Beitrittserklärung einer Gesellschaft

Die nachfolgend genannte Gesellschaft erklärt der LOGENIOS eG (im Folgenden: „LOGENIOS“) beizutreten und sich mit einem Geschäftsanteil von 1.200,00 Euro zzgl. eines Eintrittsgeldes in Höhe von 3.800,00 Euro an LOGENIOS gemäß der LOGENIOS-Satzung zu beteiligen.

Name/Firma der Gesellschaft*

Straße und Hausnummer*

PLZ und Ort*

Register und Registernummer* (bitte Registerauszug beilegen)

Telefon*

Mobiltelefon

E-Mail*

Website*

Ort, Datum*

Unterschrift/en des Beitretenden*

Name/n des/der Unterzeichnenden (Druckbuchstaben)*

Zugewiesene Mitgliedsnummer (wird durch LOGENIOS nach Aufnahme eingetragen)

Weitere Erklärungen des Beitretenden

1. Satzung

Dem Beitretenden ist bekannt, dass die Satzung der LOGENIOS unter www.logenios.com/satzung abrufbar ist. Der Beitretende bestätigt, dass ihm ein Ausdruck der Satzung angeboten wurde. Die Satzung der LOGENIOS hat der Beitretende zur Kenntnis genommen und erkennt diese an.

Ort, Datum*

Unterschrift/en des Beitretenden*

Name/n des/der Unterzeichnenden (Druckbuchstaben)*

2. Werbliche Ansprache

Über aktuelle Aktivitäten, Produktangebot, Produktverbesserungen sowie Serviceangebote der LOGENIOS möchte der Beitretende per Telefon und per E-Mail informiert werden. Die Einwilligung kann jederzeit widerrufen werden.

Ort, Datum

Unterschrift/en des Beitretenden

Name/n des/der Unterzeichnenden (Druckbuchstaben)

3. Auftragsverarbeitungsvertrag

Die datenschutzrechtlichen Verpflichtungen zwischen den Parteien sind in dem „Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO, Stand April 2020“ (siehe Anlage) enthalten.

Der Beitretende stimmt dem Abschluss dieser Vereinbarung zu.

Ort, Datum*

Unterschrift/en des Beitretenden*

Name/n des/der Unterzeichnenden (Druckbuchstaben)*

4. Verschwiegenheitsvereinbarung

Die Belehrung und Verschwiegenheitsverpflichtung der LOGENIOS für Mitglieder sind in der „Vereinbarung zur Verschwiegenheit nach, Stand Mai 2020“ (siehe Anlage) enthalten.

Der Beitretende stimmt dem Abschluss dieser Vereinbarung zu.

Ort, Datum*

Unterschrift/en des Beitretenden*

Name/n des/der Unterzeichnenden (Druckbuchstaben)*

Weitere Erklärungen des Beitretenden

5. Sonstige Angaben

☐ Der Beitretende kommt auf Empfehlung von folgendem LOGENIOS-Mitglied.

Name der Gesellschaft/Person

☐ Der Beitretende hat derzeit folgenden LOGENIOS-Ansprechpartner.

Ansprechpartner

Feststellungen der Genossenschaft

HINWEIS: Wird von LOGENIOS ausgefüllt!

☐ Der Beitritt zu der LOGENIOS eG wurde durch den Vorstand zugelassen. Der Beitretende wurde somit als Mitglied aufgenommen und in die Mitgliederliste eingetragen.

Datum Aufnahme

☐ Dem Mitglied wurde eine Mitgliedsnummer zugewiesen.

Mitgliedsnummer

Datum Zuweisung

Vertrag zur Auftragsverarbeitung

gemäß Art. 28 DS-GVO, Stand April 2020

zwischen

dem in der anliegenden Beitrittserklärung genannten Mitglied
im Folgenden „Partner“ genannt

und

LOGENIOS eG
Industriestraße 7
63829 Krombach
Amtsgericht Aschaffenburg, GenReg Nr. 126
im Folgenden „LOGENIOS“ genannt

1. Gegenstand und Dauer des Auftrags

Die Dauer dieses Auftrages richtet sich nach der Nutzung der unter §2 des SaaS Vertrages angegebenen Vertragslaufzeiten.

2. Konkretisierung des Auftragsinhalts

Art und Zweck der vorgesehenen Verarbeitung von Daten:

Berechtigtes Interesse der verantwortlichen Stelle. Optimierung der Betriebsprozesse und Abläufe beim Einsatz von Dienstfahrzeugen

EU Mitgliedsstaat / Drittland:

Die Erbringung der vertraglich vereinbarten Datenverarbeitung 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 Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind.

Art der Daten:

- Daten Berufskraftfahrer (inkl. Fahrerkarte, Unternehmerkarte)
- Daten der Zugmaschine (inkl. Standortdaten)
- Auftragsdaten/Kundendaten

3. Technisch-organisatorische Maßnahmen

Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. 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.

Der Auftragnehmer hat die Sicherheit gem. Artt. 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 [Einzelheiten in der Anlage Technische und organisatorische Maßnahmen].

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.

4. Berichtigung, Einschränkung und Löschung von Daten

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. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessen werden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

Der Auftragnehmer hat einen Datenschutzbeauftragten schriftlich bestellt, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt. Als externer Datenschutzbeauftragter des Auftraggebers ist bestellt: Herr Thorsten Hofer, eMail: datenschutz@leformatics.de, Telefon: +49 152 3404 5875

Die Wahrung der Vertraulichkeit gemäß Artt. 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.

Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in der Anlage Technische und organisatorische Maßnahmen].

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

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.

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.

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.

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

6. Unterauftragsverhältnisse

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

Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Der Auftraggeber stimmt der Beauftragung der Unterauftragnehmer zu. Eine Liste der Unterauftragnehmer kann dem Auftraggeber jederzeit zur Verfügung gestellt werden.

Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Pkt. 6.1 und 6.2 eingesetzt werden sollen.

Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform).

Aktuelle Unterauftragnehmer sind
- SPEDION GmbH, Industriestraße 7, 63829 Krombach (Hosting)
- Amazon Web Services Inc. 410 Terry Avenue North, Seattle, WA 98109-5210, USA mit Nutzung des Serverstandortes in Frankfurt (Europa-Cloud).

7. Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennendem Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

Eine Überprüfung vor Ort ist auf einen Tag pro Kalenderjahr begrenzt.

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.

Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch
- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artt. 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

- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

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

Ein Datenschutzbeauftragter beim Auftraggeber

○ wurde freiwillig oder gesetzlich bestellt:
Name: _____
Telefon: _____
E-Mail: _____

○ ist nicht notwendig.

10. Löschung und Rückgabe von personenbezogenen Daten

Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

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

11. Informationspflichten, Schriftformklausel, Rechtswahl

Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahmung, durch ein Insolvenz- oder Vergleichsverfahren, oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer dem Auftraggeber unverzüglich davon in Kenntnis zu setzen. Hoheit und Eigentum der Daten liegen ausschließlich beim Auftraggeber als verantwortliche Stelle im Sinne der DS-GVO.

Änderungen und Ergänzungen dieser Anlage zum Datenschutz und aller ihrer Bestandteile bedürfen der Schriftform.

Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit dieses Vertrags zum Datenschutz im Übrigen nicht.

12. Haftung und Schadensersatz

Die Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 83 DS-GVO getroffenen Regelung.

Krombach, der 24. April 2020

Günter Englert, Vorstand LOGENIOS eG

Wolfram Grohse, Vorstand LOGENIOS eG

Anlage 1 zum Vertrag zur Auftragsverarbeitung

gemäß Art. 23 DS-GVO, Stand April 2020

Technische und organisatorische Maßnahmen im Sinne des Art. 32 DS-GVO der von LOGENIOS eG als LOGENIOS getroffenen Maßnahmen (Art. 30 Abs. 2 lit. d DSGVO)

A: Vertraulichkeit

(gem. Art 32 Abs. 1 lit. DS-GVO)

1. Zutrittskontrolle

Zutritt Gebäude
Der Zutritt zum Bürogebäude und zu den Serverräumen erfolgt über eine Schließanlage. Für sensible Bereiche werden zusätzlich Videoüberwachung sowie Einbruchmeldeanlagen eingesetzt.
Der Zutritt wird je nach Funktion der Mitarbeiter und zugriffsberechtigte Personen vergeben.
Für Externe (Besucher, Lieferanten, Zustelldienste, u. a.) ist ein Zutritt nur mit Anmeldung am Empfang möglich.

Besucher werden persönlich in Empfang genommen und auch wieder zur Tür begleitet. Besucher sind während des gesamten Aufenthaltes in Begleitung eines Mitarbeiters.

2. Zugangskontrolle

Mitarbeiter
Jeder Mitarbeiter bekommt die für seine Tätigkeit notwendigen Berechtigungen und Systemzugänge.

Accounts
Accounts von Mitarbeitern werden personenbezogen vergeben. Technische Accounts werden entsprechend dokumentiert.
Inaktive Accounts werden unmittelbar nach Austritt deaktiviert oder gelöscht.

Umgang mit Passwörtern
Alle Passwörter werden regelmäßig geändert (technisch vorgegeben). Die Nutzung unterliegt strengen Kontrollen und darf nur von autorisierten Personen erfolgen.
Die Vergabe der Passwörter erfolgt auf Grundlage der Passwort-Vorgaben der LOGENIOS eG

Umgang mit Hardware
Die Einbindung fremder Hardware in das Unternehmensnetzwerk ist technisch unterbunden. Dies gilt für das physikalische Einbinden via Netzwerkkabel als auch die Verbindung mit WLAN, sowie andere mögliche Anbindungen.

Software

Auf dem bereitgestellten lArbeitsplatz darf ausschließlich freigegebene Software installiert und genutzt werden.
Das Herunterladen von ausführbaren Dateien (Programmen) oder Betriebssystemen ist technisch unterbunden.

Umgang mit Daten
Jeder Mitarbeiter ist auf die Vertraulichkeit nach DS-GVO verpflichtet und entsprechend im Umgang mit personenbezogenen Daten geschult.

Firewalls
Das Firmennetzwerk ist mit einer Firewall geschützt. Es wurden eine Reihe von weiteren Sicherheitsmaßnahmen getroffen, um bspw. Intrusion Detection sowie Denial of Service Attacken zu verhindern.
Funktionen, Logfiles und Sicherheitsstatus werden regelmäßig überprüft und dokumentiert.

Virenschutz
Grundsätzlich werden alle Rechner mit Virenschutz und aktivierter Firewall betrieben.

3. Zugriffskontrolle
Hier wird speziell auf die Rollen-/Rechtekonzepte eingegangen:

- Rechte werden je nach Funktion des Mitarbeiters auf Basis Need-to-Know vergeben (Rechte- und Rollenkonzept)
- Rechte werden personenbezogen vergeben, siehe Pkt. 2.2
- Zugriffsrechte werden dokumentiert
- Zugriffsrechte werden regelmäßig auf Notwendigkeit kontrolliert
- Zugriffsrechte werden im Freigabeprozess genehmigt

4. Trennungskontrolle
Die Daten der jeweiligen Kunden werden getrennt vorgehalten.

5. Pseudonymisierung (Artt. 32 Abs. 1 lit. A DS-GVO; Art. 25 Abs. 1 DS-GVO)
Daten werden da wo es möglich ist pseudonymisiert. An Stelle der Pseudonymisierung kann auch eine Anonymisierung oder Löschung erfolgen, je nach gesetzlicher oder vertraglicher Vorgabe.

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

1. Weitergabekontrolle

Daten werden bei der Übertragung verschlüsselt, so dass unberechtigter Zugriff ausgeschlossen ist.

2. Eingabekontrolle

Sollte ein Zugriff im Rahmen von Supportmaßnahmen notwendig werden, wird der Zugriff protokolliert, Veränderungen an Daten werden geloggt.

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

Backup

Es wurden umfangreiche Maßnahmen zur Sicherung und Verfügbarkeit der Daten getroffen.
Eine stichprobenartige Widerherstellung der Daten wird regelmäßig getestet und die Verfügbarkeit der Daten zu gewährleisten.

D: Verfahren zur regelmäßigen Überprüfung, Bewertung

(Art. 32 Abs.1 lit. d DS- GVO; Art. 25 Abs.1 DS-GVO)

Externer Datenschutzbeauftragter

Die LOGENIOS eG setzt einen Datenschutzbeauftragten ein, welcher alle gesetzlich vorgegebenen Maßnahmen zur Einhaltung und Überprüfung der erforderlichen datenschutzrechtlichen Maßnahmen umsetzt.

Incident-Response-Management

Die LOGENIOS eG trifft Maßnahmen zur präventiven Sicherheit.

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

Privacy by design/privacy by default. Die LOGENIOS eG hat einen Prozess zur Einbindung des Datenschutzbeauftragten bei bestehenden und neuen Verfahren. Dabei wird die Einhaltung der datenschutzrechtlichen Vorgaben umgesetzt.

Auftragskontrolle

Die LOGENIOS eG schließt im Rahmen einer Auftragsverarbeitung Verträge gem. Art. 28 DS-GVO ab.

Notfall

Notfälle können bei Feuer, Einbruch, Ausfall eines einzelnen Mitarbeiters (Administrator) oder bei Störung der IT vorliegen. Für den Notfall werden spezielle Accounts bereitgestellt, die ausschließlich im Notfall zu benutzten sind. Es gibt Vertretungsregelungen, sowie einen Alarmplan, der je nach Szenario entsprechend variiert.
Die Nutzung des Notfall-Benutzers wird protokolliert und erfolgt im 4-Augen-Prinzip.

Vereinbarung zur Verschwiegenheit

Stand Mai 2020

zwischen

dem in der anliegenden Beitrittserklärung
genannten Mitglied
im Folgenden „Partner“ genannt

und

LOGENIOS eG
Industriestraße 7
63829 Krombach
Amtsgericht Aschaffenburg, GenReg Nr. 126
im Folgenden „LOGENIOS“ genannt

§1
Der Partner beabsichtigt, der Genossenschaft LOGENIOS eG beizutreten.

Im Hinblick hierauf verpflichten der Partner und die LOGENIOS eG sich, die gegenseitig mitgeteilten geheimen Erkenntnisse und Informationen zur Information, die insbesondere im Zusammenhang mit Neuentwicklungen, Vorführungen, Versuchen und Gesprächen stehen, geheim zu halten. Sie treffen alle erforderlichen Maßnahmen, um deren Kenntnisnahme und Verwertung durch Dritte zu verhindern. Mitarbeiter und Angestellte sind, soweit sie hierzu nicht bereits aufgrund ihres Arbeitsvertrages angehalten sind, zur Geheimhaltung zu verpflichten.

§2
Der Interessent verpflichtet sich, die gegenseitig mitgeteilten Informationen, ohne ausdrückliche schriftliche Einwilligung durch die LOGENIOS nicht selbst zu verwerten.
Die LOGENIOS behält sich das alleinige und uneingeschränkte Recht zur Schutzrechtsanmeldung vor.

§3
Die Verpflichtung zur Geheimhaltung gilt nicht für Informationen, die bereits offenkundig sind (allgemein bekannt sind, zum Stand der Technik zählen etc.) und damit nicht mehr geheim oder schutzfähig sind. Wenn Offenkundigkeit einer Information später eintritt, erlischt die Verpflichtung insoweit ab diesem Zeitpunkt.

§4
Diese Verpflichtung zur Geheimhaltung gilt auch weiter, wenn die Mitgliedschaft in der Genossenschaft endet

Die Parteien werden Unterlagen, die sie jeweils vom anderen im Zusammenhang mit der Information usw. erhalten haben, nach Bekanntwerden der Offenkundigkeit, Kündigung der Absichtserklärung gem. § 1 S.1 oder Beendigung des Vertrages über die Zusammenarbeit unverzüglich dem jeweiligen Informationsgeber zurückgeben. Eventuell erstellte Dateien und sämtliche Kopien werden von sämtlichen Datenträgern gelöscht bzw. bei Verkörperung vernichtet.