Nutzungsbedingungen Wedolo

Stand: 25.08.2021

Präambel

Willkommen bei Wedolo! Die Wedolo Betriebsgesellschaft mbH (nachfolgend „Wedolo“) betreibt unter „wedolo.de“ eine internetbasierte Plattform für Unternehmen der Logistik- und Speditionsbranche (nachfolgend „Online-Plattform“). Diese Online-Plattform bündelt die Angebote des Bundesverbandes für Güterkraftverkehr Logistik und Entsorgung (BGL) e.V. und der weiteren angegliederten regionalen Organisationen, der KRAVAG-SACH Versicherung des Deutschen Kraftverkehrs VaG, der SVG Bundes-Zentralgenossenschaft Straßenverkehre G und der verschiedenen regionalen Organisationen der Straßenverkehrsgenossenschaft (SVG) sowie der SVG Akademie GmbH (nachfolgend „Partner-Portale“) und stellt diese Interessenten zentral zur Verfügung. Weiterhin bietet Wedolo eigene digitale Services (inkl. Fahrer-App), Dienste und Informationen an.

Die Online-Plattform richtet sich an Spediteure, Disponenten, LKW-Fahrer sowie andere Mitarbeiter des gewerblichen Güterverkehrs (nachfolgend „Nutzer“).

1. Geltung der Nutzungsbedingungen

1.1 Regelungsbereich

Diese Nutzungsbedingungen regeln die Rechte und Pflichten zwischen Wedolo und den Nutzern in Zusammenhang mit der Nutzung der auf den Webseiten „wedolo.de“ und „my.wedolo.de“ sowie den in der Wedolo Fahrer-App (nachfolgend „App“) angebotenen Anwendungen und Dienstleistungen.
Entgegenstehende Geschäftsbedingungen des Nutzers finden keine Anwendung, es sei denn, diese werden von Wedolo anerkannt. Ein fehlender Widerspruch fremder Geschäftsbedingungen stellt keine Zustimmung dar.

1.2 Änderung der vorliegenden Nutzungsbedingungen

Wedolo ist berechtigt, diese Nutzungsbedingungen jederzeit mit Wirkung für die Zukunft mit einer Ankündigungsfrist von vier Wochen zu ändern, wenn die Änderung unter Berücksichtigung der Interessen von Wedolo für den Nutzer zumutbar ist.
Widerspricht der Nutzer der Änderung nicht innerhalb der von Wedolo gesetzten Frist, gilt die Änderung als genehmigt. Wedolo weist dem Nutzer in der Änderungsankündigung auf diesen Umstand hin.

2. Nutzung der Plattform

2.1 Registrierte Nutzer

Der Nutzer kann sich einerseits einen regulären Zugang zum geschlossenen Nutzerbereich „my.wedolo.de“ über die Registrierung auf „wedolo.de“ beschaffen. Andererseits kann dieser Zugang auch über die Fahrer-App mithilfe einer Unternehmenseinladung erfolgen.

Wedolo bietet keine Services für Minderjährige an. Registrierte Nutzer können nur Personen sein, die das 18. Lebensjahr vollendet haben und voll geschäftsfähig sind. Wedolo als B2B-Plattform wendet sich ausschließlich an Geschäftskunden.
Handelt eine Person nicht im eigenen Namen, so versichert sie gegenüber Wedolo, vom registrierten Nutzer zur Vornahme der jeweiligen Handlung bevollmächtigt worden zu sein.

Die dem registrierten Nutzer bei der Nutzung von Wedolo zur Verfügung stehenden Inhalte sind abhängig von dem jeweiligen Zugriffsrecht des Nutzers und können unterschiedliche Funktionsumfänge haben (s. § 3.1 Account und Nutzerprofil).
Der registrierte Nutzer ist zur wahrheitsgemäßen und vollständigen Angabe der bei der Registrierung erhobenen Daten verpflichtet. Zusätzlich hat es auch die Aktualität seiner Daten zu gewährleisten. Der registrierte Nutzer muss hierbei eine aktuelle Mailadresse oder eine Handynummer angeben, die zugleich der Kommunikation zwischen dem Nutzer und Wedolo dient.

Für die Nutzung von Services externer Partner können dem registrierten Nutzer Kosten entstehen oder Gebühren anfallen. Die Nutzung dieser externen Services wird nicht in diesen Nutzungsbedingungen geregelt, sondern erfordert einen separaten Vertrag zwischen dem externen Service-Partner und dem registrierten Nutzer gemäß § 4 dieser Nutzungsbedingungen. Somit wird Wedolo nicht Vertragspartner dieses Vertrages und übernimmt daher keine Verantwortung für diesen Vertrag.

2.2 Löschung des Accounts

Der Widerruf bzw. die Löschung eines Accounts erfolgt auf „my.wedolo.de". Nach der Löschung hat der registrierte Nutzer keinen Zugriff mehr auf seinen Account bzw. sein Nutzerprofil und kann Daten, Nachrichten, Dateien oder andere auf der Online-Plattform hinterlegte Inhalte nicht mehr einsehen. Wedolo ist berechtigt, Inhalte von gekündigten Accounts zu löschen.

3. Plattformbetrieb

3.1 Account und Nutzerprofil

Jeder registrierte Nutzer erhält nach der erstmaligen Registrierung ein standardisiertes Rechtepaket, welches allgemein zugängliche Services beinhaltet.
Gibt der registrierte Nutzer die Daten seines Unternehmens an wird ihm das Rechtepaket für Unternehmer zugewiesen. Dieses ermöglicht den Zugang zu sämtlichen Services von Wedolo. Unternehmer haben zusätzlich die Möglichkeit die Rechte ihrer Mitarbeiter individuell anzupassen oder ihre Mitarbeiter im geschützten Nutzerbereich einzuladen.

