Allgemeine Geschäftsbedingungen zur Auftragsverarbeitung gemäß Art. 28 Abs. 3 DSGVO

1. Geltungsbereich und Vertragspartner

Die nachfolgende Allgemeine Geschäftsbedingungen zur Auftragsverarbeitung gemäß Art. 28 Abs. 3 DSGVO (nachfolgend **„AGB-AVV“**) konkretisieren die Verpflichtungen zum Datenschutz, die sich aus einem zwischen dem Verantwortlichen (nachfolgend geschlechtsneutral **„Auftraggeber“**) und der Ihre Helden GmbH, vertreten durch die Geschäftsführer Thomas Braun, Philip Hartmann und Christoph Hemker, Kopernikusstraße 14, 30167 Hannover, Deutschland, Tel.: +49 (0) 511 - 64726900, E-Mail: info@ihre-helden.de (nachfolgend geschlechtsneutral **„Auftragnehmer“**, gemeinsam mit dem Auftraggeber auch **„Parteien“**) geschlossenen Dienstleistungsvertrag gem. Ziffer 2.1. (nachfolgend **„Hauptvertrag“**) ergeben.

2. Vertragsgegenstand und Umfang der Auftragsverarbeitung

2.1. Im Rahmen der Leistungserbringung nach der Allgemeine Geschäftsbedingungen mit Kundeninformationen vom 05.06.2023 abrufbar unter dem Link https://hldn.li/ihreheldenagb (nachfolgend „**Hauptvertrag**“ genannt) ist es erforderlich, dass der Auftragnehmer als Auftragsverarbeiter mit personenbezogenen Daten umgeht, für die der Auftraggeber als Verantwortlicher im Sinne der datenschutzrechtlichen Vorschriften fungiert (nachfolgend „**Auftraggeberdaten**“ genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeberdaten zur Durchführung des Hauptvertrags.

2.2. Der Auftragnehmer verarbeitet die Auftraggeberdaten im Auftrag und nach Weisung des Auftraggebers i.S.v. Art. 28 DSGVO (Auftragsverarbeitung). Der Auftraggeber bleibt Verantwortlicher im datenschutzrechtlichen Sinn.

2.3. Die Verarbeitung von Auftraggeberdaten durch den Auftragnehmer erfolgt in der Art, dem Umfang und zu dem Zweck wie in **Anlage 1 („Gegenstand der Auftragsverarbeitung“)** zu diesem AV-Vertrag spezifiziert, die Verarbeitung betrifft die dort näher bezeichneten Arten personenbezogener Daten und Kategorien betroffener Personen. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.

2.4. Dem Auftragnehmer bleibt es vorbehalten, die Auftraggeberdaten zu anonymisieren oder zu aggregieren, so dass eine Identifizierung einzelner betroffener Personen nicht mehr möglich ist, und in dieser Form zum Zweck der bedarfsgerechten Gestaltung, der Weiterentwicklung und der Optimierung sowie der Erbringung des nach Maßgabe des Hauptvertrags vereinbarten Dienstes zu verwenden. Die Parteien stimmen darin überein, dass anonymisierte bzw. nach obiger Maßgabe aggregierte Auftraggeberdaten nicht mehr als Auftraggeberdaten im Sinne dieses Vertrags gelten.

2.5. Der Auftragnehmer darf die Auftraggeberdaten im Rahmen des datenschutzrechtlich Zulässigen für eigene Zwecke auf eigene Verantwortung verarbeiten und nutzen, wenn eine gesetzliche Erlaubnisvorschrift oder eine Einwilligungserklärung des Betroffenen das gestattet. Auf solche Datenverarbeitungen findet dieser Vertrag keine Anwendung.

2.6. Die Verarbeitung der Auftraggeberdaten durch den Auftragnehmer findet grundsätzlich innerhalb der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Es ist dem Auftragnehmer gleichwohl gestattet, Auftraggeberdaten unter Einhaltung der

Bestimmungen dieses Vertrags auch außerhalb des EWR zu verarbeiten, wenn er den Auftraggeber vorab über den Ort der Datenverarbeitung informiert und die Voraussetzungen der Art. 44–48 DSGVO erfüllt sind oder eine Ausnahme nach Art. 49 DSGVO vorliegt.

3. Weisungsbefugnisse des Auftraggebers

3.1. Der Auftragnehmer verarbeitet die Auftraggeberdaten gemäß den Weisungen des Auftraggebers, sofern der Auftragnehmer nicht gesetzlich zu einer anderweitigen Verarbeitung verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.2. Die Weisungen des Auftraggebers sind grundsätzlich abschließend in den Bestimmungen dieses Vertrags festgelegt und dokumentiert. Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers und erfolgen nach Maßgabe des im Hauptvertrag festgelegten Änderungsverfahrens, in dem die Weisung zu dokumentieren und die Übernahme etwa dadurch bedingter Mehrkosten des Auftragnehmers durch den Auftraggeber zu regeln ist.

