# Vereinbarung zur

# Auftragsverarbeitung

gemäß Art. 28 DS-GVO

zwischen

Firma: ……..
Straße: ……..
PLZ Ort: ……..
im Folgenden „Kunde“ oder „Verantwortlicher“ genannt

und

Evint GmbH
Ernst-Barlach-Straße 20
36041 Fulda

im Folgenden „Evint GmbH“ oder „Auftragsverarbeiter“ genannt

gemeinsam „Parteien“ genannt.

# 1 Präambel

1. Die Vertragsparteien sind mit der Freischaltung durch die Evint GmbH zur Nutzung des Portals **www.evint.net** und **mein-evint.gbg-ag.com** durch den Kunden ein Auftragsverarbeitungs-verhältnis gemäß EU Datenschutz Grundverordnung (EU-DSGVO) eingegangen. Um die Rechte und Pflichten aus diesem Auftragsverarbeitungsverhältnis gemäß der gesetzlichen Verpflichtung zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.
2. Diese Vereinbarung bezieht sich nur auf die Durchführung der technischen Erhebung, Verarbeitung und Nutzung personenbezogener Daten nach einem vom Kunden vorgegebenen Verfahren und Umfang. Dadurch begründet sich eine Auftragsverarbeitung nach Art. 28 EU-DSGVO.
3. Es gelten die Begrifflichkeiten laut Art. 4 DS-GVO.

# 2 Gegenstand und Dauer der Vereinbarung

1. Gegenstand dieser Vereinbarung ist die Verarbeitung personenbezogener Daten durch die Evint GmbH für den Kunden im Zusammenhang mit der Nutzung des Portals **www.evint.net und mein-evint.gbg-ag.com**.
2. Die Vereinbarung gilt bis zur Beendigung der Inanspruchnahme der Leistungen des Auftragsverarbeiters. Etwaige Sonderkündigungsrechte bleiben davon unberührt. Diese Vereinbarung ersetzt alle bisherigen geschlossenen Vereinbarungen zur Auftragsdaten-verarbeitung.
3. Dies umfasst alle Tätigkeiten, die die Evint GmbH gemäß den EVINT AGB und den vertraglichen Vereinbarungen mit dem Kunden (Bestellungen von Standardprodukten und Verträge über individuelle Leistungen) erbringt und die eine Auftragsverarbeitung darstellen.
4. Bei Widersprüchen zwischen einer Vereinbarung und dieser Vereinbarung zur Auftragsverarbeitung geht diese Vereinbarung zur Auftragsverarbeitung vor.

# 3 Konkretisierung der Vereinbarung

## 3.1 Art und Zweck der vorgesehenen Verarbeitung von Daten

1. Inhaltliche Vereinbarungen mit Kunden und deren Anwendern (m/w/d) umfassen die Möglichkeiten des Verantwortlichen zur Nutzung der Funktionen des Portals EVINT.
2. Die Art der Verarbeitung umfasst alle Arten von Verarbeitungen im Sinne der EU-Datenschutz-Grundverordnung (DS-GVO).
3. Die Erbringung der vertraglich vereinbarten Datenverarbeitung hinsichtlich EVINT 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 Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