Jeder Nutzer darf maximal nur einen Account bzw. ein Nutzerprofil anlegen. Dieses Profil ist nutzergebunden und darf nicht ohne ausdrückliche Zustimmung seitens Wedolo auf einen Dritten übertragen werden.

Der Account bzw. das Nutzerprofil ist durch eine gültige E-Mail-Adresse bzw. Handynummer und ein Passwort (nachfolgend „Login-Daten") geschützt, die im Rahmen der Registrierung festgelegt werden. Weiterhin erhält der registrierte Nutzer eine eindeutige Nutzernummer, die auch zum Login genutzt werden kann. Der registrierte Nutzer hat dafür Sorge zu tragen, dass seine Login-Daten Dritten nicht zugänglich sind. Im Falle des Abhandenkommens der Login-Daten oder im Falle des Verdachts, dass ein Dritter von ihnen Kenntnis hat oder den Account des Nutzers nutzt, ist der Nutzer verpflichtet, Wedolo unverzüglich zu informieren und seine Login-Daten im geschlossenen Nutzerbereich „my.wedolo.de" zu ändern.

Der registrierte Nutzer sichert zu, dass die bei der Erstellung seines Accounts bzw. seines Nutzerprofils verwendeten Daten zutreffend und vollständig sind. Der registrierte Nutzer ist verpflichtet, jegliche Änderungen seiner Account- und Profil-Daten umgehend auch in seinem Account bzw. Nutzerprofil auf der Online-Plattform zu ändern.

3.2 Single-Sign-On-Authentifizierungsdienst

Ein zentraler Service von Wedolo ist ein Single-Sign-On zu den Inhalten und Services der beteiligten Partner-Portale und Service-Partnern. Bezüglich der Nutzungsbedingungen zu diesem Single-Sign-On gelten die Anmerkungen in Anhang I dieser Nutzungsvereinbarung.

3.3 Nutzung der Plattform

Bei der Nutzung von Wedolo verpflichtet sich der Nutzer bzw. registrierte Nutzer diese Nutzungsbedingungen sowie geltendes Recht, insbesondere Straf-, Wettbewerbs-, Marken-, Urheber-, Persönlichkeits-, Datenschutz- und Jugendschutzrecht zu beachten und keine Rechte Dritter zu verletzen.

Sämtliche Rechte an der Online-Plattform (insbesondere Urheberrechte) liegen bei Wedolo.

Der Nutzer bzw. der registrierte Nutzer muss jegliche Tätigkeit unterlassen, die geeignet ist, den Betrieb der Online-Plattform oder der dahinterstehenden technischen Infrastruktur und deren Funktionen oder Zugriffsmöglichkeiten zu manipulieren, zu beeinträchtigen und / oder übermäßig zu belasten. Dazu zählen insbesondere das Blockieren, Überschreiben, Modifizieren, Kopieren von Daten und / oder sonstigen Inhalten, sowe it dies nicht für die ordnungsgemäße Nutzung der Online-Plattform erforderlich ist.

Wedolo ist berechtigt, den Zugang des registrierten Nutzers zeitweise oder dauerhaft zu sperren, wenn der begründete Verdacht eines Verstoßes besteht.

Erlangt der registrierte Nutzer Kenntnis von einem Missbrauch der Zugangsdaten oder besteht auch nur einen entsprechenden Verdacht, so wird der Nutzer Wedolo darüber unverzüglich unterrichten. Bei Missbrauch oder vermutetem Missbrauch ist Wedolo berechtigt, den Zugang sofort zu sperren. Der registrierte Nutzer haftet für alle Folgen der Drittnutzung, sofern der Missbrauch der Zugangsdaten von ihm zu vertreten ist. Zu vertreten hat der registrierte Nutzer den Missbrauch insbesondere bereits, wenn es die unbefugte Nutzung der Zugangsdaten auch nur fahrlässig ermöglich hat. Die Haftung endet erst, w enn der registrierte Nutzer den Support von Wedolo durch E-Mail (support@wedolo.de) über die unberechtigte Nutzung informiert und, falls erforderlich, das Passwort geändert hat.
Selbiges gilt entsprechend, wenn der Nutzer an einem öffentlichen oder von mehreren Benutzern verwendeten Computer arbeitend die Option „Eingeloggt bleiben“ gew ählt hat und auf diese Weise Dritte Zugriff auf die Online-Plattform erhalten.

Im Rahmen des Produkt- und Dienstleistungsangebots auf Wedolo durch die angebundenen Unternehmen bleiben sämtliche Nutzungs- und Verwertungsrechte (geistiges Eigentum, Art. 3 Abs. 1 e) der VO (EU) 2019/1150) an den vom angebundenen Unternehmen auf die Plattform hochgeladene Inhalte beim angebundenen Unternehmen. Wedolo w ird keine Löschungen, Ergänzungen oder Bearbeitungen der unternehmenseigenen Daten vornehmen.

3.4 Umgang mit Daten von Mitarbeitern des registrierten Nutzers

Für die Mitarbeiteranlage muss der registrierte Nutzer die Einwilligung der Mitarbeiter einholen, um deren Daten zu nutzen. Er ist weiterhin für die Aktualität dieser Daten verantwortlich.
Zu diesen Daten gehören Name und Vorname, das Geburtsdatum, die Mailadresse und die Handynummer vom Mitarbeiter.

Die Nutzer der Plattform dürfen Adressen, Kontaktdaten, Mailadressen usw., die sie durch die Nutzung der Plattform erhalten haben, für keinen anderen Zweck verwenden, als für die zweckbestimmte Kommunikation zwischen den Nutzern.

