

Allgemeine Vertragsbedingungen

für OUNUO, die Kontaktmanagement-Software der eGenius GmbH

Vielen Dank, dass Sie OUNUO nutzen wollen.

(1) Einführung: Was ist OUNUO?

OUNUO ist eine einfach zu bedienende Kontaktmanagement-Software der eGenius GmbH (nachfolgend: „eGenius“). OUNUO erleichtert die Nutzung von Kontakten gemeinschaftlich durch mehrere Personen im Team.

OUNUO ist ausgerichtet auf die Bedürfnisse von Vereinen, Verbänden, Behörden, Agenturen und anderen Institutionen, die sich an eine Vielzahl von Ansprechpartnern richten, ohne zugleich viele einzelne Geschäftsvorgänge wie z.B. Bestellvorgänge im eCommerce verwalten zu müssen.

OUNUO ist eine Software, die über das Internet angeboten wird, eine sogenannte Software as a Service. OUNUO ist über alle Geräte mit Internetzugang und einem Webbrowser zugänglich. Für die Nutzung von OUNUO muss außer dem meist schon vorhandenem Webbrowser keine Software auf dem Gerät des Anwenders installiert werden. Wartungsarbeiten erfolgen zentral ohne Zugriff auf die Geräte oder Programme der einzelnen Anwender.

Um OUNUO in dieser Form über das Internet anbieten zu können, arbeitet eGenius als Anbieter der Software mit Amazon Web Services (AWS) als hochleistungsfähigem Hosting-Anbieter zusammen.

Jeder Kunde von OUNUO ermächtigt eGenius zur Speicherung der Daten als Auftragsdatenverarbeiter nach Art. 28 Abs. 3 DSGVO. Alle Daten, die die Anwender in OUNUO eingeben, werden von OUNUO auf Servern von AWS in Deutschland (Frankfurt am Main) gespeichert. Vertragspartner für die Kunden von OUNUO ist immer eGenius. Details zu dem wichtigen Thema Datenschutz finden Sie in unseren Datenschutzinformationen.

(2) Vertragsgegenstand: Umfang der Nutzungsrechte

(2.1) Die Kunden von OUNUO erwerben das kostenpflichtige Nutzungsrecht an der Software in

ihrer jeweils aktuellen Version. Details des Funktionsumfangs nennt die Produktbeschreibung von OUNUO.

(2.2) OUNUO kann drei Monate kostenlos genutzt werden (siehe auch Klausel 5.2). Für die kostenlose Nutzung gelten diese Allgemeinen Geschäftsbedingungen inklusive des Vertrags über die Datenverarbeitung im Auftrag und seiner Anlagen gleichermaßen.

(2.3) eGenius verpflichtet sich, die Software fortlaufend zu warten und so auf einem technisch Stand zu halten, der den Entwicklungen bei den gängigen Betriebssystemen und dem Fortschritt der Internettechnologie entspricht. Die Wartungsverpflichtung bedeutet nicht, dass der Funktionsumfang von OUNUO erweitert wird.

(2.4) eGenius strebt an, den Funktionsumfang von OUNUO fortlaufend zu erweitern. Die Kunden erwerben jedoch keinen Anspruch auf die Einführung neuer Funktionen, speziell keinen Anspruch auf die Einführung konkreter von ihnen gewünschter Funktionen.

(2.5) Die Kunden erwerben in keiner Form eigene Rechte an den geistigen Rechten von OUNUO, also an den Rechten an der Software oder den von OUNUO verwendeten Zeichen und Symbolen. Die Software darf in keiner Form eigenständig weiterverwendet werden oder für eigene Entwicklungen genutzt werden.

(2.6) Das pünktliche Zahlen der Software-Miete ist zentrale Voraussetzung für das Fortbestehen des Nutzungsrechts durch den Kunden.

(2.7) OUNUO prüft regelmäßig, ob das Nutzungsrecht eines Anwenderlogins (bestehend aus einer E-Mail-Adresse und einem Passwort) noch gültig ist. Ein Anwenderlogin darf nur auf bis zu drei Geräten gleichzeitig verwendet werden.

(3) Gesonderte Leistungen

Neben dem allgemeinen Nutzungsvertrag können Kunden bei eGenius einzelne Supportleistungen nach Stundentarif in Anspruch nehmen. Zu den verfügbaren Leistungen zählen z.B. Assistenz beim

Allgemeine Vertragsbedingungen

primären Import des vorhandenen Datenbestandes und Schulungen.

Das Leistungsspektrum des allgemeinen Vertrags umfasst nicht die Bereitstellung neuer Funktionen in OUNUO nach individuellen Kundenwünschen, da diese im Standardprodukt nur für alle Kunden zugleich integriert werden können.

Sollten für einen Kunden individuelle Lösungen erforderlich sein, kann eGenius mit einer entsprechenden Produktfortentwicklung beauftragt werden. Ab diesem Zeitpunkt würde der Kunde jedoch ein eigenes OUNUO nutzen, dessen künftige Wartung Folgekosten für den Kunden auslösen kann, da diese zusätzlichen Wartungsaufwände nicht vom Nutzungspreis für das Standard-OUNUO umfasst sind.

(4) Anfang und Ende: Laufzeit, Kündigungsrechte, Datenlöschung

(4.1) Der Vertrag kommt zustande, indem eGenius auf Anfrage des Kunden dem Kunden das Administratoren-Login für sein eigenes OUNUO (als den Speicherbereich für seine Daten innerhalb der Software) zur Verfügung stellt. Der Kunde erhält vor Bereitstellung des Administratoren-Logins diese Allgemeinen Vertragsbedingungen inklusive der nach dem europäischen Datenschutzrecht erforderlichen Vereinbarung zur Datenverarbeitung im Auftrag. Die Datenschutzinformation wird ihm zugänglich gemacht.

(4.2) Der Kunde kann die Zahl seiner Anmeldekonto jederzeit ändern. Hierzu genügt eine E-Mail an support@ounuo.de und eGenius stellt dem Kunden weitere Anmeldekonto in OUNUO zur Verfügung, die er Mitgliedern seines Teams zuweisen kann.

(4.3) Falls nicht anders vereinbart, gilt ein Leistungszeitraum von einem Monat sowie eine Kündigungsfrist von einem Monat. Wird der Vertrag nicht gekündigt, verlängert sich der Leistungszeitraum nach Ablauf um jeweils einen weiteren Monat.

(4.4) eGenius behält sich vor, die Preise für die Nutzung von OUNUO zu ändern. Im Falle einer Preisänderung wird diese dem Kunden drei Monate vor Inkrafttreten der neuen Preise per E-Mail mitgeteilt. Dem Kunden steht im Falle einer Preisänderung ein Sonderkündigungsrecht zu bis

zum Ablauf des zweiten Monats, in dem die neuen Preise gelten.

(4.5) Dem Kunden steht das Recht auf fristlose Kündigung zu, wenn grundlegende Funktionen, die während der Testphase verfügbar waren, ihm während der Vertragslaufzeit nicht mehr zur Verfügung stehen.

(4.6) eGenius kann den Nutzungsvertrag mit einer Frist von zwölf Monaten kündigen. Wenn der Kunde mit der Zahlung seiner monatlichen Nutzungsgebühr mehr als zwei Wochen in Verzug ist, steht eGenius ein Sonderkündigungsrecht zu, dass vier Wochen nach Erklärung wirksam wird.

(4.7) eGenius steht das Recht auf fristlose Kündigung zu, wenn der Kunde OUNUO in einer Weise einsetzt, die über den nach diesem Vertrag zulässigen Rahmen hinausgeht.

Speziell alle vorsätzlichen oder fahrlässigen Maßnahmen, die die Funktionssicherheit der Software oder die Sicherheit der gespeicherten Daten gefährden, gestatten die fristlose Kündigung.

Das gleiche gilt, wenn OUNUO in einer Weise genutzt wird, in der der Kunde gegenüber den von ihm gespeicherten Kontakten gegen das Datenschutzrecht verstößt und sich daraus ein Risiko ergibt, dass eGenius von den Betroffenen in Anspruch genommen wird.

Auch jede Nutzung des Kontaktmanagements, die auf Verstöße gegen den Jugendschutz oder gegen Strafrechtsnormen zielt oder solche Verstöße gefördert hat, gewährt eGenius das Recht zur fristlosen Kündigung.

(4.8) eGenius hat das Recht, OUNUO als Service wieder einzustellen. In diesem Fall kann sie den Vertrag mit einer Frist von sechs Monaten kündigen.

(4.9) Die Kündigung muss schriftlich erfolgen. Entweder per E-Mail oder per Brief. Kündigt der Kunde, muss er sein Schreiben schicken an support@OUNUO.de oder eGenius GmbH, Elbuferstraße 86a, 21436 Marschacht.

(4.10) Wird der Vertrag gekündigt, enden die Zugriffsrechte der Anmeldekonto mit dem Ablauf

Allgemeine Vertragsbedingungen

der verbliebenen vertraglichen Nutzungszeit. Der Kunde kann dann nicht mehr über OUNUO auf seinen dort gespeicherten Datenbestand zugreifen. Zuvor hat er die Möglichkeit, seine Daten selbst aus OUNUO zu exportieren. EGenius wird die Daten des Kunden über das Ende der Vertragslaufzeit hinaus noch zwölf Monate speichern. Auf Wunsch des Kunden stellt eGenius ihm einen Export seiner Daten zur Verfügung. Der Datenexport folgt dabei den Datenstrukturen des OUNUO-Systems.

(4.11) Verlangt der Kunde ausdrücklich schon vor Ablauf der zwölf Monate nach Vertragsende eine Löschung seiner Daten aus OUNUO, wird eGenius diesem Wunsch umgehend nachkommen. Der Auftrag zur vollständigen Löschung muss schriftlich per E-Mail oder Brief erfolgen (support@OUNUO.de bzw. eGenius GmbH, Elbuferstraße 86a, 21436 Marschacht).

(5) Preise und Zahlungsbedingungen

(5.1) Der Preis für die monatliche Nutzung richtet sich nach der Zahl der bereitgestellten Anmeldekonto des Kunden. Die Preise je Konto inklusive Rabattstaffel sind in der jeweils aktuellen Preisliste angegeben.

(5.2) Jeder Vertrag beginnt mit einer Testphase von einem Monat, in der der Kunde OUNUO kostenlos in vollem Umfang nutzen kann. Während dieser Zeit kann der Kunde jederzeit ohne Angabe von Gründen den Vertrag kündigen. Ihm werden für die Nutzung von OUNUO während der Testzeit keine Kosten in Rechnung gestellt. Gesonderte Leistungen nach (3) werden jedoch auch in der Testphase nur kostenpflichtig erbracht.

(5.3) Nach Ablauf der Testphase wird jeweils zum 1. des Monats eine monatliche Nutzungsgebühr für OUNUO fällig. Der erste kostenpflichtige Monat schließt an den Monat an, in dem die Testphase des Kunden endet.

(5.4) Der Kunde erhält eine Rechnung als PDF per E-Mail geschickt. Der Kunde kann eGenius mit dem Lastschriftverfahren beauftragen.

(5.5) Zum 15. eines Monats stellt eGenius die Summe der zur Verfügung gestellten Konten fest und verwendet die Summe als verbindliche Abrechnungsgrundlage für den Folgemonat.

(5.6) Die in der Preisliste genannten Preise sind Nettopreise. Abgerechnet wird inklusive der gesetzlichen Umsatzsteuer.

(5.7) Nimmt ein Kunde am Lastschriftverfahren teil und kann die Abbuchung mangels ausreichender Deckung auf dem Konto des Kunden nicht durchgeführt werden, hat eGenius einen Anspruch gegen den Kunden auf Erstattung der Rücklastkosten zuzüglich 5,00 Euro Bearbeitungsgebühr.

(6) Haftung

(6.1) eGenius übernimmt die Gewähr dafür, dass OUNUO die in der Produktbeschreibung genannten Funktionen umfasst.

(6.2) eGenius übernimmt die Gewähr dafür, dass der Server entsprechend den Vorgaben von AWS zu 98 Prozent des Jahres technisch erreichbar ist und es entsprechend zu maximal geringen Serviceunterbrechungen kommt. Ausfälle durch außerordentliche Ereignisse wie Krieg oder vergleichbare Unruhen, Naturkatastrophen, sonstigen Ausfall der Netzinfrastruktur zwischen Server und Kunde oder eine plötzliche und nicht erwartbare Einstellung des Datenhostings durch AWS können von dieser Garantie nicht umfasst werden, sind aber auch entsprechend unwahrscheinlich.

(6.3) Sollten bei der Nutzung von OUNUO Fehler auftreten, ist der Kunde bei der Suche nach der Fehlerursache zur Zusammenarbeit mit eGenius verpflichtet. Der Kunde muss Angaben machen können zur Version des eingesetzten Betriebssystems und zur Version des eingesetzten Internetbrowsers sowie zu den Firewall-Einstellungen seines Internetzugangs. Zudem muss der User darlegen können, welche Aktion er in OUNUO ausführen wollte, was er dafür in OUNUO getan hat und welches fehlerhafte Ergebnis anschließend aufgetreten ist.

(6.4) eGenius haftet nicht für Fehler oder Schäden, die aus der unsachgemäßen Nutzung von OUNUO resultieren.

(6.5) eGenius haftet in keiner Weise für Konsequenzen, die sich aus der Verwendung der in OUNUO gespeicherten Daten durch den Kunden und seine OUNUO-Anwender ergeben.

Allgemeine Vertragsbedingungen

(6.6) Es liegt allein in der Verantwortung des Kunden, sicherzustellen dass Daten von ihm in OUNUO gespeichert werden dürfen. Das betrifft sowohl Kontaktdaten wie Fotos oder im Dokumenten-System von OUNUO gespeicherte Dateien. Der Kunde stellt eGenius von allen Rechtsverfolgungskosten und Schadenersatzforderungen frei, die sich daraus ergeben, dass natürliche oder juristische Personen gegen die Speicherung ihrer Daten in OUNUO vorgehen.

(6.7) Es ist eine zentrale Pflicht des Kunden, seine Anmeldedaten, speziell die Passwörter zu den Anmeldekonto, geheim zu halten. Es liegt auch in der Verantwortung des Kunden, Mitgliedern seines Teams bei entsprechendem Bedarf den Zugang zu OUNUO zu entziehen und deren Anmeldekonto zu sperren.

(6.8) Die vom Kunden in OUNUO gespeicherten Daten werden fortlaufend vom System gegen technischen Datenverlust gesichert. Dennoch obliegt dem Kunden die Pflicht, seine Daten aus OUNUO regelmäßig zu exportieren und auf eigenen Datenträgern zu sichern. Der Grund hierfür ist, dass OUNUO keine Vorgängerversionen der Datensätze speichert. Sollten die Anwender versehentlich Daten löschen, können diese nur aus eigenen Sicherungskopien des Kunden wiederhergestellt werden.

(6.9) eGenius schließt gegenüber ihren Kunden jede verschuldensunabhängige Haftung aus, auch die für anfängliche Mängel der Software. EGenius haftet nur für Schäden des Kunden oder seiner Anwender, die aus der Nutzung von OUNUO entstanden sind und sich auf vorsätzliches oder fahrlässiges Verhalten von eGenius bzw. der eGenius Mitarbeiter zurückführen lassen.

(7) Sonstiges

(7.1) Künftige Änderungen an diesen Allgemeinen Vertragsbedingungen bedürfen der Schriftform und werden den Kunden von eGenius per E-Mail mitgeteilt.

(7.2) Sollten einzelne Regelungen in diesen Allgemeinen Vertragsbedingungen unwirksam sein oder werden, oder sollte ein bestimmter Punkt nicht geregelt sein, bleibt die Gültigkeit der übrigen Vertragsbedingungen davon unberührt. An die Stelle der unwirksamen oder fehlenden

Vereinbarung tritt die gesetzliche Regelung für diesen Fall.

(7.3) Auf diese Allgemeinen Vertragsbedingungen ist deutsches Recht anwendbar. Erfüllungsort und Gerichtsstand für Auseinandersetzungen aus diesem Vertrag ist Hamburg.

Allgemeine Vertragsbedingungen

Vertrag über die Datenverarbeitung im Auftrag nach Art. 28 DSGVO

zwischen dem Kunden als **Auftraggeber** und der eGenius GmbH, Elbuferstraße 86a, 21436 Marschacht als **Auftragnehmer**.

1. Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers im Sinne des Art. 28 der Datenschutzgrundverordnung (DSGVO). Dieser Vertrag regelt die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung der personenbezogenen Daten.

(2) Sofern in diesem Vertrag Begriffe verwendet werden, die in Art. 4 DSGVO gesetzlich definiert sind, wird die gesetzliche Definition auch für die Begriffsverwendung in diesem Vertrag zugrunde gelegt. Die gilt z.B. für „personenbezogene Daten“, „Verarbeitung“, „Verantwortlicher“, „Auftragsverarbeiter“, „Dritter“, „Einwilligung“ und „Aufsichtsbehörde“.

(3) Der Auftraggeber entscheidet über die Mittel und Zwecke der durch diesen Vertrag geregelten Datenverarbeitung. Der Auftragnehmer handelt insoweit weisungsgebunden; allein mit Blick auf die Wahl der technischen Mittel steht dem Auftragnehmer ein eigenständiger Entscheidungsspielraum zu.

(4) Ziel dieses Vertrags ist es, die Anforderungen an den Datenschutz sicherzustellen, so dass der Auftraggeber dem Auftragnehmer Daten zur weisungsgebundenen Verarbeitung rechtskonform zugänglich machen kann.

2. Gegenstand des Auftrags

Der konkrete Gegenstand der Verarbeitung ergibt sich aus dem zwischen den Parteien vereinbarten Leistungsvertrag. Zudem sind Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen in Anlage 1 zu diesem Vertrag festgehalten.

3. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht das

Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist (siehe auch Nr. 4 Absatz 4).

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

(3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) erfolgen.

(4) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

(5) Der Auftraggeber kann weisungsberechtigte Personen benennen. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform mitteilen.

(6) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(7) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

4. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor

Allgemeine Vertragsbedingungen

der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

(2) Der Auftragnehmer verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen.

(3) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Der Auftragnehmer wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab mit dem Auftraggeber abstimmen.

(4) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

(5) Der Auftragnehmer wird die Daten, die er im Auftrag für den Auftraggeber verarbeitet, getrennt von anderen Daten verarbeiten. Eine physische Trennung ist nicht zwingend erforderlich.

(6) Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern,

wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen.

5. Datenschutzbeauftragter des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Der Auftragnehmer wird dem Auftraggeber den Namen und die Kontaktdaten seines Datenschutzbeauftragten auf Anfrage mitteilen; zudem sind die Angaben in der Datenschutzinformation des Auftragnehmers genannt, die auf der Internetseite des Auftragnehmers veröffentlicht ist.

(2) Die Pflicht zur Benennung eines Datenschutzbeauftragten nach Absatz 1 kann im Ermessen des Auftraggebers entfallen, wenn der Auftragnehmer nachweisen kann, dass er gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen.

6. Meldepflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

(2) Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

(3) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der

Allgemeine Vertragsbedingungen

Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich, spätestens aber binnen 48 Stunden ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

7. Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Nr. 11 dieses Vertrages.

(2) Der Auftragnehmer wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber mit. Er hat dem Auftraggeber die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

(3) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

8. Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle im Sinne des Absatzes 1 erforderlich ist.

(3) Der Auftraggeber kann eine Einsichtnahme in die vom Auftragnehmer für den Auftraggeber verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.

(4) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören.

(5) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber nach Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

9. Unterauftragsverhältnisse

(1) Die Beauftragung von Unterauftragnehmern durch den Auftragnehmer ist nur mit Zustimmung des Auftraggebers in Textform zulässig. Der Auftragnehmer nennt alle bereits bei Vertragsschluss bestehenden Unterauftragsverhältnisse in der Anlage 2 zu diesem Vertrag. Der Auftraggeber stimmt diesen bestehenden Unterauftragsverhältnissen durch den Abschluss des Vertrags zu. Soweit der Auftragnehmer während der Vertragslaufzeit einen weiteren Unterauftragnehmer hinzuziehen möchte oder einen Unterauftragnehmer durch einen anderen ersetzen möchte, informiert er den Auftraggeber hierüber in Textform und weist ihn auf sein Recht zum Widerspruch hin. Sollte der Auftraggeber nicht innerhalb von 14 Tagen widersprechen, gilt die Beauftragung des neuen Unterauftragnehmers als genehmigt.

Allgemeine Vertragsbedingungen

(2) Der Auftragnehmer hat jeden Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat.

(3) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.

(4) Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsdatenverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

(5) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse des Auftraggebers (Nr. 8 dieses Vertrages) und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

(6) Nicht als Unterauftragsverhältnisse im Sinne der Absätze 1 bis 5 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht

werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten.

10. Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist hierzu verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

(2) Der Auftragnehmer sichert zu, dass er seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat. Der Auftragnehmer sichert ferner zu, dass er insbesondere die bei der Durchführung der Arbeiten für den Auftraggeber tätigen Beschäftigten zur Vertraulichkeit verpflichtet hat und diese über die Weisungen des Auftraggebers informiert hat.

(3) Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Auftraggeber auf Anfrage nachzuweisen.

11. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützen. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten – insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung – durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des

Allgemeine Vertragsbedingungen

Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

12. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

(3) Ist der Auftraggeber Berufsgeheimnisträger im Sinne des § 203 Strafgesetzbuch (StGB), verpflichtet der Auftragnehmer sich, alle seine Beschäftigten, die Zugriff auf die personenbezogenen Daten des Auftraggebers erhalten, auf die entsprechende strafbewehrte Verschwiegenheit nach § 203 StGB zu verpflichten.

13. Vergütung

Die Vergütung des Auftragnehmers wird gesondert im zwischen den Parteien geschlossenem Leistungsvertrag vereinbart.

14. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies

beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als Anlage 3 zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

(3) Der Auftragnehmer wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Erforderlichkeit und Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird der Auftragnehmer den Auftraggeber informieren.

15. Dauer des Auftrags

(1) Der Vertrag beginnt mit Unterzeichnung und endet mit dem spätesten Ablauf eines zwischen den Parteien vereinbarten Leistungsvertrages, mit dem der Auftraggeber eine Verarbeitung beim Auftragnehmer in Auftrag geben hat.

(2) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

Allgemeine Vertragsbedingungen

16. Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt. Für Datenträger gilt, dass diese im Falle einer vom Auftraggeber gewünschten Löschung zu vernichten sind, wobei mindestens die Sicherheitsstufe 3 der DIN 66399 einzuhalten ist; die Vernichtung ist dem Auftraggeber unter Hinweis auf die Sicherheitsstufe gemäß DIN 66399 nachzuweisen.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle

soll mit angemessener Frist durch den Auftraggeber angekündigt werden.

17. Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Für Nebenabreden ist die Schriftform erforderlich. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Es gilt deutsches Recht.

(4) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Allgemeine Vertragsbedingungen

für OUNUO, die Kontaktmanagement-Software der eGenius GmbH

Anlage 1

Gegenstand des Auftrags

1. Gegenstand und Zweck der Verarbeitung

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:

Der Auftragnehmer stellt dem Auftraggeber die Onlinedatenbank OUNUO zur Verfügung für das Speichern und Verwalten von Kontakten. Der Auftraggeber vergibt für die gemeinsame Datennutzung OUNUO-Benutzerkonten an zugriffsberechtigte Personen.

Zweck der Datenverarbeitung ist die Bereitstellung der Kontaktmanagementfunktionen als ein cloud-gehostetes Software-as-a-Service-Angebot.

2. Art(en) der personenbezogenen Daten

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung, Details abhängig von der beauftragten Leistung:

Von den gespeicherten Kontakten:

- Name (Vorname, Nachname, Spitzname), Anrede, Titel, berufliche Position, Geburtsdatum, Geburtsname
- Adressen (private wie geschäftliche)
- Telefonnummern (Festnetz, Mobilnummern, Faxnummern)
- E-Mail-Adressen
- Zugehörigkeit zu einer Organisation (Unternehmen, Verein und sonstigen Institutionen)
- Zugehörigkeit zu einer vom Auftraggeber zusammengestellten Gruppe (z.B. „Teilnehmer einer Veranstaltung“)
- URLs von Websites und SocialMedia-Konten
- Profilfotos
- Religionszugehörigkeit
- Dokumente verschiedener Dateiformate inklusive der darin enthaltenen Daten (z.B. PDF, JPG, Word, Excel)
- schriftliche Notizen des Auftraggebers zu der Person
- Notizen des Auftraggebers zum Kontaktverlauf mit einzelnen Personen

Von den OUNUO-Benutzern:

- Login-Name (E-Mail-Adresse), Name, Abteilung, Telefonnummern und Profilfoto.
- Umfang der Nutzungsberechtigungen innerhalb der Datenbank, die der Auftraggeber dem Anwender zugewiesen hat.
- Log-Daten zu den Dateneingaben, -veränderungen und -löschungen, die der Anwender im System vorgenommen hat.

3. Kategorien betroffener Person

Kreis der von der Datenverarbeitung betroffenen Personen:

OUNUO-Benutzer und gespeicherte Kontakte

(z.B. Beschäftigte, Kunden, Mandanten, Patienten, Mitglieder, Teilnehmer, Lieferanten und Dienstleister, Ansprechpartner bei Unternehmen, Behörden, Kirchen und anderen staatlichen und zivilgesellschaftlichen Organisationen)

Allgemeine Vertragsbedingungen

für OUNUO, die Kontaktmanagement-Software der eGenius GmbH

Anlage 2

Unterauftragnehmer

Der **Auftragnehmer** nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Dabei handelt es sich um nachfolgende Unternehmen:

Unternehmen	Land	Adresse	Leistung
Amazon Web Services EMEA SARL („AWS“)	EU	5 Rue Plaetis, L-2338 Luxembourg	Hosting Datenbankanwendung

Allgemeine Vertragsbedingungen

für OUNUO, die Kontaktmanagement-Software der eGenius GmbH

Anlage 3

Technische und organisatorische Maßnahmen des Auftragnehmers

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

Bei den technischen und organisatorischen Maßnahmen ist zu unterscheiden zwischen den Maßnahmen im Rechenzentrum von AWS, in dem die Daten der im Kontaktmanagement erfassten Personen gespeichert sind, und den Geschäftsräumen des Auftragnehmers, bei dem nur Zugangsdaten zu den Administratoren-Funktionen in der Anwendung gespeichert sind. Auf den Webservern von hostNET wird die Nutzung der OUNUO-Seiten als Weblog erfasst.

Abschnitt I: AWS-Rechenzentrum (vergleichbare Standards bei hostNET)

I.1. Zutrittskontrolle

- Der Zutritt zu den Räumlichkeiten ist für Dritte nur nach Klingeln und anschließender Anmeldung möglich.
- Besucher werden von einer Mitarbeiterin oder Mitarbeiter persönlich abgeholt und müssen sich dann anmelden. Sie erhalten anschließend einen Besucherausweis der offen zu tragen ist. Dieser ist beim Verlassen der Räumlichkeiten wieder abzugeben. Die Vergabe und Abgabe des Ausweises wird protokolliert.
- Der Zutritt zu den Rechenzentren, in denen sich sämtliche datenverarbeitenden Systeme und Speichersysteme befinden, ist physisch besonders gesichert.
- Das Rechenzentrum und die Zugänge zur Bürofläche werden videoüberwacht. Der Service Desk verfügt über Monitore für die Videokameras.
- Der Service Desk ist rund um die Uhr an 365 Tagen im Jahr besetzt.

- Der Notausgang des Rechenzentrums ist alarmgesichert.
- Zutritt zum Rechenzentrum wird nur autorisierten Personen gegeben. Autorisierte Personen sind in diesem Zusammenhang die zuständigen Mitarbeiter des Rechenzentrumsbetreibers sowie die zum Zeitpunkt des Vertragsabschlusses definierten Ansprechpartner von Kunden, diese aber nur in Bezug auf ihre eigenen Systeme. Der Zutritt zu anderen Systemen ist nicht erlaubt und wird überwacht
- Das Rechenzentrum verfügt für Mitarbeiter über ein elektronisches Zutrittssystem, separierte Bereiche des Rechenzentrums sowie die Büroräumlichkeiten. Die Zutrittsrechte werden auf den jeweiligen Zutrittskarten oder Tokens der Mitarbeiter gespeichert und sind zeitlich begrenzt. Der Prozess zur Zuteilung der Rechte zum Rechenzentrumszutritt auf dem jeweiligen Zutrittskarten oder Token ist dokumentiert.
- Lieferanten, Kunden und sonstigen Dienstleistern wird nur nach Anmeldung, Identifikation und Registrierung sowie in Begleitung der Zutritt zum Rechenzentrum gewährt.
- Alle Serversysteme befinden sich in abgeschlossenen Schränken (Racks). Nur die Mitarbeiter, die zum Zutritt ins Rechenzentrum berechtigt sind, haben auch Zugriff auf die Schlüssel zu den Schränken.
- Die Systeme, für die Dienstleistungen im Sinne der Auftragsdatenverarbeitung erbracht werden, befinden sich in einem separierten Abschnitt des Rechenzentrums. Kunden erhalten keinen Zutritt zu diesem Abschnitt.

I.2. Zugangskontrolle

- Der elektronische Zugang zu Systemen über Netzwerk ist durch Firewalls und VPNs geschützt.
- Die administrativen Zugangsdaten zu den jeweiligen Serversystemen sind nur den Administratoren bekannt.

Allgemeine Vertragsbedingungen

- Jeder Nutzer erhält einen personalisierten, passwortgeschützten Account.
- Das Passwort ist im Abstand von 60 Tagen zu ändern und muss eine Kombination aus Buchstaben und Ziffern beinhalten. Dabei können die letzten 5 Passworte nicht wiederverwendet werden. Dies ist in der Sicherheitsrichtlinie Passwort-Policy dokumentiert. Wird ein Passwort nicht innerhalb der Frist geändert, wird der Account gesperrt.
- Zu Kundensystemen erhalten nur die Administratoren Zugriff, die den Kunden betreuen.
- Der Prozess zur Rechtevergabe ist dokumentiert.

1.3. Zugriffskontrolle

- Zu Kundensystemen erhalten nur die Administratoren Zugriff, die den Kunden betreuen.
- Zugriff auf Applikationen und Datenbanken wird – wo technisch realisierbar – rollenbasierend vergeben. Wo dies technisch nicht realisierbar ist, wird der Zugriff personenabhängig und individuell, je nach Aufgabenart, vergeben.
- Der Zugriff auf Netzlaufwerke erfolgt gemäß Benutzer(-gruppen)rechten. Der Prozess zur Rechtevergabe ist dokumentiert.
- Die Zugriffsrechte auf verschiedene interne Systeme wird in regelmäßigen Audits überprüft.
- Besonders schützenswerte personenbezogene Daten werden zusätzlich verschlüsselt.
- Der Umgang mit diesen Daten ist in einer Sicherheitsrichtlinie zum Umgang mit klassifizierten Informationen und Datenträgern beschrieben.

1.4. Weitergabekontrolle

- Außer zum Zwecke der Datensicherung erfolgt die Weitergabe personenbezogener Daten nur auf explizite Anweisung durch den Kunden (schriftlicher Change-Request oder Auftrag).
- Im Rahmen der Auslagerung von Sicherungsmedien werden diese Medien

transportgesichert. Diese befinden sich in einem getrennten Gebäude. Der Zutritt zu dem dort befindlichen Serverraum ist nur wenigen Mitarbeitern gestattet.

- Die Büroräumlichkeiten und der Serverraum verfügen über eine elektronische Zutrittskontrolle wie in 1.1. geschildert. Der Prozess zur Rechtevergabe ist dokumentiert.
- Die Daten sind durch Firewalls und Virenschutzsysteme vor dem Zugriff von außen, sowie Manipulationen, geschützt.
- Bei Transport personenbezogener Daten nach außen werden diese immer verschlüsselt. Die Sicherheitsrichtlinie zum Umgang mit klassifizierten Informationen und Datenträgern enthält weitere Angaben zu den integrierten Maßnahmen zur Kontrolle der Weitergabe von Daten.
- Für die Vernichtung von Dokumenten mit personenbezogenen Daten in Papierform sind Container aufgestellt. Der Zugriff auf die in den Containern enthaltenen Unterlagen/Daten ist nach Einwurf nicht mehr möglich. Diese Dokumente werden durch einen Dienstleister, unter Wahrung der datenschutzrechtlichen Regelungen vernichtet.

1.5. Eingabekontrolle

- Zur Gewährleistung der Eingabekontrolle sind Protokollierungs- und Protokollauswertungssysteme integriert.
- Das Nachverfolgen von Dateneingaben wird, wo technisch möglich, durch das etablierte logging-Verfahren gewährleistet. Somit ist es jederzeit nachvollziehbar welche User Daten eingegeben haben.

1.6. Auftragskontrolle

- Generelle Weisungen des Kunden werden zum Zeitpunkt der Vertragsunterschrift in Form einer Einzelvereinbarung dokumentiert und den zuständigen Mitarbeitern im Rahmen einer Einweisung in der Setup-Phase bekannt gemacht. Dort werden auch explizit die Weisungsbefugnisse und Kontrollrechte des Kunden schriftlich festgesetzt.

Allgemeine Vertragsbedingungen

- Weitere Aufträge des Kunden (z.B. Übertragung von Daten) unterliegen dem Change-Request-Verfahren und werden somit schriftlich dokumentiert.
- Kenntnisse über die Nicht-Einhaltung der Vorgaben des Kunden sind dem Datenschutzbeauftragten zur Kenntnis zu bringen.
- Subunternehmer werden den Vorgaben des Art. 28 Abs. 4 DSGVO entsprechend ausgewählt und verpflichtet. Dabei werden Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt. In jedem Einzelfall überzeugt sich der Rechenzentrumsbetreiber vor Beginn der Datenverarbeitung und sodann durch regelmäßige Kontrollen von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen.
- Die Verfügbarkeit der Systeme wird mithilfe eines Monitoring-Tools (Icinga) überwacht.
- Die Infrastruktur wie Backbone, USV, Strom und Klimaanlage werden ebenfalls mit dem Icinga Monitoring-Tool überwacht.
- Auf den Systemen werden regelmäßig Patches installiert. Der Patch- und Schwachstellenprozess ist in einer Sicherheitsrichtlinie „Security Prozesse“ dokumentiert.
- Die Daten sind durch Firewalls und Virenschutzsysteme vor dem Zugriff und Manipulation von außen geschützt.

I.7. Verfügbarkeitskontrolle

- Grundsätzlich werden alle Systeme, die im Zusammenhang mit der Verarbeitung von personenbezogenen Daten genutzt werden, im Rahmen des Backup-Dienstes regelmäßig gesichert und die Konsistenz der Sicherung wird geprüft.
- Datensicherungsmedien werden in einem getrennten Gebäude aufbewahrt. Der Prozess zur Gewährung von Zutritt folgt dem in I.4. und I.1. dargestellten Ablauf.
- Für Festplattensysteme an Servern werden RAID-Mechanismen eingesetzt, die die Ausfallsicherheit erhöhen.
- Alle Systeme werden über USV in den Rechenzentren gegen Spannungsspitzen, Spannungsschwankungen und Unterbrechung der Stromversorgung abgesichert.
- Das Rechenzentrum verfügt über ein Notstromaggregat und redundant ausgelegten Klimaanlage.
- Brandsensoren überwachen das Rechenzentrum rund um die Uhr.

I.8. Trennungskontrolle

- Datensicherungen und Produktivdaten werden getrennt voneinander aufbewahrt.
- Daten von Test- und Produktivsystemen werden getrennt voneinander abgelegt.
- Das Netz ist in verschiedene VLANs gegliedert und dadurch Mandantenfähig.
- Logdateien werden auf einem eigenen Log-System gespeichert.

Abschnitt II: Administration durch eGenius

II.1. Zutrittskontrolle

- Zutritt zu den Büroräumen haben grundsätzlich nur Mitarbeiter von eGenius.
- Gäste müssen sich anmelden und dürfen sich nicht unbegleitet im Büro bewegen.
- Zutritt zu den Betriebsräumen ist nur mit Sicherheitsschlüssel, Magnetkarte oder biometrischer Zutrittskontrolle möglich.
- Türen, Tore und Fenster sind außerhalb der Betriebszeiten fest verschlossen.

II.2. Zugangskontrolle

- Pro Benutzer wird eine individuelle Benutzererkennung vergeben.

Allgemeine Vertragsbedingungen

- Passwörter werden ausschließlich vom Benutzer erstellt.
- Passwörter für den Zugriff auf die Datenbanken müssen aus mindestens 8 Zeichen bestehen und müssen aus mindestens zwei der folgenden Komponenten bestehen: Kleinbuchstabe, Großbuchstabe, Zahl oder Sonderzeichen. Passwörter für die Arbeitsplätze der Mitarbeiter müssen aus mindestens sieben Zeichen bestehen.
- Geräte, von denen aus Zugriff auf Systeme besteht, auf denen Kundendaten gespeichert sind, verfügen über eine automatische Bildschirmsperre bei Inaktivität des Nutzers.

II.3. Zugriffskontrolle

- Individuelle Zuweisung von Rechten pro Benutzer (Abgestufte Zugriffsberechtigung).
- Organisatorische Berechtigungsbewilligung und technische Berechtigungsvergabe erfolgen durch verschiedene Personen (Vier-Augen-Prinzip).
- Zugriff auf Systeme mit Kundendaten haben nur ausgewählte Mitarbeiter, die einen solchen Zugriff für Ihre Tätigkeit zwingend benötigen.
- Der Auftragnehmer richtet die Datenbank für den Auftraggeber so ein, dass zwei Anwenderkonten für den Auftraggeber in der Datenbank hinterlegt sind. Das ist zum einen ein sogenanntes Master-Konto, das technisch benötigt wird, um die Datenbank initial einzurichten. Das Konto wird anschließend inaktiv gestellt und kann nur von einem sehr kleinen Mitarbeiterkreis beim Auftragnehmer in einem zweistufigen Verfahren wieder aktiviert werden. Das Master-Konto wird nur auf ausdrücklichen, schriftlichen Wunsch des Auftraggebers reaktiviert oder bei Beendigung des Vertragsverhältnisses, um die Datenbank vollständig löschen zu können. Das zweite Konto ist das OUNUO Support-Konto, welches ebenfalls bei Bereitstellung der Datenbank inaktiv geschaltet ist. Der Administrator beim Auftraggeber kann das OUNUO Support-Konto

aktiv schalten, damit Mitarbeiter im Support des Auftragnehmers bei der Lösung von Problemen mit der Datenbank helfend eingreifen können. Anschließend kann der Administrator des Auftraggebers das Konto für den OUNUO Support wieder inaktiv schalten. Der Auftragnehmer bzw. seine Mitarbeiter werden nicht ohne schriftliche Aufforderung durch den Kunden selbst Einblick in die Datenbank nehmen.

II.4. Weitergabekontrolle

- Alle Mitarbeiter sind auf das Datengeheimnis verpflichtet.
- Zugriffe auf Daten im Rechenzentrum erfolgen ausschließlich über verschlüsselte Verbindungen.

II.5. Eingabekontrolle

- Jede Eingabe oder Änderung von Kundendaten wird protokolliert.
- Jede Administratortätigkeit (z.B. Anlegen oder Löschen von Benutzern, Änderungen der Benutzerrechte) wird protokolliert (Syslog).

II.6. Auftragskontrolle

- Alle Mitarbeiter werden regelmäßig zum Datenschutz geschult.
- Arbeitsanweisungen werden in Schrift- oder Textform dokumentiert.

II.7. Verfügbarkeitskontrolle

Keine Maßnahmen erforderlich, da die Datenverarbeitung ausschließlich im Rechenzentrum erfolgt.

II.8. Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, werden logisch getrennt voneinander gespeichert.