Vereinbarung zur Auftragsverarbeitung nach Art. 28 DS-GVO

Dieser Vertrag konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der in den abgeschlossenen Dienstleistungsverträgen in ihren jeweiligen Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit den Dienstleistungsverträgen in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können. Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des jeweiligen Einzelvertrages.

§ 1 Gegenstand und Dauer des Auftrages

1. Gegenstand des Auftrages
Der Gegenstand des Auftrages ergibt sich jeweils aus dem - E-Commerce Nutzungs- und Liefervertrag (nachfolgend „Einzelverträge“) auf die hier verwiesen wird.

2. Dauer des Auftrages
Die Dauer dieses Auftrages (Laufzeit) entspricht der Laufzeit der jeweiligen Einzelverträge.

§ 2 Konkretisierung des Auftragsinhaltes

1. Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten.
Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber, insbesondere übernimmt er die Bearbeitung von Bestellungen, die Auslieferung von Waren/Inhalten an den Besteller oder den Versand an Kunden des Auftraggebers. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzes insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (Verantwortlicher i.S. Art.4 Nr. 7 DS-GVO).

2. Art der Daten
Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten können folgende Datenarten / -kategorien sein:

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten
- Kundenhistorie
- Vertragsabrechnungs-, Zahlungs- und Buchhaltungsdaten
- Planungs- und Steuerungsdaten
- Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

3. Kreis der Betroffenen
Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst:
- Beschäftigte
- Dienstleister.

Der Auftragnehmer stellt sicher, dass die oben genannten, mit der Verarbeitung der Daten befassten Personen gem. Art. 28 Abs. 3, 29 und 32 DS-GVO (Datengeheimnis) zur Verschwiegenheit und Vertraulichkeit verpflichtet und in die Schutzbestimmungen der/s DS-GVO/BDSG eingewiesen sind. Das Datengeheimnis besteht auch nach der Beendigung ihrer Tätigkeit fort.

§ 3 Technische und organisatorische Maßnahmen

Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten und dokumentieren, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zur angemessenen Sicherung des Auftraggebers vor Missbrauch und Verlust treffen, die den Anforderungen des Art. 28 Abs. 3 lit. c, 32 DS-GVO in Verbindung mit Art. 5 Abs. 1 und 2 DS-GVO entsprechen.
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.

Die ergriffenen technischen und organisatorischen Maßnahmen sind im Wesentlichen aus der Anlage 1 ersichtlich.

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.
Der Auftragnehmer hat auf Anforderung die Angaben nach Art. 39 DS-GVO dem Auftraggeber zur Verfügung zu stellen.

§ 4 Berichtigung, eingeschränkte Verarbeitung und Löschung von Daten, Anfragen Betroffener

Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, grundsätzlich nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Der Auftraggeber beauftragt hiermit den Auftragnehmer entsprechend den Erfordernissen der Durchführung des Einzelvertrages mit der Verarbeitung, Berichtigung und Löschung von Daten, das Recht Einzelweisungen zu erteilen, bleibt unbenommen.
Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Ist der Auftraggeber auf Grund geltender datenschutzrechtlicher Bestimmungen gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützten, diese Informationen bereit zu stellen, vorausgesetzt der Auftraggeber hat den Auftragnehmer hierzu schriftlich aufgefordert und der Auftraggeber erstattet dem Auftragnehmer die durch diese Unterstützung entstehenden Kosten.
Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden,

Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.
Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich.

§ 5 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:
- Schriftliche Bestellung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 37 DS-GVO ausüben kann. Dessen Kontaktdaten werden dem Auftraggeber auf Anfrage zum Zweck der direkten Kontaktaufnahme mitgeteilt.
- 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.
- 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].
- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- 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.
- 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.

- 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.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen n(z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) vorlegen.

§ 6 Unterauftragsverhältnisse

Der Einsatz von Unterauftragnehmern als weitere Auftragsverarbeiter ist nur nach vorheriger Zustimmung des Auftraggebers zulässig. Der Auftraggeber stimmt zu, dass der Auftragnehmer Unterauftragnehmer hinzuzieht. Rechtzeitig vor der Hinzuziehung oder einer Ersetzung von Unterauftragnehmern informiert der Auftragnehmer den Auftraggeber. Der Auftraggeber kann innerhalb einer Frist von 7 Tagen aus wichtigem Grund gegenüber dem Auftragnehmer widersprechen. Erfolgt innerhalb der Frist kein Widerspruch, so gilt die Zustimmung als gegeben. Mit der Hinzuziehung der in Anlage 2 genannten Unterauftragnehmern erklärt sich der Auftraggeber einverstanden.
Die nachfolgenden Voraussetzungen bei der Unterbeauftragung müssen vorliegen:
- Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem / den Unterauftragnehmer/n so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen.
- Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung und des Art. 28 DSGVO beim Unterauftragnehmer einzuräumen. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutz-relevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.
Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

§ 7 Kontrollrechte des Auftraggebers

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. 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.