Insbesondere ist es verboten, die durch die Plattform erlangten Daten weiterzuverkaufen, für das Abwerben von Mitarbeitern, den Verkauf von Waren- oder Dienstleistungen oder die Zusendung von Werbung zu verwenden.

4. Services externer Partner

Wedolo ermöglicht externen Kooperationspartnern, ihre Produkte und Dienstleistungen auf der Online-Plattform von Wedolo anzubieten. Welche Produkte und Dienstleistungen die externen Partner anbieten, w ird auf der jew eiligen, von den externen Partnern genutzten Produktdetailseite ersichtlich. Ein Vertrag über diese Produkte und Dienstleistungen kommt zw ischen dem registrierten Nutzer und dem externen Partner zustande. Wedolo ist nicht Vertragspartner dieses Vertrages und übernimmt für diesen auch keine Verantwortung. Wedolo handelt auch nicht als Vertreter des externen Partners.

Die Verträge mit den externen Partnern können von den registrierten Nutzern auf der jew eiligen Produktdetailseite des externen Partners zu den dort von dem externen Partner genannten Vertragsbedingungen abgeschlossen werden. Es gelten die Geschäftsbedingungen der externen Partner.

5. Haftungsausschlüsse

Wedolo haftet unbeschränkt, soweit die Schadensursache auf Vorsatz oder grober Fahrlässigkeit beruht.

Ferner haftet Wedolo für die fahrlässige Verletzung von wesentlichen Pflichten, deren Verletzung die Erreichung des Vertragszwecks gefährdet oder deren Erfüllung die ordnungsgemäße Durchführung des Vertrages überhaupt erst ermöglicht und auf deren Einhaltung der Vertragspartner regelmäßig vertrauen darf. In diesem Fall haftet Wedolo jedoch nur für den vorhersehbaren, vertragstypischen Schaden. Wedolo haftet nicht für die leicht fahrlässige Verletzung anderer als der in den vorstehenden Sätzen genannten Pflichten.

Die vorstehenden Haftungsbeschränkungen gelten nicht bei Verletzung von Leben, Körper und Gesundheit, für einen Mangel nach Übernahme einer Garantie für die Beschaffenheit eines Produktes und bei arglistig verschwiegenen Mängeln. Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt.

Soweit die Haftung von Wedolo ausgeschlossen oder beschränkt ist, gilt dies auch für die Haftung von gesetzlichen Organen, Vertretern, Angestellten und sonstigen Erfüllungsgehilfen.

6. Störungen und Wartung

Die Online-Plattform kann wegen Wartungsarbeiten oder anderen Gründen zeitweise nicht oder nur beschränkt zur Verfügung stehen, ohne dass der Nutzer hieraus Ansprüche gegenüber Wedolo erwachsen. Wedolo behält sich das Recht vor, technische Schutzmechanismen einzusetzen, welche die Veröffentlichung von Angeboten und Inhalten auf der Online-Plattform aus Sicherheitsgründen verzögern könnte.

Wedolo kann seine Leistungen zeitweilig beschränken, wenn dies im Hinblick auf Kapazitätsgrenzen, für die Sicherheit oder Integrität der Server oder zur Durchführung technischer Maßnahmen erforderlich ist, und dies der ordnungsgemäßen oder verbesserten Erbringung der Leistungen dient (bspw. bei Wartungsarbeiten). Wedolo berücksichtigt bei solchen Maßnahmen die Beibehaltung der Dienstleistung und informiert seine Nutzer in einer angemessenen Frist bei unausweichlichen Einschränkungen.

7. Verlinkte Webseiten

Wedolo übernimmt keine Gewähr für die Aktualität, Korrektheit, Rechtmäßigkeit, Vollständigkeit oder Qualität des Inhalts von Webseiten auf welche Wedolo Verlinkungen herstellt und schließt jegliche Haftung in diesem Zusammenhang aus.

8. Anwendbares Recht

Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.

Sofern es sich beim Kunden um einen Kaufmann oder eine juristische Person des öffentlichen Rechts handelt, ist Gerichtsstand für alle Streitigkeiten aus Vertragsverhältnissen zwischen dem registrierten Nutzer und der Wedolo Betriebsgesellschaft mbH Hamburg.

9. Alternative Streitbeilegung

Wedolo ist nicht verpflichtet und nicht bereit an einem Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle teilzunehmen. Das Gesetz über die alternative Streitbeilegung in Verbrauchersachen fordert aber, dass wir Sie trotzdem auf eine für Sie zuständige Verbraucherschlichtungsstelle hinweisen:

Die Europäische Union stellt unter https://ec.europa.eu/consumers/odr/ eine Plattform zur Online-Streitbeilegung bereit.

10. Vertrag zur Auftragsverarbeitung

Um die eigenentwickelten Services anbieten zu können, werden personenbezogene Daten von Unternehmensangehörige benötigt. Für eine datenschutzgerechte Verarbeitung dieser Daten muss ein Auftragsverarbeitungsvertrag zwischen dem Unternehmen als Auftraggeber und dem Betreiber der Wedolo-Plattform als Auftragnehmer abgeschlossen werden. Der Vertrag wird mit der Einwilligung des registrierten Nutzers zum Vertragsgegenstand zwischen ihm und dem Betreiber der Plattform (s. Anhang II).

