

Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO

mobileObjects AG
Lindberghring 2-4
33142 Büren

- Auftragsverarbeiter - nachstehend „Auftragnehmer“ genannt

Präambel

Diese Zusatzvereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich durch den Vertragsabschluss der Software Dienstleistungen ergeben.

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung des Servicevertrags, auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung). Bereitstellung des Telematikportals als Software-as-a-Service (SaaS) aus einem deutschen Rechenzentrum heraus.

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung des Servicevertrags.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung des Software-Servicevertrags.

Im Wesentlichen handelt es sich dabei um Daten, die notwendig sind zur Ortung und Spurfollowung von Fahrzeugen, Auftragsanalyse, Tankkontrolle sowie zur grundlegenden Kommunikation mit Nachrichten und / oder zum Auftragsmanagement, mit dem Zweck die



Arbeitsabläufe des Kunden zu verbessern, und die Auftragsverarbeitung vom Eingang bis zu Rechnungsstellung papierlos zu erledigen.

Zusätzlich wird zur Erfüllung der vertraglich vereinbarten Supportverpflichtung durch den Auftragnehmer ein dauerhafter Support Zugang im Portal des Auftraggebers geschaltet. Die Nutzung des Zugangs wird protokolliert und kann über die Portaleinstellung durch den Auftraggeber beschränkt werden.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produktinformationen)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten (Tourenpläne, LKW-Einsatz)

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden
- Beschäftigte
- Ansprechpartner

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Als Datenschutzbeauftragter ist beim Auftragnehmer Herr Oliver Baldner, Tel.: +49 5251 688948-0, datenschutz@mobileobjects.de bestellt.
- b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].
- d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
- g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit,



Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Firma Unterauftragnehmer	Anschrift/Land	Leistung
VegaSystems GmbH & Co.KG	Karl-Schurz-Str. 35, 33100 Paderborn	Hosting RZ

b) Die Auslagerung auf Unterauftragnehmer oder

der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer

bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);

sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditor, Qualitätsauditor);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

- a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsergebnissen ermöglichen

- b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
- c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
- d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
- e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Vergütung

Eine gesonderte Vergütung schuldet der Auftraggeber dem Auftragnehmer für dessen Leistungen im Zusammenhang mit diesem Vertrag nicht.

12. Schlussbestimmungen

Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

Die Anlagen zu diesem Vertrag sind Bestandteil dieses Vertrages.

Änderungen und Ergänzungen sowie die Aufhebung dieses Vertrages, seiner Anlagen sowie dieser Schriftformklausel bedürfen zu ihrer Wirksamkeit der gesetzlichen Schriftform.

Sollten Bestimmungen dieses Vertrages oder seiner Anlagen ganz oder teilweise unwirksam oder undurchführbar sein oder werden, so wird die Wirksamkeit der Bestimmungen im Übrigen hiervon nicht berührt. Die Vertragspartner verpflichten sich, die unwirksamen oder undurchführbaren Bestimmungen oder Teile der Bestimmungen durch wirksame und durchführbare Bestimmungen zu ersetzen, die dem von den Vertragspartnern mit den ganz oder teilweise unwirksamen oder undurchführbaren Bestimmungen verfolgten wirtschaftlichen Zweck am nächsten kommen. Dies gilt auch für den Fall, dass dieser Vertrag oder seine Anlagen Regelungslücken enthalten.

Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB und die Einrede des nicht erfüllten Vertrages gemäß § 320 BGB werden hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Anlage 1: Technische und organisatorische Maßnahmen (TOM) i.S.d. Art 32 DS-GVO

