Anlage2) nuwacom Auftragsverarbeitungsvertrag
(Stand: 01.05.2025)

1. Präambel

Dieser Auftragsverarbeitungsvertrag regelt die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Auftraggebers und ist Bestandteil des zwischen dem Auftragsverarbeiter und dem Auftraggeber geschlossenen Hauptvertrages. Im Falle eines Widerspruchs zwischen der anwendbaren Vereinbarung und dem Auftragsverarbeitungsvertrag ist der Auftragsverarbeitungsvertrag maßgeblich.

2. Definitionen

Aufsichtsbehörde: Eine unabhängige Behörde, zuständig für die Überwachung der Anwendung des Datenschutzrechts.

Anwendbares Recht zum Schutz der Privatsphäre: Bezieht sich auf die europäische Datenschutzgrundverordnung 2016/679 (DSGVO), sowie das Datenschutzgesetz (BDSG).

Personenbezogene Daten: Informationen, die sich auf eine direkt oder indirekt identifizierbare natürliche Person beziehen.

Unterauftragsverarbeiter: Ein vom Auftragsverarbeiter oder ihren verbundenen Unternehmen beauftragter Auftragsverarbeiter zur Unterstützung bei der Erfüllung ihrer Verpflichtungen. Zu den Unterauftragsverarbeitern können auch Dritte oder verbundene Unternehmen des Auftragsverarbeiters gehören.

Verbundenes Unternehmen: Jede juristische Person, die entweder die Kontrolle über den Auftragsverarbeiter ausübt, von dem Auftragsverarbeiter kontrolliert wird, oder die unter gemeinsamer Kontrolle mit dem Auftragsverarbeiter steht. „Kontrolle“ in diesem Zusammenhang bedeutet den direkten oder indirekten Besitz von mehr als 50% der stimmberechtigten Anteile einer juristischen Person oder die Fähigkeit, auf andere Weise maßgeblichen Einfluss auf die Geschäftspolitik oder die Entscheidungen der juristischen Person auszuüben.

Verletzung des Schutzes Personenbezogener Daten: Eine Sicherheitsverletzung, die zu unbeabsichtigter oder unrechtmäßiger Zerstörung, Verlust, Veränderung, unbefugter Offenlegung oder unbefugtem Zugang zu personenbezogenen Daten führt, die vom (Unter-)Auftragsverarbeiter übermittelt, gespeichert oder verarbeitet wurden.

Weisungen: Schriftliche Anweisungen des Auftraggebers an den Auftragsverarbeiter für die Verarbeitung personenbezogener Daten, die vorgeben wie personenbezogene Daten zu verarbeiten sind, einschließlich der Übertragung, Art der Verarbeitung, der Dauer, des Zwecks, der Art der personenbezogenen Daten und der Kategorien betroffener Personen. Weisungen müssen im Einklang mit den geltenden Datenschutzgesetzen, insbesondere der DSGVO, stehen und schriftlich oder in einem dokumentierten elektronischen Format erteilt werden. Änderungen oder Ergänzungen dieser Weisungen bedürfen ebenfalls einer dokumentierten Form.

Verantwortlicher, betroffene Person, Auftragsverarbeiter, Verarbeitung: Begriffe mit den Bedeutungen gemäß der DSGVO.

3. Anwendungsbereich, Gegenstand, Zweck und Dauer der Verarbeitung

3.1 Die Vereinbarung findet Anwendung auf die Erhebung, Verarbeitung und Löschung aller personenbezogener Daten, die Gegenstand der Leistungsvereinbarung sind oder im Rahmen von deren Durchführung anfallen oder dem Auftragsverarbeiter bekannt werden.

3.2 Gegenstand und Dauer der Auftragsverarbeitung sowie Umfang, Art und Zweck der vorgesehenen Verarbeitung von Daten bestimmen sich nach der Leistungsvereinbarung.

3.3 Folgende Datenarten oder -kategorien sind Gegenstand der Verarbeitung durch den Auftragsverarbeiter:

- Berufliche Kontakt-, bzw. Profildaten (z.B. Vor- und Nachname, E-Mail-Adresse, Position, Abteilung, Standort, sowie weitere erforderliche oder freiwillige Profilinformationen)
- Anmeldedaten (E-Mail-Adresse, Passwort oder per SSO-Verfahren vom Auftraggeber übertragene Daten (Claims)))
- Inhalte (weitere personenbezogene Daten, die von Nutzern des Auftraggebers an den Auftragsverarbeiter übermittelt werden oder in Auftraggeber-Daten enthalten sind)
- Nutzungsdaten (z.B. IP-Adresse, Geräteeigenschaften, Zugriffszeiten, User-ID)

3.4 Kategorien betroffener Personen:

- Mitarbeiter des Auftraggebers
- Dritte, die vom Auftraggeber autorisiert wurden (z.B. verbundene Unternehmen, Dienstleister, Berater oder Agenturen) oder deren Daten in Inhalten vorhanden sind.

4. Verantwortlichkeit und Weisungsbefugnis

4.1 Die Vertragsparteien stellen die Einhaltung der datenschutzrechtlichen Bestimmungen sicher. Die Parteien verstehen und vereinbaren, dass in Bezug auf die Verarbeitung personenbezogener Daten der Auftraggeber der Verantwortliche und der Auftragnehmer der Auftragsverarbeiter ist. Der Verantwortliche kann jederzeit die Herausgabe, Berichtigung, Anpassung, Löschung und Einschränkung der Verarbeitung der Daten verlangen.

4.2 Zur Gewährleistung des Schutzes der Rechte der betroffenen Personen unterstützt der Auftragsverarbeiter den Verantwortlichen angemessen, insbesondere durch die Gewährleistung geeigneter technischer und organisatorischer Maßnahmen.

4.3 Soweit sich eine betroffene Person zwecks Geltendmachung eines Betroffenenrechts unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

4.4 Der Auftragsverarbeiter darf Daten ausschließlich im Rahmen der Weisungen des Verantwortlichen verarbeiten, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder des Mitgliedstaates, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

4.5 Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie von Seiten des Verantwortlichen bestätigt oder geändert wird. Die weisungsberechtigten Personen auf Seiten des Verantwortlichen sowie die zum Empfang der Weisungen berechtigten Personen auf Seiten des Auftragsverarbeiters sowie die vorgesehenen Informationswege sind in **Anlage 1: Liste der weisungsbefugten Personen** festgelegt. Sind keine weisungsbefugten Personen in Anlage 1 hinterlegt, wird der Zeichner der Orderform als weisungsbefugte Person bestimmt.

4.6 Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder die betroffene Person darf der Auftragsverarbeiter nur nach vorheriger ausdrücklicher schriftlicher Zustimmung durch den Verantwortlichen erteilen. Der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Außerhalb notwendiger Sicherheitskopien (Backups) werden Kopien und Duplikate ohne Wissen des Verantwortlichen nicht erstellt.

4.7 Der Verantwortliche führt das Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 DSGVO. Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Wunsch Informationen zur Aufnahme in das Verzeichnis zur Verfügung. Der Auftragsverarbeiter führt entsprechend den Vorgaben des Art. 30 Abs. 2 DSGVO ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.

4.8 Die Verarbeitung der Daten im Auftrag des Verantwortlichen findet ausschließlich auf dem Gebiet der der Europäischen Union statt. Eine Verarbeitung in einem Staat außerhalb des in Satz 1 genannten Territoriums ist nur zulässig wenn sichergestellt ist, dass unter Berücksichtigung der Voraussetzungen des Kapitels V der DSGVO das durch die DSGVO gewährleistete Schutzniveau nicht unterlaufen wird und bedarf der vorherigen Zustimmung des Verantwortlichen. Die Zustimmung gilt als erteilt, wenn der Auftragsverarbeiter den Verantwortlichen vorab mit einer Frist von 8 Wochen über die Maßnahme informiert und der Verantwortliche nicht innerhalb dieser Frist aus wichtigem Grunde widerspricht. Im Falle des Widerspruchs kann der Auftragsverarbeiter das Vertragsverhältnis mit einer Frist von 3 Monaten kündigen. Die grundlegenden Voraussetzungen für die Rechtmäßigkeit der Verarbeitung bleiben unberührt.

4.9 Der Auftragsverarbeiter stellt sicher, dass ihm unterstellte natürliche Personen, die Zugang zu Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten. Der Verantwortliche erteilt dem Auftragsverarbeiter anhand der in **Anlage 3: Technische und organisatorische Maßnahmen** festgestellten Verarbeitungssituation, die Zustimmung zur Verarbeitung von Daten außerhalb der Betriebsräume des Auftragsverarbeiters (z.B. Home Office, mobiles Arbeiten).

5. Beachtung zwingender gesetzlicher Pflichten durch den Auftragsverarbeiter

5.1 Der Auftragsverarbeiter stellt sicher, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und weist dies dem Verantwortlichen auf Wunsch nach. Dies umfasst auch die Belehrung über die in diesem Auftragsverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung.

5.2 Die Vertragsparteien unterstützen sich gegenseitig beim Nachweis und der Dokumentation der ihnen obliegenden Rechenschaftspflicht im Hinblick auf die Grundsätze ordnungsgemäßer Datenverarbeitung einschließlich der Umsetzung der notwendigen technischen und organisatorischen Maßnahmen (Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO). Der Auftragsverarbeiter stellt dem Verantwortlichen hierzu bei Bedarf entsprechende Informationen zur Verfügung.

5.3 Der Auftragsverarbeiter hat einen Datenschutzbeauftragten zu benennen, der seine Tätigkeit entsprechend den gesetzlichen Vorschriften ausübt. Die Kontaktdaten des Datenschutzbeauftragten sind heyData GmbH, Schützenstr. 5, 10117 Berlin, datenschutz@heydata.eu.

5.4 Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde im Rahmen ihrer Zuständigkeit bei dem Auftragsverarbeiter anfragt, ermittelt oder sonstige Erkundigungen einzieht, insofern Daten des Verantwortlichen von dieser Maßnahme betroffen sind.

6. Sicherstellung der technischen und organisatorischen Maßnahmen

6.1 Die Vertragsparteien vereinbaren die in der **Anlage 3: Technische und organisatorische Maßnahmen** zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen. Der Anhang ist Gegenstand dieser Vereinbarung.

6.2 Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in der **Anlage 3: Technische und organisatorische Maßnahmen** festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

6.3 Der Auftragsverarbeiter wird dem Verantwortlichen alle erforderlichen Informationen zur Verfügung stellen, die zum Nachweis der Einhaltung der in dieser Vereinbarung getroffenen und der gesetzlichen Vorgaben erforderlich sind. Er wird insbesondere Überprüfungen/Inspektionen, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und deren Durchführung unterstützen. Der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann dabei auch durch Vorlage eines aktuellen Testats, von Berichten hinreichend qualifizierter und unabhängiger Instanzen (z.B. Wirtschaftsprüfer, unabhängige Datenschutzauditoren), durch die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO, einer Zertifizierung nach Art. 42 DSGVO oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz, ISO 27001) erbracht werden. Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen über den Ausschluss von genehmigten Verhaltensregeln gemäß Art. 41 Abs. 4 DSGVO, den Widerruf einer Zertifizierung gemäß Art. 42 Abs. 7 und jede andere Form der Aufhebung oder wesentlichen Änderung der vorgenannten Nachweise unverzüglich zu unterrichten.

6.4 Der Verantwortliche kann sich mit einer Frist von 2 Wochen angekündigt zu Prüfzwecken in den Betriebsstätten des Auftragsverarbeiters zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der gesetzlichen Vorgaben oder der zur Durchführung dieses Vertrages erforderlichen technischen und organisatorischen Erfordernisse überzeugen. Die Pflicht zur fristgerechten Ankündigung entfällt bei Vorliegen eines wichtigen Grundes, der eine unmittelbare Überprüfung erforderlich macht.

6.5 Der Auftragsverarbeiter stellt dem Verantwortlichen darüber hinaus alle erforderlichen Informationen zur Verfügung, die er für die Prüfungen nach Absatz 4 sowie für eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz der Daten (Datenschutz-Folgenabschätzung i.S.d. Art. 35 DSGVO) benötigt.

6.6 Der Auftragsverarbeiter hat im Benehmen mit dem Verantwortlichen alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Stands der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

6.7 Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen im Rahmen einer vorherigen Konsultation i.S.d. Art. 36 DSGVO.

6.8 Eine Weitergabe personenbezogener Daten in ein Drittland (außerhalb des EWR) darf unter den Voraussetzungen der Art. 44 ff. DSGVO stattfinden.

7. Mitteilung von Verstößen durch den Auftragsverarbeiter

Der Auftragsverarbeiter unterrichtet den Verantwortlichen bezüglich der Verarbeitung der Daten des Verantwortlichen umgehend bei schwerwiegenden Störungen seines Betriebsablaufes, bei Verdacht auf Verstöße gegen diese Vereinbarung sowie gesetzliche Datenschutzbestimmungen, bei Verstößen gegen solche Bestimmungen oder anderen Unregelmäßigkeiten. Dies gilt insbesondere im Hinblick auf die Meldepflicht nach Art. 33 Abs. 2 DSGVO sowie auf korrespondierende Pflichten des Verantwortlichen nach Art. 33 und Art. 34 DSGVO. Der Auftragsverarbeiter sichert zu, den Verantwortlichen erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen. Meldungen nach Art. 33 oder 34 DSGVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung gem. Abschnitt 4 dieses Vertrages durchführen.

8. Löschung und Rückgabe von Daten

8.1 Überlassene Datenträger und Datensätze verbleiben im Eigentum des Verantwortlichen.

8.2 Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch den Verantwortlichen, jedoch spätestens mit Beendigung der Leistungsvereinbarung, hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigte Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen datenschutzgerecht zu vernichten. Ein Löschungsprotokoll ist dem Verantwortlichen auf Anforderung vorzulegen. Die Rückgabe von Datenbeständen erfolgt durch bereitgestellte Exportschnittstellen, die es dem Verantwortlichen ermöglichen die Daten entsprechend zu sichern. Der Verantwortliche stellt sicher bei Bedarf die Datensätze vor Ende des Leistungszeitraums zu sichern, da ein späterer Zugriff aufgrund implementierter automatisierter Löschprozesse nicht mehr möglich ist. Sicherungskopien (Backups) werden spätestens nach 90 Tagen nach Beendigung der Leistungsvereinbarung datenschutzgerecht vernichtet.

8.3 Der Auftragsverarbeiter kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen bis zu deren Ende auch über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben. Für die nach Satz 1 aufbewahrten Daten gelten nach Ende der Aufbewahrungsfrist die Pflichten nach Absatz 2.

9. Unterauftragnehmer

9.1 Der Auftragsverarbeiter darf weitere Auftragsverarbeiter (Subunternehmen) in Anspruch nehmen. Die grundlegenden Voraussetzungen für die Rechtmäßigkeit der Verarbeitung bleiben unberührt. Die zur Erfüllung dieses Vertrages hinzugezogenen Subunternehmen sind in der **Anlage 2: Liste der Unterauftragnehmer** im Einzelnen bezeichnet. Mit deren Beauftragung erklärt sich der Verantwortliche einverstanden. Da es sich um eine allgemeine schriftliche Genehmigung handelt, informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, jedoch mindestens mit einer Frist von 4 Wochen vor der beabsichtigten Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subunternehmen. Der Verantwortliche kann derartigen Änderungen aus wichtigem Grunde innerhalb dieser Frist widersprechen. Im Falle des Widerspruchs kann der Auftragsverarbeiter das Vertragsverhältnis mit einer Frist von 3 Monaten kündigen. Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise

Telekommunikationsdienstleistungen. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

9.2 Wenn Subunternehmen durch den Auftragsverarbeiter eingeschaltet werden, hat der Auftragsverarbeiter sicherzustellen, dass seine vertraglichen Vereinbarungen mit dem Subunternehmen so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter entspricht und alle vertraglichen und gesetzlichen Vorgaben beachtet werden; dies gilt insbesondere auch im Hinblick auf den Einsatz geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus der Verarbeitung.

9.3 Der Verantwortlichen ist berechtigt, auf schriftliche Anforderung vom Auftragsverarbeiter Auskunft über den Inhalt des mit dem Subunternehmen geschlossenen Vertrages bezüglich der darin enthaltene Umsetzung der datenschutzrelevanten Verpflichtungen des Subunternehmens zu erhalten.

9.4 Kommt das Subunternehmen seinen datenschutzrechtlichen Verpflichtungen nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Subunternehmens. Der Auftragsverarbeiter hat in diesem Falle auf Verlangen des Verantwortlichen die Beschäftigung des Subunternehmens ganz oder teilweise zu beenden oder das Vertragsverhältnis mit dem Subunternehmen zu lösen, wenn und soweit dies nicht unverhältnismäßig ist.

10. Schlussbestimmungen

10.1 Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile bedürfen einer Vereinbarung in gleicher Form und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

10.2 Verlangt diese Vereinbarung die Schriftform, so wird dieses Erfordernis durch elektronische Formate erfüllt.

10.3 Auf den Vertrag ist das Recht der Bundesrepublik Deutschland anzuwenden. Die Sprache des
Verfahrens ist Deutsch. Der Gerichtsstand ist Koblenz.

10.4 Jegliches Zurückbehaltungsrecht des Auftragsverarbeiters hinsichtlich der im Auftrag verarbeiteter personenbezogener Daten und der dazugehörigen Datenträger, sofern sie sich im Eigentum des Verantwortlichen befinden, ist ausgeschlossen.

10.5 Sollten einzelne Regelungen dieser Vereinbarung unwirksam oder undurchführbar sein, wird davon die Wirksamkeit der übrigen Regelungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt diejenige wirksame und durchführbare Regelung, deren Wirkungen der Zielsetzung am nächsten kommt, die die Vertragsparteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.

Anlage 1: Liste der weisungsbefugten Personen

1. **Weisungsbefugte Personen des Auftraggebers**

   Name: [Vollständiger Name]
   - Position: [Position im Unternehmen]
   - Kontaktdetails: [E-Mail-Adresse, Telefonnummer]

   Name: [Vollständiger Name]
   - Position: [Position im Unternehmen]
   - Kontaktdetails: [E-Mail-Adresse, Telefonnummer]

   (Weitere Personen können hier aufgelistet werden.)

2. **Autorisierte Personen des Auftragsverarbeiters (nuwacom GmbH)**

Namentlich

Name: Sascha Böhr
- Position: CEO nuwacom GmbH
- Kontaktdetails: sascha.boehr@nuwacom.ai

Name: Alexander Kleinen
- Position: CTO nuwacom GmbH
- Kontaktdetails: alexander.kleinen@nuwacom.ai

Funktional
- Der Accountmanager des Auftraggebers
- Mitarbeiter der Abteilung Customer Success
- Mitarbeiter der Abteilung Kundensupport

Über ihre im Rahmen der Kundenbetreuung bekanntgemachten jeweiligen persönlichen E-Mail-Adressen oder entsprechende Sammel-E-Mail-Adressen.

Änderungen der weisungsbefugten Personen sind schriftlich sowie von den weisungsbefugten Personen zu benennen.

Anlage 2: Liste der Unterauftragnehmer

Firma, Anschrift	Auftragsinhalt	Umfang der Datenverarbeitung, Serverstandort
Microsoft Ireland Operations, Ltd. **One Microsoft Place** **South County Business Park** **Leopardstown** Dublin 18, D18 P521, Ireland	Bereitstellung der Azure Cloud Infrastruktur	Hosting Partner: Verarbeitet alle personenbezogenen Daten, die der Auftragsverarbeiter für den Auftraggeber verarbeitet. Serverstandort ist EU.
Intercom R&D Unlimited Company 2nd Floor, Stephen Court, 18-21 St. Stephen's Green, Dublin 2, Irland	Customer support	Dienstleister für Customer Support Software-Anwendung. Serverstandort ist USA.
Amazon Web Services EMEA Sàrl, Avenue John F. Kennedy 38, 1855 Luxemburg *	Hosting der LLMs	Hosting Partner: Verarbeitet alle personenbezogenen Daten, die der Auftragsverarbeiter für den Auftraggeber verarbeitet. Serverstandort ist EU.
Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Dublin, Irland *	Hosting der LLMs	Hosting Partner: Verarbeitet alle personenbezogenen Daten, die der Auftragsverarbeiter für den Auftraggeber verarbeitet. Serverstandort ist EU.
Mixpanel Inc., **One Front Street, Floor 28, San Francisco, CA 94111, USA**	Produktanalyse	Dienstleister für Fehlerbehebung, Optimierung & Verbesserung. Serverstandort ist EU
AlphaAI Technologies Inc. **315 W 36th St, New York, NY 10018, USA**	Websuche	Dienstleister für Websuche Serverstandort is USA.

* Hinweis: Der Auftraggeber hat die Möglichkeit, bei Bedarf, einzelne LLMs in der Software nuwacom ausblenden bzw. deaktivieren zu lassen.

Anlage 3: Technische und organisatorische Maßnahmen

1. **Zutrittskontrolle**
   Maßnahmen, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, verwehren:

   - Die Anwendung wird in ISO 27001, ISO 27018 & SOC2-zertifizierten Datenzentren gehostet. Der Zutritt ist durch ein personalisiertes Zutrittskontrollsystem stark eingeschränkt
   - Büroräume des Auftragsverarbeiters sind gesichert und der Zugang auf Mitarbeiter, sowie autorisierte Dienstleister (z.B. Reinigungsdienste) mittels personalisierter Chipkarten beschränkt.
   - Gäste werden an der Tür begrüßt und zur Kontaktperson begleitet. Die Ausgabe und Rückgabe der Zugangsmedien wird schriftlich dokumentiert.
   - Arbeit im Homeoffice: Unbefugte haben kein Zutritt zur Wohnstätte der Mitarbeiter.
   - Arbeit im Homeoffice: Anweisung an Mitarbeiter, wenn möglich, in von Wohnräumen abgetrennten Arbeitszimmer zu arbeiten.

2. **Zugangskontrolle**
   Maßnahmen die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

   - Der Zugang zu Datenverarbeitungssystemen ist auf autorisierte Personen beschränkt und erfordert eine Identifizierung und erfolgreiche Authentifizierung durch Benutzername und Passwort unter Verwendung modernster Sicherheitsmaßnahmen (z.B. MFA).
   - Die Datenverarbeitungssystemen zugrundeliegende Datenträger verwenden dem Stand der Technik entsprechende Verschlüsselungsverfahren.
   - Zugänge werden persönlich und namensscharf ausgestellt, es werden keine Sammelkonten verwendet.
   - Es werden Firewalls eingesetzt.
   - Verwendung von Gehäuseverriegelungen.
   - Verschlüsselung von Datenträgern, Smartphones und Notebooks / Tablets.

3. **Zugriffskontrolle**
   Maßnahmen 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:

   - Der Zugriff auf Daten des Auftraggebers ist durch ein strenges Berechtigungskonzept eingeschränkt und sowohl organisatorisch, als auch technisch implementiert (Role Based Access Control Management). Die Vergabe von Berechtigungen wird protokolliert und mindestens jährlich überprüft.
   - Zugriffe werden protokolliert und überwacht. Protokolle werden stichprobenartig manuell, bzw. soweit vorhanden automatisch auf Anomalien ausgewertet.
   - Vernichtung von Datenträgern mindestens nach DIN 66399.
   - Anzahl der Administratoren ist so klein wie möglich gehalten.
   - Sichere Aufbewahrung von Datenträgern.
   - Verwaltung der Benutzerrechte durch Systemadministratoren.

4. **Weitergabekontrolle**
   Maßnahmen die 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:

   - Die Übertragung von Daten erfolgt grundsätzlich verschlüsselt (z.B. HTTPS mittels TLS 1.2, TLS 1.3). Mobile Datenträger sind verschlüsselt.
   - Integritätsprüfungen stellen sicher, dass Daten vollständig und nicht korrupt übertragen werden.
   - Elektronische Verschlüsselungs- und Signaturverfahren sind nach dem Stand der Technik implementiert (z.B. A+ Rating, regelmäßige Überprüfung auf weak ciphers)

5. **Eingabekontrolle**
   Maßnahmen die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

   - Datenverarbeitungssysteme setzen Audit Logs ein, um revisionssicher die Nachvollziehbarkeit von Änderungen an Datensätzen sicherzustellen
   - Manuelle oder automatische Kontrolle der Protokolle
   - Erstellen einer Übersicht, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können
   - Nachvollziehbarkeit der 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

6. **Auftragskontrolle**
   Maßnahmen die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können:

   - Der Auftragsverarbeiter hat für die Verarbeitung von personenbezogenen Daten entsprechende Prozesse und Arbeitsabläufe definiert. Die Kontrolle der Umsetzung wird regelmäßig durch den internen Datenschutzkoordinator, sowie durch den externen Datenschutzbeauftragten sichergestellt.
   - Mitarbeiter erhalten jährlich eine Schulung zum Thema Sicherheits- und Datenschutzbewusstsein. Die Teilnahme wird durch entsprechende Dokumentationen nachgewiesen.
   - Personen, die seitens des Auftragsverarbeiters befugt sind Weisungen entgegenzunehmen und auszuführen, sind in **Anlage Liste der weisungsbefugten Personen** verbindlich definiert.
   - Schriftliche Weisungen an den Auftragnehmer oder Weisungen in Textform (z.B. durch Auftragsverarbeitungsvertrag)
   - Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags, z.B. durch Anfrage entsprechender Bestätigungen
   - Bestätigung von Auftragnehmern, dass sie ihre eigenen Mitarbeiter auf das Datengeheimnis verpflichten (typischerweise im Auftragsverarbeitungsvertrag)
   - Sorgfältige Auswahl von Auftragnehmern (insbesondere hinsichtlich Datensicherheit)
   - Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags, z.B. durch Anfrage entsprechender Bestätigungen

7. **Verfügbarkeitskontrolle**
   Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

   - Es werden hochmoderne und bewährte Dienstleister eingesetzt, die bei der Leistungserbringung unterstützen. Dazu zählt insbesondere der Einsatz redundanter Rechenzentren, sowie deren eigene Schutzkonzepte.
   - Tägliche Backups mit einer Aufbewahrungsdauer von mindestens 30 und höchstens 90 Tagen stehen für Wiederherstellungsverfahren zur Verfügung. Erzeugte Backup-Versionen werden auf Integrität geprüft und die Eignung zur Wiederherstellung durch regelmäßige backup & restore Tests sichergestellt.
   - Die Anwendung ist horizontal skaliert um failover Prozesse sicherzustellen.
   - Feuerlöschgeräte in Serverräumen
   - Feuer- und Rauchmeldeanlagen
   - Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
   - Klimaanlage in Serverräumen
   - Schutzsteckdosenleisten in Serverräume
   - Unterbrechungsfreie Stromversorgung (USV)
   - RAID-System / Festplattenspiegelung
   - Videoüberwachung in Serverräumen
   - Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
   - Erstellung eines Backup- & Recoverykonzepts
   - Kontrolle des Sicherungsvorgangs
   - Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
   - Erstellen eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)
   - Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
   - Keine sanitären Anlagen im oder oberhalb des Serverraums
   - Trennung von Betriebssystemen und Daten

8. **Trennungskontrolle**
   Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

   - Test-, Staging- und Produktivsysteme sind voneinander getrennt.
   - Die dem Auftraggeber zur Verfügung gestellte Anwendung ist als eigener Tenant ausgelegt und ist von anderen Kunden separiert.
   - Innerhalb der Anwendung steht dem Auftraggeber eine Berechtigungsverwaltung zur Verfügung, welche durch row level security Datensätze logisch voneinander trennt.

9. **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung**
   - Verwendung der heyData-Plattform zum Datenschutz-Management
   - Bestellung des Datenschutzbeauftragten heyData
   - Verpflichtung der Mitarbeiter auf das Datengeheimnis
   - Regelmäßige Schulungen der Mitarbeiter im Datenschutz
   - Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO)
   - Durchführung jährlicher Datenschutz-Audits inkl. Prüfung der TOMs