Anhang I: Besondere Nutzungsbedingungen für den Single-Sign-On-Authentifizierungsdienst von Wedolo

In Ergänzung zu den Nutzungsbedingungen von Wedolo gelten die Besonderen Nutzungsbedingungen für den Single-Sign-on-Authentifizierungs-Dienst der Logistikplattform Wedolo.
Wedolo stellt registrierten Nutzern (im Folgenden kurz „Nutzer" genannt) einen Single-Sign-On-Authentifizierungsdienst (im Folgenden „SSO" genannt) zur Verfügung. Der „SSO" ermöglicht es den Nutzern von Wedolo auf geschützte Inhalte von Partner-Portalen zuzugreifen, ohne, dass bei jedem Zugriff die erforderlichen Login-Daten erneut eingegeben werden müssen.
Der Nutzer authentifiziert sich einmalig aus Wedolo heraus bei dem entsprechenden Dienst des Partner-Portals und erhält eine Zugangsberechtigung, die von Wedolo als kryptischer, elektronischer Schlüssel (im Folgenden „Token" genannt) gespeichert und über die der Nutzer bei zukünftigen Logins zu dem entsprechenden Partner-Dienst im Hintergrund automatisch authentifiziert und autorisiert wird.
Der Zugang zur Nutzung der zugangsbeschränkten Inhalte und Angebote der teilnehmenden Partner-Portale aus Wedolo heraus erfordert die vorherige Registrierung des Nutzers auf den jeweiligen Seiten der Partner und die Zuweisung und Freischaltung der erforderlichen Zugangsdaten durch die jeweiligen Instanzen der Partner-Dienste.
Zugang zu den geschützten Bereichen der angeschlossenen Portale der Partner erhält der Nutzer dann durch Login auf Wedolo. Der Login-Vorgang gegen den Globalen-Login-Service (im Folgenden „GLS" genannt) von Wedolo stellt sicher, dass dem Nutzer über das ihm zugewiesene „Token" nach erfolgreicher Authentifizierung und Autorisierung auf dem Partner-Portal Zugriff auf die für ihn relevanten Inhalte hat.
Der Login-Service der Partnerportale ist für die Sicherstellung der korrekten Authentifizierung und Autorisierung an ihrem jeweiligen Portal zuständig.
Wedolo bietet mit dem „GLS" einen zentralen Registrierungsdienst für das „SSO"-Verfahren, über den der Nutzer die erforderlichen Zugangsdaten für alle teilnehmenden Portale der Wedolo-Partner verwalten kann. Nach der Registrierung bei Wedolo und einmaligem Login auf den jeweiligen Partner-Portalen übernimmt der „GLS" als zentrales Werkzeug die Anmeldung bei den teilnehmenden Partner-Portalen.

1. Geltungsbereich

1.1 Die nachfolgenden Besonderen Nutzungsbedingungen gelten für die Nutzung des Single-Sign-on-Authentifizierungs-Dienstes und alle von Wedolo in diesem Verhältnis angebotenen und erbrachten Leistungen. Anbieter des „SSO"-Authentifizierungs-Dienstes ist Wedolo, betrieben von der Wedolo Betriebsgesellschaft mbH, Heidenkampsweg 102, 20097 Hamburg, E-Mail: kontakt@wedolo.de.
1.2 Für die Vertragsverhältnisse des Nutzers mit den teilnehmenden Partner-Portalen und deren Onlineangebote, in denen der „SSO"-Authentifizierungs-Dienst genutzt wird bzw. werden kann, gelten gegebenenfalls eigene allgemeine Geschäfts- bzw. Nutzungsbedingungen der Diensteanbieter, bzw. der Partner-Portale.

2. Leistungen

2.1 „SSO" bedeutet im Falle des „SSO"-Authentifizierungs-Dienstes von Wedolo, dass jeder Nutzer sich nach einer einmaligen Registrierung und Authentifizierung für alle zugangsbeschränkten Dienste, Bereiche und Anwendungen auf den Portalen der Wedolo-Partner, die den „SSO"-Authentifizierungs-Dienst verwenden, mit einheitlichen Zugangsdaten anmelden (einloggen) kann, ohne dass er für die jeweiligen Internet-Portale eigene Login-Prozesse durchlaufen muss, wie das sonst der Fall wäre.
2.2 Der Nutzer erhält durch den „SSO"-Authentifizierungs-Dienst eine portalübergreifende „Identität", die von den teilnehmenden Internet-Portalen erkannt und verifiziert werden kann.
2.3 Der „SSO"-Authentifizierungs-Dienst ermöglicht dem Nutzer über das Modul „Externe Services verwalten" die einfache und zentrale Verwaltung seines „SSO"-Account. Der Nutzer kann auf diesem Weg seinem Account mögliche weitere Zugänge zu Partner-Portalen hinzufügen oder wieder löschen.
2.4 Der „SSO"-Authentifizierungs-Dienst selbst ist für den Nutzer von Wedolo kostenlos.

3. Identifizierung und Registrierung

3.1 Für die Nutzung des „SSO"-Authentifizierungs-Dienstes muss sich der Nutzer auf Wedolo registrieren.
3.2 Sofern der Nutzer sich bei einem Internet-Portal eines teilnehmenden Partner-Portals anmeldet, und ein solches erstmals besucht, wird die Zugangsberechtigung auf einer Login-Maske des Partner-Portals abgefragt.
3.3 Die Eingabe der Login-Daten auf der Login-Maske des Partner-Portals stellt die Angebotserklärung des Nutzers auf Abschluss der Vereinbarung über die Nutzung des „SSO"-Authentifizierungs-Dienstes (nachfolgend auch bezeichnet als „Nutzungsvereinbarung") dar. Wedolo nimmt dieses Angebot an, indem der Nutzer zu den geschützten Inhalten des Partner-Portals freigeschaltet wird. Die Nutzungsvereinbarung ist damit jeweils zustande gekommen.
3.4 Der Nutzer hat keinen Anspruch auf Freischaltung und Zulassung zu den Partner-Portalen.
3.5 Wedolo ist berechtigt, einzelne Registrierungen ohne Angabe von Gründen abzulehnen.

