351 4188 6693

Anlage 2 Technische und organisatorische Maßnahmen des Auftragnehmers

1. Vertraulichkeit Art. 32 Abs. 1 lit. b DS-GVO

Zutrittskontrolle = Niemand kann unbefugt den Raum, in dem sich die Datenverarbeitungsanlage befindet, betreten	☒ Chipkarte-/Transponder-Schließsystem ☒ Schlüsselregelung (z.B. Schlüsselausgabe) ☒ Sorgfältige Auswahl von Reinigungspersonal
Serverraum Wo befindet sich der Server?	☒ Serverschrank ☒ Schrank verschlossen? ☒ Datenleitungen offen verlegt? Andere Leitungen im Raum? ☒ Strom ☒ Wasser ☒ Serverräume nicht unter sanitären Anlagen, wasserführenden Leitungen
Zugangskontrolle = keine unbefugte Systembenutzung	☒ Vergabe von Benutzerrechten ☒ Passwortrichtlinie inkl. Passwortlänge, -zusammensetzung ☒ Authentifikation mit Benutzername und Passwort ☒ Forderung verschiedener Passwörter für verschiedene Dienste ☒ Passwortsave ☒ Keine unverschlüsselte Speicherung von Passwörtern ☒ Sperrung des Bildschirms oder Herunterfahren bei Inaktivität ☒ Zuordnung von Benutzerprofilen zu IT-Systemen ☒ Automatische Sperrung bei mehrmaliger Fehleingabe ☒ Sperre von externen Schnittstellen (USB) ☒ Beschränkung auf firmeneigene mobile Datenträger ☒ Einsatz einer Software-Firewall ☒ Einsatz einer Hardware-Firewall ☒ VPN (Virtual Privat Network) ☒ Einsatz von Anti-Viren-Software
Zugriffskontrolle = Kein unbefugtes Lesen, Kopieren, Verändern oder	☒ Rechtsvergabe nach dem „need to know“ Prinzip (Abgestuft: Löschen, Schreiben, Lesen…

Entfernen innerhalb des Systems.	☒ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten ☒ Verwaltung der Rechte durch Systemadministrator ☒ Anzahl der Administratoren auf das „Notwendigste“ reduziert ☒ Gesonderter Passwortschutz für einzelne, besonders sensible DV-Anwendungen ☒ Verschlüsselung von mobilen Datenträgern ☒ Verschlüsselung von Datenträgern in Notebooks ☒ Verschlüsselung von Smartphone-Inhalten/Tablets ☒ physische Löschung von Datenträgern vor Wiederverwendung ☒ ordnungsgemäße Vernichtung von Datenträger (DIN 32757) ☒ Einsatz von Aktenvernichtern bzw. Dienstleistern ☒ Sichere Aufbewahrung von Datenträgern Wo? Im abgeschlossenen Schrank von GF Herr Schütze Regeln? Nur Herr Schütze gibt die Datenträger aus
Trennungskontrolle = Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden.	☒ physikalische Trennung ☒ logische Kundentrennung (softwareseitig) ☒ Erstellung eines Berechtigungskonzepts ☒ Sandboxing / Trennung von Produktiv- und Testsystem
Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO) = Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.	☒ Nutzung von Pseudonymisierung wo möglich (u. a. bei Weitergabe) ☒ geeignete Wahl der Pseudonymisierungsschlüssel

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle = Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport	☒ VPN ☒ E-Mail TLS Verschlüsselung ☒ Verschlüsselung von mobilen Datenträgern ☒ Verschlüsselung von Datenträgern in Notebooks ☒ Verschlüsselung von Smartphone-Inhalten/Tablets ☒ Weitergabe von Daten in anonymisierter oder mindestens pseudonymisierter Form
Eingabekontrolle =Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	☒ Dokumentenmanagement ☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle = Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust / Sicherung.	☒ gespiegelte Festplatten (RAID) ☒ gespiegelte Systeme/Cluster ☒ Einsatz einer Software-Firewall ☒ Einsatz einer Hardware-Firewall ☒ Einsatz von Anti-Viren-Software ☒ Regelmäßige Aktualisierung der Systeme ☒ Erstellen eines Backup- & Recoverykonzepts (u. a. online/offline; on-site/off-site) ☒ regelmäßige Datenwiederherstellungstests ☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort ☒ Feuer- und Rauchmeldeanlagen ☒ Feuerlöschgeräte in Serverräumen (CO2)
rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lilt. c DS-GVO)	☒ Automatisiertes aufsetzen von Server