## 3.2 Art der Daten und Kategorien betroffener Personen

1. Art der personenbezogenen Daten sind alle Arten personenbezogener Daten, die die Evint GmbH im Auftrag des Kunden verarbeitet. Darunter können ggf. auch besondere Kategorien personenbezogener Daten fallen.
2. Hinsichtlich der Verarbeitung von personenbezogenen Daten besonderer Art ist der Kunde verpflichtet, in eigener Verantwortung dafür Sorge zu tragen, dass die hierzu geltenden gesetzlichen Vorgaben eingehalten werden.
3. Kategorien betroffener Personen sind insbesondere:
    1. Beschäftigte und Geschäftspartner/Mandanten des Kunden;
    2. Beschäftigte und Geschäftspartner des Geschäftspartners/Mandanten;
    3. Nutzer einer der Evint GmbH-Leistungen.
4. Ein detaillierter Umfang der einzelnen Leistungen ergibt sich aus den jeweiligen Einzelaufträgen. Die von den Vertragsparteien vereinbarte Auftragsverarbeitung beinhaltet unter anderem:
    1. Pflege und Verwaltung von Arbeitnehmerdaten;
    2. Erfassung und Verarbeitung von Arbeitszeiten und Abwesenheiten;
    3. Erfassung und Verarbeitung von Überlassungsverhältnissen;
    4. Abrechnung von Personalleistungen;
    5. Erfassung qualifiziert signierter Verträge;
    6. Zutrittskontrolle und Verwaltung von Sicherheitsbereichen.
5. Folgenden Datenarten oder -kategorien können dabei Gegenstand der Erhebung, Verarbeitung und/oder Nutzung durch den Auftragsverarbeiter sein:
    1. Personenstammdaten;
    2. Kommunikationsdaten (z. B. Telefon, E-Mail);
    3. Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse);
    4. Kundenhistorie;
    5. Planungs- und Steuerungsdaten;
    6. Vertragsabrechnungs- und Zahlungsdaten;
    7. Ggf. Ausweisdokumente und Qualifikationen.

Der Kreis derer, die durch den Umgang mit ihren personenbezogenen Daten betroffen sind, umfasst:

- Kunden;
- Beschäftigte (auch Auszubildende, Praktikanten, Zeitarbeitnehmer, Lieferanten);
- Ansprechpartner bei anderen Unternehmern.

# 4 Verantwortlichkeit und Weisungsbefugnis

1. Der Verantwortliche ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenverarbeitung verantwortlich. Er kann jederzeit die Herausgabe, Berichtigung, Löschung und Sperrung der Daten verlangen. Soweit ein Betroffener sich zwecks Ausübung seiner Rechte nach EU-DSGVO Art. 12 – 23 (z.B. Löschung, Berichtigung oder Datenübertragung) unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortliche weiterleiten.
2. Der Auftragsverarbeiter darf Daten ausschließlich im Rahmen der Weisungen des Verantwortlichen erheben, verarbeiten oder nutzen.
    1. Eine Weisung ist die auf einen bestimmten Umgang des Auftragsverarbeiters mit personenbezogenen Daten gerichtete schriftliche Anordnung des Verantwortlichen.

2. Die Weisungen werden zunächst durch die Konkretisierung in Punkt 3 dieser Vereinbarung definiert und können von dem Verantwortlichen danach in schriftlicher Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden.
3. Trifft den Auftragsverarbeiter eine gesetzliche Verpflichtung oder eine rechtliche Anordnung zur Verarbeitung oder Herausgabe personenbezogener Daten, für die der Verantwortliche die Verantwortung trägt, informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3. Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis diese Weisung durch den Verantwortlichen bestätigt oder geändert wird.
4. Verfahrensänderungen des Verarbeitungsgegenstandes dürfen nur mit dokumentierter Zustimmung des Verantwortlichen umgesetzt werden.
5. Auskünfte an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger schriftlicher Zustimmung durch den Verantwortlichen erteilen. Der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, diese Daten an Dritte weiterzugeben.
6. Der Verantwortliche führt ein Verzeichnis über Verarbeitungstätigkeiten. Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Wunsch Informationen über das Verzeichnis zur Verfügung.
7. Weisungsbefugte Beschäftigte des Verantwortlichen sowie Weisungsempfänger des Auftragsverarbeiters sind im Anhang „Weisungsbefugte Beschäftigte und Weisungsempfänger“ namentlich zu nennen. Eine Änderung der benannten Personen ist der entsprechend anderen Vertragspartei dokumentiert mitzuteilen.

# 5 Technisch-organisatorische Maßnahmen

1. Der Auftragsverarbeiter stellt dem Verantwortlichen eine Beschreibung der technischen und organisatorischen Maßnahmen nach Art. 32 Abs. 1 DS-GVO vor Beginn der Verarbeitung zur Verfügung. Die im Anhang “Technische und organisatorische Maßnahmen” beschriebene Auswahl der technischen und organisatorischen Maßnahmen stellt nach Stand der Technik und unter Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer diese Maßnahmen dar.
2. Diese Beschreibung wird mit der Akzeptanz durch den Verantwortlichen zum Vertragsbestandteil.
3. Der Auftragsverarbeiter 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.
4. Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das vereinbarte Sicherheitsniveau nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

5. Der Kunde informiert sich vor Abschluss der Vereinbarung zur Auftragsverarbeitung und anschließend in regelmäßigen Abständen über diese technischen und organisatorischen Maßnahmen. Der Kunde trägt die Verantwortung dafür, dass die jeweils aktuell geltenden, vertraglich vereinbarten technischen und organisatorischen Maßnahmen für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

# 6 Berichtigung, Einschränkung und Löschung von Daten

1. Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Verantwortlichen unmittelbar durch den Auftragsverarbeiter sicherzustellen.
2. Überlassene Datenträger und Datensätze verbleiben im Eigentum des Verantwortlichen. Kopien und Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zu Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungs-pflichten des Auftragsverarbeiters erforderlich sind.
3. Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung des Verantwortlichen, jedoch spätestens mit Beendigung der Leistungsvereinbarung hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigten Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung des Verantwortlichen in einem dem Schutzniveau entsprechenden Verfahren zu vernichten. Gleiches gilt für Test- und Ausschussmaterial.
4. Der Auftragsverarbeiter kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahren. Alternativ kann er diese zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben.
5. Die Evint GmbH ist berechtigt, für diese Leistungen eine angemessene Vergütung vom Kunden zu verlangen.
6. Diese Vereinbarungen gelten auch im Fall einer Kündigung durch den Verantwortlichen aufgrund der Bestimmungen des Punkt 11 dieser Vereinbarung.

# 7 Mitteilung bei Verstößen durch den Auftragsverarbeiter

1. Der Auftragsverarbeiter unterrichtet den Verantwortlichen umgehend bei schwerwiegenden Störungen seines Betriebsablaufes, bei Verdacht auf Verstöße gegen vertragliche oder gesetzliche Datenschutzbestimmungen, bei Verstößen gegen solche Bestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten, damit dieser seiner Meldepflicht nachkommen kann.

# 8 Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

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

1. Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Dessen aktuelle Kontaktdaten sind auf der Homepage leicht zugänglich hinterlegt.
2. Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO.
    1. 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.
    2. 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.
3. Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
4. 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. 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.
6. 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.
7. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Verantwortlichen im Rahmen seiner Kontrollbefugnisse.

# 9 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 Auftragsverarbeiter 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 Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Verantwortlichen auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

2. Die Evint GmbH informiert den Kunden, wenn sich eine Änderung in Bezug auf die Hinzuziehung weiterer oder die Ersetzung bestehender Auftragsverarbeiter ergeben hat.
3. Der Kunde kann gegen derartige Änderungen Einspruch innerhalb von vier Wochen erheben. Ohne Einspruch wird die Änderung nach vier Wochen rechtsverbindlich anerkannt.
4. Im Fall des Einspruchs kann die Evint GmbH nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder – sofern die Erbringung der Leistung ohne die beabsichtigte Änderung der Evint GmbH nicht zumutbar ist - die von der Änderung betroffene Leistung gegenüber dem Kunden innerhalb von vier Wochen nach Zugang des Einspruchs kündigen oder die gesamte Leistungserbringung kündigen.
5. Wenn Subunternehmer durch den Auftragsverarbeiter eingeschaltet werden, hat der Auftragsverarbeiter sicherzustellen, dass seine vertraglichen Vereinbarungen mit dem Subunternehmer so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter entspricht, hinreichende Garantien für die Sicherheit der Verarbeitung vorliegen und alle gesetzlichen und vertraglichen Pflichten beachtet werden.
6. Dem Verantwortlichen sind in der vertraglichen Vereinbarung mit dem Subunternehmer Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Ebenso ist der Verantwortliche berechtigt, auf schriftliche Anforderung vom Auftragsverarbeiter Auskunft über den wesentlichen Vertragsinhalt, die Umsetzung der datenschutzrelevanten Verpflichtungen des Subunternehmers und die Garantien zur Sicherheit der Verarbeitung zu erhalten.
7. Zu Beginn der Verarbeitung sind die beauftragten Subunternehmer in der Anlage „Subunternehmer“ aufzuführen.