3.3. Der Auftragnehmer gewährleistet, dass er die Auftraggeberdaten im Einklang mit den Weisungen des Auftraggebers verarbeitet. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder das geltende Datenschutzrecht verstößt, ist er nach einer entsprechenden Mitteilung an den Auftraggeber berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen. Die Parteien stimmen darin überein, dass die alleinige Verantwortung für die weisungsgemäße Verarbeitung der Auftraggeberdaten beim Auftraggeber liegt.

4. Verantwortlichkeit des Auftraggebers

4.1. Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der Auftraggeberdaten sowie für die Wahrung der Rechte der Betroffenen im Verhältnis der Parteien zueinander allein verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund der Verarbeitung von Auftraggeberdaten nach Maßgabe dieses Vertrages Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen.

4.2. Dem Auftraggeber obliegt es, dem Auftragnehmer die Auftraggeberdaten rechtzeitig zur Leistungserbringung nach dem Hauptvertrag zur Verfügung zu stellen und er ist verantwortlich für die Qualität der Auftraggeberdaten. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

4.3. Der Auftraggeber hat dem Auftragnehmer auf Anforderung die in Art. 30 Abs. 2 DSGVO genannten Angaben zur Verfügung zu stellen, soweit sie dem Auftragnehmer nicht selbst vorliegen.

4.4. Ist der Auftragnehmer gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung von Auftraggeberdaten zu erteilen oder mit diesen Stellen anderweitig zusammenzuarbeiten, so ist der Auftraggeber verpflichtet, den

Auftragnehmer auf erstes Anfordern bei der Erteilung solcher Auskünfte bzw. der Erfüllung anderweitiger Verpflichtungen zur Zusammenarbeit zu unterstützen.

5. Anforderungen an Personal

Der Auftragnehmer hat alle Personen, die Auftraggeberdaten verarbeiten, bezüglich der Verarbeitung von Auftraggeberdaten zur Vertraulichkeit zu verpflichten.

6. Sicherheit der Verarbeitung

6.1. Der Auftragnehmer wird gemäß Art. 32 DSGVO erforderliche, geeignete technische und organisatorische Maßnahmen ergreifen, die unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung der Auftraggeberdaten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Auftraggeberdaten zu gewährleisten.

6.2. Dem Auftragnehmer ist es gestattet, technische und organisatorische Maßnahmen, insbesondere die näher in **Anlage 2 („Technisch-organisatorische Maßnahmen“)** zu diesem Vertrag aufgeführten Maßnahmen, während der Laufzeit des Vertrages zu ändern oder anzupassen, solange sie weiterhin den gesetzlichen Anforderungen genügen.

7. Inanspruchnahme weiterer Auftragsverarbeiter

7.1. Der Auftraggeber erteilt dem Auftragnehmer hiermit die allgemeine Genehmigung, weitere Auftragsverarbeiter hinsichtlich der Verarbeitung von Auftraggeberdaten hinzuzuziehen. Die zum Zeitpunkt des Vertragsschlusses hinzugezogenen weiteren Auftragsverarbeiter ergeben sich aus **Anlage 3 („Unterauftragsverarbeiter“)**. Generell nicht genehmigungspflichtig sind Vertragsverhältnisse mit Dienstleistern, die die Prüfung oder Wartung von Datenverarbeitungsverfahren oder -anlagen durch andere Stellen oder andere Nebenleistungen zum Gegenstand haben, auch wenn dabei ein Zugriff auf Auftraggeberdaten nicht ausgeschlossen werden kann, solange der Auftragnehmer angemessene Regelungen zum Schutz der Vertraulichkeit der Auftraggeberdaten trifft.

7.2. Der Auftragnehmer wird den Auftraggeber über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter informieren. Dem Auftraggeber steht im Einzelfall ein Recht zu, Einspruch gegen die Beauftragung eines potentiellen weiteren Auftragsverarbeiters zu erheben. Ein Einspruch darf vom Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden Grund erhoben werden. Soweit der Auftraggeber nicht innerhalb von 14 Tagen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Erhebt der Auftraggeber Einspruch, ist der Auftragnehmer berechtigt, den Hauptvertrag und diesen Vertrag mit einer Frist von 3 Monaten zu kündigen.

7.3. Der Vertrag zwischen dem Auftragnehmer und dem weiteren Auftragsverarbeiter muss letzterem dieselben Pflichten auferlegen, wie sie dem Auftragnehmer kraft dieses Vertrages obliegen. Die Parteien stimmen überein, dass diese Anforderung erfüllt ist, wenn der Vertrag ein diesem Vertrag entsprechendes Schutzniveau aufweist bzw. dem

weiteren Auftragsverarbeiter die in Art. 28 Abs. 3 DSGVO festgelegten Pflichten auferlegt sind.