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO)

Datenschutz-Management	☒ Bestellung eines Datenschutzbeauftragten ☒ Verzeichnis von Verarbeitungstätigkeiten ☒ Datenschutz-Folgeabschätzungen ☒ Schulungsmaßnahme/Sensibilisierungsmaßnahmen mit Nachweis ☒ Verpflichtung auf Vertraulichkeit der Mitarbeiter ☒ definierte und dokumentierte Prozesse ☒ Arbeitsanweisungen/Polices mit Datenschutzhintergrund
Incident-Response-Management	☒ Definition von Zuständigkeiten und Verantwortlichkeiten für Vorfälle (z. B. Vorfallteam) ☒ definierter Meldeprozess ☒ definierte Maßnahmen für relevante und denkbare Vorfälle ☒ definierte Eskalationswege ☒ aktuelle Melde- und Kontaktlisten
Auftragskontrolle Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z. B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen	☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten ☒ Sicherstellung der Verpflichtung auf die Vertraulichkeit durch den Auftragnehmer ☒ Auftragnehmer hat Datenschutzbeauftragten bestellt (falls gesetzlich vorgeschrieben) ☒ vertraglich festgelegte Verpflichtungen und Zuständigkeiten ☒ Auftragsverarbeitungsverträge ☒ wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart ☒ schriftliche Weisungen an den Auftragnehmer (Textform ausreichend) ☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

Anlage 3 - Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“). Dabei handelt es sich um nachfolgende Unternehmen:

Unterauftragnehmer	**Adresse**	**Art der Leistung**
Hetzner Online GmbH	Industriestr. 25 91710 Gunzenhausen Deutschland	Anbieter Rechenzentrum
Strato AG	Pascalstraße 10 10587 Berlin Deutschland	Anbieter Rechenzentrum
Loumaris UG (haftungsbeschränkt)	Mühlenstr. 6 06420 Könnern Deutschland	Dienstleistungen zur Serveradministration
FastBill GmbH	Wildunger Str. 6 60487 Frankfurt am Main Deutschland	Softwaredienst zur Rechnungslegung
HubSpot, Inc.	25 First Street Cambridge MA 02141 USA	CRM-System
Google Ireland Ltd	Gordon House Barrow Street Dublin	Crashreports in Firebase, Google Analytics, Google-Marketing-Services
1&1 IONOS SE	Elgendorfer Straße 57 56410 Montabaur Deutschland	Anbieter Rechenzentrum
Microsoft Ireland Operations, Ltd.	Attn: Data Protection One Microsoft Place South County Business Park Leopardstown, Dublin 18, D18 P521	Microsoft Onlinedienste, MS Exchange, MS Office, MS Teams
Stripe Payments Europe Ltd.	1 Grand Canal Street Lower Grand Canal Dock Dublin	Zahlungsanbieter

Unterauftragnehmer	Adresse	Art der Leistung
Atlassian Pty Ltd.	Level 6, 341 George Street Sydney, NSW 2000 Australia	Softwaredienst
Zoho Corporation B.V. **(Zoho Netherlands)**	Hoogoorddreef 15 Amsterdam, 1101 BA NETHERLANDS	Rechnungslegung
Elbe Inkasso GmbH	Tiergartenstraße 8 01219 Dresden	Inkasso
DeepL GmbH	Maarweg 165 50825 Köln	Übersetzungsdienstleister
DSI GmbH Daten Service Informationssysteme	Carolinenstraße 1 01097 Dresden	IT Service Dienstleister
Adobe Systems Software Ireland Limited	4-6 Riverwalk City West Business Campus Saggart D24 Dublin Irland	Adobe cloud Servicenutzung (Adobe sign)
Github Inc.	88 Colin P. Kelly Jr. Street San Francisco California 94107 USA	Onlinedienst zur Versionsverwaltung für Software-Entwicklungsprojekte
Tempo Software Inc.	67 South Bedford Street Suite 400 West Burlington MA 01803 USA	Softwaredienst
Pitch Software GmbH	Joachimstraße 7 10119 Berlin	Plattform für Präsentationen

Die laufend aktualisierte Auflistung der Unterauftragnehmer können Sie auf unserer Homepage (https://fodjan.com/de/auftragsverarbeitung/) einsehen.