# 10 Kontrollrechte des Verantwortlichen

1. Der Verantwortliche hat das Recht, im Benehmen mit dem Auftragsverarbeiter Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die rechtzeitig mindestens 14 Kalendertage vorher anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen.
    1. Die Ausübung des Inspektionsrechts darf den Geschäftsbetrieb von die Evint GmbH nicht über Gebühr stören oder missbräuchlich sein.
    2. Die Evint GmbH ist berechtigt, für Inspektionen eine angemessene Vergütung vom Kunden zu verlangen.
2. Der Auftragsverarbeiter stellt sicher, dass sich der Verantwortliche von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DS-GVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen 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
    1. die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
    2. die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
    3. aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

4. eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI Grundschutz).

4. Der Kunde hat die Evint GmbH unverzüglich und vollständig zu informieren, wenn er im Hinblick auf die Verarbeitung bezüglich datenschutzrechtlicher Bestimmungen Fehler oder Unregelmäßigkeiten feststellt.
5. Der Kunde nennt der Evint GmbH den Ansprechpartner für im Rahmen dieser Vereinbarung zur Auftragsverarbeitung anfallende Datenschutzfragen:

   Weisungsbefugter Ansprechpartner ist: ……

# 11 Verarbeitung auf dokumentierte Weisung

1. Die Evint GmbH – und jede ihr unterstellte Person – darf die personenbezogenen Daten nur im Rahmen der Leistungsbeschreibungen und den jeweiligen vertraglichen Vereinbarungen zwischen der Evint GmbH und dem Kunden und der Weisungen des Kunden verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 Satz 2 lit. a DS-GVO vor.
2. Die Evint GmbH nimmt Weisungen des Kunden in schriftlicher Form sowie über die hierfür von Evint GmbH angebotenen elektronischen Formate entgegen.
3. Mündliche Weisungen sind durch den Kunden unverzüglich schriftlich oder in einem von der Evint GmbH angebotenen elektronischen Format zu bestätigen.
4. Sind die Weisungen des Kunden nicht vom vertraglich vereinbarten Leistungsumfang umfasst, werden diese als Antrag auf Leistungsänderung behandelt.
5. Bei Änderungsvorschlägen teilt die Evint GmbH dem Kunden mit, welche Auswirkungen sich auf die vereinbarten Leistungen, insbesondere die Möglichkeit der Leistungserbringung, Termine und Vergütung ergeben.
6. Ist der Evint GmbH die Umsetzung der Weisung nicht zumutbar, so ist die Evint GmbH berechtigt, die Verarbeitung zu beenden.
7. Im Übrigen gelten die Leistungsbeschreibungen und jeweiligen vertraglichen Vereinbarungen.

# 12 Vereinbarung weiterer Vertragszwecke

1. Die Evint GmbH ist berechtigt, die von dieser Vereinbarung umfassten personenbezogenen Daten zum Zweck der Fehlerbehebung in dem Evint GmbH-Produkt, in dem die Daten gespeichert sind, zu verarbeiten.
2. Die Evint GmbH ist berechtigt, die von dieser Vereinbarung umfassten personenbezogenen Daten zum Zweck der Qualitätssicherung für das Evint GmbH-Produkt, in dem die Daten gespeichert sind bzw. für eine neuere Version des Evint GmbH-Produkts zu verarbeiten.
3. Die Evint GmbH ist berechtigt, die von dieser Vereinbarung umfassten personenbezogenen Daten zum Zweck der Entwicklung neuer oder Weiterentwicklung bestehender Evint GmbH-Produkte in einer angemessen gesicherten Umgebung zu verarbeiten. Die Evint GmbH berücksichtigt auch in diesem Verarbeitungsprozess, dass vom Kunden gelöschte oder zur Löschung angewiesene Daten nicht mehr verarbeitet werden.
4. Die Evint GmbH ist berechtigt, die von dieser Vereinbarung umfassten personenbezogenen Daten zu verarbeiten,
   1. soweit sie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig erachtet,