7.4. Unter Einhaltung der Anforderungen der Ziffer dieses Vertrags gelten die Regelungen in dieser Ziffer 7 auch, wenn ein weiterer Auftragsverarbeiter in einem Drittstaat eingeschaltet wird. Der Auftraggeber bevollmächtigt den Auftragnehmer hiermit, in Vertretung des Auftraggebers mit einem weiteren Auftragsverarbeiter einen Vertrag unter Einbeziehung der EU-Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern vom 5.2.2010 zu schließen. Der Auftraggeber erklärt sich bereit, an der Erfüllung der Voraussetzungen nach Art. 49 DSGVO im erforderlichen Maße mitzuwirken.

8. Rechte der betroffenen Personen

8.1. Der Auftragnehmer wird den Auftraggeber mit technischen und organisatorischen Maßnahmen im Rahmen des Zumutbaren dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der ihnen zustehenden Rechte betroffener Personen nachzukommen.

8.2. Soweit eine betroffene Person einen Antrag auf Wahrnehmung der ihr zustehenden Rechte unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen zeitnah an den Auftraggeber weiterleiten.

8.3. Der Auftragnehmer wird dem Auftraggeber Informationen über die gespeicherten Auftraggeberdaten, die Empfänger von Auftraggeberdaten, an die der Auftragnehmer sie auftragsgemäß weitergibt, und den Zweck der Speicherung mitteilen, sofern dem Auftraggeber diese Informationen nicht selbst vorliegen oder er sie sich selbst beschaffen kann.

8.4. Der Auftragnehmer wird es dem Auftraggeber ermöglichen, im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten, Auftraggeberdaten zu berichtigen, zu löschen oder ihre weitere Verarbeitung einzuschränken oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung oder Einschränkung der weiteren Verarbeitung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.

8.5. Soweit die betroffene Person gegenüber dem Auftraggeber ein Recht auf Datenübertragbarkeit bezüglich der Auftraggeberdaten nach Art. 20 DSGVO besitzt, wird der Auftragnehmer den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten bei der Bereitstellung der Auftraggeberdaten in einem gängigen und maschinenlesbaren Format unterstützen, wenn der Auftraggeber sich die Daten nicht anderweitig beschaffen kann.

9. Mitteilungs- und Unterstützungspflichten des Auftragnehmers

9.1. Soweit den Auftraggeber eine gesetzliche Melde- oder Benachrichtigungspflicht wegen einer Verletzung des Schutzes von Auftraggeberdaten (insbesondere nach Art. 33, 34 DSGVO) trifft, wird der Auftragnehmer den Auftraggeber zeitnah über etwaige meldepflichtige Ereignisse in seinem Verantwortungsbereich informieren. Der Auftragnehmer wird den Auftraggeber bei der Erfüllung der Melde- und Benachrichtigungspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten unterstützen.

9.2. Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten bei etwa vom Auftraggeber durchzuführenden Datenschutz-Folgenabschätzungen und sich gegebenenfalls anschließenden Konsultationen der Aufsichtsbehörden nach Art. 35, 36 DSGVO unterstützen.

10. Datenlöschung

10.1. Der Auftragnehmer wird die Auftraggeberdaten nach Beendigung dieses Vertrages löschen, sofern nicht gesetzlich eine Verpflichtung des Auftragnehmers zur weiteren Speicherung der Auftraggeberdaten besteht.

10.2. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung von Auftraggeberdaten dienen, dürfen durch den Auftragnehmer auch nach Vertragsende aufbewahrt werden.

11. Nachweise und Überprüfungen

11.1. Der Auftragnehmer wird dem Auftraggeber auf dessen Anforderung alle erforderlichen und beim Auftragnehmer vorhandenen Informationen zum Nachweis der Einhaltung seiner Pflichten nach diesem Vertrag zur Verfügung stellen.

11.2. Der Auftraggeber ist berechtigt, den Auftragnehmer bezüglich der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen, zu überprüfen; einschließlich durch Inspektionen.

11.3. Zur Durchführung von Inspektionen nach Ziffer 11.2 ist der Auftraggeber berechtigt, im Rahmen der üblichen Geschäftszeiten montags bis freitags von 08:00 bis 17:00 Uhr (unter Ausnahme gesetzlicher Feiertage am Sitz des Auftragnehmers) nach rechtzeitiger Vorankündigung gemäß Ziffer 11.5 auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers die Geschäftsräume des Auftragnehmers zu betreten, in denen Auftraggeberdaten verarbeitet werden.

