Vertrag über die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten im Auftrag

(§ 11 Bundesdatenschutzgesetz, BDSG)

zwischen

der **myfactory International GmbH**
Agnes-Pockels-Bogen
80992 München

Auftragnehmer (im Folgenden „AN“ genannt)

und

der

Auftraggeber (im Folgenden „AG“ genannt)

alle gemeinsam im Folgenden „Parteien“ genannt.

1. Begriffsdefinitionen

1.1. Personenbezogene Daten sind nach § 3 Abs.1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

1.2. Datenverarbeitung im Auftrag ist die weisungsgebundene Erhebung und Verarbeitung und Nutzung personenbezogener Daten durch den Auftragnehmer im Auftrag des AG.

1.3. Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (z.B. Anonymisierung, Sperrung, Löschung, Herausgabe, Vernichtung) des Auftragnehmers mit personenbezogenen Daten gerichtete Anordnung des AG. Bestehende Weisungen (z.B. durch diese Vertragsergänzung) können vom AG danach durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

2. Gegenstand und Dauer des Auftrags

2.1. Dieser Vertrag regelt den Rahmen der datenschutzrechtlichen Rechte und Pflichten bei der Erhebung und Verarbeitung und Nutzung personenbezogener Daten durch den AN für den AG (im Folgenden „AG-Daten“) in dessen Auftrag und nach dessen Weisungen gemäß § 11 BDSG im Zusammenhang mit den im "Public Cloud (SaaS) - Vertrag" beschriebenen Aufgaben und Tätigkeiten.

2.2. Der AG bleibt verantwortliche Stelle im Sinne des § 3 Abs. 7 BDSG und entscheidet allein über Zwecke und Mittel der Erhebung, Verarbeitung und Nutzung. Er ist für die Rechtmäßigkeit der auftragsgemäßen Erhebung, Verarbeitung und Nutzung der AG-Daten verantwortlich. Ist der AG selbst Auftragnehmer für die Datenverarbeitung, bleibt der jeweilige Auftraggeber verantwortliche Stelle.

2.3. Der AN wird AG-Daten nach Maßgabe des Vertrags im Namen und im Auftrag des AG unter Einhaltung der organisatorischen und technischen Vorgaben nach Ziff. 4 erheben und verarbeiten. Der AN wird AG-Daten nicht im Sinne des § 3 Abs. 5 BDSG. Hierbei verpflichtet sich der AN besonders zu beachten:

- die technischen und organisatorischen Maßnahmen (Ziff. 4)
- die Pflichten zur Berichtigung, Löschung oder Sperrung von Daten (Ziff. 5)
- die besonderen datenschutzrechtlichen Pflichten (Ziff. 6)
- die Vorgaben zu Unterauftragsverhältnissen (Ziff. 7)
- die Kontrollrechte des AG und der verantwortlichen Stelle (Ziff. 8)
- die Mitteilungspflichten (Ziff. 9)
- das allgemeinen Weisungsrechts des AG (Ziff. 10)
- die Rückgabepflichten (Ziff. 12)

2.4. Dieser Vertrag wird auf unbestimmte Zeit geschlossen und kann von beiden Parteien zum Monatsende gekündigt werden.

2.5. Dieser Vertrag endet auch bei Kündigung nicht vor der Beendigung aller laufenden Verpflichtungen aus diesem Vertrag und aus allen Einzelvereinbarungen, soweit die Erhebung und Verarbeitung von AG-Daten betroffen ist.

2.6. Die Parteien können diesen Vertrag und jede Einzelvereinbarungen jederzeit ohne Einhaltung von Kündigungsfristen aus wichtigem Grund kündigen, der AG insbesondere

- wenn ein schwerwiegender Verstoß des AN gegen datenschutzrechtliche Bestimmungen oder gegen datenschutzrechtliche Festlegungen dieses Vertrages oder einer Einzelvereinbarung vorliegt,
- wenn der AN eine datenschutzrechtliche Weisung des AG missachtet oder
- wenn der AN den Zugang des AG, der verantwortlichen Stelle, eines entsprechend Beauftragten oder einer Datenschutzaufsichtsbehörde zu den Betriebsräumen, in denen AG-Daten auf Grund dieses Vertrages erhoben, verarbeitet werden, vertrags- oder weisungswidrig verweigert.