2. soweit dadurch die Fähigkeit eines Netzes oder Informationssystems gewährleistet wird, mit dem vereinbarten Grad der Zuverlässigkeit Störungen oder widerrechtliche oder mutwillige Eingriffe abzuwehren, die die Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit von gespeicherten oder übermittelten personenbezogenen Daten sowie die Sicherheit damit zusammenhängender Dienste, die über diese Netze oder Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen. Dies umfasst insbesondere auch, den Zugang Unbefugter zu elektronischen Kommunikationsnetzen und die Verbreitung schädlicher Programmcodes zu verhindern sowie Angriffe in Form der gezielten Überlastung von Servern („Denial of service"-Angriffe) und Schädigungen von Computer- und elektronischen Kommunikationssystemen abzuwehren.

# 13 Formerfordernis

Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – sind gemäß DS-GVO schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann, 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.

# 14 Salvatorische Klausel

Sollten sich einzelne Bestimmungen dieser Vereinbarung als ungültig erweisen, so wird hierdurch die Gültigkeit der übrigen Bestimmungen nicht berührt. Die ungültige Bestimmung ist durch eine solche Regelung zu ersetzen, die die Parteien getroffen hätten, hätten sie bei Abschluss des Vertrags an die Ungültigkeit des jeweiligen Punktes gedacht. Soweit diese Vereinbarung eine unbewusste Regelungslücke enthält, ist diese durch eine solche Regelung zu ersetzen, die die Parteien getroffen hätten, hätten sie bei Abschluss des Vertrags an die Regelungsbedürftigkeit des jeweiligen Punktes gedacht.

# 15 Schlussbestimmungen

1. Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich der Garantien des Auftragsverarbeiters - 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.
2. Der Anhang „Technische und organisatorische Maßnahmen" ist Bestandteil dieser Vereinbarung.
3. Der Anhang „Weisungsbefugte Beschäftigte und Weisungsempfänger" ist Bestandteil dieser Vereinbarung.
4. Der Anhang „Subunternehmer" ist Bestandteil dieser Vereinbarung.

| | |
|---|---|
| ..... | ..... |
| Roland Günther (Geschäftsführer) | Datum, Name, Unterschrift |
| Evint GmbH | |

# Anlage 1

## 16 Technische und organisatorische Maßnahmen

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

### 16.1.1 Zutrittskontrolle

Das Ziel:
Ein unbefugter Zutritt zu Datenverarbeitungsanlagen ist zu verhindern.

Die Maßnahmen:
Die Zutrittskontrolle zu DV-Anlagen wird durch ein technisches Zutrittskontrollsystem gewährleistet, das Folgendes beinhaltet:

1. Das Gebäude, die Büroräume und das Rechenzentrum sind mit einer Alarmanlage gesichert und werden von einem Sicherheitsdienst überwacht.
2. Die Eingangstüren zu den Büroräumen sind mit einem Chipkartensystem versehen.
3. Die Zutrittsberechtigungen der Mitarbeiter sind namensscharf dokumentiert.
4. Der Zutritt von Fremdfirmen/Besuchern/Gästen wird namensscharf dokumentiert.
5. Der Zutritt zu dem Rechenzentrum wird nur berechtigten Personen gewährt und dokumentiert.
6. Mit Beendigung der Arbeitsverhältnisse werden die Zutrittsberechtigungen der Mitarbeiter entzogen.

### 16.1.2 Zugangskontrolle

Das Ziel:
Eine unbefugte Systemnutzung ist zu verhindern.

Die Maßnahmen:

1. Das Firmennetzwerk ist durch eine Firewall geschützt.
2. Die Mitarbeiter sind auf ein individuell geheim zu haltendes Computerkennwort verpflichtet.
3. Es werden keine Sammelkennwörter benutzt.
4. Bei der Passwortvorgabe sollen folgende Komplexitätsvoraussetzungen erfüllt sein: alphanumerisch (Zahlen, Buchstaben und Sonderzeichen), Mindestlänge: 8 Zeichen
5. Es erfolgt ein regelmäßiger Wechsel des Kennworts nach maximal 90 Tagen.
6. Die Bildschirme werden nach max. 10 Minuten automatisch gesperrt.
7. Auf allen Arbeitsplatzcomputern werden Virenscanner eingesetzt. Die Schutzsoftware dafür wird regelmäßig aktualisiert.
8. Sicherheitsupdates werden regelmäßig installiert.