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

- Zutrittskontrolle
Die mobileObjects AG betreibt in den Rechenzentren des Service Providers Vega Systems GmbH & Co. KG am Standort Paderborn eigene dedizierte Server, die ausschließlich von mobileObjects genutzt werden.
Die Zutrittskontrolle erfolgt durch die jeweiligen Provider und beinhaltet:
 - Einbruchmeldesysteme mit Magnetmeldern und Schließkontakten, Alarmfolien bei leicht zugänglichen Bereichen, Vorhangmelder und Infrarotbewegungsmelder sowie zentrale Scharfschalteneinrichtungen, die durch eine Sicherheitsleitstelle überwacht werden
 - Zugang zu den sensiblen Bereichen ist nur nach telefonischer Anmeldung, mit gültigem amtlichem Ausweis und mit gültiger Accesskarte möglich.
 - Videoüberwachungssystem mit Bewegungsdetektoren innerhalb und außerhalb des Gebäudes
 - Brandmeldeanlage
 - Überwachung durch Sicherheitspersonal 24h/365 Tage
- Zugangskontrolle
Die Zugangskontrolle erfolgt über Benutzername / Passwort. Nur die jeweils autorisierten Entwickler haben Zugang auf die für sie relevanten Bereiche. Die Server sind über eine Firewall abgesichert. Der Zugang auf die Server im Rechenzentrum erfolgt über eine verschlüsselte VPN-Verbindung.
- Zugriffskontrolle
Es wurde ein detailliertes Berechtigungskonzept entwickelt und implementiert, das sicherstellt, dass die Zugriffsrechte produkt- aufgaben- und mitarbeiterbezogen gewährt werden.
- Trennungskontrolle
Die Daten sind logisch getrennt (nach Mandantenummer) auf den Systemen gespeichert und durch detaillierte Zugriffsrechte vor zweckfremdem Zugriff geschützt.
- Pseudonymisierung Die personenbezogenen Daten werden ausschließlich im Auftrag und gemäß der ausdrücklichen Weisung des Kunden verarbeitet. Eine Pseudonymisierung ist daher auf Auftragnehmerseite nicht vorgesehen.

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

- Weitergabekontrolle
Die Datenübertragung erfolgt grundsätzlich über eine verschlüsselte Verbindung. Dies gilt für den Abruf der Daten durch Kunden und den Zugriff auf Daten im Rahmen von Wartungs- und Entwicklungsarbeiten.
- Eingabekontrolle
Login-Daten und alle Änderungen an systemrelevanten Daten oder Dateien werden protokolliert.

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

- Verfügbarkeitskontrolle
Die Speicherung der Daten erfolgt 3-fach redundant auf hardwareseitig getrennten Servern.
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);
Die Daten können innerhalb weniger Stunden aus Snapshots wiederhergestellt werden

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

I. Datenschutz-Management;

- Ein Datenschutzbeauftragter ist schriftlich bestellt:
 - Oliver Baldner, Tel.: +49 5251 688948 0, datenschutz@mobileobjects.de
 - Fachkundennachweis des Datenschutzbeauftragten liegen vor.
- Die Mitarbeiter werden in regelmäßig angebotenen Schulungen für das Thema Datenschutz sensibilisiert.
 - Es existieren Nachweise über Verpflichtungen auf das Datengeheimnis für jeden Mitarbeiter
 - Es erfolgen regelmäßig Hinweise und Sensibilisierungsmaßnahmen, um das datenschutz-rechtliche Problembewusstsein zu fördern.
- Ein Verzeichnis von Verarbeitungstätigkeiten ist vorhanden und wird fortlaufend aktualisiert.
- Die folgenden Dokumentationen liegen vor:
 - Technisch-organisatorische Maßnahmen, siehe dieses Dokument
 - Schriftliche Arbeitsanweisungen/Richtlinien/Merkblätter
- Es ist ein Konzept zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung implementiert. Insbesondere wird 1x jährlich mit dem zuständigen IT-Mitarbeiter ein Review der technischen und organisatorischen Maßnahmen durchgeführt, entsprechende Schritte formuliert und nachgehalten sowie im Jahresbericht dokumentiert.
- Die Aufbewahrung der Protokolle zu Datenschutzthemen ist geregelt.
- Es werden Datenschutz-Folgeabschätzung gem. Art. 35 DS-GVO durchgeführt und protokolliert.
- Es liegen keine Verträge mit Unternehmen in Drittländern (gem. Art. 44 ff. DS-GVO) vor.
- Es finden gelegentliche, unangekündigte Kontrollen der Einhaltung von Datenschutz- und Datensicherungsmaßnahmen statt.

II. Incident-Response-Management;

Nr	Prozess-Schritt	Verantwortlich	Hinweise	Mitgel-tende Doku-mente/ Verweise
1	Kenntniserlangung von einem Datenschutzvorfall	Alle	Definition: Als Datenschutzvorfall wird ein Ereignis bezeichnet, das die Vertraulichkeit, Verfügbarkeit und Integrität personenbezogener Daten beeinträchtigt. Ein Datenschutzvorfall ist insbesondere die unrechtmäßige Übermittlung oder unrechtmäßige Kenntniserlangung von personenbezogener Daten durch Dritte.	
2	Sofortige Weitergabe der Information durch Stelle, die Kenntnis erlangt hat, an den Datenschutz-Koordinator (oder falls vorhanden: IT-Sicherheitsbeauftragter)	Stelle, die Kenntnis erlangt hat		

III. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO) obliegt dem Kunden;

IV. 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.