Auftragsverarbeitungsvereinbarung (Cloud) im Sinne des Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO)

Stand Juli 2024

1. Gegenstand und Dauer der Vereinbarung

1.1 Gegenstand der Vereinbarung ist die Bereitstellung von Hosting und Cloud Leistungen im Rahmen des mit der Auftraggeberin vereinbarten Umfangs gemäß Vertrag (nachfolgend auch „Hauptvertrag“) bzw. Zusatzbeauftragungen im Rahmen des Hauptvertrages und dieser Vereinbarung zum Datenschutz.

1.2 Gegenstand der Vereinbarung ist **nicht** die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch die Auftragnehmerin. Im Zuge der Leistungserbringung der Auftragnehmerin als zentraler IT-Dienstleister im Bereich des Hostings, des Supports bzw. der Administration von Server-Systemen, der Erbringung von Entwicklungsleistungen, der Durchführung von Tätigkeiten im Rahmen des Business Managements und der Speicherung von Daten der Auftraggeberin kann ein Zugriff auf personenbezogene Daten jedoch nicht ausgeschlossen werden bzw. kann auf ausdrückliche Beauftragung zugegriffen werden.

1.3 Die Laufzeit und die Kündigung dieser Vereinbarung richten sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrages. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieser Vereinbarung. Eine isolierte Kündigung dieser Vereinbarung ist ausgeschlossen.

2. Konkretisierung des Vereinbarungsinhalts: Umfang, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und Kategorien betroffener Personen

2.1 Umfang, Art und Zweck der Zugriffsmöglichkeit der Auftragnehmerin auf Daten der Auftraggeberin ergeben sich aus den Leistungsbeschreibungen der einzelnen Auftragsbestätigungen der Auftragnehmerin. Zusammengefasst entsteht die Zugriffsmöglichkeit:

- beim Hosting von virtuellen Computern, Netzwerk- und Storage-Komponenten als auch den dort betriebenen Anwendungen (wie bspw. Web-, App-, Solr-, Datenbank-, Backup-, Transfer-Server oder Storage-Diensten);
- bei der technischen Administration der Systeme und zugehörigen Diensten;
- bei sonstigen Tätigkeiten im Rahmen des Application Managements (z.B. im Zuge des proaktiven Monitorings);
- bei der technischen Analyse von Anfragen sowie der Umsetzung von vereinbarten Leistungen (u.a. Migration von Kundendaten, …)
- bei der Durchführung von Qualitätssicherungsmaßnahmen
- bei der Durchführung vereinbarter Leistungen im Rahmen des Business Managements

Zum Zwecke der Vertragserfüllung kann ein Zugriff der Auftragnehmerin auf die unter 2.2 aufgeführten Daten nicht ausgeschlossen werden bzw. erfolgt ein Zugriff nach 1.2.

2.2 Art der Daten

Die von der Auftragstätigkeit betroffenen Datenkategorien von Kunden und deren Endkunden, Lieferanten, Geschäftspartnern und Beschäftigten der Auftraggeberin lauten wie folgt:

- Stammdaten
- Kontaktdaten
- Vertragsdaten
- E-Commerce-Daten
- Vertragssteuerungsdaten
- Protokolldaten

2.3 Kategorien betroffener Personen

Die Kategorien der durch den Umgang mit ihren Daten im Rahmen dieser Vereinbarung Betroffenen umfasst:

- Kunden und potentielle Kunden der Auftraggeberin (Endverbraucher);
- Beschäftigte, Lieferanten und Geschäftspartner der Auftraggeberin.

Soweit im Hinblick auf die Aufzählung unter 2.2 und 2.3. Anpassungsbedarf besteht, werden die Parteien dies in einem Anhang zu diesem Auftrag regeln.

3. Technisch-organisatorische Maßnahmen

3.1 Die Auftragnehmerin gestaltet die innerbetriebliche Organisation in der Weise, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Die Auftragnehmerin hat die Sicherheit gem. Art. 28 Abs. 3 lit. c. sowie gem. Art. 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. Die Auftragnehmerin trifft hierzu insbesondere die in der **Anlage 1** definierten technisch-organisatorischen Maßnahmen zur angemessenen Sicherung der personenbezogenen Daten vor Missbrauch und Verlust.

3.2 Die Parteien sind sich einig, dass die technischen und organisatorischen Maßnahmen dem technischen Fortschritt und der Weiterentwicklung unterliegen. Insoweit ist es der Auftragnehmerin gestattet, alternative adäquate Maßnahmen umzusetzen. Sie muss die Auftraggeberin hierüber zeitnah informieren und sicherstellen, dass das Sicherheitsniveau der festgelegten Maßnahme nicht unterschritten wird. Wesentliche Änderungen sind mit der Auftraggeberin vorab abzustimmen und von der Auftragnehmerin zu dokumentieren.