11.4. Der Auftragnehmer ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Auftraggebers, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragnehmers sind oder wenn der Auftragnehmer durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Auftraggeber ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, zu Informationen hinsichtlich Kosten, zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragnehmers, die nicht unmittelbar relevant für die vereinbarten Überprüfungszwecke sind, zu erhalten.

11.5. Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens zwei Wochen vorher) über alle mit der Durchführung der Überprüfung zusammenhängenden Umstände zu informieren. Der Auftraggeber darf eine Überprüfung pro Kalenderjahr durchführen. Weitere Überprüfungen erfolgen gegen Kostenerstattung und nach Abstimmung mit dem Auftragnehmer.

11.6. Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Überprüfung, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund von dieser Ziffer 11 dieses Vertrags gegenüber dem Auftragnehmer verpflichtet ist. Zudem hat der Auftraggeber den Dritten auf Verschwiegenheit und Geheimhaltung

zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber ihm die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Wettbewerber des Auftragnehmers mit der Kontrolle beauftragen.

11.7. Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der Pflichten nach diesem Vertrage anstatt durch eine Inspektion auch durch die Vorlage eines geeigneten, aktuellen Testats oder Berichts einer unabhängigen Instanz (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit – z.B. nach BSI-Grundschutz – („Prüfungsbericht“) erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.

12. Vertragsdauer und Kündigung

Die Laufzeit und Kündigung dieses Vertrags richtet sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

13. Haftung

13.1. Für die Haftung des Auftragnehmers nach diesem Vertrag gelten die Haftungsausschlüsse und -begrenzungen gemäß dem Hauptvertrag. Soweit Dritte Ansprüche gegen den Auftragnehmer geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftraggebers gegen diesen Vertrag oder gegen eine seiner Pflichten als datenschutzrechtlich Verantwortlicher haben, stellt der Auftraggeber den Auftragnehmer von diesen Ansprüchen auf erstes Anfordern frei.

13.2. Der Auftraggeber verpflichtet sich, den Auftragnehmer auch von allen etwaigen Geldbußen, die gegen den Auftragnehmer verhängt werden, in dem Umfang auf erstes Anfordern freizustellen, in dem der Auftraggeber Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

14. Schlussbestimmungen

14.1. Das anwendbare Recht bestimmt sich nach dem Hauptvertrag.

14.2. Der Gerichtsstandort bestimmt sich nach dem Hauptvertrag.

14.3. Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieses Vertrags vor.

14.4. Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und dabei den Anforderungen des Art. 28 DSGVO genügt.

14.5. Dieser Auftragsverarbeitungsvertrag ist ein Teil des Hauptvertrages und wird mit dessen Abschluss wirksam.

Stand: 05.06.2023

Anlage 1: Gegenstand der Auftragsverarbeitung

Zwecke der Auftragsverarbeitung

Personenbezogene Daten des Auftraggebers werden auf Grundlage dieses Auftragsverarbeitungsvertrages zu den folgenden Zwecken verarbeitet:

- Beratungsleistungen.
- Einrichtung, Wartung und Betreuung von informationstechnischen Anlagen und Systemen (IT).
- Einrichtung, Wartung- und Betreuung von Telekommunikationsanlagen und -systemen (TK).
- Kundenmanagement und / oder Kundensupport.
- Leistungen im Bereich der Wartung.
- Verwaltungs-, Administrations- und Managementleistungen.
- Web- und Cloud-Hosting.

Arten und Kategorien von Daten

Zu den auf Grundlage dieses Auftragsverarbeitungsvertrages verarbeiteten Arten und Kategorien von personenbezogenen Daten gehören:

- Bestandsdaten.
- Kontaktdaten.
- Inhaltsdaten.
- Bild- und/ oder Videoaufnahmen.
- Vertragsdaten.
- Zahlungsdaten und Abrechnungsdaten,
- Bonitätsdaten.
- Nutzungsdaten.
- Protokolldaten.
- Meta- und Verbindungsdaten.
- Telemetriedaten.

Kategorien der betroffenen Personen

Zu den durch die Verarbeitung von personenbezogenen Daten auf Grundlage dieses Auftragsverarbeitungsvertrages betroffenen Personengruppen gehören:

- Softwarenutzer.
- Geschäftskunden.
- Geschäftspartner.

- Freie Mitarbeiter.
- Beschäftigte/ Arbeitnehmer.
- Zielgruppen von Marketingmaßnahmen

Quellen der verarbeiteten Daten

Die auf Grundlage dieses Auftragsverarbeitungsvertrages verarbeiteten Daten werden aus den im Folgenden genannten Quellen, bzw. im Rahmen genannter Verfahren erhoben oder sonst empfangen:

- Erhebung bei betroffenen Personen.
- Eingaben, bzw. Angaben des Auftraggebers.
- Erhebung im Rahmen der Nutzung von Software, Applikationen, Webseiten und anderen Onlinediensten.
- Erhebung über Schnittstellen zu Diensten anderer Anbieter.
- Externe Datenbanken und Datensammlungen.

Anlage 2: Technisch-organisatorische Maßnahmen

Es wird für die konkrete Auftragsverarbeitung und die in ihrem Rahmen verarbeiteten personenbezogenen Daten ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau Gewähr geleistet. Dazu werden insbesondere die Schutzziele der Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

Organisatorische Maßnahmen

Es sind organisatorische Maßnahmen ergriffen worden, die ein angemessenes Datenschutzniveau und dessen Aufrechterhaltung gewährleisten.

- Es sind interne Sicherheitsricht- bzw. -leitlinien definiert, die unternehmensintern gegenüber Mittarbeitern als verbindliche Regeln kommuniziert werden.
- Regelmäßige anlasslose Auswertung der Log-Dateien zur Erkennung von ungewöhnlichen Einträgen.
- Die Entwicklung des Standes der Technik und sowie der Entwicklungen, Bedrohungen und Sicherheitsmaßnahmen werden fortlaufend beobachtet und in geeigneter Art und Weise auf das eigene Sicherheitskonzept abgeleitet.
- Es besteht ein Konzept, das die Wahrung der Betroffenenrechte durch den Auftraggeber gewährleistet (insbesondere im Hinblick auf Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, Datentransfer, Widerrufe & Widersprüche). Zu dem Konzept gehört die Unterrichtung der Mitarbeiter über die Informationspflichten gegenüber dem Auftraggeber, Einrichtung von Umsetzungsverfahren und die Benennung zuständiger Personen sowie regelmäßige Kontrolle und Evaluierung der ergriffenen Maßnahmen.
- Sicherheitsvorkommnisse werden konsequent dokumentiert, auch wenn sie nicht zu einer externen Meldung (z. B. an die Aufsichtsbehörde, betroffene Personen) führen (sogenanntes "Security Reporting").

- Dienstleister, die zur Erfüllung nebengeschäftlicher Aufgaben herangezogen werden (Wartungs-, Wach-, Transport- und Reinigungsdienste, freie Mitarbeiter, etc.), werden sorgfältig ausgesucht und es wird sichergestellt, dass sie den Schutz personenbezogener Daten beachten. Sofern die Dienstleister im Rahmen ihrer Tätigkeit Zugang zu personenbezogenen Daten des Auftraggebers erhalten oder sonst das Risiko eines Zugriffs auf die personenbezogenen Daten besteht, werden sie speziell auf Verschwiegenheit und Vertraulichkeit verpflichtet.
- Der Schutz von personenbezogenen Daten wird unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen bereits bei der Entwicklung, bzw. Auswahl von Hardware, Software sowie Verfahren, entsprechend dem Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen berücksichtigt.
- Eingesetzte Software und Hardware wird stets auf dem aktuell verfügbaren Stand gehalten und Softwareaktualisierungen werden ohne Verzug innerhalb einer angesichts des Risikograde und eines eventuellen Prüfnotwendigkeit angemessenen Frist ausgeführt. Es wird keine Software und Hardware eingesetzt, die von den Anbietern im Hinblick auf Belange des Datenschutzes- und Datensicherheit nicht mehr aktualisiert wird (z. B. abgelaufene Betriebssysteme).
- Standardsoftware und entsprechende Updates werden nur aus vertrauenswürdigen Quellen bezogen.
- Eine Geräteverwaltung erlaubt die Bestimmung, welche Beschäftigten oder Beauftragten welche Geräte in welchen Bereichen einsetzen.
- Es wird ein „papierloses Büro“ geführt, d. h. Unterlagen werden grundsätzlich nur digital gespeichert und nur in Ausnahmefällen in Papierform aufbewahrt.
- Unterlagen im Papierformat werden nur dann aufbewahrt, wenn keine im Hinblick auf die Auftragsverarbeitung, ihrem Zweck und den Interessen der von den Inhalten der Unterlagen betroffenen Personen adäquate digitale Kopie vorliegt oder eine Aufbewahrung mit dem Auftraggeber vereinbart wurde oder gesetzlich erforderlich ist.

Zutrittskontrolle

Es sind Maßnahmen zur physischen Zutrittskontrolle ergriffen worden, die es Unbefugten verwehren, sich den Systemen, Datenverarbeitungsanlagen oder Verfahren physisch zu nähern, mit denen personenbezogene Daten verarbeitet werden.