### 16.1.3 Zugriffskontrolle

Das Ziel:
Es darf kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems möglich sein.

Die Maßnahmen:

1. Das Berechtigungskonzept ist dokumentiert.

2. Es werden differenzierte Berechtigungen (Profile) je nach Rolle vergeben.
3. Die Mitarbeiter bekommen die Zugriffsberechtigungen je zugewiesene Rolle.
4. Es erfolgt eine Protokollierung sämtlicher Zugriffe.
5. Fernzugriff für die Mitarbeiter erfolgt per VPN.
6. Für die Notebooks wird ein Festplatten-Verschlüsselungssystem eingesetzt.

### 16.1.4 Trennungskontrolle

Das Ziel:
Getrennte Verarbeitung von Daten sicherstellen, die zu unterschiedlichen Zwecken erhoben werden.

Die Maßnahmen:

1. Kundendaten sind physisch getrennt von Entwicklungsdaten und Testdaten und innerhalb der Systeme nochmals logisch getrennt.
2. Die Entwicklungsdaten sind jeweils auf getrennten Servern gespeichert (physische Trennung).
3. Es wird die Mandantentrennung eingesetzt. Die Daten je Kunde werden logisch getrennt transferiert, verarbeitet und gespeichert. Zugang zu den Daten ist nur den Mitarbeitern gewährt, die für die Datenverarbeitung zuständig sind.

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

1. Weitergabekontrolle
   Es darf kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport möglich sein.

   Die Maßnahmen:
   1. Der Datentransfer erfolgt immer verschlüsselt oder kryptisch auf den vereinbarten Übertragungswegen.
   2. Für die verschlüsselte Übertragung werden nur sichere Protokolle (SFTP, FTPS, SSL) eingesetzt.

2. Eingabekontrolle
   Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

   Die Maßnahmen:
   1. Die Protokollierung von Zugriffen auf personenbezogene Daten erfolgt über ein Erfassungssystem.
   2. Die personenbezogenen Daten werden nur innerhalb des geschlossenen Systems von autorisierten Usern bearbeitet.

### 16.1.6 Fähigkeit der Verfügbarkeit

Verfügbarkeit meint den Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust. Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

Maßnahmen:

1. Es erfolgt die aktive Überwachung sämtlicher Systeme während der Arbeitszeit.
2. Die unternehmensrelevanten Daten werden täglich gesichert.

3. Das Verfahren für Wiederherstellung und Hoch-/Herunterfahren der Systeme wird regelmäßig dokumentiert, geprüft und getestet.
4. Es wird eine unterbrechungsfreie Stromversorgung eingesetzt.

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

Die Maßnahmen:

1. Verfügbarkeitskontrolle
2. Backup-Konzeption
3. Unterbrechungsfreie Stromversorgung (USV)
4. Virenschutz
5. Firewall
6. Meldeverfahren
7. Monitoring
8. Notfallplanung
9. Spiegeln von Festplatten
10. Klimaanlagen
11. Brand- und Löschwasserschutz
12. geeignete Archivierungsräumlichkeiten

### 16.1.7 Fähigkeit der Belastbarkeit

Systeme sind belastbar, wenn sie so widerstandsfähig sind, dass ihre Funktionsfähigkeit selbst bei starkem Zugriff bzw. starker Auslastung gegeben ist.

Die Maßnahmen:

1. Monitoring
2. managed services
3. clusterfähige Systeme

### 16.1.8 Datenschutzmanagement

Die Evint GmbH verfügt über ein Incident-Response-Management und über ein Datenschutzmanagement. 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.
Es werden die gesetzlichen Bestimmungen zum Schutz natürlicher Personen bei der Verarbeitung derer personenbezogenen Daten nach EU-DSGVO berücksichtigt, eingehalten und periodisch überprüft.