3.3. Die Auftraggeberin stimmt zu, dass zum Zwecke der Vertragserfüllung die Verarbeitung in Privatwohnungen der Mitarbeiter der Auftragnehmerin oder im Rahmen von Telearbeit erfolgen darf, soweit dies erforderlich ist. Die Auftragnehmerin stellt sicher, dass bei in der Privatwohnung oder in Form von Telearbeit erbrachten Diensten oder Arbeiten ausschließlich verschlüsselte Systeme der Auftragnehmerin genutzt werden (VPN-Verschlüsselung etc.).

4. Berichtigung, Einschränkung und Löschung von Daten

4.1 Die Rechte der durch den Datenumgang bei der Auftragnehmerin betroffenen Personen insbesondere auf Berichtigung, Einschränkung und Löschung sind gegenüber der Auftraggeberin geltend zu machen. Sie ist allein verantwortlich für die Wahrung dieser Rechte. Die Auftragnehmerin darf personenbezogene Daten nicht eigenmächtig, sondern nur nach dokumentierter Weisung der Auftraggeberin berichtigen, löschen oder deren Verarbeitung einschränken. Die Auftragnehmerin hat entsprechende Weisungen der Auftraggeberin unverzüglich umzusetzen, sofern nicht eine gesetzliche Verpflichtung der Auftragnehmerin zur Speicherung der personenbezogenen Daten besteht.

4.2 Die Auftragnehmerin ist verpflichtet, im Rahmen ihrer Tätigkeit für die Auftraggeberin an sie gerichtete Ersuchen Betroffener oder Aufsichtsbehörden zur sachgerechten Bearbeitung unverzüglich an die Auftraggeberin weiterzuleiten. Sie ist nicht verpflichtet, diese Ersuchen ohne Abstimmung mit der Auftraggeberin selbständig zu bescheiden.

4.3 Die Auftragnehmerin wird die Auftraggeberin auf deren Aufforderung nach besten Kräften bei der Erfüllung der Rechte der betroffenen Personen unterstützen, insb. im Hinblick auf das Recht auf Vergessenwerden und das Recht auf Datenübertragbarkeit. Die Berichtigung, Einschränkung und Löschung der betroffenen Daten während der Leistungserbringung erfolgt durch die Auftragnehmerin in Namen der Auftraggeberin.

4.4 Für die Unterstützung der Auftraggeberin bei der Wahrung der Rechte der betroffenen Personen steht der Auftragnehmerin eine Vergütung zu. Diese richtet sich mangels anderweitiger Vereinbarung nach dem Zeitaufwand und den Vergütungssätzen der jeweils aktuellen Preisliste der Auftragnehmerin.

5. Pflichten der Auftragnehmerin

5.1 Die Auftragnehmerin erhebt, verarbeitet und nutzt personenbezogene Daten im Rahmen des Hauptvertrags sowie der speziellen Einzelweisungen der Auftraggeberin.

5.2 Die Auftragnehmerin hat im Zusammenhang mit der Erfüllung der Meldepflicht der Auftraggeberin entsprechend Art. 33 und 34 DS-GVO dieser unverzüglich schriftlich Meldung zu erstatten in allen Fällen, in denen durch sie oder die bei ihr beschäftigten Personen oder Unterauftragsverarbeiter Verstöße gegen Vorschriften zum Schutz personenbezogener Daten der Auftraggeberin oder gegen die in der Vereinbarung getroffenen Festlegungen vorgefallen sind. Dies gilt auch im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten und bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten der Auftraggeberin. Dies gilt weiter auch für den Fall von Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach Art. 58 DS-GVO. Dies gilt auch, soweit eine zuständige Behörde nach Art. 82, 83 DS-GVO bei der Auftragnehmerin ermittelt.

5.3 Die Auftragnehmerin unterrichtet die Auftraggeberin unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diese Vereinbarung beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeiten- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung bei der Auftragnehmerin ermittelt.

5.4 Soweit die Auftraggeberin ihrerseits 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 bei der Auftragnehmerin ausgesetzt ist, unterstützt sie die Auftragnehmerin nach besten Kräften.

5.5 Die Auftragnehmerin wird unter Berücksichtigung der Art der Verarbeitung und der ihr zur Verfügung stehenden Informationen die Auftraggeberin bei der Einhaltung der in den Artikeln 32 bis 36 DS-GVO genannten gesetzlichen Pflichten unterstützen. 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 Verletzungsereignissen ermöglichen,

b. die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an die Auftraggeberin zu melden,

c. die Verpflichtung, der Auftraggeberin im Rahmen ihrer Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihr in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen,

d. die Unterstützung der Auftraggeberin für deren Datenschutz-Folgenabschätzung,

e. die Unterstützung der Auftraggeberin im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

Für Unterstützungsleistungen, die nicht auf ein Fehlverhalten der Auftragnehmerin zurückzuführen sind, kann die Auftragnehmerin eine Vergütung beanspruchen. Diese richtet sich mangels anderweitiger Vereinbarung nach dem Zeitaufwand und den Vergütungssätzen der jeweils aktuellen Preisliste der Auftragnehmerin.

5.6 Die Auftraggeberin ist jederzeit berechtigt, eine Berichtigung, Löschung und Sperrung von personenbezogenen Daten zu verlangen.

5.7 Die Auftragnehmerin dokumentiert die Datenverarbeitung und stellt der Auftraggeberin die

Dokumentation auf Wunsch zur Verfügung.

5.8 Die Auftragnehmerin verpflichtet sich zum Führen eines Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DS-GVO. Das Verzeichnis ist schriftlich oder in einem elektronischen Format zu führen und der Auftraggeberin und/oder dessen Datenschutzbeauftragten jederzeit auf Verlangen vorzulegen.

6. Vertraulichkeit

6.1 Die Auftragnehmerin gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Wahrung des Datengeheimnisses und zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Auftragnehmerin hat die von ihr eingesetzten Mitarbeiter vorsorglich über die Einhaltung des Telekommunikationsgeheimnisses gemäß § 3 TTDSG informiert.

6.2 Es ist sicherzustellen, dass die Verpflichtung zur Wahrung des Datengeheimnisses und zur Vertraulichkeit auch nach Beendigung dieser Vereinbarung fortbesteht.

7. Datenschutzbeauftragter

7.1 Die Auftragnehmerin hat einen Datenschutzbeauftragten bestellt. Zum Zeitpunkt des Vertragsschlusses ist dies:

Herr Dr. Uwe Schläger
datenschutz nord GmbH
E-Mail: Datenschutzbeauftragter@Intershop.de

7.2 Die Auftragnehmerin wird der Auftraggeberin von einer Abberufung bzw. einer Neubestellung des Datenschutzbeauftragten unverzüglich schriftlich in Kenntnis zu setzen.

8. Übermittlung in Nicht-EWR Staaten

8.1 Vorbehaltlich der Regelungen in Ziffer 9.4 , 9.5 und 9.6 ist die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten durch die Auftragnehmerin räumlich auf Mitgliedsstaaten der Europäischen Union oder einen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum beschränkt. Die Übermittlung von personenbezogenen Daten durch die Auftragnehmerin an eine im EWR-Ausland belegene Stelle, d.h. ein Unternehmen mit Sitz außerhalb des EWR, ist nur unter Einhaltung der gesetzlichen Vorschriften, der vorherigen Information der Auftraggeberin und einem nicht erklärten Widerspruch möglich. Ausnahmen hiervon sind nur in den in Art. 28 Abs. 3 lit a. DS-GVO genannten Fällen unter den dort genannten zusätzlichen Voraussetzungen möglich.

8.2 Ist die Auftragnehmerin nach dem anwendbaren Recht eines Mitgliedstaates oder der Europäischen Union verpflichtet, Daten an eine im EWR-Ausland belegene Stelle zu übermitteln, teilt die Auftragnehmerin dies entsprechend ihrer Verpflichtung aus Art. 28 Abs. 3 lit. a DS-GVO der Auftraggeberin vor der Verarbeitung mit, sofern das anwendbare Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

8.3 Auf den Einsatz von Microsoft (Azure Dienste), Atlassian (Cloud Dienstleistung Confluence), New Relic (Monitoring Dienstleistungen) als Subunternehmer im Sinne der Ziffer 9 wird ausdrücklich hingewiesen.

9. Unterauftragsverhältnisse

9.1 Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die die Auftragnehmerin bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Hierzu zählen z.B. Telekommunikationsdienstleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Die Auftragnehmerin ist jedoch verpflichtet, auch bei fremd vergebenen Nebenleistungen angemessene und gesetzkonforme vertragliche

Vereinbarungen zu treffen, um den Schutz und die Sicherheit der Daten der Auftraggeberin zu gewährleisten.

9.2 Die Auftragnehmerin darf Unterauftragnehmer (weitere Auftragsverarbeiter) beauftragen, bestimmte oder unterstützende Dienstleistungen für die Auftragnehmerin zu erbringen.

Die Auftraggeberin ist damit einverstanden, dass die Auftragnehmerin zur Erfüllung ihrer vertraglich vereinbarten Leistungen verbundene Unternehmen der Auftragnehmerin zur Leistungserfüllung heranzieht bzw. andere dritte Unternehmen mit Leistungen unterbeauftragt, wenn die Auftragnehmerin mit dem Unterauftragnehmer eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO schließt, deren Schutzniveau mindestens demjenigen dieses Auftrags entspricht. Die vorgenannten Autorisierungen stellen die vorherige allgemeine schriftliche Zustimmung der Auftraggeberin zur Untervergabe der Verarbeitung von Kundendaten und personenbezogenen Daten durch die Auftragnehmerin dar, wenn eine solche allgemeine Zustimmung nach den Standardvertragsklauseln oder den Bestimmungen der DS-GVO erforderlich ist.