4. Gebrauch der Zugangsdaten, Zugang zu den Portalen

4.1 Hat der Nutzer sich beim „SSO“- Authentifizierungs-Dienst von Wedolo für die Nutzung eines Partner-Portals freigeschaltet, so erhält er Zugang zu den zugangsbeschränkten Inhalten und Angeboten der teilnehmenden Partner-Portale, indem er lediglich auf Wedolo seine Login-Daten, E-Mail-Adresse und Passwort, auf der Login-Maske eingibt.

4.2 Der Globale-Login-Service (im Folgenden „GLS“ genannt) von Wedolo hat zu keiner Zeit Kenntnis der Zugangsdaten einzelner Nutzer zu den Partner-Portalen. Dementsprechend können und werden auch keine Zugangsdaten im „GLS“ gespeichert. Bei positiver Authentifizierung und Autorisierung an einem Partner-Portal bekommt der „GLS“ lediglich „Token“ zurück, der vom „GLS“ zum Nutzer abgespeichert wird. Dieser „Token“ wird bei allen weiteren Aufrufen der Partner-Portale aus Wedolo heraus mit übermittelt und kann von den Login-Diensten der Partner-Portale ausgewertet werden.

4.3 Die Zugangsdaten zu Wedolo sind ausschließlich für die persönliche Nutzung durch den betreffenden Nutzer bestimmt. Der Nutzer darf die Daten, insbesondere sein Passwort, nicht an Dritte weitergeben, auch nicht an Familienangehörige oder Kollegen. Der Nutzer ist verpflichtet, die Zugangsdaten, insbesondere das Passwort, stets geheim zu halten sowie die unberechtigte Nutzung der teilnehmenden Portale durch Dritte zu verhindern. Der Nutzer hat sicherzustellen, dass Zugangsdaten Dritten nicht unrechtmäßig bekannt werden und diese vor Dritten geheim zu halten.

4.4 Der durch die Zugangsdaten gewährte Zugangsumfang auf den Partner-Portalen ist abhängig von den Nutzungsbedingungen des jeweiligen Portals.

4.5 Wedolo weist darauf hin, dass die Internet-Portale der Partner jeweils von der in der Anbieterkennzeichnung des Portals genannten Gesellschaft betrieben werden. Wedolo ist für die dortigen Inhalte und Angebote nicht verantwortlich.

5. Ende und Entziehung der Zugangsberechtigung zu den Partner-Portalen

5.1 Wedolo behält es sich vor, die Zugangsdaten des Nutzers bei Verstößen gegen diese Nutzungsbedingungen, insbesondere wegen

- falscher Angaben bei oder nach der Registrierung und/oder
- unbefugter Weitergabe oder Offenlegung der Zugangsdaten, insbesondere des Passwortes,

zeitweilig oder dauerhaft zu sperren und/oder dem Nutzer den Zugang mit sofortiger Wirkung oder mit einer in unserem Ermessen stehenden Frist endgültig zu entziehen und/oder die Nutzungsvereinbarung außerordentlich und fristlos zu kündigen. Nach einem solchen Fall darf sich der Nutzer ohne unsere vorherige ausdrückliche Zustimmung von Wedolo nicht erneut registrieren.

5.2 Die Zugangsberechtigung zu Partner-Portalen erlischt ferner automatisch, sobald der Nutzer nicht mehr zu der auf dem Partner-Portal registrierten Personengruppe gehört. In diesem Fall wird der „Token“ nicht positiv identifiziert und der Nutzer wird vom Login-Dienst des Partner-Portals abgewiesen.

6. Beendigung der Nutzungsvereinbarung

Die Besondere Nutzungsvereinbarung zum „SSO“ ist Teil der Allgemeinen Nutzungsvereinbarung. Sie endet mit dem Ende der Registrierung des Nutzers für den Single-Sign-On-Authentifizierungsdienst.

7. Datenschutz

Der Schutz und die Sicherheit der personenbezogenen Daten unserer Nutzer ist uns sehr wichtig. Alle Informationen hierzu finden sich in der Datenschutzerklärung von Wedolo.

8. Änderungen der Besonderen Nutzungsbedingungen

Wedolo ist berechtigt, diese Nutzungsbedingungen jederzeit mit Wirkung für die Zukunft aus folgenden Gründen zu ändern:

- aus rechtlichen und regulatorischen Gründen,
- aus Sicherheitsgründen,
- um bestehende Services weiterzuentwickeln und/oder neue Services einzuführen sowie
- um technische Anpassungen vorzunehmen und die Funktionsfähigkeit der Services sicherzustellen.

<u>ANHANG II:</u> Vertrag zur Auftragsverarbeitung

Vertrag zur Auftragsverarbeitung

zwischen

Auftraggeber:
Auftraggeber dieses Vertrags sind die jeweiligen Unternehmen welche die Wedolo Plattform nutzen

und

Auftragnehmer:

Wedolo Betriebsgesellschaft mbH
Heidenkampsweg 102
20097 Hamburg

1. Gegenstand, Art und Zweck der Beauftragung

Der Auftragnehmer wird im Zusammenhang mit den folgenden Leistungen als Auftragsverarbeiter gem. Art. 28 Datenschutzgrundverordnung (DSGVO) tätig:

- **Service: Kontrolle inkl Berichte**
- **Service: Notfallhilfe**
- **Service: Mitarbeiter**

Nähere Information zu diesen Services sind der Nutzungsvereinbarung sowie der Datenschutzerklärung zur Wedolo Plattform zu entnehmen.

2. Dauer der Beauftragung

Die Laufzeit dieses Vertrages entspricht der Laufzeit der Nutzungsvereinbarung im Hinblick auf die oben genannten Services.

3. Art der personenbezogenen Daten

Folgende Kategorien von personenbezogenen Daten werden im Rahmen dieses Vertrages durch den Auftragnehmer verarbeitet.

