Vertrag über die Erhebung, Verarbeitung personenbezogener Daten im Auftrag Art. 28 DSGVO („AVV“) für den Einsatz der

Remoteunterstützung

zwischen

…

…

(Verantwortlicher)

und der

Haufe Service Center GmbH

Munzinger Straße 9

79111 Freiburg

(Auftragsverarbeiter)

1. Gegenstand und Dauer des Auftrags

1.1 Gegenstand des Auftrags

Der Gegenstand dieses Vertrages ergibt sich aus dem Lizenzvertrag, auf den hier verwiesen wird (im Weiteren „Lizenzvertrag“). Dabei handelt es sich um die Verarbeitung personenbezogener Daten (im Weiteren „Daten“) durch den Auftragsverarbeiter für den Verantwortlichen im Zusammenhang mit der Nutzung der:

Remoteunterstützung

1.2 Dauer der Vereinbarung

Die Dauer dieses Auftrages (Laufzeit) entspricht der Laufzeit des Supportvorgangs.

2. Konkretisierung des Auftragsinhalts

2.1 Art und Zweck der vorgesehenen Verarbeitung von Daten

Im Supportfall ist es dem Auftragsverarbeiter möglich sich unter direkter/aktiver Mitwirkung auf einen Rechner/Server des Verantwortlichen mit Sicht,- oder Steuerungsrechten (z.B. zur Anpassung von produktspezifischen Systemeinstellungen) zu verbinden. Bei Bedarf dürfen für zusätzliche Analysezwecke nach Rücksprache mit dem Verantwortlichen während der Remotesitzung ein Screenshot vom Bildschirm gemacht oder Dateien mit Belegdaten heruntergeladen werden. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union, in einem anderen Vertragsstaat des Abkommens über den europäischen Vertragsraum (Beschluss 94/1/EG) oder den USA statt. Jede Verlagerung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Das angemessene Schutzniveau in den USA wird hergestellt durch Standarddatenschutzklauseln „EU-Model Clauses“ (Art. 46 Abs. 2 litt. c und d DSGVO).

2.2 Art der Daten

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

- Namen der Kunden des Auftraggebers,
- Namen von Beschäftigten des Auftraggebers,
- Software-Applikationsdaten der Produkte der Haufe Group (z.B. Adressdaten, Rechnungsbeträge, Skontobeträge, Bankdaten, Lohnabrechnungsdaten, Buchhaltungsdaten, Warenwirtschaftsdaten),
- Bildschirminhalt (Live-Desktop) des Verantwortlichen
- IP-Adresse.

2.3 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden des Auftraggebers
- Beschäftigte des Auftraggebers

3. Technische und organisatorische Maßnahmen

3.1 Der Auftragsverarbeiter 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 Verantwortlichen in **Anlage 2** zur Prüfung zu übergeben. Bei Akzeptanz durch den Verantwortlichen werden die dokumentierten Maßnahmen Grundlage des Auftrags.

3.2 Der Auftragsverarbeiter hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO 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 DSGVO zu berücksichtigen (Einzelheiten in **Anlage 2**).

3.3 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen werden unter https://download.lexware.de/pub/dsgvo_avv/AVVCatalog.html oder durch Zustimmung im Produkt dokumentiert.

4. Berichtigung, Einschränkung und Löschung von Daten

4.1 Der Auftragsverarbeiter darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Verantwortlichen berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten. Screenshots und PDFs oder Dateien, die für zusätzliche Analysezwecke vom Verantwortlichen im Rahmen des Remotesupportvorgangs bereitgestellt worden sind, werden spätestens 24 Monate nach Abschluss des Vorgangs automatisiert gelöscht.

4.2 Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Verantwortlichen unmittelbar durch den Auftragsverarbeiter sicherzustellen.

4.3 Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Verantwortliche verantwortlich. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung seiner Pflichten gegenüber den Betroffenen (Art. 12-23 DSGVO).

5. Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

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

5.1 Der Auftragsverarbeiter hat einen Datenschutzbeauftragten, schriftlich bestellt, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt:

Herr Raik Mickler
Konzerndatenschutzbeauftragter
E-Mail: dsb@haufe-lexware.com
Telefon: +49 (0) 761/898-0

5.2 Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragsverarbeiter 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 Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Verantwortlichen verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

5.3 Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO (Einzelheiten in **Anlage 2**).

5.4 Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

5.5 Die unverzügliche Information des Verantwortlichen 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 Auftragsverarbeiter ermittelt.

5.6 Soweit der Verantwortliche 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 Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen.

5.7 Der Auftragsverarbeiter 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.

5.8 Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Verantwortlichen im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

6.1 Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in **Anlage 1** genannten Unterauftragsverarbeiter durchgeführt. Der Auftragsverarbeiter ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Unterauftragsverarbeitern befugt, soweit er den Verantwortlichen hiervon unverzüglich in Kenntnis setzt und der Verantwortliche nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragsverarbeiter schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird. Im Falle des Einspruchs des Verantwortlichen steht beiden Parteien ein außerordentliches Kündigungsrecht hinsichtlich dieser Vereinbarung zu.

6.2 Der Auftragsverarbeiter ist verpflichtet, Unterauftragsverarbeiter sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragsverarbeiter hat bei der Einschaltung von Unterauftragsverarbeitern diese entsprechend den Regelungen dieser Vereinbarung zur Einhaltung der Anforderungen aus Art. 28 Abs. 3 und Abs. 4 DSGVO zu verpflichten. Sofern eine Einbeziehung von Unterauftragsverarbeitern in einem Drittland erfolgen soll, hat der Auftragsverarbeiter sicherzustellen, dass beim jeweiligen Unterauftragsverarbeitern ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragsverarbeiter wird dem Verantwortlichen auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Unterauftragsverarbeitern nachweisen. Ein Unterauftragsverarbeitungsverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragsverarbeiter 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 Auftragsverarbeiter für den Verantwortlichen erbringt und Bewachungsdienste.

6.3 Dem Verantwortlichen sind vor Beginn der Verarbeitung die Unterauftragnehmer nach **Anlage 1** mitgeteilt worden.

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

6.5 Der Auftragsverarbeiter hat die Einhaltung dieser Pflichten des Unterauftragsverarbeiters regelmäßig zu überprüfen.

7. Kontrollrechte des Verantwortlichen

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

7.2 Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf dessen mündliche, schriftliche oder elektronische Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragsverarbeiters erforderlich sind.

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

7.4 Der Auftragsverarbeiter weist dem Verantwortlichen die Verpflichtung der Mitarbeiter auf das Datengeheimnis auf Verlangen nach.

7.5 Der Verantwortliche vergütet dem Auftragsverarbeiter den Aufwand, der ihm im Rahmen der Kontrolle entsteht.

8. Mitteilung bei Verstößen des Auftragsverarbeiters

8.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.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;
- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Verantwortlichen zu melden;
- die Verpflichtung, den Verantwortlichen im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;
- die Unterstützung des Verantwortlichen für dessen Datenschutz-Folgenabschätzung;
- die Unterstützung des Verantwortlichen im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

9. Weisungsbefugnis des Verantwortlichen

9.1 Der Auftragsverarbeiter darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Verantwortlichen erheben, nutzen oder auf sonstige Weise verarbeiten.

9.2 Die Weisungen des Verantwortlichen werden anfänglich durch diesen Vertrag festgelegt und können vom Verantwortlichen danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Verantwortliche ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten.

9.3 Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Verantwortlichen an den Auftragsverarbeiter entstehen, bleiben unberührt.

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

10. Löschung und Rückgabe von personenbezogenen Daten

10.1 Kopien oder Duplikate der Daten werden ohne Wissen des Verantwortlichen 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.

10.2 Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Verantwortlichen – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, und nicht Daten in der vertragsgegenständlicher Software sind, dem Verantwortlichen auszuhändigen oder datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Für die Daten in der vertragsgegenständlichen Software gilt Ziffer 4.2.

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

11. Haftung

11.1 Die Parteien haften gegenüber Dritten nach Art. 82 DSGVO.

11.2 Der Innenausgleich zwischen dem Verantwortlichen und dem Auftragsverarbeiter richtet sich nach Art. 82 Abs. 5 DSGVO.

12. Außerordentliches Kündigungsrecht

12.1 Der Verantwortliche kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragsverarbeiter seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DSGVO oder sonstige anwendbare Datenschutzvorschriften vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Verantwortlichen nicht ausführen kann oder will oder der Auftragsverarbeiter sich den Kontrollrechten des Verantwortlichen auf vertragswidrige Weise widersetzt. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art.
28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

13. Schlussbestimmungen

13.1 Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragsverarbeiter i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

13.2 Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform oder der Textform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

13.3 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.

13.4 Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Freiburg im Breisgau.

13.5 Diese Vereinbarung zur Auftragsverarbeitung ersetzt alle bisherigen Vereinbarungen gem. Art. 28 DSGVO oder § 11 BDSG (alt) zu der in Punkt 1.1 genannten Software und tritt mit Unterzeichnung des Lizenzvertrags (Hauptvertrag) in Kraft.

Anlagen:

Anlage 1 – Genehmigte Unterauftragsverarbeiter

Anlage 2 – Technisch-organisatorische Maßnahmen

Anlage 1: Genehmigte Unterauftragsverarbeiter

Der Verantwortliche stimmt der Beauftragung der nachfolgenden Unterauftragsverarbeiter zu:

Unterauftragsverarbeiter (Firma, Anschrift)	Leistung
Haufe Group	
Haufe-Lexware Services GmbH & Co. KG Munzingerstr. 9 79111 Freiburg – Germany *(Ein Unternehmen der Haufe Group)*	Marketing, Vertriebsdienstleistungen, Supporttätigkeiten
Haufe-Lexware GmbH & Co. KG Munzingerstr. 9 79111 Freiburg – Germany *(Ein Unternehmen der Haufe Group)*	Softwareentwicklung, Softwaretest, Softwaresupport, Produktmanagement, Marketing
Haufe Group Romania SRL Piata Consiliul Europei nr. 2, UBC0, et. 15 Timisoara 300627, Timis – Romania *(Ein Unternehmen der Haufe Group)*	Softwareentwicklung, Softwaretest, Softwaresupport
Weitere Unterauftragsverarbeiter	
Baden IT GmbH Tullastr. 61 79108 Freiburg - Germany	Hosting
Wolters Kluwer Software und Service GmbH Stuttgarter Str. 35 71638 Ludwigsburg – Germany	Supporttätigkeiten
Wolters Kluwer Deutschland GmbH Akademische Arbeitsgemeinschaft Postfach 10 01 61 68001 Mannheim – Germany	Supporttätigkeiten
Majorel Cottbus GmbH Am Seegraben 21 03051 Cottbus – Germany	Supporttätigkeiten
Avedo II GmbH Wilhelm-Becker-Str. 11a 75179 Pforzheim – Germany	Supporttätigkeiten
VALUE5 Dialogmanagement GmbH Charlottenstr. 16 10117 Berlin – Germany	Supporttätigkeiten

Auxilium Communications GmbH Eiswerderstraße 20a 13585 Berlin – Germany	Supporttätigkeiten
AMEVIDA Freiburg GmbH Zinkmattenstr. 6a 79108 Freiburg – Germany	Supporttätigkeiten
Selbstständiger Datenverarbeiter	
GoTo Technologies Ireland Unlimited Company The Reflector Building 10 Hanover Quay Dublin 2, D02R573, Ireland	Dienstleister für Remotesupport-Lösung (End-to-End-Verschlüsselung)

Anlage 2: Technisch-organisatorische Maßnahmen

1. Haufe-Lexware Services GmbH & Co. KG, Haufe-Lexware GmbH & Co. KG, Haufe Service Center GmbH, Haufe-Lexware SRL

1.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1.1 Zutrittskontrolle Gebäude allgemein:

- Schlüssel-/Chipkartenregelung
- Tragen von Firmenausweisen
- Videoüberwachung

Rechenzentrumsräume zusätzlich:

- verschlossene Türen in Rechenzentren, keine Fenster
- Aufenthalt von Besuchern nur in Anwesenheit von Mitarbeitern
- Alarmanlage

1.1.2 Zugangskontrolle

- Benutzername und Passwort
- Vorgaben per Passwortrichtlinie
- Protokollierung aller erfolgreichen und erfolglosen Logins
- Einsatz von Spamfilter und Virenscanner (Exchange, Gateway)

1.1.3 Zugriffskontrolle

- Zuordnung von Zugriffsrechten zu jedem Benutzer
- Einrichten von Administrationsrechten
- Verschlüsselung von Funknetzen (WLAN)
- Berechtigungskonzept

1.1.4 Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, über die Zuordnung der individuellen ID, auf die nur der jeweilige Bearbeiter Zugriffsrechte hat.

1.1.5 Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a EU-DSGVO, Art. 25 Abs. 1 EU-DSGVO)

Im Supportfall ist es dem Verantwortlichen möglich eine Datensicherung verschlüsselt auf einen Server des Subdienstleister Baden-IT des Auftragnehmers zu übertragen. Die Daten sind grundsätzlich nur für den Ticket-Bearbeiter beim Auftragnehmer einsehbar, der die Datensicherung analysiert/repariert und als Download für den Kunden verschlüsselt bereitstellt. Zusätzlich wird der Download durch eine nur dem Kunden bekannte PIN abgesichert. (Dieser legt die PIN beim Upload selbst fest.)

1.2 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

1.2.1 Weitergabekontrolle

- Einrichtung einer Standleitung
- Verschlüsselung von Funknetzen (WLAN)
- Dokumentation der Datenempfänger, der übermittelten Daten und der Zeitspanne für die geplante Überlassung
- Protokollierung der Abrufe und Übermittlungsaktivitäten
- Verwenden von VPN-Verbindungen

1.2.2 Eingabekontrolle

- Protokollierung

1.3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.3.1 Verfügbarkeitskontrolle und Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO);

- Sicherungskopien und Backups
- Konzept zur Rekonstruktion der Datenbestände
- Notfallplan
- Einsatz von gespiegelten Festplatten und RAID-Systemen
- Unterbrechungsfreie Stromversorgung (USV) und Notstromaggregat
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in den Räumen
- Alarmanlage zur Diebstahlsicherung
- Schutz-Steckdosenleisten (zentral in Grundversorgung)
- Klimaanlage

1.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

1.4.1 Datenschutz-Management und Incident-Response-Management

Die Haufe Group verfügt über ein Incident-Response-Management und über ein Datenschutzmanagementsystem. Mit entsprechender Planung zu Maßnahmen zum Umgang mit Chancen/Risiken und die Ausstattung mit angemessenen Ressourcen, Kompetenzen, Awareness und Kommunikation. Die Überwachung, Messung, Analyse und Bewertung, zusammen mit internen Audits und Managementbewertungen finden zur fortlaufenden Verbesserung des Managementsystems kontinuierlich statt.

1.4.2 Auftragskontrolle

- Verbot, Daten unzulässigerweise zu kopieren
- Klare, eindeutige Weisungen (Arbeitsanweisungen)
- Vergabe von Einzelaufträgen nur über namentlich benannte Ansprechpartner o Vereinbarungen über Art des Datentransfers und deren Dokumentation
- Kontrollrechte durch den Auftraggeber

2. Alle Unterauftragnehmer haben alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen ergriffen.