2.7. Dieser Vertrag geht bei der Festlegung der datenschutzrechtlichen Pflichten, Verantwortlichkeiten und Konsequenzen bei Widersprüchen allen anderen vertraglichen Regelungen vor, es sei denn, es wird mit ausdrücklichem Bezug auf diesen Vertrag etwas anderes vereinbart.

3. Umfang, Art und Zweck der vorgesehenen Datenerhebung und -verwendung, Datenarten und Kreis der Betroffenen

3.1. Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Umfang, Art und Zweck der Aufgaben des AN:

Bereitstellung der Vertragssoftware "myfactory.com" zur Nutzung durch den AG. Die Erhebung und Nutzung der Daten sowie die Verarbeitung auf fachlicher Ebene erfolgt ausschließlich durch den AG.

3.2. Art der Daten

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten sind folgende Datenarten / -kategorien (Aufzählung / Beschreibung der Datenkategorien):

☐ Personenstammdaten (Name, Vorname, Geschlecht, Geburtsdatum, Anschrift)

- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Vertragsdaten / Bestelldaten
- ☐ Kundenhistorie
- ☐ Interessentendaten (Produktinteresse, Angaben zu Kaufabsichten, Angaben zu im Besitz befindlichen Produkten)
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Bank- oder Kreditkartendaten
- ☐ Befragungsergebnisse
- ☐ Personaldaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☐ Sonstige:

3.3. Kreis der Betroffenen

Der Kreis der durch den Umgang mit den personenbezogenen AG-Daten im Rahmen dieses Auftrags Betroffenen umfasst (Aufzählung / Beschreibung der betroffenen Personenkategorien):

- ☐ Interessenten
- ☐ Kunden
- ☐ Beschäftigte und Stellenbewerber i. S. d. § 3 Abs. 11 BDSG
- ☐ Lieferanten / Dienstleister
- ☐ Handelsvertreter
- ☐ Sonstige:

4. Gewährleistung der technischen und organisatorischen Maßnahmen

4.1. Der AN gewährleistet im Rahmen des ihm nach dieser Vereinbarung und den Einzelvereinbarungen zugewiesenen Verantwortungsbereichs die Umsetzung und Einhaltung derjenigen technischen und organisatorischen Maßnahmen, die erforderlich sind, um die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere derjenigen des Bundesdatenschutzgesetzes (BDSG), des Telekommunikationsgesetzes (TKG) und des Telemediengesetzes (TMG) – soweit anwendbar – sicherzustellen.

4.2. Im Rahmen der automatisierten Verarbeitung trifft er dabei insbesondere die Maßnahmen, die die Erfüllung der Anforderungen des § 9 BDSG nebst derjenigen der Anlage zu § 9 Satz 1 BDSG gewährleisten. Der AN übergibt dem AG dazu eine Aufstellung der technischen und organisatorischen Maßnahmen zum Schutz der AG-Daten (Anlage 1).

4.3. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem AN gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen werden durch den AN dokumentiert.

5. Datenschutzrechtliche Berichtigung, Löschung, Sperrung und Auskunft

5.1. Der AN erhält die Weisung, dem AG unverzüglich mitzuteilen, wenn ein Betroffener eines oder mehrere der folgenden Rechte bzgl. seiner personenbezogenen Daten geltend macht:

- Auskunft (§ 34 BDSG)
- Berichtigung (§ 35 Abs.1 BDSG)
- Widerspruch gegen die Verarbeitung oder Nutzung für Werbung und/oder Markt- oder Meinungsforschung (§ 28 Abs. 4 BDSG)
- Widerruf einer dem AG erteilten datenschutzrechtlichen Einwilligung
- teilweise oder vollständige Löschung aus den Datenbeständen (§ 35 Abs.2 BDSG)
- Sperrung (§ 35 Abs.3 und Abs.4 BDSG)

5.2. Der AN ist verpflichtet, AG-Daten auf Weisung des AG unverzüglich zu berichtigen, zu löschen und/oder zu sperren und auf Weisung des AG dem Betroffenen unverzüglich Auskunft zu erteilen. Ist dem AN aus technischen Gründen oder aufgrund unverhältnismäßigem Aufwands das Löschen nicht möglich, kann der AN die AG-Daten hilfsweise sperren.

5.3. Der AN ist verpflichtet, es zu unterlassen, Betroffene zu Werbezwecken zu kontaktieren, zu denen dem AN vom AG, von dem Betroffenen selbst oder von einer Datenschutz-Aufsichtsbehörde ein Widerspruch gegen eine Kontaktaufnahme zu Werbezwecken mitgeteilt worden ist.

5.4. Sofern der Auftragnehmer AG-Daten erhebt, verarbeitet oder nutzt, ist der AN verpflichtet, sicherzustellen, dass ein Datensatz auch nach Eintragung eines sonstigen Sperrvermerks nicht mehr für den AG durch den AN verarbeitet oder genutzt werden kann.

6. Besondere datenschutzrechtliche Pflichten des AN

6.1. **Datengeheimnis**

Den mit der Erhebung, Verarbeitung und Nutzung der AG-Daten beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind bei der Aufnahme ihrer Tätigkeit schriftlich auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort, § 5 BDSG.

Der AN hat bei Auswahl und Einsatz der Mitarbeiter darauf hinzuwirken, dass diese die gesetzlichen Bestimmungen über den Datenschutz beachten und die aus der Sphäre des AG erlangten Informationen nicht an Dritte weitergeben oder sonst verwerten.

Der AN trägt insbesondere dafür Sorge, dass Mitarbeiter AG-Daten nicht unbefugt kopieren, übermitteln oder löschen.

6.2. **Beauftragter für den Datenschutz**

Der AN hat nach Maßgabe von §§ 4f und 4g BDSG einen betrieblichen Beauftragten für den Datenschutz bestellt. Der Beauftragte für den Datenschutz ist

vom AN über Vorhaben automatisierter Datenverarbeitung und -nutzung im Rahmen dieser Vereinbarung rechtzeitig zu unterrichten.

6.3. **Zusammenarbeit mit den Aufsichtsbehörden.** Der AN ist verpflichtet nach Maßgabe der Weisungen des AG mit den Aufsichtsbehörden für den Datenschutz zu kooperieren und die entsprechenden Auskünfte zu den AG-Daten zu erteilen.

7. Begründung von Unterauftragsverhältnissen

7.1. Der AN ist ohne entsprechende Vereinbarung oder schriftliche Weisung des AG nicht berechtigt, Dritte im datenschutzrechtlichen Sinn (externe Unternehmen, aber auch gesellschaftsrechtlich verbundene Unternehmen) als Subunternehmen zur Erhebung, Verarbeitung oder Nutzung von AG-Daten einzuschalten. Als Dritte in diesem Sinne gelten nicht die mit dem AN arbeitsvertraglich verbundenen Mitarbeiter, die nachweislich unter Beachtung des Datengeheimnisses (Ziff. 6.1) verpflichtet wurden.

7.2. Ist ein Einsatz von Dritten als Subunternehmer vorgesehen, so ist dieser Umstand, der konkret zu beauftragende Subunternehmer und der konkrete Einsatzzweck des Subunternehmens schriftlich zwischen den Parteien zu vereinbaren.

7.3. Die vertraglichen Vereinbarungen mit Subunternehmern sind vom AN so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen AG und AN entsprechen und auch beim Subunternehmer ein angemessenes Datensicherheitsniveau nach Ziff. 4 gewährleistet ist.

7.4. Die Zustimmung des AN zur Begründung eines Unterauftragsverhältnisses darf nicht verweigert werden, wenn der AN die Einhaltung der aus § 11 BDSG resultierenden Rechte und Pflichten des AG vertraglich sicherstellt.

7.5. Der AG willigt ein, dass der AN den folgenden Unterauftragnehmer mit dem Hosting der für die AG-Daten genutzten Serversysteme beauftragt:

Host Europe GmbH, Welserstr. 14, 51149 Köln

8. Kontrollrechte des AG, Mitwirkungs- und Duldungspflichten des AN

8.1. Der AG oder deren schriftlich Beauftragte haben das Recht, die Befolgung sämtlicher Weisungen und Bestimmungen dieser Vereinbarung durch den AN nach schriftlicher Vorankündigung (Terminvereinbarung) und Vereinbarung eines Entgelts für den damit verbundenen Aufwand (zu Grunde gelegt wird der aktuelle Tagessatz gemäß Preisliste Partner von derzeit 960 Euro zzgl. Umsatzsteuer) zu den üblichen Geschäftszeiten in den Geschäftsräumen des AN zu kontrollieren, soweit diese für die Erhebung und Verarbeitung von AG-Daten genutzt werden.

8.2. Dies umfasst insbesondere die Überprüfung der technischen und organisatorischen Maßnahmen vor Beginn der Datenverarbeitung und weitere regelmäßige Überprüfungen, insbesondere der genehmigten Datenschutz- und Sicherheitsmaßnahmen.

8.3. Der AN verpflichtet sich, entsprechende Überprüfungen zu dulden, Zugang, Auskunft und Einsicht in alle dazu erforderlichen Unterlagen und Datenverarbeitungssysteme zu gewähren, soweit diese für diese für die Erhebung und Verarbeitung von AG-Daten genutzt werden

9. Mitteilungspflichten des AN

9.1. Der AN wird den AG unverzüglich von jedem Empfang von Anfragen oder Aufforderungen von einem Betroffenen oder einer Datenschutzaufsichtsbehörde bezüglich des Gegenstandes dieses Vertrages, insbesondere nach Ziff. 5.1, informieren.

9.2. Bei besonderen Vorkommnissen wie Verlust von AG-Daten, Verdacht auf Datenschutz- oder Datensicherheitsverletzungen im Zusammenhang der Erhebung und Verarbeitung von AG-Daten wird der AG vom AN unverzüglich informiert.

9.3. Mitteilungen nach Ziff. 9.1 und 9.2 müssen in Textform (z. B. Brief, Telefax oder E-Mail) im Regelfall innerhalb von einem Arbeitstag ab Kenntnisnahme bezogen auf den Sitz des AN übermittelt werden.

10. Weisungsrecht des AG, Auftragsdatenverarbeitung, Haftungsfreistellung

10.1. Der AN erhebt und verarbeitet AG-Daten ausschließlich im Rahmen dieser vertraglichen Vereinbarung und weiterer Weisungen des AG insbesondere aus den Einzelvereinbarungen (§ 11 BDSG).

10.2. Der AG wird weitere Weisungen per Brief, Fax oder E-Mail erteilen. In begründeten Einzelfällen mündlich oder fernmündlich ausgesprochene Weisungen werden umgehend per Brief, Fax oder E-Mail bestätigt.

10.3. Weisungen dürfen nur durch die vom AG hierzu schriftlich in den Einzelvereinbarungen als Ansprechpartner zu benennenden Personen (nachfolgend „Weisungsberechtigte“ genannt) erteilt werden. In jedem Fall weisungsberechtigt sind der/die Geschäftsführer des AG.

10.4. Ist der AN der Ansicht, dass eine Weisung gegen das BDSG oder andere Vorschriften über den Datenschutz verstößt, weist der AN den AG unverzüglich per Brief, Telefax oder E-Mail darauf hin. Der AN ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie vom AG ausdrücklich bestätigt wird.

10.5. Der AG ist gegenüber dem AN alleine verantwortlich für die Beurteilung der rechtlichen Zulässigkeit der auftragsgemäßen Erhebung, Verarbeitung und Nutzung der AG-Daten durch den AN für den AG insbesondere im Hinblick auf die Regelungen des BDSG, andere Vorschriften über den Datenschutz und die wettbewerbsrechtliche Zulässigkeit der beauftragten Datenverwendung. Sofern Weisungen des AG zu Rechtsverletzungen führen, stellt der AG den AN von Ansprüchen Dritter frei; außerdem übernimmt der AG die erforderlichen Kosten der Rechtsverteidigung.

11. Pflichten der verantwortlichen Stelle

11.1. Die Pflicht zur Führung des öffentlichen Verfahrensverzeichnisses gem. § 4g Abs. 2 S. 2 BDSG liegt bei der verantwortlichen Stelle.

11.2. Der verantwortlichen Stelle obliegen die aus § 42a BDSG resultierenden Informationspflichten.

12. Rückgabe- und Löschungspflichten

12.1. Bei Beendigung des Auftrags vom AN gespeicherte AG-Daten – wenn nicht bereits zuvor geschehen – werden nach Weisung des AG beim AN und dessen Beauftragten unwiderruflich gelöscht. Aus technischen Gründen verbleiben gelöschte Daten für den Zeitraum von 2 Wochen in der Datensicherung des AN.

12.2. Auf Anfrage des AG bestätigt der AN, dass der AN die überlassenen Daten vollständig zurückgegeben, vernichtet bzw. unwiderruflich gelöscht hat.

12.3. Die Pflicht zur Löschung bzw. Vernichtung besteht nicht, solange eine gesetzliche Aufbewahrungspflicht des AN entgegensteht.

13. Entgelte

13.1. Soweit der Auftraggeber Unterstützung nach Ziffer 5.2 für die Beantwortung von Anfragen Betroffener benötigt, hat er die hierdurch entstehenden Kosten zu erstatten.

13.2. Soweit der Auftraggeber nach Ziffer 8 Kontrollrechte ausüben wird, orientiert sich die vorab zu vereinbarende Höhe des Entgelts an dem aktuellen myfactory Tagessatz gemäß Preisliste Partner von derzeit 960 Euro zzgl. Umsatzsteuer des für die Betreuung vom AN abgestellten Mitarbeiters.

13.3. Erteilt der AG dem AN Weisungen nach Ziffer 10, so hat er durch diese Weisung entstehende Kosten zu erstatten.

Die Anlage 1 (Technische und organisatorische Maßnahmen) ist Bestandteil dieses Vertrags.

……..	……..
Ort, Datum	Ort, Datum
……..	……..
myfactory International GmbH	
Dr. Robert Meyer	

Dokumentation der technischen und organisatorischen Maßnahmen

Die myfactory International GmbH, im Folgenden kurz „myfactory“ genannt, hat als Auftragsdatenverarbeiter durch die Bereitstellung ihre selbst entwickelte betriebswirtschaftliche Software (Warenwirtschaft, Finanzbuchhaltung, Auftragsverwaltung, usw.) eine besondere Verantwortung für die Daten seiner Interessenten und Kunden. Ein Verlust dieser Daten hätte für alle Nutzer dieser Software als auch für myfactory selber weit reichende Folgen.

Datenarten

myfactory unterscheidet zwei Arten von personenbezogenen Daten. Zum einen die Daten die zur Verwaltung und Abrechnung erforderlichen Daten (Name und Anschrift des Kunden, usw.), Adressdaten von Interessenten, Mitarbeitern sowie Bewerberdaten sowie Daten von Lieferanten. Die Nutzung, Erhebung und Verarbeitung dieser Verwaltungsdaten erfolgt durch myfactory-Mitarbeiter oder auch durch die Interessenten und Kunden selbst, über einen SSL-geschützten Bereich des myfactory-Internetportals (myfactory.com).
Die zweite Art personenbezogener Daten sind diejenigen, die von Interessenten und Kunden mit der von myfactory bereitgestellten Software erhoben, verarbeitet und genutzt werden. Die Erhebung, Verarbeitung und Nutzung dieser Daten erfolgt ausschließlich durch die Interessenten und Kunden selber, über eine SSL-verschlüsselte Internetverbindung (zu erkennen am „https://“ vor der Internetadresse). Im Rahmen einer technischen Wartung besteht die Möglichkeit des Zugriffs auf Kunden-Daten durch autorisierte myfactory-Mitarbeiter und durch den Rechenzentrumsbetreiber. Nur diese Kundendaten sind Gegenstand der Auftragsdatenverarbeitung.
Wenn im Folgenden personenbezogenen Daten genannt werden, sind beide zuvor beschriebenen Arten dieser Daten gemeint.

Das Gesetz

Jeder myfactory-Kunde ist laut §11 BDSG dazu verpflichtet, sich von der Einhaltung der technischen und organisatorischen Maßnahmen zur Einhaltung des Datenschutzes zu überzeugen. Grundlage hierfür bildet diese Dokumentation. In der Anlage zu §9 Satz 1 BDSG sind die erforderlichen Maßnahmen genannt.
Um Kunden und Interessenten eine Prüfung gemäß §11 BDSG zu erleichtern, richtet sich die Gliederung dieser Dokumentation nach der Anlage zu §9 Satz 1 BDSG.

Zutrittskontrolle

Alle Server der myfactory werden im Rechenzentrum der Host Europe GmbH, im Folgenden HostEurope genannt, betrieben. Dort werden beide Arten von personenbezogenen Daten gespeichert und verarbeitet.
Das Rechenzentrum der Host Europe GmbH wurde vom eco-Verband mit der Bestnote zertifiziert und gilt als eines der sichersten in Deutschland. Der Zugang zum Rechenzentrum wird durch den Rechenzentrumsbetreiber selber kontrolliert. Das Rechenzentrum, daß im Rahmen des Data Center Star Audits vom eco-Verband überprüft wurde, umfasst unter Anderem folgende Merkmale:

- benutzerbezogener Authentifizierung
- Zugang zum Rechenzentrum über mind. 2 Türsysteme
- Vereinzelungsanlage (Kundenzutritt) oder Schleusensystem
- Physikalischer Zugangsschutz mit Logging (Stahltüren/Sicherheitsschlösser/fensterloser Raum oder gesicherte Fenster)
- Alarmierung/Einbruchssicherung

Alle Büroräume der myfactory sind am Firmensitz in München, Agnes-Pockels-Bogen 1. Die Sicherungsmechanismen der myfactory-Büroräume entsprechen denen normaler gewerblich genutzter Räumlichkeiten, da dort keine unverschlüsselten personenbezogenen Daten gespeichert werden. Lediglich temporäre Kopien einzelner Kunden-Datenbanken werden für spezielle Support-Aufgaben zur Fehlersuche, bzw. Debugging auf einem Rechner mit verschlüsseltem Dateisystem gespeichert. Alle unbesetzten Büroräume werden immer verschlossen gehalten. Einzelnen Mitarbeitern ist gestattet, von anderen Orten aus zu arbeiten (z.B. von zu Hause aus).

Zugangskontrolle

Die von myfactory genutzten Server im Rechenzentrum von HostEurope verfügen zur Administration über entsprechende Benutzerkonten. Die Administration der Server erfolgt über das Internet über eine geschützte Verbindung. Die Kennwörter für diese Benutzerkonten sind nur einzelnen, autorisierten und festen Vollzeit-Mitarbeitern bekannt.
Um unautorisierten Zugang zu verhindern, sind die Server der myfactory über zwei hintereinander geschalteten Firewalls geschützt. Bei der ersten Firewall handelt es sich um eine externe hardwarebasierte Cisco-Firewall, bei der zweiten Firewall um eine softwarebasierte Firewall. Beide Firewalls sind so konfiguriert, dass nur der Datenverkehr zugelassen ist, der für den Betrieb der Software zwingend erforderlich ist.
Der Zugang zu den Rechnern in den Büroräumen wird über Benutzerkonten kontrolliert. Hierzu hat jeder Mitarbeiter ein eigenes Benutzerkonto für den lokalen Rechner, als auch für die intern genutzte myfacory-Instanz.

Zugriffskontrolle

Support-Mitarbeiter haben generell keinen Zugriff auf die Daten in den Datenbanken der Interessenten und Kunden. Lediglich durch zusätzliche Software (beamyourscreen3.com) ist dem Supportmitarbeiter der Zugriff auf den Bildschirm des Kunden möglich. Erst nachdem der Interessent/Kunde zugestimmt hat, kann der Supportmitarbeiter die Steuerung der Maus über diese zusätzliche Software übernehmen.
Zur Vereinfachung der Fehersuche oder zum Debuggung können Kopien von einzelnen Datendanken einzelner Kunden auf einem Computer mit verschlüsseltem Dateisystem gespeichert werden. Nach dem der Sachverhalt geklärt ist, wird diese Daten-Kopie unverzüglich gelöscht.

Weitergabekontrolle

Die Weitergabekontrolle wird bei myfactory durch den einzigen Speicherort der personenbezogenen Daten im HostEurope-Rechenzentrum und die restriktive Zutritts- und Zugangskontrolle zu diesem Speicherort sichergestellt. Das unbefugte lesen, kopieren, verändern oder entfernen von im Rechenzentrum gespeicherten Daten durch den Rechenzentrumsbetreiber ist vertraglich ausgeschlossen. Alle Mitarbeiter der myfactory die in den Kontakt mit personenbezogenen Daten kommen haben sich nach §5 BDSG zur Verschwiegenheit verpflichtet.

Eingabekontrolle

Die Eingabekontrolle wird bei myfactory über ein Protokoll gewährleistet. Das Protokoll wird innerhalb der von myfactory verwendeten Software-Instanz gespeichert und sind für alle Mitarbeiter einsehbar aber nicht änderbar. In den Protokolldateien sind sämtliche Eingaben aufgezeichnet, die Kunden oder Mitarbeiter über das https Protokoll in Kunden- oder Verwaltungsdaten gemacht haben. Die Aufbewahrungszeit für die Protokolle ist nicht begrenzt.
Zum anderen haben Kunden die Möglichkeit in ihrem Programm selbst zu sehen, welcher Benutzer zu welchem Zeitpunkt einen Datensatz (z.B. Kunde) zuletzt geändert hat.

Auftragskontrolle

Mit HostEurope ist eine schriftliche Vereinbarung zur Auftragsdatenverarbeitung geschlossen, so dass die Daten nur entsprechend den Weisungen von myfactory verarbeitet werden. Eine Nutzung oder Weitergabe der Daten durch Mitarbeiter von HostEurope ist vertraglich ausgeschlossen. Support-Aufträge an HostEurope werden nur durch autorisierte Mitarbeiter der myfactory entgegengenommen. Die Aufträge von myfactory an HostEurope liegen in elektronischer Form vor und können nachträglich überprüft werden.

Verfügbarkeitskontrolle

Ein mehrstufiges Sicherheitskonzept gewährleistet die Verfügbarkeit aller Daten. Das vollklimatisierte Rechenzentrum von HostEurope bietet Schutz vor Gas, Wasser und Feuer. Jede Nacht erstellt HostEurope eine Kopie des kompletten Servers auf ein dafür vorgesehenes Backup-System. Die verschlüsselte Serverkopie wird in einem räumlich getrennten Backuprechenzentrum archiviert. HostEurope verfügt für den Fall eines lokalen Stromausfalls über eine Notstrom-System. Mit HostEurope wurde ein Service-Vertrag mit sehr kurzer Reaktionszeit (7x24) geschlossen der auch den Austausch eines defekten Servers beinhaltet. Der Ausfall einer Festplatte hat keinen Datenverlust zur Folge; defekte Festplatten können im laufenden Betrieb

ausgetauscht werden (RAID-System Hot-Plug). Der Status des RAID-Systems wird regelmäßig überwacht und bei einer Störung wird HostEurope mit dem Austausch der defekten Festplatte beauftragt.

Getrennte Verarbeitung

Zur Gewährleistung der getrennten Verarbeitung sind die Daten unterschiedlicher Kunden auf dem Server in unterschiedlichen Datenbanken voneinander getrennt gespeichert.