- **Service: Kontrolle inkl. Berichte**
  Name, Vorname, GPS – Ortung
- **Service: Notfallhilfe**
  GPS - Ortung
- **Service: Mitarbeiter**
  Name, Vorname, Mobilnummer, Mailadresse, Geburtsdatum, Nationalität

4. Kategorien betroffener Personen

Es werden die personenbezogenen Daten folgender Betroffener verarbeitet:

- personenbezogene Daten der durch den Auftraggeber angelegten Mitarbeiter

5. Verarbeitung personenbezogenen Daten auf Weisung des Auftraggebers

Der Auftragnehmer wird personenbezogene Daten ausschließlich im Rahmen der Weisungen des Auftraggebers verarbeiten. Die Regelungen dieser Vertragsanlage und der sonstigen zu Grunde liegenden Verträge stellen hierbei abschließend die Weisungen des Auftraggebers dar. Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, falls er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen verstößt.

6. Drittstaatentransfer

Sofern für die Erfüllung des Auftragszwecks eine Datenübermittlung nach Drittstaaten erforderlich ist, wird der Auftragnehmer die besonderen Voraussetzungen der Artikel 44 ff. DSGVO einhalten. Insbesondere wird der Auftragnehmer nur solche Subunternehmer mit Datenverarbeitung in Drittstaaten einsetzen, sofern für den Drittstaat ein Angemessenheitsbeschluss der EU Kommission vorliegt, mit den Subunternehmern die jeweils passenden EU-Standardvertragsklauseln vereinbart wurden oder für diese genehmigte verbindliche interne Datenschutzvorschriften (sog. Binding Corporate Rules) bestehen.

7. Vertraulichkeit

Der Auftragnehmer wird die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichten.

8. Sicherheit der Verarbeitung

Der Auftragnehmer wird ausreichende technische und organisatorische Maßnahmen implementieren.
Die getroffenen Maßnahmen sind in der Anlage *„Beschreibung der technischen und organisatorischen Maßnahmen“* beschrieben. Der Auftragnehmer wird die technischen und organisatorischen Maßnahmen stets an Hand des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen weiterentwickeln und anpassen. Hierbei darf der Schutzstandard der im Vertrag beschriebenen technischen und organisatorischen Maßnahmen nicht unterschritten werden.

Der Auftragnehmer wird dem Auftraggeber auf Anforderung alle erforderlichen Informationen zum Nachweis der vertraglichen Pflichten zur Verfügung stellen, insbesondere im Hinblick auf Einhaltung der technischen und organisatorischen Maßnahmen (z.B. durch eine schriftliche Einhaltungsbestätigung des betrieblichen Datenschutzbeauftragten des Auftragnehmers).

Der Auftragnehmer ist berechtigt, selbst oder durch von ihm beauftragte Prüfer, die Einhaltung der vertraglichen Pflichten durch Inspektionen zu prüfen. Von diesem Recht wird der Auftragnehmer nur dann Gebrauch machen, wenn Auskünfte und zur Verfügung gestellte Dokumentationen des Aufragnehmers zur Überzeugungsbildung im Einzelfall nicht ausreichend sind.

9. Subunternehmer

Der Auftragnehmer ist grundsätzlich berechtigt, Subunternehmer für die Erbringung der vertraglich vereinbarten Leistungen zu beauftragen.

Der Auftraggeber ist mit der Beauftragung folgender Subunternehmer einverstanden:

Subunternehmer	**Sitz des Subunternehmers**	**Art der Beauftragung**
BLUE Consult GmbH	Krefeld	Auftragsverarbeitung
BLUE Smart Services GmbH	Krefeld	Auftragsverarbeitung

Der Auftragnehmer informiert den Auftraggeber bei einer Anpassung der AGB über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, die als Subunternehmer tätig werden. Der Auftraggeber kann gegen derartige Änderungen Einspruch erheben, sofern berechtigte Gründe vorliegen. Im Falle eines Einspruches durch den Auftraggeber, hat der Auftragnehmer die Wahl, ob er die vertragliche Leistung weiter ohne die beabsichtigte Beauftragung des Subunternehmers durchführen möchte oder ob er den Vertrag außerordentlich mit sofortiger Wirkung kündigt.

Der Auftragnehmer hat vertraglich sicherzustellen, dass die mit seinen Subunternehmern vereinbarten Regelungen ein mit diesem Vertrag vergleichbares Datenschutzniveau gewährleisten. Dies gilt insbesondere im Hinblick auf die beim Subunternehmer implementierten technischen und organisatorischen Maßnahmen.

10. Unterstützungsleistungen des Auftragnehmers

Der Auftragnehmer wird den Auftraggeber unterstützen, sofern betroffene Personen im Zusammenhang mit der vertraglichen Leistung Anträge auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte stellen. Die Beantwortung der Anträge gegenüber den Betroffenen erfolgt dabei grundsätzlich durch den Auftraggeber.

Der Auftragnehmer wird den Auftraggeber bei der Einhaltung der in den Artikel 32 - 36 DSGVO geregelten Pflichten unterstützen.

Insbesondere wird der Auftragnehmer dem Auftraggeber unverzüglich solche Verletzungen des Schutzes personenbezogen Daten von Betroffenen anzeigen, bei denen Meldepflichten nach Artikel 33, 34 DSGVO nicht ausgeschlossen werden können.

11. Rückgabe oder Löschung der personenbezogenen Daten

Der Auftragnehmer wird nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Auftraggebers löschen oder zurückgeben, sofern nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

Beschreibung der technischen und organisatorischen Maßnahmen

Die nach Art. 32 EU DSGVO erforderlichen technischen und organisatorischen Maßnahmen werden wie im Folgenden beschrieben umgesetzt:

I. Organisatorische Maßnahmen

1. Wedolo hat für die Verarbeitung eigener Daten und im Rahmen der Auftragsdatenverarbeitung ein umfassendes Datensicherheitskonzept realisiert, das sowohl in baulicher, personeller, organisatorischer als auch technischer Hinsicht alle erforderlichen Vorkehrungen enthält, um die Sicherheit der zu verarbeitenden Daten und des Datenbestandes sowie den ungestörten Betriebsablauf zu gewährleisten.