§ 8 Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.
Es ist bekannt, dass nach Art. 33 DS-GVO Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Auftraggeber mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen von Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers. Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den Auftraggeber Pflichten nach Art. 33 DSGVO treffen, hat der Auftragnehmer ihn hierbei zu unterstützen.

§ 9 Weisungsbefugnis des Auftraggebers

Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Sofern Weisungen nicht bereits im Vertrag festgelegt sind, können diese vom Auftraggeber auch danach in schriftlicher Form, in Textform oder mündlich an die vom Auftragnehmer bezeichnete Stelle durch Einzelanweisung ergänzt, ersetzt oder geändert werden. Mündliche Weisungen sind unverzüglich mindestens in Textform zu bestätigen. Der Auftragnehmer hat den Auftraggeber zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutz-rechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

§ 10 Löschung von Daten und Rückgabe von Datenträgern

Mit Beendigung des Auftragsverhältnisses oder früher nach Aufforderung durch den Auftraggeber hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten, sofern dem nicht gesetzliche Aufbewahrungsfristen entgegenstehen. Gleiches gilt für Test- und Ausschussmaterial. 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 Sonstiges, Allgemeines

Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Anlagen einschließlich etwaiger Zusicherungen des Auftragnehmers bedürfen einer schriftlichen Vereinbarung und des

ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
Es gilt deutsches Recht.

Anlage 1:
Technische und organisatorische Maßnahmen des Auftragnehmers
Anlage 2:
Unterauftragnehmer

Anlage 1 - Technische und organisatorische Maßnahmen des Auftragnehmers

1. Vertraulichkeit (Art. 32 Abs.1 lit. b DS-GVO)
Zutrittskontrolle
Verwaltungsgebäude
Der Zutritt in das Verwaltungsgebäude Stuttgart ist durch ein Zutrittsberechtigungssystem (Zutrittskarte) gesichert, zudem gibt es im Eingangsbereich eine Anmeldung. Bestimmte Gebäudeabschnitte werden darüber hinaus zusätzlich mit Schließzylindern oder Kartensystemen gesichert. Zylinder bzw. Schlüssel werden nur in begründeten Ausnahmefällen ausgegeben. Zur Beantragung eines Zylinders bzw. Schlüssels steht ein Formular zur Verfügung, das vom zuständigen Genehmigungsberechtigten unterschrieben werden muss.
Für das Gebäude sind verschiedene Sicherheitszonen (z.B. Technikräume) definiert. Zutrittsberechtigungen werden nur aufgrund einer durch den jeweiligen Kompetenzträger erfolgten Beantragung vergeben. Weiterhin gibt es auch Regelungen über die Vergabe von Zutrittsberechtigungen betriebsfremder Personen. Betriebsfremde Personen werden durch den zu Bürozeiten besetzten Empfang mit Besucherausweisen versorgt und im Gebäude durch eigene Mitarbeiter begleitet.

Zutritt zu den Rechenzentren
Der Zutritt ist durch ein Zutrittsberechtigungssystem (Zutrittskarte + biometrisches Merkmal), Personenvereinzelungsanlage sowie Videoüberwachung gesichert. Zudem gibt es 7x24 im Eingangsbereich eine Anmeldung. Der Zutritt zu den Rechenzentren ist neben den genannten Mechanismen zusätzlich über Verfahren geregelt, die beispielsweise den Umgang mit Betriebsfremden (z.B. Servicetechniker) definieren. Über das Zutrittsberechtigungssystem kann nachvollzogen werden, welche Zutrittskarte in welchem Bereich zu welcher Zeit genutzt wurde. Eine Verfahrensanweisung regelt den Ablauf der Zutrittsgenehmigung. Es erfolgt eine regelmäßige Kontrolle der Zutrittsberechtigungen.

Zugangskontrolle
Der Zugangsschutz zu den Systemen wird primär über eine entsprechend starke Authentisierungsmaßnahme realisiert. Um Zugang zu erhalten, muss man sich mit kryptischer Userkennung und Passwort am System authentifizieren. Zugangsberechtigungen werden nur aufgrund einer durch den jeweiligen Kompetenzträger erfolgten Beantragung vergeben.
Um den Zugangsschutz zu gewährleisten, sind für die genutzten Systemzugänge und Anwendungen entsprechende Passwortrestriktionen erlassen.
Pro User gibt es ausschließlich einen Benutzerstammsatz. Die Weitergabe von Passwörtern ist nicht erlaubt. Gleiches gilt für das Arbeiten mit fremden Usern.