9.3 Die Auftragnehmerin beauftragt gelegentlich möglicherweise neue Unterauftragnehmer. Über jeden neuen Unterauftragnehmer informiert die Auftragnehmerin die Auftraggeberin mindestens 1 Monat bevor dieser Zugriff auf Kundendaten erhält (durch Bereitstellung eines Mechanismus zur Benachrichtigung der Auftraggeberin über diese Aktualisierung).

Die Auftraggeberin kann der Verwendung eines neuen Unterauftragnehmers durch die Auftragnehmerin in angemessener Weise widersprechen (z. B. wenn die Bereitstellung personenbezogener Daten an den Unterauftragnehmer gegen geltende Datenschutzgesetze verstößt oder den Schutz solcher personenbezogenen Daten schwächt), indem sie der Auftragnehmerin unverzüglich schriftlich, spätestens jedoch innerhalb von 14 Kalendertagen, nachdem die Auftraggeberin von einer solchen Änderung Kenntnis erlangt hat, entsprechend benachrichtigt. Diese Mitteilung muss an die E-Mail Adresse Datenschutzbeauftragter@intershop.de gesendet werden, das Datum enthalten, an dem der Auftraggeber von dem neuen Unterauftragnehmer Kenntnis erlangt hat, und die angemessenen Gründe für den Widerspruch darlegen. Falls die Auftraggeberin entsprechend der vorstehenden Regelung einem neuen Unterauftragnehmer widerspricht, wird die Auftragnehmerin wirtschaftlich angemessene Anstrengungen unternehmen, um der Auftraggeberin eine Änderung der Dienstleistungen von der Auftragnehmerin zur Verfügung zu stellen oder eine wirtschaftlich angemessene Änderung der Konfiguration oder der Nutzung der Dienstleistungen von der Auftragnehmerin empfehlen, um die Verarbeitung personenbezogener Daten durch den widersprochenen neuen Unterauftragnehmer ohne Grund zu vermeiden.

Sollte die Auftragnehmerin nicht in der Lage sein, eine solche Änderung innerhalb einer angemessenen Frist, die 14 Kalendertage ab dem Datum beträgt, an dem die Auftragnehmerin eine schriftliche Benachrichtigung der Auftraggeberin erhalten hat, zur Verfügung zu stellen, steht jeder Partei nur dann ein Recht zu, den Hauptvertrag zu kündigen, sofern die vertraglich aus dem Hauptvertrag geschuldeten Leistungen in ihren wesentlichen Bestandteilen nicht mehr erbracht werden können.

9.4 Microsoft Azure: Die Auftraggeberin gestattet hiermit der Auftragnehmerin die Einschaltung von Microsoft (Microsoft Ireland Operations Ltd., „Microsoft“) unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO als Unterauftragnehmer.

a. Die Auftragnehmerin darf von Microsoft insbesondere Infrastruktur- und Plattformdienstleistungen in Anspruch nehmen, (insgesamt „Microsoft-Dienste“). Derzeit nimmt die Auftragnehmerin die folgenden Dienste von Microsoft in Anspruch: Compute, Network, Storage und zugehörige Development und Operation Tools.

b. Die Nutzung der Microsoft-Dienste erfolgt durch die Auftragnehmerin im Rahmen der Nutzungsbedingungen und Sicherheitsmaßnahmen von Microsoft, die als **Anlage** diesem Vertrag beigefügt sind (Microsoft Bedingungen für Onlinedienste).

c. Microsoft und die von ihr kontrollierten Tochtergesellschaften haben Standard-Vertragsklauseln vereinbart, um ein angemessenes Schutzniveau sicherzustellen. Einzelheiten sind der der Anlage 2 (Microsoft Bedingungen für Onlinedienste und Standardvertragsklauseln) zu entnehmen.

d. Die Auftragnehmerin hat mit Microsoft einen Vertrag geschlossen, der den inhaltlichen Anforderungen an Auftragsverarbeitungsvereinbarungen nach Art. 28 Abs. 3 DS-GVO

genügt. Soweit erforderlich, ermächtigt die Auftraggeberin die Auftragnehmerin, in ihrem Namen mit Microsoft die Geltung der EU-Standardvertragsklauseln zu vereinbaren.

9.5 Atlassian: Die Auftraggeberin gestattet hiermit der Auftragnehmerin die Einschaltung der Atlassian (Atlassian PTY Ltd, Atlassian, Inc., Trello Inc., Dogwood Labs, Inc., OpsGenie, Inc., Agile Craft LLC and Halp Inc., which are all Atlassian entities, „Atlassian“) unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO als Unterauftragnehmer.

a. Die Auftragnehmerin darf von Atlassian insbesondere Cloud-Dienstleistungen für die Nutzung von Confluence, ein Kollaborations-Tool für Wissensmanagement und Projektzusammenarbeit, in Anspruch nehmen (insgesamt „Atlassian-Dienste“). Derzeit nimmt die Auftragnehmerin die folgenden Dienste von Atlassian in Anspruch: Cloud Dienstleistungen für Confluence Kollaborations-Tool für Wissensmanagement und Projektzusammenarbeit.

b. Die Auftragnehmerin hat mit Atlassian einen Vertrag geschlossen, der den inhaltlichen Anforderungen an Auftragsverarbeitungsvereinbarungen nach Art. 28 Abs. 3 DS-GVO genügt. Soweit erforderlich, ermächtigt die Auftraggeberin die Auftragnehmerin, in ihrem Namen mit Atlassian die Geltung der EU-Standardvertragsklauseln zu vereinbaren.

9.6 New Relic: Die Auftraggeberin gestattet hiermit der Auftragnehmerin die Einschaltung von New Relic (New Relic Inc. a Delaware corporation, 188 Spear Street, Suite 1000, San Francisco, CA 94105) unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO als Unterauftragnehmer.

a. Die Auftragnehmerin darf von New Relic insbesondere Monitoring-Dienstleistungen in Anspruch nehmen (insgesamt „New Relic Dienste“). Derzeit nimmt die Auftragnehmerin die folgenden Dienste von New Relic in Anspruch: Monitoring und Log Analysen.

b. Die Auftragnehmerin hat mit New Relic einen Vertrag geschlossen, der den inhaltlichen Anforderungen an Auftragsverarbeitungsvereinbarungen nach Art. 28 Abs. 3 DS-GVO genügt. Soweit erforderlich, ermächtigt die Auftraggeberin die Auftragnehmerin, in ihrem Namen mit New Relic die Geltung der EU-Standardvertragsklauseln zu vereinbaren.

10. Kontrollrechte der Auftraggeberin

10.1 Die Auftraggeberin hat das Recht, vor Beginn der Datenverarbeitung durch die Auftragnehmerin und sodann regelmäßig, auf eigene Kosten eine Auftragskontrolle im Benehmen mit der Auftragnehmerin in Bezug auf die von der Auftragnehmerin vorzunehmenden Datenverarbeitungsprozesse durchzuführen oder durch im Einzelfall von der Auftraggeberin zu benennende Prüfer durchführen zu lassen, vorausgesetzt, die Auftraggeberin bzw. die benannten Prüfer verpflichtet sich zum Abschluss einer Geheimhaltungsvereinbarung gegenüber der Auftragnehmerin bzw. Unterauftragnehmern, es sei denn, die benannten Prüfer unterliegen einer beruflichen Verschwiegenheitsverpflichtung. Sollte der durch die Auftraggeberin bestellte Prüfer in einem Wettbewerbsverhältnis zur Auftragnehmerin stehen, hat die Auftragnehmerin gegen diesen ein Einspruchsrecht. Die Auftragsgeberin hat das Recht, sich durch Stichprobenkontrollen nach rechtzeitiger vorheriger Anmeldung (in der Regel mindestens 2 Wochen vorher) zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Einhaltung dieser Vereinbarung durch die Auftragnehmerin in ihrem Geschäftsbetrieb zu überzeugen. Einer vorherigen Anmeldung bedarf es in Fällen, bei denen der begründete Verdacht von Datenschutzverletzungen oder anderen Störungen besteht, nicht. Die Auftraggeberin darf in der Regel eine Kontrolle pro Kalenderjahr durchführen. Hiervon unbenommen ist das Recht der Auftraggeberin, weitere Kontrollen im Fall von besonderen Vorkommnissen durchzuführen. Die Auftragnehmerin verpflichtet sich, der Auftraggeberin auf Anforderung die zur Wahrung ihrer Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen, soweit dies möglich ist.

10.2 Die Auftragnehmerin stellt sicher, dass die Auftraggeberin sich von der Einhaltung der Pflichten der Auftragnehmerin nach Art. 28 DS-GVO überzeugen kann. Auf Anfrage weist die Auftragnehmerin die Implementierung der getroffenen technischen und organisatorischen Maßnahmen nach.

10.3 Die Auftragnehmerin verpflichtet sich, der Auftraggeberin auf Anforderung die zur Wahrung ihrer bei der Verarbeitung der oben genannten Daten bestehenden Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und Nachweise zu führen, soweit vorhanden. Der Nachweis der Umsetzung geeigneter Maßnahmen kann auch durch Vorlage aktueller Testate sowie von Berichten unabhängiger Prüfer (Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, etc.) erbracht werden. Dies gilt auch, soweit die Auftragnehmerin die Kontrolle ihrer Unterauftragnehmer für die Auftraggeberin durchführt.

10.4. Für die durch Subauftragnehmer erbrachten Leistungen gelten die Regelungen der Ziffer 9.

10.5 Stellt die Auftraggeberin im Rahmen der Auftragskontrolle Mängel bei der Einhaltung der technischen und organisatorischen Maßnahmen fest, beseitigt die Auftragnehmerin die Mängel unverzüglich. Die zur Mangelbeseitigung erforderlichen Kosten trägt die Auftragnehmerin.