2. Es ist ein Datenschutzbeauftragter (DSB) bestellt, der die Geschäftsleitung berät und auf die Einhaltung der gesetzlichen und die weitergehenden betrieblichen Datenschutzvorschriften hinwirkt. Zu seinem Aufgabenbereich gehört die Überwachung der ordnungsgemäßen Entwicklung von Anwendungsprogrammen und des Einsatzes von EDV-Systemen und Programmen, die Führung des Verfahrensverzeichnis, die Vorabkontrolle bei besonders risikoreichen automatisierten Verarbeitungen sowie das Vertraut-Machen der Mitarbeiter mit den Anforderungen des Datenschutzes durch geeignete Maßnahmen (z.T. durch Informationen, elektronische und persönliche Schulungsveranstaltungen) sowie die Beratung der Geschäftsleitung bzw. der Mitarbeiter in Datenschutzfragen. In der Wahrnehmung seiner Aufgaben hat der DSB uneingeschränkte Kontrollrechte.

3. Alle Mitarbeiter sind auf das Datengeheimnis und soweit sie an der elektronischen Kommunikation für Dritte mitwirken, auf das Fernmeldegeheimnis verpflichtet.

II. Sicherheit der Verarbeitung

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

- **Zutrittskontrolle**
  Maßnahmen die Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden verwehren:

1. Die Betriebsareale sind in mehrere Bereiche mit differenzierten Zugangsberechtigungen aufgeteilt.

2. Der Zutritt in Rechenzentren und andere sensible Bereiche ist nur berechtigten Personen gestattet.

3. Zutritte werden soweit möglich über elektronische Zutrittskontrollsysteme geregelt, z.B. Kartenleser, Transponder, hybride Systeme (Schlüssel mit Transponder). Zutritte in die Rechenzentren werden über das elektronische Zutrittskontrollsystem protokolliert.

4. Der Zutritt zum Produktionsbereich des Rechenzentrums ist den Mitarbeitern der Systemtechnik und der Systemprogrammierung vorbehalten. Die Erteilung von weiteren Berechtigungen zum Zutritt erfolgt nur nach schriftlicher Beantragung und Genehmigung.

5. Videokameras überwachen die Zugänge in die RZ-Bereiche.

- **Zugangskontrolle**

  Maßnahmen die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

1. Benutzerzugänge

   Durch geeignete technische Maßnahmen wird sichergestellt, dass ein Zugang zu Systemen und Anwendungen erst nach erfolgreicher Authentifizierung erfolgen kann. Die Authentifizierung an IT-Ressourcen sowie der Umgang mit Authentifizierungsdaten sind verbindlich geregelt. Minimaler Standard sind dabei eine individuelle Kennung und ein Passwort, das nur dem Benutzer selbst bekannt ist. Auf EDV-Systemen gespeicherte Benutzer-Passworte sind kryptographisch vor unberechtigter Kenntnisnahme geschützt.

   Nach 5 erfolglosen Anmeldeversuchen erfolgt eine automatische Sperrung des Zugangs. Die Rücksetzung erfolgt durch verbindlich geregelte Prozesse, die die Verifikation des Nutzers sicherstellen.

   Eine verbindliche Richtlinie regelt den Umgang mit Benutzerkennungen und Passwortern für alle Benutzer und IT-Systeme.

2. Netzwerkzugänge

   Alle Netzwerkzugänge von und zu fremden Netzen (wie z.B. Internet, Geschäftspartnern, Auftragnehmern, Kunden) werden durch Firewalls abgesichert. Die Übertragung sensibler Daten über fremde Netze wird durch eine geeignete Verschlüsselung geschützt.

   Die Kommunikation mit mobilen Arbeitsplätzen wird durch zusätzliche Maßnahmen auf Basis kryptographischer Verfahren abgesichert.

3. Systemkontrollen

   Bereinigungen von sicherheitsrelevanten Fehlern in Software (Schwachstellen) werden regelmäßig nach vereinbarten Kriterien durchgeführt.

   Schadcodeschutz (z. B. Anti-Virus, Anti-Spyware) ist auf allen Systemen etabliert, die dafür anfällig sind. Ein mehrstufiger Schadcodeschutz findet beim Datenaustausch mit dem Internet (z.B. E-Mail, Web) Verwendung. Sämtliche Schadcodeschutzlösungen werden regelmäßig auf aktuellem Stand gehalten.

   Auffällige System- und Netzwerkereignisse werden automatisch erfasst und regelmäßig ausgewertet. Auffälligkeiten werden analysiert und erforderliche Maßnahmen eingeleitet.

   Es erfolgt eine automatische Zugangssperre bei einer Benutzerinaktivität von mehr als 15 Minuten. Die Nutzung von Arbeitsplatzsystemen erfolgt standardmäßig ohne administrative Berechtigungen. Die Administration von Systemen erfolgt nur über verschlüsselte Anbindungen bzw. Protokolle.

   Auf Arbeitsplätzen werden sämtliche Daten verschlüsselt gespeichert.

- **Zugriffskontrolle**

  Maßnahmen die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden:

1. IT-Systeme und Anwendungen können ausschließlich von berechtigten Benutzern aufgerufen werden. Innerhalb der Anwendungen können Zugriffseinschränkungen rollenspezifisch festgelegt werden. Jeder Benutzer hat nur Zugriff auf die Daten, die er für seine Aufgabenerfüllung benötigt.