PC’s und Laptops werden, soweit von diesen personenbezogene Daten verarbeitet werden, automatisch nach wenigen Minuten gesperrt, wenn sie vom Benutzer nicht genutzt werden und können erst nach Eingabe des Passworts wieder entsperrt werden.
Eine Zwei-Faktor-Authentifizierung ist zwingend für den Zutritt zu den Rechenzentren in Stuttgart vorgegeben (s. oben), für die Serveradministratoren ist eine zwei-Faktor Authentifizierung in der Evaluation. Datenträger mit sensiblen Daten sowie die Datenträger von Laptops sind durch geeignete Verfahren zu verschlüsseln und zugriffsgeschützt aufzubewahren. Zugriffskontrolle
Es besteht ein geregeltes Verfahren bzgl. der Benutzereinrichtung, -änderung und -löschung. Hierüber wird sichergestellt, dass nur berechtigte Personen

Zugang und Zugriff auf personenbezogene Daten erhalten.
Die Vergabe der Zugriffsberechtigungen erfolgt nur aufgrund einer durch den jeweiligen Kompetenzträger vorgenommenen Beantragung gemäß Profilen, Rollen, Transaktionen oder Objekte und orientiert sich an den Notwendigkeiten von Beispielusern. Die internen Netze sind über eine 2-stufige Firewall gegen unberechtigten Zugriff von außen geschützt.
Es finden systemspezifische Protokollierungen u.a. für Firewall-Systeme und den Virenschutz statt.
Trennungskontrolle Die jeweiligen Daten werden nur zur Zweckerfüllung erhoben, verarbeitet und genutzt. Eine Bereitstellung der Daten für andere Systeme / Zwecke ist verfahrenstechnisch ausgeschlossen. Insbesondere wird sichergestellt, dass eine notwendige Trennung nach Mandanten durch die Applikationen stattfindet. Des Weiteren sind die Systeme nach ihrer Zweckbestimmung separiert (Entwicklung, Test, Produktion). Eine produktive Verarbeitung von Daten findet nur in den Produktivsystemen statt. Damit können auch nur berechtigte Personen Zugriff und Zugang zu den produktiven Daten erlangen.

Pseudonymisierung (Art. 32 Abs.1 lit. a DS-GVO; Art. 25 Abs.1 DS-GVO)
Zur Auftragsabwicklung ist eine Pseudonymisierung nicht möglich, die Löschverfahren unterliegen den gesetzlichen Regelungen.

2. Integrität (Art. 32 Abs.1 lit. b DS-GVO)
Weitergabekontrolle
Zugriffe von außen auf die Systeme durch Lieferanten, Dienstleister, Servicepersonal erfolgen in der Regel über abgesicherte, d.h. verschlüsselte VPN Verbindungen (Tunnel, Virtual Private Network).
Der Austausch der Daten kann auf unterschiedlichen Wegen erfolgen:
a) Per Mail an zuvor mit dem Auftragnehmer abgestimmte Personen.
b) Per Datenfernübertragung über Internet oder Kommunikationsdienste mit geschlossenen Benutzergruppen (aktuell X.400). Die Art der eingesetzten Sicherheitsmaßnahmen hat den gebräuchlichen Standards der IT-Sicherheit zu entsprechen.
c) Einwahlmöglichkeit über VPN-Tunnel.
d) Client basierte Sicherheitsverfahren wie AS2, SFTP, HTTPS o.ä. Eingabekontrolle
Werden personenbezogene Daten in Datenverarbeitungssystemen (z.B. Bewerbermanagement, Personalverwaltung und -abrechnung) eingegeben, verändert oder entfernt, so kann dies durch entsprechende Protokollierung in den Applikationen nachverfolgt werden.

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

Die Komponenten in den Serverräumen sind über eine unterbrechungsfreie Stromversorgung (USV) und Netzersatzanlage (Notstromaggregate/Dieselgeneratoren) gesichert. Alle Räume verfügen über eine Klimaanlage. Die Serverräume sind über Rauchmelder/Brandfrüherkennung und Brandlöschanlage (Gas) gesichert.
Die KNV besitzt ein mehrstufiges Virenschutzkonzept, über das die Sicherheit der Clients und Server sowie der mobilen Arbeitsplätze gewährleistet werden kann.
Die logischen Strukturen der Rechenzentren (interne Anwendungen bzw. Anwendungen zum Zugriff von außen durch Kunden oder Interessenten) werden durch mehrstufige Firewalls geschützt.

Die Backupsysteme können bei einem Ausfall des Hauptsystems umgehend die Verarbeitungslast übernehmen. Haupt- und Backupsystem stehen in getrennten Rechenzentren. Produktionsdaten werden stets ins Backuprechenzentrum gespiegelt. Verbindungen nach Außen (Internetanbindung, Telefonie)sind stets redundant und mit mehreren unabhängigen Kommunikationsdienstleistern geschaltet. Damit besteht ein Notfallkonzept, das die Aufrechterhaltung der kritischsten Systeme und Geschäftsprozesse im Störungs- sowie im Notfall bzw. ihre schnellstmögliche Wiederverfügbarkeit sicherstellt. Es besteht ein dokumentiertes Datensicherungskonzept. Im Rahmen des derzeit bestehenden Verfahrens werden sämtliche Server über Tivoli Storage Manager (TSM) gesichert. Als Standard werden mehrere Generationen (Veränderungen) gespeichert und vorgehalten. Gelöschte Generationen oder gelöschte Dateien (auf dem Client) werden entsprechend der internen Verfahrensanweisung noch ausreichend lange vorgehalten, bevor sie aus dem TSM gelöscht werden. Sicherungen werden zum Schutz vor möglichen Datenträgerdefekten vorsorglich in zwei voneinander unabhängigen Sicherungsrobotern in getrennten Brandabschnitten abgelegt. Die Sicherung erfolgt täglich inkrementell. Zusätzlich erfolgt einmal in der Woche eine Vollsicherung. Weiterhin werden alle Sicherungs- und Archivierungsdaten über Verfahren wie z.B. IBM Tapelibrary gespeichert, die nicht ausgelagert werden müssen
Die Systeme sind in der Regel redundant ausgelegt, so dass der Ausfall eines Systems aufgefangen werden kann. Wichtige Infrastrukturkomponenten sind stets mit Wartungsverträgen mit kurzer Reaktionszeit ausgestattet, um Ausfallzeiten durch technische Defekte zu minimieren.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung
(Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)
Datenschutz-Management
Die Verwendung eines Datenschutzmanagement-Systems kontrolliert die Compliance, hält den Standard auf den jeweilig aktuell notwendigen organisatorischen Stand und unterstützt die Kontrolle bzgl. des notwendigen technischen Standes. Dazu wird a) ein Verfahrensverzeichnis elektronisch geführt, welches b) Verfahrensbeschreibungen, technisch-organisatorischen Maßnahmen, Subunternehmer, Verantwortliche, Schulungsbelege und sonstige notwendige Nachweise zur Erhöhung der Transparenz der Verarbeitung dokumentarisch vorhält.

Incident-Response-Management
Es bestehen Verfahren, um bei eventuellen Datenschutzvorfällen durch Information des direkten Vorgesetzten und des Datenschutzbeauftragen eventuelle Meldepflichten bei der zuständigen Behörde zu erkennen und die vorgegebenen Fristen einzuhalten.
Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Privacy by design und privacy by default werden bei Projektierung, Testphase und Umsetzung von IT-Anwendungen und sonstigen Prozessen berücksichtigt und im Datenschutzmanagement dokumentiert, Fach - und Führungskräfte werden hierzu auf das notwendige Vorgehen geschult. Auftragskontrolle Personenbezogene Daten, die im Auftrag verarbeitet werden, werden entsprechend den Weisungen des Auftraggebers verarbeitet. Die Beauftragung neuer Dienstleister erfolgt durch eindeutige Vertragsgestaltung und entsprechende Überprüfung der Datenschutz- und Datensicherheitsmechanismen risikoorientiert anhand einer Checkliste oder Kontrolle gegebenenfalls direkt vor Ort, dieses Ergebnis wird entsprechend dokumentiert.

– Unterauftragnehmer
F. Volckmar GmbH & Co. KG
Industriestraße 23
70565 Stuttgart

KNV Logistik GmbH
Ferdinand-Jühlke-Straße 7
99095 Erfurt

Episerver GmbH
Wallstraße 16 - 10179 Berlin

Pocketbook Readers GmbH
Richard-Wagner-Str. 11
01445 Radebeul

Leins Aktenvernichtungs GmbH
Bertha-Benz-Straße 11
72141 Walddorfhäslach