- Es werden, bis auf die Arbeitsplatzrechner und mobile Geräte, keine Datenverarbeitungsanlagen in den eigenen Geschäftsräumlichkeiten unterhalten. Die Daten des Auftraggebers werden bei externen Server-Anbietern unter Beachtung der Vorgaben für Auftragsverarbeitung gespeichert.
- Der Zutritt zu Datenverarbeitungsanlagen ist zusätzlich gesichert und nur befugten Mitarbeitern möglich.
- Es findet eine Personenkontrolle beim Pförtner oder am Empfang statt.
- Die Besucher werden protokolliert.
- Um den Zutritt durch Unbefugte zu verhindern, wird Videoüberwachungstechnologie eingesetzt.
- Um den Zutritt durch Unbefugte zu verhindern, wird eine Alarmanlage eingesetzt.

- Eine geeignete Umzäunung des Betriebsgeländes.
- Fenster, Schächte und ähnliche Zugangsmöglichkeiten, die eine potentielle Zutrittsmöglichkeit bieten könnten (z. B. Fenster im Erdgeschoss) sind gegen den unberechtigten Zutritt gesichert.
- Nach den Betriebsstunden finden regelmäßige Kontrollgänge durch das Sicherheitspersonal statt.
- Der Zutritt ist durch ein manuelles Schließsystem gesichert.
- Der Zutritt ist durch ein elektronisches Schließsystem mit Sicherheitsschlössern gesichert.
- Der Zutritt ist durch ein manuelles Schließsystem mit Sicherheitsschlössern gesichert.
- Der Zutritt ist durch ein Chipkarten- oder Transponder-Schließsystem gesichert.
- Der Zutritt ist durch ein Schließsystem mit Codesperre (Zugangscode) gesichert.
- Die Ausgabe und Rückgabe von Schlüsseln und/ oder Zugangskarten wird protokolliert.
- Mitarbeiter werden verpflichtet, Geräte zu sperren oder sie besonders zu sichern, wenn sie ihre Arbeitsumgebung oder die Geräte verlassen.
- Unterlagen (Akten, Dokumente, etc.) werden sicher, z. B. in Aktenschränken oder sonstigen angemessen gesicherten Containern aufbewahrt und angemessen vor Zugriff durch unbefugte Personen gesichert.
- Datenträger werden sicher aufbewahrt und angemessen vor Zugriff durch unbefugte Personen gesichert.

Zugangskontrolle

- Ein Passwortkonzept legt fest, dass Passwörter eine dem Stand der Technik und den Anforderungen an Sicherheit entsprechende Mindestlänge und Komplexität haben müssen.
- Sämtliche Datenverarbeitungsanlagen sind passwortgeschützt.
- Passwörter werden grundsätzlich nicht im Klartext gespeichert und nur gehashed oder verschlüsselt übertragen.
- Es wird eine Passwort-Management-Software eingesetzt.
- Für den Zugang zu Daten des Auftraggebers wird eine Zwei-Faktor-Authentifizierung verwendet.
- Fehlversuche beim Login auf betriebsinterne Systeme werden auf eine angemessene Anzahl beschränkt (z.B. Sperrung von Logindaten).
- Zugangsdaten werden, wenn deren Benutzer das Unternehmen oder Organisation des Auftragsverarbeiters verlassen haben, gelöscht oder deaktiviert.
- Es werden Serversysteme und Dienste eingesetzt, die über Angriffserkennungssysteme ("Intrusion-Detection-Systeme") verfügen.
- Es werden Serversysteme und Dienste eingesetzt, die über Angriffsvermeidung- und Abwehrsysteme ("Intrusion-Protection-Systeme") verfügen.
- Es wird auf dem aktuellen Stand gehaltene Anti-Viren-Software eingesetzt.
- Einsatz von Hardware-Firewall(s).
- Einsatz von Software-Firewall(s).
- Backups werden verschlüsselt gespeichert.

Interne Zugriffskontrolle und Eingabekontrolle (Berechtigungen für Benutzerrechte auf Zugang zu und Änderung von Daten)

Es sind Maßnahmen zur Zugriffskontrolle ergriffen worden, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Ferner sind Maßnahmen zur Eingabekontrolle ergriffen worden, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert, entfernt oder sonst verarbeitet worden sind.

- Ein Rechte- und Rollenkonzept (Berechtigungskonzept) sorgt dafür, dass der Zugriff auf personenbezogenen Daten nur für einen nach Erforderlichkeitsmaßstäben ausgewählten Personenkreis und nur in dem erforderlichen Umfang möglich ist.
- Das Rechte- und Rollenkonzept (Berechtigungskonzept) wird regelmäßig, innerhalb einer angemessenen zeitlichen Frequenz sowie wenn ein Anlass es erfordert (z. B. Verstöße gegen die Zugriffsbeschränkungen), evaluiert und bei Bedarf aktualisiert.
- Die Zugriffe auf einzelne Dateien des Auftraggebers werden protokolliert.
- Die Eingabe, Veränderung und Löschung einzelner Daten des Auftraggebers wird protokolliert.
- Anmeldungen in den Datenverarbeitungsanlagen, bzw. Verarbeitungssystemen werden protokolliert.
- Die Protokoll-, bzw. Logdateien werden vor Veränderung sowie vor Verlust und gegen unberechtigten Zugriff geschützt.
- Die Tätigkeiten der Administratoren werden im Rahmen rechtlich zulässiger Möglichkeiten und im Rahmen technisch vertretbaren Aufwandes angemessen überwacht und protokolliert.
- Es wird sichergestellt, dass nachvollziehbar ist, welche Beschäftigten oder Beauftragten auf welche Daten wann Zugriff hatten (z.B. durch Protokollierung der Softwarenutzung oder Rückschluss aus den Zugriffszeiten und dem Berechtigungskonzept).
- Die im Rahmen des Auftrags verarbeiteten personenbezogenen Daten werden beim E-Mail-Versand auf Weisung des Auftraggebers ende-zu-ende-verschlüsselt übertragen.

Weitergabekontrolle

Es sind Maßnahmen zur Weitergabekontrolle ergriffen worden, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern 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.

- Beim Zugriff auf betriebsinterne Systeme von außen (z.B. bei Fernwartung), werden verschlüsselte Übertragungstechnologien verwendet (z.B. VPN).

- E-Mails werden während der Übertragung verschlüsselt, was bedeutet, dass die E-Mails auf dem Weg vom Absender zum Empfänger davor geschützt sind, von jemandem gelesen zu werden, der Zugang zu den Netzwerken hat, durch die die E-Mail gesendet wird.
- Die im Rahmen des Auftrags verarbeiteten personenbezogenen Daten werden, vorbehaltlich anderweitiger Weisungen des Auftraggebers, ende-zu-ende-verschlüsselt übertragen.
- Die Übermittlung und Verarbeitung von personenbezogenen Daten des Auftraggebers über Onlineangebote (Webseiten, Apps, etc.), erfolgt geschützt mittels einer TLS oder einer gleichwertig sicheren Verschlüsselung.

Auftragskontrolle, Zweckbindung und Trennungskontrolle

Es sind Maßnahmen zur Auftragskontrolle ergriffen worden, die sicherstellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden. Die Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten des Auftraggebers getrennt verarbeitet werden und keine Vermengung, Verschnitt oder sonstige dem Auftrag widersprechende gemeinsame Verarbeitung dieser Daten erfolgt.

- Sorgfältige Auswahl von Unterauftragsverarbeitern und sonstigen Dienstleistern.
- Der Auftragsverarbeiter darf keine weiteren Unterauftragsverarbeiter ohne Zustimmung oder ohne Information des Auftraggebers (dieser hat dann ein Widerspruchsrecht) aufnehmen.
- Mitarbeiter und Beauftragte werden verständlich und deutlich über die Weisungen des Auftraggebers und den zulässigen Verarbeitungsrahmen informiert und entsprechend instruiert. Eine gesonderte Information und Instruktion sind nicht erforderlich, wenn die Einhaltung des zulässigen Rahmens ohnehin, z. B. aufgrund anderweitiger Vereinbarungen oder betrieblicher Übung, verlässlich zu erwarten ist.
- Die Einhaltung von Weisungen des Auftraggebers und des zulässigen Rahmens der Verarbeitung der personenbezogenen Daten durch Mitarbeiter und Beauftragte wird in angemessenen Abständen überprüft.
- Die für die Verarbeitung der personenbezogenen Daten des Auftraggebers geltenden Löschfristen werden innerhalb des Löschkonzepts des Auftragsverarbeiters, sofern erforderlich gesondert, dokumentiert.
- Erforderliche Auswertungen und Analysen der Verarbeitung der personenbezogenen Daten des Auftraggebers werden, soweit möglich und zumutbar, anonymisiert verarbeitet (d. h. ohne jeglichen Personenbezug) oder zumindest entsprechend Art. 4 Nr. 5 DSGVO pseudonymisiert verarbeitet (d. h. in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können wobei diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden).
- Die personenbezogenen Daten des Auftraggebers werden von Daten anderer Verarbeitungsverfahren des Auftragsverarbeiters logisch getrennt verarbeitetet und vor unberechtigtem Zugriff oder Verbindung oder Verschneidung mit anderen Daten geschützt (z.B. in unterschiedlichen Datenbanken oder durch angemessene Attribute).

- Produktiv- und Testdaten werden streng getrennt voneinander in unterschiedlichen Systemen gespeichert. Die Produktivsysteme werden getrennt und unabhängig von den Entwicklungs- und Testsystemen betrieben.

Sicherung der Integrität und Verfügbarkeit von Daten sowie der Belastbarkeit von Verarbeitungssystemen

- Es werden ausfallsichere Serversysteme und Dienste eingesetzt, die doppelt, bzw. mehrfach ausgelegt sind.
- Die Verfügbarkeit der Datenverarbeitungssysteme wird permanent, insbesondere auf Verfügbarkeit, Fehler sowie Sicherheitsvorfälle überwacht und kontrolliert.
- Die personenbezogenen Daten werden bei externen Hosting-Anbietern gespeichert. Die Hosting-Anbieter werden sorgfältig ausgewählt und erfüllen die Vorgaben an den Stand der Technik, im Hinblick den Schutz vor Schäden durch Brand, Feuchtigkeit, Stromausfälle, Katastrophen, unerlaubte Zugriffe sowie an Datensicherung und Patchmanagement, als auch an die Gebäudesicherung.
- Die Verarbeitung von personenbezogenen Daten erfolgt auf Datenverarbeitungssystemen, die einem regelmäßigen und dokumentierten Patch-Management unterliegen, d. h. insbesondere regelmäßig aktualisiert werden.
- Die zur Verarbeitung eingesetzten Serversysteme und Dienste werden in angemessenen Abständen Belastbarkeitstests und Hardwaretests unterzogen.
- Die zur Verarbeitung eingesetzten Serversysteme verfügen über einen Schutz gegen Denial of Service (DoS) Angriffe.
- Die zur Verarbeitung eingesetzten Serversysteme verfügen über eine unterbrechungsfreie Stromversorgung (USV), die gegen Ausfälle angemessen gesichert ist und ein geregeltes Herunterfahren in Notfällen ohne Datenverlust sicherstellt.
- Videoüberwachung am Serverstandort.
- Einbruchs- und Kontaktmelder am Serverstandort.
- Die zur Verarbeitung eingesetzten Serversysteme verfügen über einen angemessenen Brandschutz (Feuer- und Rauchmeldeanlagen sowie entsprechende Feuerlöschvorrichtungen oder Feuerlöschgeräte).
- Es werden Serversysteme eingesetzt, die über einen Schutz vor Feuchtigkeitsschaden (z. B. Feuchtigkeitsmelder) verfügen.
- Es werden Serversysteme und Dienste eingesetzt, die ein Backupsystem an anderen Orten, auf dem die aktuellen Daten vorgehalten werden und so ein lauffähiges System auch im Katastrophenfall zur Verfügung stellen, bereithalten.
- Die Datensätze des Auftraggebers werden systemseitig vor versehentlicher Änderung oder Löschung geschützt (z.B. durch Zugriffsbeschränkungen, Sicherheitsabfragen und Backups).
- Es werden Serversysteme und Dienste eingesetzt, die über ein angemessenes, zuverlässiges und kontrolliertes Backup- & Wiederherstellungskonzept verfügen.
- Es werden regelmäßig in einem angemessenen Zeitabstand Wiederherstellungstests zur Überprüfung durchgeführt, dass die Datensicherungen tatsächlich wieder eingespielt werden können (Datenintegrität der Backups).

Anlage 3: Unterauftragsverarbeiter

Der Auftragsverarbeiter setzt die folgenden Unterauftragsverarbeiter im Rahmen der Verarbeitung von Daten für den Auftraggeber ein:

Firma, Anschrift	Art der Verarbeitung	Zweck	Art der Daten	Kategorien der betroffenen Personen
NinjaOne (NinjaRMM GmbH), Alexanderstraße 1 10178 Berlin	Verarbeitung zum Zwecke der Erfüllung der Dienstleistungen für den Auftraggeber	Erbringung der Auftragsnehmer Dienstleistungen	IP-Adresse(n), Benutzernamen, Systemnamen für Geräte, Hardware-Details der Geräte, Softwaredetails von Geräten, Browser-/Benutzeragenten-Details, Leistungs- und Auslastungsmetriken von Geräten, Fehlercodes von Geräten	Kunden und Interessenten des Auftraggebers & Mitarbeiter des Auftraggebers
Microsoft Ireland Operations, Ltd., One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland	E-Mail-Versand, Online-Meetings	Kommunikation	Personenstammdaten, Kommunikationsdaten, Protokolldaten	Kunden und Interessenten des Auftraggebers & Mitarbeiter und Lieferanten des Auftraggebers
Hetzner Online GmbH, Gunzenhausen	Hosting	Webhosting	Personenstammdaten, Kommunikationsdaten, Protokolldaten	Kunden und Interessenten des Auftraggebers & Mitarbeiter und Lieferanten des Auftraggebers
Halo Service Solutions Limited, 86 Eastburn Tower Eastburn Drive, Falkirk, United Kingdom, FK1 1TX	Servicedesk und Kundenverwaltung	Kommunikation & Erbringung der Auftragsnehmer Dienstleistungen	Personenstammdaten, Kommunikationsdaten, Protokolldaten	Kunden und Interessenten des Auftraggebers & Mitarbeiter und Lieferanten des Auftraggebers