11. Weisungsbefugnisse der Auftraggeberin

11.1 Die Auftragnehmerin erhebt, verarbeitet und nutzt personenbezogene Daten im Auftrag und auf Weisung der Auftraggeberin zur Erfüllung der ihr aufgrund des Hauptvertrags obliegenden Leistungspflichten. Die Auftraggeberin ist im Rahmen dieser Vereinbarung 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 („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DS-GVO).

11.2 Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen. Die Auftraggeberin ist berechtigt, Weisungen über Art und Umfang der Datenverarbeitung im Hinblick auf die Umsetzung von Datenschutzanforderungen auch während des Auftrages (Einzelweisungen) zu erteilen. Die Weisungen bedürfen in jedem Fall der Textform und dürfen der vertraglich vereinbarten Leistungserbringung durch die Auftragnehmerin nicht zu wider laufen. Einzelweisungen, die von den Festlegungen dieses Auftrags abweichen oder zusätzlichen Anforderungen enthalten, bedürfen einer vorherigen Zustimmung der Auftragnehmerin.

11.3 Weisungen der Auftraggeberin sind von der Auftragnehmerin zu dokumentieren.

11.4 Ist die Auftragnehmerin der Ansicht, eine Weisung der Auftraggeberin verstoße gegen die DS-GVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten, hat sie die Auftraggeberin schriftlich darauf hinzuweisen. Die Auftragnehmerin ist in diesen Fällen berechtigt, die Durchführung der Weisung auszusetzen, bis die Auftraggeberin die Weisung bestätigt oder abändert. Eine Rechtsberatung und/oder juristische Recherche durch die Auftragnehmerin ist jedoch nicht geschuldet.

11.5 Die Auftragnehmerin verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen der Auftraggeberin nicht erstellt. Hiervon ausgenommen sind Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Leistungserbringung erforderlich sind.

12. Löschung und Rückgabe personenbezogener Daten

12.1 Mit Ende des Hauptvertrags gibt die Auftragnehmerin die betroffenen Daten an die Auftraggeberin heraus oder löscht sie auf Wunsch nach dem Stand der Technik, soweit nicht im Einzelfall etwas Abweichendes vereinbart wurde oder die Auftragnehmerin gesetzlich zur weiteren Aufbewahrung verpflichtet ist; entsprechende Daten sind dann jedoch zu sperren und gemäß den Bestimmungen dieser Vereinbarung zu verwahren. In jedem Fall werden die Daten spätestens 90 Tage nach Ablauf oder Kündigung des Hauptvertrages gelöscht. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

12.2 Zu einem Datenträgeraustausch zwischen den Beteiligten dieser Vereinbarung kommt es nicht. Insoweit ist eine Rückgabe hier nicht zu regeln. Anderenfalls werden sich die Parteien gesondert abstimmen.

12.3 Die Auftragnehmerin hat kein Zurückbehaltungsrecht an den vertragsgegenständlichen Daten.

12.4 Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch die Auftragnehmerin entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Sie kann sie zu ihrer Entlastung bei Vertragsende der

Auftraggeberin übergeben. Die Auftragnehmerin wird auch über das Ende des Auftrages hinaus Stillschweigen über die Daten der Auftraggeberin bewahren.

13. Haftung

Eine zwischen den Parteien im Leistungsvertrag (Hauptvertrag) vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, außer soweit ausdrücklich etwas anderes vereinbart ist. Im Übrigen gilt Art. 82 DSG-VO.

14 Schlussbestimmungen

14.1 Die Parteien sind sich darüber einig, dass diese Auftragsverarbeitungsvereinbarung alle früheren Vereinbarungen zwischen den Parteien über die Auftragsverarbeitung zwischen den Parteien ersetzt.

14.2 Sollten die Daten der Auftraggeberin bei der Auftragnehmerin durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat die Auftragnehmerin die Auftraggeberin unverzüglich darüber zu informieren. Die Auftragnehmerin wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich bei der Auftraggeberin als „Verantwortlicher“ im Sinne der DS-GVO liegen.

14.3 Soweit im Rahmen dieses Auftrages, insbesondere im Zusammenhang mit Unterstützungshandlungen, der Herausgabe oder der Löschung von Daten Kosten anfallen, trägt diese die Auftraggeberin.

14.4 Bei Änderungen der tatsächlichen Ausgestaltung der Leistungsbeziehungen zwischen den Parteien werden die Parteien die Anlagen entsprechend anpassen und einvernehmlich austauschen. Mit Unterzeichnung der geänderten Anlage durch die Parteien wird diese wirksam und ersetzt insoweit die bislang geltende Anlage.

14.5 Änderungen oder Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt für die Änderung oder Aufhebung des vorstehenden Schriftformerfordernisses entsprechend.

14. 6 Änderungen in der Person oder der Zuständigkeit der Weisungsberechtigten sind der jeweils anderen Partei unverzüglich schriftlich mitzuteilen.

