Neurapix

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen

dem **Verantwortlichen**

im Folgenden: **Auftraggeber**

und

der **neurapix UG (haftungsbeschränkt)**, Am Feuerschanzengraben 10, 37083 Göttingen

- Auftragsverarbeiter – im Folgenden: **Auftragnehmer**

1. Gegenstand und Dauer des Vertrags

(1) Gegenstand

Dieser Vertrag regelt den Umgang des Auftragnehmers mit den ihm vom Auftraggeber zur Verfügung gestellten Bilddateien. Näheres ergibt sich aus der zwischen den Parteien geschlossenen Leistungsvereinbarung, auf die hier verwiesen wird (im Folgenden: Leistungsvereinbarung).

(2) Dauer

(a) Die Dauer dieses Vertrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

(b) Der Vertrag gilt unbeschadet des vorstehenden Absatzes so lange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet (einschließlich Backups).

(c) Soweit sich aus anderen Vereinbarungen zwischen Auftraggeber und Auftragnehmer anderweitige Abreden zum Schutz personenbezogener Daten ergeben, soll dieser Vertrag zur Auftragsverarbeitung vorrangig gelten, es sei denn die Parteien vereinbaren ausdrücklich etwas anderes.

Neurapix

2. Konkretisierung des Vertragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Der Auftraggeber stellt dem Auftragnehmer von ihm aufgenommene und bearbeitete Fotoaufnahmen zur Verfügung, auf denen überwiegend Personen abgebildet sind. Bei diesen Fotoaufnahmen könnte es sich um personenbezogene Daten handeln. Der Auftraggeber verwendet die ihm überlassenen Fotoaufnahmen zum einen, um mittels künstlicher Intelligenz neuronale Netze (im Folgenden: KI-Assistenten) zu trainieren, die sodann zum Zwecke der Bearbeitung von unbearbeiteten Fotoaufnahmen von dem Auftraggeber und nach Absprache ggf. auch von anderen Fotografen genutzt werden können. Darüber hinaus übersendet der Auftraggeber dem Auftragnehmer unbearbeitete Fotoaufnahmen, die sodann mittels der KI-Assistenten bearbeitet und an ihn zurückübersandt werden.

(2) Art der Daten

Die überlassenen Fotoaufnahmen können persönliche Daten der dort abgebildeten Personen enthalten (z.B. Aufenthaltsort der abgebildeten Personen zu einem bestimmten Zeitpunkt, Tätigkeit der abgebildeten Person zu einem bestimmten Zeitpunkt).

(3) Kategorien betroffener Personen

Bei den durch die Verarbeitung betroffenen Personen handelt es sich um Kunden des Auftraggebers sowie Gäste der von den Kunden abgehaltenen Veranstaltungen.

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer ergreift in seinem Verantwortungsbereich alle erforderlichen technisch-organisatorische Maßnahmen gem. Art. 32 DS-GVO zum Schutz der personenbezogenen Daten und übergibt dem Auftraggeber die Dokumentation zur Prüfung [Anlage 1]. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Vertrags.

(2) Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(3) Die vereinbarten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer zukünftig gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Über wesentliche Änderungen, die durch den Auftragnehmer zu dokumentieren sind, ist der Auftraggeber unverzüglich in Kenntnis zu setzten.

4. Rechte von betroffenen Personen

(1) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren, berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind die Rechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung sowie Datenportabilität nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat, zusätzlich zu der Einhaltung der Regelungen dieses Vertrags, eigene gesetzliche Pflichten gemäß der DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die berechtigterweise Zugang zu

personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

b) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

c) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Vertrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

d) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten, einem anderen Anspruch oder einem Informationsersuchen im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

e) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

f) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Vertrags.

g) Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere nach Artt. 33, 34 DS-GVO nachkommen kann. Er fertigt über den gesamten Vorgang eine Dokumentation an, die er dem Auftraggeber für weitere Maßnahmen zur Verfügung stellt.

h) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber

Neurapix

Aufsichtsbehörden und Betroffenen und stellt ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung.

i) Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, unterstützt ihn der Auftragnehmer unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.

(2) Dieser Vertrag entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DS-GVO.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Die Auslagerung auf Unterauftragnehmer oder der Wechsel der gemäß Anhang 2 bestehenden Unterauftragnehmer sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber in einer angemessenen Zeit, die 14 Tage nicht unterschreiten darf, vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und

- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Die Einhaltung und Umsetzung der technisch-organisatorischen Maßnahmen beim Unterauftragnehmer wird unter Berücksichtigung des Risikos beim Unterauftragnehmer vorab der Verarbeitung personenbezogener Daten und sodann regelmäßig durch den Auftragnehmer kontrolliert. Der Auftragnehmer stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung. Der Auftragnehmer stellt ferner sicher, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Kontrollrechte) auch direkt gegenüber den Unterauftragnehmern wahrnehmen kann.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform). Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Internationale Datentransfers

(1) Jede Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation bedarf einer dokumentierten Weisung des Auftraggebers und bedarf der Einhaltung der Vorgaben zur Übermittlung personenbezogener Daten in Drittländer nach Kapitel V der DS-GVO.

Der Auftraggeber gestattet eine Datenübermittlung in ein Drittland. In der Anlage 2 werden die Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus aus Art. 44 ff. DS-GVO im Rahmen der Unterbeauftragung spezifiziert.

(2) Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DS-GVO verantwortlich.

Neurapix

8. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb während der üblichen Geschäftszeiten zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis der technisch-organisatorischen Maßnahmen zur Einhaltung der besonderen Anforderungen des Datenschutzes allgemein sowie solche, die den Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Soweit der Auftraggeber Kontrollrechte nach dieser Ziffer ausüben möchte, steht dem Auftragnehmer hierfür ein Entgelt zu. Die Höhe dieses Entgelts ist vorab zu vereinbaren und orientiert sich an einem festzulegenden Stundensatz des für die Betreuung vom Auftragnehmer abgestellten Mitarbeiters.

Neurapix

9. Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf Basis dokumentierter Weisungen des Auftraggebers, es sei denn er ist nach dem Recht des Mitgliedstaats oder nach Unionsrecht zu einer Verarbeitung verpflichtet. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Die anfänglichen Weisungen des Auftraggebers werden durch diesen Vertrag festgelegt.

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(3) Erteilt der Auftraggeber dem Auftragnehmer Weisungen nach dieser Ziffer, so hat er durch diese Weisung entstehende Kosten zu erstatten.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der 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 erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens aber mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

Neurapix

Anlage 1 - Technisch-organisatorische Maßnahmen

Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten:

- Sämtliche Datenübertragungen zwischen Endgeräten des Auftraggebers und des Auftragnehmers erfolgen unter Einsatz einer https/SSL- Verschlüsselung
- Sämtliche auf Festplatten des Auftragnehmers gespeicherte Daten werden mit einem angemessenen Standardverfahren nach dem Stand der Technik und des eingesetzten Betriebssystems verschlüsselt

Maßnahmen zur Gewährleistung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung:

- Regelmäßige Unterweisung der Mitarbeiter über datenschutzrechtliche Entwicklungen, Verfahrensanweisungen und Benutzerrichtlinien
- Regelmäßige Datenschutzaudits durch externe Rechtsanwaltskanzlei

Maßnahmen zur Identifizierung und Authentifizierung von Nutzern:

- Bei der Datenübermittlung über sämtliche vom Auftragnehmer zur Verfügung gestellten Kanäle findet eine Authentifizierung durch Eingabe eines Passworts sowie eines Nutzernamens statt
- Die Absicherung der Requests erfolgt durch JSON-Web-Tokens

Maßnahmen zur Gewährleistung einer physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden:

- Zutritt zu Serverräumen nur durch autorisierte Mitarbeiter
- Datenschutzrechtliche Instruierung der Mitarbeiter
- Zutritt betriebsfremder Personen nur in Begleitung instruierter Mitarbeiter
- Zugriff auf Systeme nur für autorisierte Mitarbeiter möglich (Passwort Verfahren)

Neurapix

Maßnahmen zum Schutz personenbezogener Daten bei der Heim- oder Telearbeit:

- Ein Zugriff auf die Server des Auftragnehmers durch Mitarbeiter in Heimarbeit erfolgt nur über verschlüsseltes VPN
- Eine Remotezugriff auf die Server des Auftragnehmers erfolgt nur per SSH
- Ein Remotezugriff erfolgt lediglich durch instruierte Mitarbeiter über zu diesem Zweck festgelegte Endgeräte

Anforderungen an die Ereignisprotokollierung (z.B. bei der Nutzerauthentifizierung oder der Dateneingabe, -veränderung oder –löschung):

- Die verarbeiteten Daten sind ihrem Wesen nach nicht veränderbar
- Protokollierung erfolgter Logins

Technisch-organisatorischer Maßnahmen im Rahmen der Unterstützungspflichten des Auftragnehmers (z.B. bei den Betroffenenrechten):

- Bestehende Implementierung von Verfahren zur Durchsuchung aller gespeicherten Fotos
- Auf Anfrage unter Benennung konkret zu löschender Bilddateien wird eine endgültige Löschung dieser Bilddateien durchgeführt

Verfügbarkeit der personenbezogenen Daten

- Übertragene Bilddateien werden lediglich in dem im Hauptvertrag vereinbarten Umfang gespeichert und verfügbar gehalten. Eine Archivierung die Bilddateien obliegt dem Auftraggeber.

Neurapix

Anlage 2 - Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer"). Dabei handelt es sich um nachfolgendes Unternehmen:

Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen:

Zwischenspeicherung der zwischen den Parteien wechselseitig übertragenen Bilddateien