### 16.1.9 Auftragskontrolle

Das Ziel:
Keine Auftragsverarbeitung im Sinne von Art. 28 EU-DSGVO ohne entsprechende Weisung des Verantwortlichen.

Die Maßnahmen:

1. Es werden generell mit Kunden und Dienstleistungspartnern Vereinbarungen zur Auftragsverarbeitung geschlossen, die den Anforderungen des Art. 28 DS-GVO entsprechen.
2. Es werden generell mit eingesetzten Unterauftragnehmern Vereinbarungen zur Auftragsverarbeitung geschlossen, die den Anforderungen des Art. 28 DS-GVO entsprechen.
3. Nach Durchführung jedes Auftrags erfolgt eine Qualitätskontrolle des Auftragsergebnisses sowie eine Freigabe mit 4-Augen-Prinzip vor Auslieferung.
4. Es ist ein betrieblicher Datenschutzbeauftragter bestellt, der im Rahmen der Datenschutzorganisation in die relevanten betrieblichen Prozesse eingebunden ist. Der Datenschutzbeauftragte führt jährlich ein Selbstaudit hinsichtlich der getroffenen technischen und organisatorischen Maßnahmen durch.

### 16.1.10 Pseudonymisierung

Pseudonymisierung ist die Verarbeitung personenbezogener Daten in der Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren Person zugewiesen werden.

Die Maßnahmen:

1. Das System bietet die Möglichkeit, mit Pseudonymen in Stammdatenfeldern zu arbeiten.

### 16.1.11 Verschlüsselung

Die Verschlüsselung transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die "Schlüssel" genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll.

Die Maßnahmen:

1. Nutzung von kryptografischen Tools
2. Data Hashing
3. Transportverschlüsselung (SSL/TLS)
4. Nutzung von VPN

### 16.1.12 Fähigkeit der Vertraulichkeit

Vertraulichkeit bedeutet, dass personenbezogene Daten vor unbefugter Preisgabe geschützt sind.

Die Maßnahmen im Rechenzentrumsbetrieb:

1. Physische Zugangskontrolle
   Unsere Server und Datenbanksysteme sind in einem Rechenzentrum entsprechend der ISO 27001-Zertifzierung installiert. Somit ist kein unbefugter Zugang zu diesen Datenverarbeitungseinrichtungen möglich.
2. Zutritt nur für befugte Personen (Betriebsangehörige);
3. Berechtigungsausweise (RFID) oder Schlüssel;
4. Firmenfremde sind nicht zugangsberechtigt und werden wie Besucher behandelt;
5. Anwesenheitsaufzeichnungen;
6. Besucherausweise;
7. Die Sicherung durch Alarmanlagen;
8. Definierte Sicherheitsbereiche;

9. RFID-gesicherter Eingang wird auch für Lieferungen genutzt;
10. Türen sind gesichert durch elektrische Türschließer und Ausweisleser;
11. Sicherheitstüren und/oder -fenster;
12. Videoüberwachung;

weitere Maßnahmen:

1. Spezielle Schutzvorkehrungen für den Serverraum am Standort;
2. Elektronische Zugangskontrolle;
3. Passwortrichtlinie nach Stand der Technik;
4. Log-Screen nach kurzer Inaktivität;
5. Berechtigungskonzept nach dem Need-to-Know-Prinzip;
6. Zusätzlicher Log-In für bestimmte Anwendungen;
7. E-Mail-Versand verschlüsselter oder passwortgeschützter Dateianhänge;
8. Downloadmöglichkeit sensibler Dokumente über das Portal;
9. Verschlüsselung von Datenträgern;
10. VPN (Virtual Private Network);
11. Gesichertes WLAN / Gäste-WLAN;
12. SSL-Verschlüsselung bei Web-Access;
13. Regelmäßige Schulungs- und Sensibilisierungsmaßnahmen;
14. Mitarbeiterverpflichtung auf Vertraulichkeit;
15. Vertragsgestaltung mit Dienstleistern.

### 16.1.13 Fähigkeit der Integrität

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. Maßnahmen sollten ergriffen werden, die die Beschädigung/Veränderung der geschützten Daten während der Verarbeitung oder Übertragung verhindern.

Die Maßnahmen:

1. Interne Zugangskontrolle
2. Transportverschlüsselung bei Datenübermittlungen über EVINT
3. Kontrolle der Dateneingabe in EVINT
4. Funktionelle Verantwortlichkeiten / Rollenkonzept
5. Vertreterregelung
6. Berechtigungskonzept nach dem Need-to-Know-Prinzip
7. Protokollierung von Zugriffen: Lesen, kopieren, ändern oder löschen

### 16.1.14 Wiederherstellbarkeit der Verfügbarkeit und des Zugangs

Wie wird gewährleistet, dass personenbezogene Daten nach Sicherheitsvorfällen rasch wieder verfügbar und zugänglich sind?

Die Maßnahmen:

1. Durch unsere hochverfügbare technische Clusterumgebung ist eine rasche Wiederherstellung und die Verfügbarkeit der Systeme und Daten sichergestellt.
2. Backup-Verfahren

3. Unterbrechungsfreie Stromversorgung (USV)
4. Vertretungsregelungen

### 16.1.15 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Es wird gewährleistet, dass die genannten Datensicherungsmaßnahmen regelmäßig überprüft werden.

Die Maßnahmen:

1. Datenschutzmanagement
2. Reaktionsmanagement
3. Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen bei Eigenentwicklungen
4. Auftrags- oder Vertragskontrolle

### 16.1.16 Unrechtmäßiger Zugang zu personenbezogenen Daten

Wie wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können?

Die Maßnahmen:

1. Individueller Log-In und Kennwortverfahren
2. Zusätzlicher Log-In für bestimmte Anwendungen
3. Automatische Sperrung der Clients (Zeitablauf)
4. Verwaltung von Berechtigungen
5. Dokumentation von Berechtigungen

### 16.1.17 Verarbeitung personenbezogener Daten nur nach Anweisung

Wie wird gewährleistet, dass personenbezogene Daten nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden?

Die Maßnahmen:

1. Mitarbeiter sind zu Verhaltensregeln verpflichtet
2. Definierte Weisungsempfänger
3. Implementierung unternehmensinterner Datenschutz-Richtlinien
4. Verpflichtung der Mitarbeiter auf Vertraulichkeit
5. Schulungen aller zugriffsberechtigten Mitarbeiter
6. Rollenkonzept
7. Dokumentation von Verantwortlichkeiten

# Anlage 2

## 17 Subunternehmer

### 17.1 Global Business Group AG

Kontaktdaten
Ernst-Barlach-Straße 20
36041 Fulda

Frau Michelle Hergenröder
michelle.hergenroeder@gbg-ag.com

Leistungen:
1. Abrechnung von Lizenzen und Leistungen
2. Datenpflege und Verwaltung

Datenkategorien
1. Personenstammdaten
2. Arbeitszeiten
3. Zeitarbeitnehmer
4. Mitarbeiter der Auftraggeber und deren Partner

### 17.2 Global Business IT GmbH

Kontaktdaten
Ernst-Barlach-Straße 20
36041 Fulda

Herr Denis Stolz
denis.stolz@global-bit.de

Leistungen:
1. Betrieb der IT-Infrastruktur,
2. technischer Support
3. Protokolldaten, User-Profile
4. Abrechnung von Lizenzen und Leistungen
5. Datenpflege und Verwaltung

Datenkategorien
1. Personenstammdaten
2. Arbeitszeiten
3. Zeitarbeitnehmer
4. Mitarbeiter der Auftraggeber und deren Partner

## 17.3 DTS Systeme GmbH

Aufgabe: Betrieb des Rechenzentrums

Schrewestraße 2
D - 32051 Herford

## 17.4 Meisterlabs GmbH

Aufgabe: Software für Aufgaben- und Taskmanagement

Zugspitzstrasse 2
85591 Vaterstetten

## 17.5 Alroma

Aufgabe: Rechenzentrum für Archiv und Backup

Paulstraße 8
39218 Schönebeck

## 17.6 Candis GmbH

Aufgabe: Software zur Bearbeitung der Eingangsrechnungen

Perleberger Straße 42
10559 Berlin