14.7 Es gilt deutsches Recht, Gerichtsstand ist Jena.

14.8 Dieser Vertrag hat folgende Bestandteile:

- Vorliegender Vertragstext
- Anlage 1 „Technisch-organisatorische Maßnahmen (TOM)“
- Anlage 2 Microsoft Bedingungen für Onlinedienste und Standardvertragsklauseln (für Global Cloud)
- Hauptvertrag

Im Falle von Unklarheiten und/oder Widersprüchen zwischen den einzelnen Dokumenten oder Vertragsbestandteilen gelten die Bestandteile in absteigender Reihenfolge.

14.9 Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der Vereinbarung im Übrigen unberührt. An die Stelle der unwirksamen Bestimmung tritt eine wirksame Regelung, die in ihrem wirtschaftlichen Gehalt der unwirksamen Bestimmung möglichst nahekommt. Entsprechendes gilt im Falle von Regelungslücken.

Anlage 1: Technisch-organisatorische Maßnahmen gem. Art. 32 DS-GVO

Anlage 2: Microsoft Bedingungen für Onlinedienste und Standardvertragsklauseln

Anlage 1 Technisch-organisatorische Maßnahmen (TOM)

Gem. Art. 32 Abs. 1 Verantwortliche (Art. 30 Abs. 1 lit. g) und Auftragsverarbeiter (Art. 30 Abs. 2 lit. d) gem. Art. 32 DS-GVO

Diese Anlage beschreibt die technischen und organisatorischen Sicherheitsmaßnahmen in der Betriebsstätte Jena von INTERSHOP. Für die Speicherung der Daten im Rechenzentrum gilt Ziffer 9.4.

Zugangskontrolle

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte:

- Aufenthalt von Besuchern nur in Anwesenheit von Mitarbeitern
- Authentifikation durch Benutzername und Passwort bzw. Schlüssel
- Automatische Türschließung und akustische Offen-Meldung bei Eingangstüren
- Einbruchhemmende Fenster
- Einsatz von Firewalls
- Einsatz von VPN
- Enge Begrenzung und Einschränkung der befugten Nutzer (Need-to-know und Least-privilege Prinzip)
- Festlegung der zutrittsberechtigten Personen
- getrennte Systeme je Kunde (virtual private cloud)
- Passwortrichtlinie
- Richtlinien zum Datenschutz und zur IT-Sicherheit
- Temporäre Sperrung des Zugangs (z.B. bei mehr als drei erfolglosen Anmeldeversuchen)
- Unique User IDs, die Anmeldung mit einem allg. Administrator-Account ist eingeschränkt
- Unterteilung in Sicherheitszonen, beschränkte Bereiche
- Wartungsarbeiten durch externe Dienstleister nur nach vorhergehender Anmeldung
- Zentrale Benutzerverwaltung inkl. Rollen- und Rechtesystem
- Zentrale Schlüsselverwaltung

Datenträgerkontrolle

Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern:

- Abgabe von Datenträgern nur an autorisierte Personen
- Authentifikation durch Benutzername und Passwort bzw. Schlüssel
- Enge Begrenzung und Einschränkung der befugten Nutzer (Need-to-know und Least-privilege Prinzip)
- Identifikation und Berechtigungsprüfung der Benutzer
- Inventarisierung von Datenträgern
- Ordnungsgemäße Vernichtung von Datenträgern und datenschutzgerechte Datenträgerentsorgung
- Organisatorische Trennung von Entwicklung, Betrieb und Operativer Bereich
- Richtlinien zum Datenschutz und zur IT-Sicherheit
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Überprüfung der Lagerung von Datenträgern

Speicherkontrolle

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten:

- Enge Begrenzung und Einschränkung der befugten Nutzer (Need-to-know und Least-privilege Prinzip)
- Identifikation und Berechtigungsprüfung der Benutzer
- Ordnungsgemäße Vernichtung von Datenträgern und datenschutzgerechte Datenträgerentsorgung
- Richtlinien zum Datenschutz und zur IT-Sicherheit
- Verschlüsselung von mobilen Datenträgern

Benutzerkontrolle

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte:

- Authentifikation durch Benutzername & Passwort bzw. Schlüssel
- Enge Begrenzung und Einschränkung der befugten Nutzer (Need-to-know und Least-privilege Prinzip)
- Netzwerkszugriffkontrolle
- Richtlinien zum Datenschutz und zur IT-Sicherheit
- Unique User IDs, die Anmeldung mit einem allg. Administrator-Account ist eingeschränkt
- Zentrale Benutzerverwaltung inkl. Rollen- und Rechtesystem

Zugriffskontrolle

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben:

