Vertrag über die Verarbeitung von Daten im Auftrag
- Auftragsverarbeitung i. S. d. Art. 28 DSGVO -

zwischen

Unternehmen oder Person, die gemäß den Nutzungsbedingungen einen Nutzeraccount auf der TAWNY-Plattform erstellt hat oder die in einem über einen anderen Vertrag geregelten Auftragsverhältnis („Hauptvertrag“) mit der TAWNY GmbH steht.

Verantwortlicher i.S.d. Art. 4 Abs. 7 DSGVO- nachstehend

Auftraggeber genannt

und

TAWNY GmbH
Schellingstraße 45
D-80799 München

Auftragsverarbeiter i.S.d. Art. 4 Abs. 8 DSGVO - nachstehend

Auftragnehmer genannt -

Inhalt

1 Präambel

Bei der Erbringung der Leistungen gemäß den Nutzungs- bzw. Hauptvertragsbedingungen verarbeitet der Plattformbetreiber personenbezogene Daten ("Nutzerinhalte"), die der Verantwortliche zur Erbringung der Leistungen zur Verfügung gestellt hat.

Dieser Vertrag konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus dem geschlossenen Vertrag und der in den Nutzungs-/Hauptvertragsbedingungen in ihren Einzelheiten beschriebenen Auftragsverarbeitung i. S. d. Art.28 DSGVO ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten des Auftraggebers verarbeiten.

Im Rahmen der Wartung eines IT-Systems ist nicht auszuschließen, dass der Auftragnehmer personenbezogene Daten einsehen kann. Obwohl der Auftragnehmer keine eigentliche Verarbeitung der Daten durchführt, ist es aufgrund der möglichen Einsichtnahme in personenbezogene Daten notwendig, eine Datenschutzvereinbarung abzuschließen, welche die Anforderungen an die Regelungen der Auftragsvereinbarung gem. Art. 28 DSGVO erfüllt.

2 Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i. S. d. Art. 4 Abs. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i. S. d. Art. 4 Abs. 2 DSGVO zugrunde gelegt.

3 Gegenstand des Auftrags

Der Gegenstand der Verarbeitung, d.h. Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen, sind in **Anlage 1** zu diesem Vertrag festgelegt.

4 Dauer des Auftrags

(1) Der Vertrag beginnt mit dem entsprechend den Nutzungs-/Hauptvertragsbedingungen geschlossenen Vertrag und wird für unbestimmte Zeit geschlossen.

(2) Der Vertrag endet automatisch mit Löschung des Nutzeraccounts bzw. mit Ende des Hauptvertrags.

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

5 Erbringung der Leistungen

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

Das angemessene Schutzniveau bei Google in Irland (EU)* wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c und d DSGVO).
* Der Unterauftragsverarbeiter Google verarbeitet die Daten innerhalb der EU, setzt die Regelungen der EU-Standardvertragsklauseln um und bietet zusätzliche Garantien, das europäische Datenschutzrecht einzuhalten.
Nach der Rechtsprechung des EuGH (Urteil vom 16.07.2020, Az.: C-311/18 ("Schrems II")) besteht für US-Unternehmen kein angemessenes Datenschutzniveau. Es besteht insbesondere das Risiko, dass personenbezogene Daten trotz der Speicherung und Verarbeitung innerhalb der EU durch US-Behörden, zu Kontroll- und zu Überwachungszwecken, möglicherweise auch ohne Rechtsbehelfsmöglichkeiten, verarbeitet werden können.

6 Technisch-organisatorische Maßnahmen

Bei den zu treffenden Maßnahmen handelt es sich um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei werden der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen (Art. 32 Abs. 1 DSGVO) berücksichtigt

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben zur Sicherheit der Verarbeitung aus Art. 28 Abs. 3 lit. c, Art. 32 DSGVO, insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO.

(2) Der Auftragnehmer fügt den zum Zeitpunkt des Vertragsschlusses bestehenden Stand der technischen und organisatorischen Maßnahmen, insbesondere hinsichtlich der konkreten Auftragsdurchführung als **Anlage 4** vor Beginn der Verarbeitung zu diesem Vertrag bei. Soweit die Prüfung oder ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

(4) Der Auftragnehmer wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren.

7 Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i. S. d. Art. 4 Abs. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer.

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

(3) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich.

(4) Der Auftraggeber nennt dem Auftragnehmer einen Ansprechpartner für im Rahmen des Vertrags anfallende Datenschutzfragen.

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

7.1 Weisungsbefugnis des Auftraggebers

Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Art. 28 Abs. 3 a) DSGVO vor.

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

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

(3) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(4) Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden, sind diese in Textform zu dokumentieren. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform mitteilen.

7.2 Kontrollrechte des Auftraggebers

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

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu geben, soweit dies zur Durchführung der Kontrolle i. S. d. Absatzes 1 erforderlich ist.

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

sofern diese das Plattform-Konto bzw. die Plattform-Projekte des Auftraggebers betreffen und der Datenschutz für weitere Auftraggeber, die die TAWNY-Plattform nutzen, gewahrt bleibt.

(4) Der Auftraggeber hat das Recht, im Einvernehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer, die in keinem Wettbewerbsverhältnis zum Auftragnehmer stehen, 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 Betriebsstätte während der regelmäßigen Bürozeiten des Auftragnehmers zu überzeugen.

(5) Zum Nachweis der Einhaltung der vereinbarten Pflichten, kann der Auftragnehmer, dem Auftraggeber u.a. folgende Nachweise, die nicht nur den konkreten Auftrag betreffen, vorlegen:

- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitäts-auditoren)
- Ergebnisse eines Selbstaudits
- unternehmensinterne Verhaltensregeln einschließlich eines externen Nachweises über deren Einhaltung
- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz, ISO 27001)

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

8 Rechte und Pflichten des Auftragnehmers

Dem Auftragnehmer steht das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

8.1 Allgemeine Pflichten

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten oder diese erlauben. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß DSGVO; insofern gewährleistet er insbesondere die Einhaltung nachfolgender Vorgaben.

8.2 Datenschutzbeauftragter des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO bzw. für inländische Unternehmen gemäß § 38 BDSG 2018 benannt hat.

(2) Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Der Auftragnehmer wird dem Auftraggeber die Kontaktdaten seines Datenschutzbeauftragten in Anlage 3 mitteilen.

(3) Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich in Textform mitzuteilen.

(4) Die Pflicht zur Bestätigung kann im Ermessen des Auftraggebers entfallen, wenn der Auftragnehmer nachweisen kann, dass er gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu bestellen und dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften, der Regelungen dieses Vertrages sowie etwaiger weiterer Weisungen des Auftraggebers gewährleisten.

(5) Sofern der Auftragnehmer seinen Sitz außerhalb der EU hat, benennt er in Textform den Vertreter nach Art. 27 Abs. 1 DSGVO in der EU.

8.3 Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von personenbezogenen Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über die Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Zur Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 lit. b, 32 Abs. 4 DSGVO setzt der Auftragnehmer bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf Vertraulichkeit im Umgang mit personenbezogenen Daten verpflichtet sind und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.

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

8.4 Weisungsgebundenheit

(1) Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu den auftragsbezogenen personenbezogenen Daten hat, dürfen diese Daten entsprechend Art. 29 u. Art. 32 Abs. 4 DSGVO ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet oder befugt sind.

(2) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers 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.

(3) 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.

(4) Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Sofern weisungsempfangsberechtigte Personen benannt werden, sind diese in Textform zu dokumentieren.
Für den Fall, dass sich die Weisungsempfänger beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen.

8.5 Meldepflichten des Auftragnehmers

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

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

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.

(3) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich, spätestens aber binnen 48 Stunden ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze
- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

8.6 Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber im angemessenen Umfang und nur soweit dies dem Auftragnehmer zumutbar ist, bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

- die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung bzw. die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

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

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

(4) 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.

(5) Der Auftragnehmer unterstützt den Auftraggeber im angemessenen Umfang und nur soweit dies dem Auftragnehmer zumutbar ist, bei seiner Pflicht nach Art. 12-23 DSGVO bei der Umsetzung seiner Informationspflicht gegenüber dem Betroffenen und zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten und stellt ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung. Es gelten die Regelungen von Ziff. 8.7 dieses Vertrages.

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

8.7 Wahrung von Betroffenenrechten

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

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

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

9 Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht als Unterauftragsverhältnisse sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in

Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste.

Der Auftragnehmer ist verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen, um den Schutz personenbezogener Daten zu gewährleisten.

(2) Die Wartung und Pflege von IT-System oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i. S. d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

(3) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln.

(4) Der Auftraggeber stimmt der Beauftragung der in **Anlage 2** dokumentierten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zu.

Die Auslagerung auf weitere Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit 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 DSGVO zugrunde gelegt wird.

(5) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(6) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform).

(7) Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

(8) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen i. S. d. Kap. V DSGVO sicher.

10 Beendigung / Löschung und Rückgabe der Daten

(1) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung des Vertrages, hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Die Löschung ist in geeigneter Weise zu dokumentieren, das Protokoll der Löschung ist auf Anforderung vorzulegen.

Für Datenträger gilt, dass diese im Falle einer vom Auftraggeber gewünschten Löschung zu vernichten sind, wobei mindestens die Sicherheitsstufe 3 der DIN 66399 einzuhalten ist; die Vernichtung ist dem Auftraggeber unter Hinweis auf die Sicherheitsstufe gemäß DIN 66399 nachzuweisen.

(2) 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 oder sonstiger Pflichten zur Speicherung der Daten erforderlich sind.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

(4) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist von mindestens zwei Wochen durch den Auftraggeber angekündigt werden.

10.1 Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

11 Haftung und Schadensersatz

(1) Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

(2) Im Innenverhältnis zwischen dem Auftraggeber und dem Auftragnehmer gelten die im Hauptvertrag vereinbarten Haftungsbeschränkungen.

(3) Im Übrigen wird vereinbart, dass der Auftraggeber den Auftragnehmer von der Haftung freistellt, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

12 Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des

Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

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

13 Schlussbestimmungen

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter, etwa durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer Vereinbarung in Schriftform und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieses Vertrags handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Hauptvertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen nicht.

_____ München, den _____

Ort, Datum

_____ _____

- Auftraggeber - - Auftragnehmer -

Anlage 1 – Konkretisierung des Auftragsinhalts

(1) Art und Zweck der Verarbeitung

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind:

- Bereitstellung, Betrieb und Wartung einer Plattform zur Analyse von Bildern, Videos, Audiodaten oder physiologischer Daten hinsichtlich der darin enthaltenen Inhalte, insbesondere der von den aufgenommenen Personen gezeigten Emotionen und Verhaltensweisen.

(2) Art(en) der personenbezogenen Daten

Die Datenarten/-kategorien der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind:

- Emotionsanalyse
  - Bilder, Videos, Audioaufnahmen und physiologische Daten von Personen
  - Pseudonymisierte Bezeichnung Proband (ggf. auch Name)
  - Analysedaten/-ergebnisse
- Protokolle
  - Plattform-Benutzeroberfläche
  - Plattform-API
  - Datenbank / Storage
- Daten Benutzeraccount
  - Name
  - E-Mail-Adresse
  - Passwort (verschlüsselt)
  - Firma
  - Tätigkeitsbereich

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen sind:

- Probanden:
  - Personen, die vom Nutzer per Einwilligung zur Teilnahme rekrutiert werden
  - Personen, bei denen der Nutzer ein nachweisbares Nutzungsrecht für das Video besitzt
- Nutzer der Plattform

Anlage 2 – Genehmigte Unterauftragnehmer

Firma Unterauftragnehmer	Anschrift/Land	Web-Adresse	Leistung
Hetzner Online AG	Stuttgarter Str. 1 91710 Gunzenhausen	https://www.hetzner.com/de/	Bereitstellung von Computing-Services (Hosting, Datenverarbeitung, Speicher)
Google Ireland Limited	Gordon House, Barrow Street Dublin 4 Ireland	https://cloud.google.com/gcp/?hl=de	Bereitstellung von Computing-Services (Hosting, Datenverarbeitung, Speicher)
HYVE AG	Schellingstr. 45 80799 München	https://www.hyve.net	Bereitstellung von Computing-Services (Hosting, Datenverarbeitung, Speicher)

Anlage 3 – Datenschutzbeauftragter Auftragnehmer

Datenschutzbeauftragter Auftragnehmer

Vorname, Name	Dr. Eddie Kohfeldt
E-Mail-Adresse	datenschutz@tawny.ai
Telefon	+49 8133 9179310

Anlage 4 – Technisch-organisatorische Maßnahmen

Technische und organisatorische Maßnahmen zur Datensicherheit

Für die TAWNY-Plattform sind nachfolgende technische und organisatorische Maßnahmen (TOM) zur Datensicherheit i. S. d. Art. 32 DSGVO getroffen worden. Die Schutzmaßnahmen für die Datenverarbeitung in Kundenprojekten über die TAWNY-Plattform werden zusätzlich zu denen für die interne IT-Infrastruktur angewendet. Sie gelten für alle Tätigkeiten, bei denen Mitarbeiter von TAWNY oder beauftragte Dritte (Auftragsverarbeiter) personenbezogene oder sensible Daten des Auftraggebers verarbeiten.

Technische Basis:

Die von TAWNY erbrachten Services werden über zwei Rechenzentrumsinfrastrukturen bereitgestellt:

Google Cloud Platform

Ein Teil der von TAWNY erbrachten Services wird geobasiert innerhalb der EU auf der Google Cloud Platform (GCP) gehostet. Betreiber ist Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland (im Folgenden "Google").

Die GCP Rechenzentrums- und Netzwerkarchitektur erfüllt sehr hohe Anforderungen, die als Voraussetzung für den sicheren Betrieb von TAWNY notwendig sind: Hierdurch werden Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit sowie rasche Wiederherstellbarkeit gewährleistet. Die GCP ist unter anderem nach ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27701, SOC 1-3, PCI DSS und CSA STAR zertifiziert. Dies sind international anerkannte Standards für IT-Betrieb sowie Informations- und Datensicherheit.

Hetzner Online AG

Ein Teil der von TAWNY erbrachten Services wird in einem sicheren Rechenzentrum innerhalb von Deutschland (Nürnberg, Falkenstein) gehostet. Betreiber ist die Hetzner Online AG, Stuttgarter Str. 1, 91710 Gunzenhausen (im Folgenden "Hetzner").

Hetzner Online ist nach DIN ISO/IEC 27001 zertifiziert. Der international anerkannte Standard für Informationssicherheit bescheinigt der Hetzner Online GmbH und der Hetzner Finland Oy, dass ein geeignetes Informationssicherheits-Managementsystem, kurz ISMS, implementiert wurde und gelebt wird. Das ISMS findet an den Standorten Nürnberg und Falkenstein sowie Helsinki unter dem Scope "Der Anwendungsbereich des Informationssicherheits-Managementsystems umfasst die Infrastruktur, den Betrieb und den Kundensupport der Rechenzentren." seine Anwendung. Das entsprechende Zertifizierungs-Verfahren wurde durch die FOX Certification GmbH durchgeführt.

Das Zertifikat weist ein adäquates Sicherheitsmanagement, die Sicherheit der Daten, die Vertraulichkeit der Informationen und die Verfügbarkeit der IT-Systeme nach. Es bestätigt zudem, dass die Sicherheitsstandards kontinuierlich verbessert und nachhaltig kontrolliert werden.

1. Pseudonymisierung

Pseudonymisierung wird zurzeit nicht angewendet. Die Anwendung von Pseudonymisierungsverfahren obliegt dem Auftraggeber.

2. Vertraulichkeit

Zutrittskontrolle - Kein unbefugter Zutritt zu Datenverarbeitungsanlagen

Die physische Sicherheit des jeweiligen Rechenzentrums wird durch die Betreiber Google und Hetzner bereitgestellt.

Zugangskontrolle - Keine unbefugte Systembenutzung

Die Kontrolle des Zugangs zu Datenverarbeitungsanlagen mit Kundenprojekten ist durch folgende Maßnahmen sichergestellt.

Technische Maßnahmen:

- Der Zugang zur TAWNY-Plattform ist nur mit einem passwortgeschützten Benutzeraccount möglich.
- Der Zugang auf die Administrationstools der Backendsysteme ist nur über speziell mit 2-Faktor-Authentifizierung abgesicherten Adminstratoraccounts möglich.
- Der Zugang zur unterliegenden Serverinfrastruktur ist nur per SSH mit Public/Private-Key-Authentifizierung (mit per Passphrase zusätzlich verschlüsselten Keys) möglich.
- Die Protokollierung des Zugangs auf die Systeme von Google und Hetzner erfolgt über die Protokollierungsfunktionen des jeweiligen Anbieters.
- Die Protokollierung des Zugangs auf Linux-Server erfolgt über das lokale Syslog.

Organisatorische Maßnahmen:

- Die Erstellung eines Benutzeraccounts auf der TAWNY-Plattform erfordert die Validierung der verwendeten E-Mail-Adresse.
- Administratorenrechte sind einigen wenigen Kern-Entwicklern des Auftragnehmers vorbehalten
- Der Kreis dieser Administratoren wird so klein wie möglich gehalten.
- Die Administratoren sind speziell instruiert, wie mit diesen Zugangsmöglichkeiten umzugehen ist, und sind selbstverständlich zur Vertraulichkeit verpflichtet.

Zugriffskontrolle – Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems

Der kontrollierte Zugriff auf personenbezogene Daten nach dem „Need-to-Know“ Prinzip ist durch folgende Maßnahmen sichergestellt:

Technische Maßnahmen:

- Der Zugriff auf ein Projekt auf der TAWNY-Plattform (und die darin enthaltenen Daten) ist nur mit einem passwortgeschützten Benutzeraccount möglich, der die entsprechenden Berechtigungen besitzen muss. Die Durchsetzung dieser Regeln ist über die Mechanismen der unterliegenden Datenbanken und Storage-Server sichergestellt.
- Der Zugriff auf Daten des Auftraggebers direkt über die Administrationstools der Backendsysteme ist nur über speziell mit 2-Faktor-Authentifizierung abgesicherte Adminstratoraccounts möglich.

- Der Zugriff auf Daten des Auftraggebers direkt über die unterliegende Serverinfrastruktur ist nur per SSH mit Public/Private-Key-Authentifizierung möglich.

Organisatorische Maßnahmen:

- Die grundsätzliche Organisationseinheit für Kundendaten auf der TAWNY-Plattform ist ein "Plattform-Projekt". Der Auftraggeber kann beliebig viele solcher Projekte anlegen und die nachfolgenden Maßnahmen individuell pro Projekt festlegen.
- Der Verwaltung der Zugriffsrechte auf ein Plattform-Projekt und die darin enthaltenen Daten liegt im Verantwortungsbereich des Projektinhabers, d.h. des Auftraggebers.
- Im Grundzustand hat nur der Projektinhaber selbst mit seinem Benutzeraccount Zugriff auf das Projekt.
- Der Projektinhaber kann weiteren Benutzeraccounts explizit die Freigabe auf ein Projekt (und damit die darin enthaltenen Daten) erteilen und auch wieder entziehen.
- Auch TAWNY-Mitarbeitern, die evtl. zu Supportzwecken Zugriff auf das Projekt erhalten sollen, muss explizit vom Projektinhaber über den gleichen Mechanismus die Freigabe für das Projekt erteilt werden.
- Über die Backendsysteme und die Serverinfrastruktur ist grundsätzlich ein Zugriff auf die Daten des Auftraggebers unter Umgehung der vorher beschriebenen Regeln möglich. Die hierfür notwendigen Administratorenrechte sind jedoch einigen wenigen Kern-Entwicklern des Auftragnehmers vorbehalten, deren Accounts speziell mit 2-Faktor-Authentifizierung und/oder Public/Private-Key-Authentifizierung (mit per Passphrase zusätzlich verschlüsselten Keys) abgesichert sind.
- Der Kreis dieser Administratoren wird so klein wie möglich gehalten.
- Die Administratoren sind speziell instruiert, wie mit diesen Zugriffsmöglichkeiten umzugehen ist, und sind selbstverständlich zur Vertraulichkeit verpflichtet.

Weitergabekontrolle

Die Vertraulichkeit der personenbezogenen Daten bei der elektronischen Übertragung oder während ihres Transports ist durch folgende Maßnahmen sichergestellt:

Technische Maßnahmen

- Die elektronische Übertragung der Daten findet ausschließlich verschlüsselt nach dem Stand der Technik statt (SSL, SSH, etc.)

Organisatorische Maßnahmen

- Der Transport von Daten auf physischen Datenträgern (USB-Stick, externe Festplatte, etc.) ist nur in Ausnahmefällen erlaubt.
- Beim Transport von Daten auf physischen Datenträgern (USB-Stick, externe Festplatten) werden die Daten grundsätzlich verschlüsselt.

3. Integrität

Maßnahmen, um die Integrität der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen.

Technische Maßnahmen:

- Die Änderung von Daten in einem Plattform-Projekt ist nur mit einem passwortgeschützten Benutzeraccount möglich, der die entsprechenden Berechtigungen besitzen muss.
- Wesentliche Aktivitäten innerhalb von Plattform-Projekten werden automatisch protokolliert (inkl. Art der Aktion, Zeitstempel und ausführender Benutzer).
- Die Änderung von Daten des Auftraggebers direkt über die Administrationstools der Backendsysteme ist nur über speziell mit 2-Faktor-Authentifizierung abgesicherte Adminstratoraccounts möglich.
- Die Änderung von Daten des Auftraggebers direkt über die unterliegende Serverinfrastruktur ist nur per SSH mit Public/Private-Key-Authentifizierung möglich.

Organisatorische Maßnahmen:

- Administratorenrechte sind einigen wenigen Kern-Entwicklern des Auftragnehmers vorbehalten, deren Accounts speziell mit 2-Faktor-Authentifizierung und/oder Public/Private-Key-Authentifizierung (mit per Passphrase zusätzlich verschlüsselten Keys) abgesichert sind.
- Der Kreis dieser Administratoren wird so klein wie möglich gehalten.
- Administratoren protokollieren etwaige Änderungen an Daten des Auftraggebers, die über die Administratorzugriffsrechte durchgeführt wurden.
- Automatisierte Änderungen an Daten des Auftraggebers (z.B. im Rahmen des Ausrollens einer neuen Plattform-Software-Version) werden vorher auf Test- und Staging-Umgebungen getestet, um die Erhaltung der Integrität der Daten zu prüfen.

4. Verfügbarkeit und Belastbarkeit

Maßnahmen, um die Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen

Technische Maßnahmen:

- Die verwendeten Rechenzentren erfüllen internationale Standards (z.B. ISO/IEC 27001, weitere siehe Auflistung oben).
- Die Daten der TAWNY-Plattform werden in Multi-Region-Buckets georedundant in der Europäischen Union gespeichert.
- Die TAWNY-Plattform nutzt die Möglichkeiten der automatischen Skalierung von Ressourcen in den Rechenzentren, um auch bei Lastspitzen die Verfügbarkeit aufrecht zu erhalten.
- Die TAWNY-Plattform wird auf virtualisierten Systemen betrieben, um möglichst unabhängig von darunterliegender Hardware / Hardware-Fehlern zu sein.
- Backups werden automatisiert und regelmäßig erstellt.

Organisatorische Maßnahmen:

- Reaktionszeiten bei Störungen basieren auf den Arbeitszeiten des TAWNY-Plattform-Supportteams (Mo-Fr 9-18 Uhr) sowie den Verfügbarkeiten des technischen Supports von Google und Hetzner.

5. Rasche Wiederherstellbarkeit

Maßnahmen, um die Verfügbarkeit der personenbezogenen Daten und den Zugang zu diesen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Technische Maßnahmen:

- Die Datenbanken der TAWNY-Plattform können automatisiert aus Backups wiederhergestellt werden.
- Die Plattform-Software oder bestimmte Teile davon können in anderer Umgebung (z.B. neue Cloud-Instanzen) automatisiert neu deployed werden.

Organisatorische Maßnahmen:

- Prozess, Verantwortliche und Meldewege sind festgelegt.

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

- Regelmäßige Überprüfung der technischen Maßnahmen und möglicher Verbesserungen dieser auf Basis des Stands der Technik im Rahmen der Weiterentwicklung der TAWNY-Plattform.
- