vlott

Vertrag zur Auftragsverarbeitung „Auftragsverarbeitungsvereinbarung“

zwischen

Nutzern von vlott Prozesse | Urlaub & Krankheit

(Auftraggeber)

und

vlott UG (haftungsbeschränkt)

Eschstraße 19

48712 Gescher

(Auftragnehmer)

Der Auftraggeber und der Auftragnehmer werden nachfolgend gemeinsam als „Parteien“ oder einzeln als „Partei“ bezeichnet.

Präambel

Der Auftragnehmer ist mit der Verarbeitung personenbezogener Daten des Auftraggebers oder von angeschlossenen Unternehmen gem. Art. 28 der EU-Datenschutzgrundverordnung (EUDSGVO) betraut aufgrund des zwischen den Parteien geschlossenen Vertrags über die Nutzung der Services (Apps) der vlott UG (haftungsbeschränkt) („Hauptvertrag“).
Diese Vereinbarung zur Auftragsverarbeitung gilt für alle bestehenden und künftigen Verträge zwischen den Parteien.
Die rechtliche Grundlage für die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten wird durch den vorliegenden Vertrag zur Auftragsverarbeitung dergestalt geschaffen,dass für die Parteien nachfolgende Regelungen gelten.

§ 1
Geltungsbereich

1. Dieser Vertrag zur Auftragsverarbeitung („**Auftragsverarbeitungsvereinbarung**“) regelt jeweils die bilateralen rechtlichen Beziehungen zwischen dem Auftraggeber und dem Auftragnehmer.
2. Der Auftraggeber verfügt über ein Weisungsrecht gegenüber dem Auftragnehmer. Eine Weisung („**Weisung**“) ist eine Anordnung oder Richtlinie des Auftraggebers an den Auftragnehmer, die den formellen Anforderungen nach § 3 Abs. 2 entspricht. Das Recht, Weisungen zu erteilen, bleibt durch die Auftragsverarbeitungsvereinbarung inhaltlich unberührt.
3. **Rangfolge, „lex posterior“.** Soweit nicht anders vereinbart, geht eine Weisung dieser Auftragsverarbeitungsvereinbarung vor; ferner verdrängt die spätere Regelung die zeitlich frühere (so ersetzt bspw. eine jüngere Auftragsverarbeitungsvereinbarung eine ältere Weisung).

§ 2
Umfang

Diese Auftragsverarbeitungsvereinbarung regelt die Verpflichtungen der Parteien in Zusammenhang mit der Verarbeitung personenbezogener Daten des Auftraggebers durch den Auftragnehmer. Gegenstand, Umfang sowie Art und Zweck der Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch den Auftragnehmer sind in **ANNEX 2** konkret beschrieben.

§ 3
Pflichten des Auftraggebers

1. **Rechtmäßigkeit, Rechte Betroffener.** Der Auftraggeber bleibt verantwortliche Stelle im Sinne des Datenschutzrechts. Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Die Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten (Art. 15 ff. EU-DSGVO) der Betroffenen erfolgt ausschließlich und erkennbar im Namen des Auftraggebers.
2. **Form von Weisungen.** Der Auftraggeber erteilt Weisungen, die sich auf Art, Umfang und Verfahren der Datenverarbeitung beziehen. Die Weisung erfolgt zumindest in Textform (E-Mail). Mündlich erteilte Weisungen sind durch den Auftragnehmer unverzüglich in Textform zu bestätigen. Die weisungsberechtigte Person, ebenso wie der Weisungsempfänger sind in ANNEX 1 genannt.

§ 4
Pflichten des Auftragnehmers

1. **Weisungsgebundenheit, Zweckbindung.** Der Auftragnehmer verarbeitet personenbezogene Daten des Auftraggebers ausschließlich für die im ANNEX 2 genannten Zwecke und im Rahmen der Auftragsverarbeitungsvereinbarung sowie im Auftrag und gemäß den Weisungen des Auftraggebers. Der Auftragnehmer verwendet die personenbezogenen Daten für keine anderen Zwecke, sofern er hierzu nicht rechtlich verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtliche(n) Verpflichtung(en) mit, es sei denn, eine solche Mitteilung ist aufgrund wichtiger

öffentlicher Interessen verboten. Kopien oder Duplikate personenbezogener 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 benötigt werden. Sofern die Daten für verschiedene Zwecke verarbeitet werden, wird der Auftragnehmer die Daten mit dem jeweiligen Zweck kennzeichnen.

2. **Richtlinien, Anweisungen und Betriebsvereinbarungen.** Der Auftragnehmer führt die Datenverarbeitung unter Beachtung der für den Auftragsgegenstand beim Auftraggeber relevanten Richtlinien, Anweisungen und Betriebsvereinbarungen durch, soweit deren Inhalt dem Auftragnehmer bei Vertragsschluss oder nachträglich (etwa durch Weisung) zur Kenntnis gegeben wurde.
3. **Datenschutzbeauftragter.** Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.
4. **Prüfungen von Aufsichtsbehörden.** Der Auftragnehmer verpflichtet sich, dem Auftraggeber über Kontrollhandlungen und Maßnahmen der Datenschutzaufsichtsbehörden unverzüglich zu unterrichten, soweit diese mit der Verarbeitung der Daten des Auftraggebers in Zusammenhang stehen. Etwa festgestellte Beanstandungen wird der Auftragnehmer innerhalb angemessener Frist beheben und dies dem Auftraggeber mitteilen.
5. **Keine Verarbeitung in Drittstaaten.** Die Verarbeitung der Daten durch den Auftragnehmer findet grds. ausschließlich auf bzw. aus dem Gebiet der Bundesrepublik Deutschland, eines Mitgliedsstaates der Europäischen Union oder eines anderen Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein sonstiges Land bedarf der vorherigen ausdrücklichen Zustimmung des Auftraggebers und darf zudem nur erfolgen, wenn die besonderen Voraussetzungen für Datenexporte in Drittländer erfüllt sind. Der Auftragnehmer beachtet in diesem Fall die strengen Vorgaben der Datenübermittlung in Drittstaaten aus Art. 44 DSGVO und schließt entsprechende Vereinbarungen mit Auftragsverarbeitern in diesen Drittstaaten.
6. **Schulungen, Datenschutzgeheimnis.** Der Auftragnehmer hat die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut zu machen, auf das Datengeheimnis zu verpflichten und sie über die sich aus dieser Auftragsverarbeitungsvereinbarung ergebenden besonderen Datenschutzpflichten, Zweckbindungen und Weisungen zu belehren. Auf Anforderung wird der Auftragnehmer dies dem Auftraggeber nachweisen.
7. **Überwachung.** Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften dieser Auftragsverarbeitungsvereinbarung und der Weisungen des Auftraggebers regelmäßig während der gesamten Vertragslaufzeit. Die Ergebnisse der Kontrollen sind dem Auftraggeber auf Verlangen vorzulegen, soweit diese für die Verarbeitung der Daten des Auftraggebers relevant sind.
8. **Datentrennung.** Die verarbeiteten Daten bleiben von sonstigen Datenbeständen strikt getrennt.

§ 5
Technische und Organisatorische Maßnahmen zur Datensicherheit

1. **Umfang, Dokumentation.** Der Auftragnehmer wird angemessene technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten vor unbeabsichtigter oder unrechtmäßiger Veränderung, Löschung oder Vernichtung sowie unbefugtem Zugriff bzw. unbefugter Offenlegung treffen (Art. 32 EU-DSGVO)). Dabei sind der Stand der Technik, die Durchführungskosten, die Art, der Umfang und die Zwecke der Verarbeitung personenbezogener Daten sowie die Eintrittswahrscheinlichkeit und die Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Die derzeit vom Auftraggeber konkret getroffenen technischen und organisatorischen Maßnahmen sind in **ANNEX 3** dokumentiert. Diese Maßnahmen unterliegen dem Fortschritt und sind mit dem Stand der Technik weiterzuentwickeln. Insoweit ist es dem Auftragnehmer auch gestattet, seine konkret getroffenen Maßnahmen zu ändern, soweit das

vertraglich vereinbarte Schutzniveau hierdurch nicht unterschritten wird. Änderungen an den konkret getroffenen technischen und organisatorischen Maßnahmen sind zu dokumentieren und dem Verantwortlichen regelmäßig mitzuteilen, z.B. durch die regelmäßige Bereitstellung einer aktualisierten Liste konkret getroffener Maßnahmen in **ANNEX 3**. Wesentliche Änderungen sind schriftlich zu vereinbaren. Mitarbeiter des Auftragnehmers und Mitarbeiter des Unterauftragnehmers dürfen personenbezogene Daten des Auftraggebers auch außerhalb der Geschäftsräume des Auftragnehmers bzw. Unterauftragnehmers verarbeiten (Remote Work). Alle in dieser AVV festgelegten Pflichten gelten auch für das Remote Work, wobei der Auftragnehmer hierzu, wie in **ANNEX 3** beschrieben, spezielle technische und organisatorische Maßnahmen getroffen hat, um ein ausreichendes Datenschutzniveau sicherzustellen.

2. **Beurteilung der Zulässigkeit, Kontrolle.** Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich. Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind. Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers sowie nicht häufiger als alle 12 Monate statt. Kontrollen finden stichpunktartig statt, soweit nicht aus vom Auftraggeber zu dokumentierenden Gründen, eine vollumfängliche Kontrolle erforderlich ist.

§ 6
Berechtigung, Sperrung und Löschung von Daten

Auf Aufforderung durch den Auftraggeber oder nach Beendigung der Auftragsverarbeitungsvereinbarung hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände mit personenbezogenen Daten des Auftraggebers dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung bei sich datenschutzgerecht zu vernichten, soweit gesetzliche Aufbewahrungsfristen nicht entgegenstehen. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist dem Auftraggeber auf Verlangen vorzulegen. Die vollständige Löschung bzw. Herausgabe der Daten an den Auftraggeber ist diesem auf Verlangen mit Datumsangabe schriftlich zu bestätigen. Ist eine Löschung nur mit unverhältnismäßigem Aufwand möglich, können die Parteien eine Sperrung der Daten vereinbaren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer diesen Antrag unverzüglich an den Auftraggeber weitergeben.

§ 7
Unterauftragsverarbeiter

1. **Einwilligungsvorbehalt.** Soweit bei der Verarbeitung personenbezogener Daten des Auftraggebers vom Auftragnehmer Unterauftragsverarbeiter einbezogen werden sollen, bedarf dies der vorherigen Zustimmung des Auftraggebers. Die in **ANNEX 1** genannten Unterauftragnehmer gelten als vom Auftraggeber genehmigte Unterauftragsverarbeiter. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

2. **Verträge mit Unterauftragsverarbeiter.** Der Auftragnehmer hat die vertraglichen Vereinbarungen mit Unterauftragsverarbeitern so zu gestalten und auch durchzuführen, dass sie mindestens dasselbe Schutzniveau aufweisen, wie es aufgrund dieser Auftragsverarbeitungsvereinbarung und etwaigen Weisungen zwischen Auftraggeber und Auftragnehmer vereinbart wurde. Auf schriftliche Anforderung des Auftraggebers wird der Auftragnehmer dem Auftraggeber Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis erteilen, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen. Kommerzielle Bedingungen darf der Auftragnehmer dabei schwärzen. Der Auftraggeber ist zur Geheimhaltung der gewonnen Informationen verpflichtet.
3. **Kontrollrechte gegenüber Unterauftragsverarbeitern.** Bei der Unterbeauftragung sind dem Auftraggeber nach Möglichkeit direkte Kontrollrechte beim Unterauftragsverarbeiter einzuräumen, die bestenfalls denjenigen entsprechen, die der Auftraggeber nach dieser Auftragsverarbeitungsvereinbarung gegenüber dem Auftragnehmer hat.

§ 8
Hinweis- und allgemeine Unterstützungspflichten

1. **Rechtswidrige Weisungen.** Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn eine vom Auftraggeber erteilte Weisung nach Meinung des Auftragnehmers gegen gesetzliche Vorschriften zum Datenschutz verstößt. Die beanstandete Weisung braucht nicht befolgt zu werden, solange sie nicht durch den Auftraggeber geändert oder ausdrücklich bestätigt wird. Zu einer materiell-rechtlichen Prüfung von Weisungen ist der Auftragnehmer nicht verpflichtet.
2. **Meldung von Fehlern und Unregelmäßigkeiten.** Der Auftragnehmer hat bei der Feststellung von Fehlern oder Unregelmäßigkeiten der Datenverarbeitung für den Auftraggeber unverzüglich den Auftraggeber zu informieren. Dies gilt insbesondere für Fälle des Bekanntwerdens einer Verletzung der Datensicherheit, die unbeabsichtigter- und/oder unrechtmäßigerweise zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung bzw. unbefugten Zugang zu personenbezogenen Daten führt, die im Auftrag des Auftraggebers im Rahmen dieser Auftragsverarbeitungsvereinbarung verarbeiten werden.
3. Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragnehmer den Auftraggeber bei der Erfüllung seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten (Art. 15 ff. EU-DSGVO) sowie den datenschutzrechtlichen Pflichten aus Art. 32 bis 36 EU-DSGVO (Dokumentation der getroffenen technischen und organisatorischen Maßnahmen, Meldung von Datenschutzverletzungen an die Datenschutzaufsicht und ggf. die betroffenen Personen sowie Durchführung von Datenschutz-Folgenabschätzungen / Vorabkonsultationen der Datenschutzaufsicht).

§ 9
Dauer des Auftrags

1. Die Auftragsverarbeitungsvereinbarung beginnt und endet nach den Maßgaben des Hauptvertrags.
2. Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund liegt insbesondere vor, wenn
   - personenbezogene Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch Insolvenz oder Vergleichsverfahren oder durch sonstige vergleichbare Ereignisse gefährdet sind,
   - der Auftragnehmer gegen gesetzliche oder vertragliche Datenschutzbestimmungen verstößt,
   - der Auftragnehmer eine berechtigte Weisung nicht ausführen will oder kann, oder
   - Aufsichtsbehörden Zweifel an der Rechtmäßigkeit der Auftragsverarbeitung äußern.
3. Die Kündigungserklärung bedarf der Textform (E-Mail).
4. **Fortgeltung.** Soweit der Auftragnehmer über die Laufzeit der Auftragsverarbeitungsvereinbarung personenbezogene Daten des Auftraggebers weiterverarbeitet (z.B. Speicherung aufgrund von Aufbewahrungspflichten), gelten die vertraglichen Vereinbarungen zur Zweckbindung und Einhaltung der technischen und organisatorischen Maßnahmen zur Datensicherheit entsprechend fort.

§ 10
Geheimhaltungspflichten

1. Die Parteien verpflichten sich, alle Informationen und Materialien, die sie im Zusammenhang mit der Durchführung dieser Auftragsvereinbarung in mündlicher, schriftlicher, elektronischer, körperlicher oder anderer Form von der anderen Partei erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung dieser Auftragsverarbeitungsvereinbarung zu verwenden.
2. Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne dabei zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

§ 11
Haftung und Schadensersatz

1. Macht ein Betroffener gegenüber einer Partei Schadensersatzansprüche wegen Verstoßes gegen datenschutzrechtliche Bestimmungen geltend, so hat die beanspruchte Partei die andere Partei hierüber unverzüglich zu informieren.
2. Die Parteien haften gegenüber Betroffenen Personen entsprechend der in Art. 82 EUDSGVO getroffenen Regelungen.
3. Die Parteien unterstützen sich wechselseitig bei der Abwehr von Schadensersatzansprüchen betroffener Personen, es sei denn, dies würde die Rechtsposition der einen Partei im Verhältnis zur anderen Partei oder zur Aufsichtsbehörde gefährden.

§12
Sonstiges

1. **Maßnahmen Dritter.** Sind personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch Insolvenz oder Vergleichsverfahren oder durch sonstige vergleichbare Ereignisse gefährdet, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren.
2. **Schriftform.** Änderungen der Auftragsverarbeitungsvereinbarung bedürfen der Schriftform. Dieses Formerfordernis gilt auch für die Abbedingung der Formklausel.
3. **Salvatorische Klausel.** Sollten einzelne Teile dieser Auftragsverarbeitungsvereinbarung unwirksam sein oder werden, so berührt dies die Wirksamkeit der Auftragsverarbeitungsvereinbarung im Übrigen nicht.
4. **Anwendbares Recht, Gerichtsstand.** Die Auftragsverarbeitungsvereinbarung unterliegt dem Recht der Bundesrepublik Deutschland unter Ausschluss des UN Kaufrechts. Ausschließlicher Gerichtsstand ist derjenige des Auftragnehmers
5. **Vertragsstrafe**. Bei Verstoß gegen die Abmachungen dieses Vertrages wird eine verschuldensunabhängige Vertragsstrafe von € 500,- je Einzelfall vereinbart. Die Vertragsstrafe wird insbesondere bei Mängeln in der Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen verwirkt. Bei dauerhaften Verstößen gilt jeder Kalendermonat, in dem der Verstoß ganz oder teilweise vorliegt, als Einzelfall. Für vorsätzlich begangene Zuwiderhandlungen wird die Einrede des Fortsetzungszusammenhangs ausgeschlossen. Die Vertragsstrafe hat keinen Einfluss auf andere Ansprüche des Auftraggebers
6. **Nebenabreden**. Für Nebenabreden ist die Schriftform erforderlich.

ANNEX 1

1. Ansprechpartner / Weisungsempfänger beim Auftragnehmer

Name, Vorname / Zuständigkeit oder Funktion	Kontaktdaten
Weghake, Jens / Geschäftsführer Schmitz, Marcel / Geschäftsführer	Vlott UG (haftungsbeschränkt) Eschstraße 19 48712 Gescher Tel.: +49 170 603 10 66 E-Mail: contact@vlott.io

2. Datenschutzbeauftragter des Auftragnehmers

Beim Auftragnehmer wurde kein Datenschutzbeauftragter bestellt, weil die Unternehmensgröße des Auftragnehmers aktuell in der Größenordnung eines Kleinstunternehmens ist.

3. Unterauftragsverarbeiter

- Amazon Web Services EMEA SARL (“AWS EUROPE”)

ANNEX 2

Konkretisierung der Datenverarbeitung

1. Gegenstand der Verarbeitung & Dauer der Auftragsverarbeitung

Gegenstand und Dauer des Auftrags ergibt sich aus dem Hauptvertrag.

2. Zweck der Verarbeitung

Die Tätigkeit des Auftragnehmers dient folgenden vereinbarten Zwecken:
Bereitstellung von digitalen Prozessen (Workflows) wie beispielsweise Urlaubsanträge und Krankmeldung sowie den dazugehörigen administrativen Voraussetzungen (Anlage und Pflege von Urlaubsprofilen, Speicherung und Bereitstellung von Übersichten, Führen von Urlaubskonten, etc.).

3. Kategorien personenbezogener Daten

Die von der Verarbeitung betroffenen Kategorien personenbezogener Daten hängen von der Nutzung der Leistungen des Auftragnehmers durch den Auftraggeber ab. Als Gegenstand der Verarbeitung in Betracht kommende Kategorien von Daten sind möglich

- Stammdaten (z.B. Namen, Personalnummern, Abwesenheitszeiten)
- Kontaktdaten (z.B. E-Mail-Adressen, Telefonnummern),
- Inhaltsdaten (z.B. Texteingaben, Fotografien, Namen von Dokumenten),
- Nutzungsdaten (z.B. Verlauf auf unseren Web-Diensten, Nutzung bestimmter Inhalte, Zugriffszeiten),
- Verbindungsdaten (z.B. Geräte-Informationen, IP-Adressen, URL-Referrer) und

Ob die Leistungen des Anbieters für die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO geeignet sind, bedarf einer Risikobewertung durch den Auftraggeber.

4. Kategorien betroffener Personen

Die von der Verarbeitung betroffenen Kategorien betroffener Personen hängen von der Nutzung der Leistungen des Auftragnehmers durch den Auftraggeber ab. Als Kategorien betroffener Personen kommen dabei in Betracht (ehemalige) Beschäftigte, Auszubildende und Praktikanten, Bewerber, freie Mitarbeiter, Gesellschafter, Organe der Gesellschaft, Angehörige von Beschäftigten, Kunden, Interessenten, Lieferanten, Dienstleister, Mieter, Geschäftspartner, externe Berater, Besucher und Pressevertreter.

ANNEX 3

Technische und organisatorische Maßnahmen (TOM)
vlott UG (haftungsbeschränkt)

1. Maßnahmen zur Sicherstellung der Vertraulichkeit der Systeme und Dienste (Art. 32 Abs. 1 lit. b EU-DSGVO)

a. Zutrittskontrolle

Vorgabe / Anforderung:

Ein unbefugter Zutritt zu Datenverarbeitungsanlagen ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Berechtigungskonzept für Zugang zu Räumen
- Manuelles Schließsystem
- Räume werden geschlossen gehalten (Fenster und Türen), wenn niemand im Raum ist
- Arbeitsräume werden nicht privat genutzt

b. Zugangskotrolle

Vorgabe / Anforderung:

Eine Nutzung der DV-Systeme durch Unbefugte ist zu verhindern.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Authentifizierung mit persönlicher Benutzerkennung und Passwort
- Passwortrichtlinie mit Mindestanforderungen an Passwörtern
- Einsatz einer dem Stand der Technik entsprechenden Software-Firewall
- Einsatz einer dem Stand der Technik entsprechenden Anti-Viren-Software
- Automatische Bildschirmsperre
- Patch-Management in zentraler Datenhaltung durch Einspielen manueller Updates (Sichtung der Updatelage und Einspielen von Updates in sicherheitsrelevanten Fällen)

c. Zugriffskontrolle

Vorgabe / Anforderung:

Es ist zu gewährleisten, dass die zur Benutzung eines DV-Systems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Vom Auftragnehmer konkret getroffene Maßnahmen:
Passende Einrichtung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

- Differenzierte Berechtigungen (Profile, Rollen, Gruppen) o
    - Dateisystem
    - Anwendungen
- Wartungsrichtlinien
- Authentifizierung durch Benutzername und Passwort

- Teilweise Zwei-Faktoren-Authentifizierung
- Anzahl der Personen mit „Administrator-Status“ minimiert
- Regelmäßige Anwendung von Sicherheits-Patches

d. Trennungskontrolle

Vorgabe / Anforderung:

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- logische Trennung der Daten der jeweiligen Kunden des (Unter-) Auftraggebers, d. h. Daten verschiedener verantwortlicher Stellen und/oder (Unter-)Auftraggeber sind getrennt zu verarbeiten und gegenseitiger Zugriff ist auszuschließen
- Berechtigungskonzept
- Trennung von Produktiv- und Testsystem

2. Maßnahmen zur Sicherstellung der Integrität der Systeme und Dienste (Art. 32 Abs. 1 lit. b EU-DSGVO)

a. Weitergabekontrolle

Vorgabe / Anforderung:

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

Vom Auftragnehmer konkret getroffenen Maßnahmen:

- Dem Industriestandard entsprechende verschlüsselte Datenübertragungen (SSL)
- Sicherheit auf Servern des Auftraggebers wird durch SSL-Verschlüsselung gewährleistet
- Protokollierungssystem
- Schnittstellenanalyse
- Weitergabe von Daten an Dritte ist untersagt

b. Eingabekontrolle

Vorgabe / Anforderung:

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

3. Maßnahmen zur Sicherstellung der Verfügbarkeit und Belastbarkeit der Systeme und Dienste (Art. 32 Abs. 1 lit. b und c EU-DSGVO)

a. Verfügbarkeitskontrolle

Vorgabe / Anforderung:

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Erstellung eines Backup- und Recovery-Konzepts (redundante Datenspeicherung)
- Notfallprozeduren und Test zur Datenwiderherstellung aus Backup
- Aufbewahrung der Datensicherung an einem sicheren Ort
- Einsatz dem Stand der Technik entsprechender Anti-Viren-Software
- Einsatz dem Stand der Technik entsprechender Software-Firewall

b. Rasche Wiederherstellung

Vorgabe / Anforderung:

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Sicherstellung vollständiger, konsistenter Backups

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

a. Auftragskontrolle

Vorgabe / Anforderung:

Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Vertrag zur Auftragsdatenverarbeitung mit Dienstleistern nach Art. 28 EU-DSGVO
- Eindeutige Vertragsgestaltung mit Sub-Auftragnehmer auf der Grundlage des Hauptvertrages mit dem Auftraggeber
- Prozess zur Erteilung und/oder Befolgung von Weisungen
- Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern
- Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung
- Verpflichtung der Beschäftigten auf die Vertraulichkeit
- Sorgfältige Auswahl von Auftragnehmern
- Kontrolle der technischen und organisatorischen Maßnahmen beim (Unter-)Auftragnehmer

b. Incident-Response-Management

Vorgabe / Anforderung:

Eine Meldung bei Verletzung personenbezogener Daten ist zu gewährleisten.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Meldeprozess nach Art. 33, 34 EU-DSGVO

c. Datenschutzrechtliche Voreinstellungen

Vorgabe / Anforderung:

Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten.

Vom Auftragnehmer konkret getroffene Maßnahmen:

- Verwendung von https
- vlott Apps werden stets datenschutzfreundlich vorkonfiguriert ausgeliefert und intern bereitgestellt. Verarbeitungen, die nicht erforderlich sind, werden nur auf Veranlassung des Anwenders oder nach einer vorherigen Einwilligung vorgenommen. Optionale Eingabefelder in Anwendungen sind ersichtlich, eine Verpflichtung zum Ausfüllen besteht selbstverständlich nicht.