2. Die Berechtigungsrollen werden in den Zugriffs-Schutzsystemen der Anwendungen oder zentral durch das Berechtigungsmanagement verwaltet. Berechtigungsrollen werden durch Antrag und nach Genehmigung vergeben, wobei je nach Kritikalität mindestens das 4-Augen-Prinzip oder weitere Genehmigungsstufen vorgesehen sind.

3. Zugriffe auf Systeme zur Verarbeitung von Daten werden über Berechtigungsprofile und Berechtigungsgruppen erteilt. Der Kreis der dafür verantwortlichen Systemprogrammierer und Administratoren wird über ein gesondertes Berechtigungsverfahren verwaltet. Zudem werden nachgelagerte Kontrollen durchgeführt (Überprüfung der systemimmanenten Kontrolle, des Zugangsschutzes und der Rechtevergabe).

4. Das Netzwerk ist durch ein mehrstufiges Firewall-System vor unberechtigten Zugriffen aus dem Internet geschützt. Der Zugriff auf Dienste im Internet wird vom Firewall-System ebenfalls kontrolliert und ist durch zusätzliche Authentisierungsmechanismen abgesichert. Die Datenübertragung von personenbezogenen Daten erfolgt verschlüsselt.

- **Trennungskontrolle**
  Maßnahmen die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

1. In allen wichtigen Bereichen besteht das Prinzip der Funktionstrennung; das heißt, alle mit der Datenverarbeitung befassten Abteilungen sind funktionell und organisatorisch getrennt.

2. Das Berechtigungskonzept sowie die vorhandenen Benutzerprofile stellen eine logische Trennung der Daten, die zu unterschiedlichen Zwecken erhoben und entsprechend dieser Zwecke getrennt zu verarbeiten sind, sicher.

3. Es besteht grundsätzliche Trennung zwischen Test und Produktionsbetrieb.

- **Pseudonymisierung (Art. 32 Abs. 1 lit. a EU DSGVO)**
  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

  Sofern eine Pseudonymisierung nach dem Auftragszweck möglich ist, werden die Daten der Betroffenen ganz oder teilweise pseudonymisiert.

2. Integrität (Art. 32 Abs. 1 lit. b EU DSGVO)

- **Weitergabekontrolle**
  Maßnahmen die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

1. Der Transport von Datenträgern wird grundsätzlich vermieden. Sollte ein Transport in Ausnahmefällen erforderlich sein, wird gewährleistet, dass Daten während des Transports von Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Datenträger werden in verschlossenen Behältnissen und/oder verschlüsselter Form nach Stand der Technik versandt. Die Beschriftungen der Datenträger lassen keinen Rückschluss auf die enthaltenen Daten zu.

2. Leitungen, Anschlüsse und Verteiler für Datenfernübertragung in den Betriebsstätten liegen in nicht frei zugänglichen Sicherheitsbereichen.

3. Automatisierte sowie manuelle Datenfernübertragungen personenbezogener Daten erfolgen auf geschütztem Weg, z.B. durch verschlüsselten Dateitransfer, verschlüsselte Kommunikationswege (Leitungsverschlüsselung), durch verschlüsselte E-Mail oder mittels verschlüsselter E-Mail-Anhänge.

4. Vertrauliche bzw. personenbezogene Daten auf Papier sowie Entsorgungsgut mit schutzwürdigem Inhalt werden über spezielle Sicherheitscontainer durch externe Entsorger unter Einhaltung einer hohen Sicherheitsstufe vernichtet.

   Sofern die Entsorgung vertraulicher bzw. personenbezogener Daten auf Papier nicht über Sicherheitscontainer möglich ist, werden diese mit Schreddern mindestens der Schutzklasse 3 gemäß DIN 66399 geschreddert.

5. Datenträger für die Datensicherung (Magnetbänder, Bandkassetten) werden in einem besonderen Sicherheitsbereich aufbewahrt.

- **Eingabekontrolle**

1. Es wird protokolliert, ob und wann sich ein Benutzer an einer IT-Anwendung angemeldet hat.

2. Eingaben in die IT-Anwendung werden inkl. Erfassungszeitpunkt und User-ID des Erfassens systemseitig protokolliert.

3. Es ist gewährleistet, dass Benutzer und Prozesse nur mittels der getesteten und freigegebenen Programmversion auf Daten zugreifen können.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c EU DSGVO)

- **Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit**
  Maßnahmen die gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind:

1. Für die Rechenzentren (RZ) sind umfangreiche Brandschutz-, Verlustsicherungs- und Katastrophenschutz-Maßnahmen umgesetzt. Hierzu gehören die Absicherung sämtlicher Flächen in den RZ und deren Umgebung durch Brandmelde- und stationäre Feuerlöschanlagen, Maßnahmen zur Datensicherung sowie die Auslagerung von Datensicherungsbeständen.

2. Es ist ein vollständiges Backup- und Recovery-Konzept mit täglicher Sicherung und katastrophensicherer Aufbewahrung der Datenträger im Sinne eines Business Continuity Management installiert.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d EU DSGVO)

- **Datenschutz-Management**

1. Der Datenschutzbeauftragte wird durch die Datenschutzorganisation in die relevanten betrieblichen Prozesse eingebunden.

2. Es finden regelmäßige Prüfungen durch die Innenrevision statt.

- **Auftragskontrolle**
  Maßnahmen die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden:

  In der IT-Anwendung ist sichergestellt, dass die zur Verarbeitung gespeicherten Daten entsprechend den gesetzlichen Vorschriften nur im Rahmen der Weisungen des jeweiligen Auftraggebers verarbeitet und insbesondere auch nicht an unbefugte Dritte weitergegeben werden.