- Abgabe von Datenträgern nur an autorisierte Personen
- Authentifikation durch Benutzername & Passwort bzw. Schlüssel
- Einsatz von Virenscannern
- Enge Begrenzung und Einschränkung der befugten Nutzer (Need-to-know und Least-privilege Prinzip)
- getrennte Systeme je Kunde (virtual private cloud)
- Identifikation und Berechtigungsprüfung der Benutzer
- Ordnungsgemäße Vernichtung von Datenträgern und datenschutzgerechte Datenträgerentsorgung
- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Richtlinien zum Datenschutz und zur IT-Sicherheit
- Unique User IDs, die Anmeldung mit einem allg. Administrator-Account ist eingeschränkt
- Zentrale Schlüsselverwaltung

Übertragungskontrolle

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können:

- Einsatz von E-Mail Verschlüsselung an relevanten Stellen
- Einsatz von VPN
- Protokollierung von Übertragungen
- Richtlinien zum Datenschutz und zur IT-Sicherheit
- Schulung und Sensibilisierung der Mitarbeiter

Eingabekontrolle

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind:

- Identifikation und Berechtigungsprüfung der Benutzer

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Richtlinien zum Datenschutz und zur IT-Sicherheit
- Unique User IDs, die Anmeldung mit einem allg. Administrator-Account ist eingeschränkt

Transportkontrolle

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden:

- Abgabe von Datenträgern nur an autorisierte Personen
- Einsatz von E-Mail Verschlüsselung an relevanten Stellen
- Einsatz von VPN
- Richtlinien zum Datenschutz und zur IT-Sicherheit

Wiederherstellbarkeit

Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können:

- Redundante Auslegung der produktiven Datenbank
- Regelmäßige Replikation der Datenbank (mehrfach innerhalb einer Stunde)
- Richtlinien zum Datenschutz und zur IT-Sicherheit
- Stichprobenartige Restoretests
- Tägliches Backup der Datenbank

Zuverlässigkeit

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden:

- Aktives Update- und Patchmanagement
- Proaktives Monitoring der Kundenumgebung
- Richtlinien zum Datenschutz und zur IT-Sicherheit
- Stichprobenartige Restoretests

Datenintegrität

Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können:

- Aktives Update- und Patchmanagement
- Datenschutzmanagement-System (interne Audits, Risikomanagement)
- getrennte Systeme je Kunde (virtual private cloud)
- Ordnungsgemäße Vernichtung von Datenträgern und datenschutzgerechte Datenträgerentsorgung
- Regelmäßige Replikation der Datenbank (mehrfach innerhalb einer Stunde)
- Richtlinien zum Datenschutz und zur IT-Sicherheit
- Schulung und Sensibilisierung der Mitarbeiter
- Stichprobenartige Restoretests
- Tägliches Backup der Datenbank

Auftragskontrolle

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

- Auswahl von Subauftragnehmers unter Sorgfaltsgesichtspunkten insbesondere hinsichtlich Informationssicherheit
- Kontrollrechte
- Richtlinien zum Datenschutz und zur IT-Sicherheit
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Verpflichtung zur Einhaltung datenschutzrechtlicher Bestimmungen der Beschäftigten

Verfügbarkeitskontrolle

Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind:

- Aktives Update- und Patchmanagement
- Einsatz von Firewalls
- Einsatz von Load Balancer
- Einsatz von Virenscannern
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in den Räumen
- Gaslöschanlage
- Klimatisierung
- Rauchverbot
- Regelmäßige Replikation der Datenbank (mehrfach innerhalb einer Stunde)
- Richtlinien zum Datenschutz und zur IT-Sicherheit
- Tägliches Backup der Datenbank
- Umfassendes System Monitoring
- Unterbrechungsfreie Stromversorgung (USV)

Trennbarkeit

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können:

- Einsatz von Firewalls
- getrennte Systeme je Kunde (virtual private cloud)
- Organisatorische Trennung von Entwicklung, Betrieb und Operativer Bereich
- Richtlinien zum Datenschutz und zur IT-Sicherheit
- Trennung von Test- und Produktivsystem
- Unterteilung in Sicherheitszonen, beschränkte Bereiche
- Zentrale Benutzerverwaltung inkl. Rollen- und Rechtesystem

Vertraulichkeit

Schutz vor unbefugter Kenntnisnahme der Daten:

- Pseudonymisierung von personenbezogenen Daten im Rahmen von Tests auf nicht-produktiven Kundensystemen (Pre-Production, Integration, Development)
- Richtlinien zum Datenschutz und zur IT-Sicherheit
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Verschlüsselte Übertragung von personenbezogenen Daten außerhalb der Kundenumgebung

Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

- Datenschutzmanagement-System (interne Audits, Risikomanagement)
- Incident-Management

Anlage 2: Microsoft Bedingungen für Onlinedienste und Standardvertragsklauseln

Die Nutzung der Microsoft-Dienste erfolgt durch die Auftragnehmerin im Rahmen der Nutzungsbedingungen und Sicherheitsmaßnahmen von Microsoft, die unter folgenden Links zu finden sind:

- https://www.microsoft.com/licensing/terms/product/ForOnlineServices/EAEAS und
- https://www.microsoft.com/licensing/terms/product/PrivacyandSecurityTerms/EAEAS.