Proven Expert

It's All About Trust

VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG

Zwischen

Muster Firma GmbH
vertreten durch Max Mustermann
Musterstraße 1
12345 Musterort
Deutschland

ProvenExpert-Kundennummer: 123

- nachfolgend „**Auftraggeber**" genannt -

Und

der Expert Systems AG
vertreten durch den Vorstand Remo Fyda
Quedlinburger Str. 1
10589 Berlin

- nachfolgend „**Auftragnehmer"** genannt -

Auftraggeber und Auftragnehmer werden nachfolgend gemeinsam als „**Parteien**" oder einzeln als „**Partei**" bezeichnet.

PRÄAMBEL

Der Auftragnehmer bietet den Dienst provenexpert.com an, den der Auftraggeber nutzt. Zwischen den Parteien besteht zu diesem Zweck eine Nutzungsvereinbarung (die „Nutzungsvereinbarung"), die die Grundpflichten der Parteien regelt. Die vorliegende Vereinbarung wird geschlossen, um den Anforderungen des Datenschutzrechts, insbesondere der Europäischen Datenschutzgrundverordnung (DS-GVO) Rechnung zu tragen. Die Nutzungsvereinbarung stellt ein Auftragsverarbeitungsverhältnis im Sinne von Art. 28 DS-GVO dar. Um die Rechte und Pflichten aus dem Auftragsverarbeitungsverhältnis gemäß der gesetzlichen Verpflichtung zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung. Zudem vereinbaren die Vertragsparteien, dass bis zum Inkrafttreten der DS-GVO und der ggf. ergänzenden nationalen Gesetze in Deutschland, die analogen Regelungen des BDSG auf diese Vereinbarung Anwendung finden.

1. GEGENSTAND, DAUER

1.1 Gegenstand, Art und Zweck der Datenverarbeitung ergeben sich aus der Nutzungsvereinbarung, auf die hier verwiesen wird.

1.2 Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten sind folgende Datenarten / -kategorien:

- Personenstammdaten (z.B. Vorname, Nachname)
- Kommunikationsdaten (z.B. Telefon, E-Mail)

1.3 Der Kreis der durch den Umgang mit personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst:

- Die Kunden, Nutzer, Clienten des Auftraggebers

1.4 Die Dauer dieser Vereinbarung (Laufzeit) entspricht der in der Nutzungsvereinbarung vereinbarten. Diese Vereinbarung endet in jedem Fall automatisch mit Beendigung der Nutzungsvereinbarung. Das Recht beider Parteien zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

2. TECHNISCH-ORGANISATORISCHE MAßNAHMEN

2.1 Der Auftragnehmer dokumentiert die Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen und übergibt diese dem Auftraggeber auf Anfrage zum Zwecke der

Prüfung. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

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

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

3. BERICHTIGUNG, EINSCHRÄNKUNG UND LÖSCHUNG VON DATEN

3.1 Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken.

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

4. QUALITÄTSSICHERUNG UND SONSTIGE PFLICHTEN DES AUFTRAGNEHMERS

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

4.1.1 Ansprechpartner für Datenschutz - Der Ansprechpartner, für alle Fragen zum Thema Datenschutz, des Auftragnehmers ist:

Expert Systems AG
Jan Reimann
Quedlinburger Str. 1
10589 Berlin
E-Mail: privacy@provenexpert.com

Über Änderungen der Person und/oder Kontaktdaten wird der Auftragnehmer den Auftraggeber informieren.

4.1.2 Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

4.1.3 Die Zusammenarbeit mit der Aufsichtsbehörde. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

4.1.4 Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

4.1.5 Die Unterstützung des Auftraggebers. Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

4.1.6 Die Kontrolle der internen Prozesse. Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen

des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

4.1.7 Die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 5 dieser Vereinbarung.

5. KONTROLLRECHTE DES AUFTRAGGEBERS

5.1 Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die mindestens 14 Tage im Voraus anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb während üblichen Geschäftszeiten (werktags außer samstags zwischen 9 und 18 Uhr) zu überzeugen. Die Kosten dafür trägt der Auftraggeber.

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

6. MITTEILUNG BEI VERSTÖßEN DES AUFTRAGNEHMERS

6.1 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 der DS-GVO 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 Auftraggeber zu melden;
- die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;
- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung.

7. WEISUNGSBEFUGNIS DES AUFTRAGGEBERS

7.1 Der Umgang mit den Daten gemäß Ziffer 1 dieser Vereinbarung erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers.

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

8. ORT DER VERARBEITUNG UND NUTZUNG VON DATEN

8.1 Die Verarbeitung und Nutzung der Daten durch den Auftragnehmer findet im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

8.2 Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artikel 44 ff. DS-GVO erfüllt sind.

9. UNTERAUFTRAGSVERHÄLTNISSE, ART. 28 ABS. 4 DS-GVO

9.1 Der Auftragnehmer kann zur Verarbeitung oder Nutzung personenbezogener Daten des Auftraggebers Unterauftragnehmer nur mit vorheriger schriftlicher Zustimmung des Auftraggebers einbeziehen.

9.2 Für folgende Unterauftragnehmer hat der Auftraggeber diese Zustimmung bereits vorab bei Abschluss dieser Vereinbarung erteilt:

Name und Anschrift des Unterauftragnehmers	**Beschreibung der Teilleistungen**
Telekom Deutschland GmbH Postfach 30 04 64 53184 Bonn Deutschland	Hosting-Leistungen
MessageBird B.V. Baarsjesweg 285-H 1058 AE Amsterdam Netherlands	SMS-Dienstleister

9.3 Die Einschaltung von Unterauftragnehmern bedarf einer schriftlichen Beauftragung durch den Auftragnehmer. Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem Unterauftragnehmer so zu gestalten, dass sie den Datenschutzbestimmungen dieser Vereinbarung entsprechen.

9.4 Sofern der Unterauftragnehmer seinerseits weitere Unterauftragnehmer einsetzen will, gelten die Bestimmungen dieser Ziffer 9. entsprechend.

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

9.6 Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/ des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen gemäß Ziffer 8.2 dieser Vereinbarung sicher.

10. HAFTUNG

10.1 Schadensersatzansprüche des Auftraggebers wegen Pflichtverletzung und aus unerlaubter Handlung, sowie Ansprüche auf Ersatz vergeblicher Aufwendungen sind sowohl in Bezug auf den Auftragnehmer, als auch gegenüber dessen jeweiligen Erfüllungs- und Verrichtungsgehilfen ausgeschlossen.

10.2 Diese Haftungsbeschränkung gilt nicht, wenn der Schaden vorsätzlich oder grob fahrlässig verursacht wurde, und des Weiteren nicht für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, wenn der Auftragnehmer die Pflichtverletzung zu vertreten hat.

10.3 Die Haftungsbeschränkung gemäß Ziffer 10.1 gilt ferner nicht für Schäden, die auf dem Fehlen einer zugesicherten Eigenschaft beruhen oder für die eine Haftung nach dem Produkthaftungsgesetz vorgesehen ist, sowie im Falle der Verletzung vertragswesentlicher Pflichten, das heißt solcher vertraglicher Pflichten, deren Erfüllung die ordnungsgemäße Durchführung des Vertrages überhaupt erst ermöglicht und auf deren Einhaltung der Vertragspartner regelmäßig vertrauen darf, und deren Verletzung auf der anderen Seite die Erreichung des Vertragszwecks gefährdet. Im Falle der Verletzung vertragswesentlicher Pflichten ist die Haftung der Höhe nach auf den typischerweise vorhersehbaren Schaden begrenzt.

11. LÖSCHUNG VON DATEN UND RÜCKGABE VON DATENTRÄGERN

Bei Beendigung dieser Vereinbarung hat der Auftragnehmer auf schriftliche Aufforderung unverzüglich sämtliche für den Auftraggeber verwalteten Datenbestände auf Datenträgern zu speichern und diese Datenträger an den Auftraggeber zu übergeben. Zurückbehaltungsrechte des Auftragnehmers hieran sind ausgeschlossen. Der Auftragnehmer hat die für den Auftraggeber verwalteten Datenbestände anschließend einschließlich Sicherungskopien auf schriftliche Aufforderung des Auftraggebers auf den Trägersystemen vollständig zu löschen. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Die Kosten dafür trägt der Auftraggeber.

12. SCHLUSSBESTIMMUNGEN

12.1 Änderungen oder Ergänzungen dieser Vereinbarung bedürfen zu ihrer Wirksamkeit der Schriftform und sind von beiden Parteien zu unterzeichnen. Kündigungen bedürfen zu ihrer

Schriftform bedarf zu ihrer Wirksamkeit der Schriftform. Änderungen und Ergänzungen müssen als solche ausdrücklich gekennzeichnet sein.

12.2 Sollte eine Bestimmung dieser Vereinbarung unwirksam sein, wird die Wirksamkeit der übrigen Bestimmungen dadurch nicht berührt. Die Parteien werden die unwirksame Bestimmung unverzüglich durch eine solche wirksame ersetzen, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung am nächsten kommt.

12.3 Diese Vereinbarung unterliegt dem Recht der Bundesrepublik Deutschland unter Ausschluss der Regelungen des deutschen Internationalen Privatrechts.

12.4 Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit dieser Vereinbarung ist Berlin.

Musterort, den 22.05.2018	Berlin, den 22.05.2018
_____	_____
Auftraggeber	CEO – Remo Fyda Auftragnehmer

ANLAGE 1– TECHNISCH-ORGANISATORISCHE MAßNAHMEN

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

- Zutrittskontrolle
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;

- Zugangskontrolle
  Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;

- Zugriffskontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;

- Trennungskontrolle
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;

- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
  Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

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

- Weitergabekontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

- Eingabekontrolle
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme ein-

gegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

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

- Verfügbarkeitskontrolle
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;

- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

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

- Datenschutz-Management

- Incident-Response-Management

- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

- Auftragskontrolle
  Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen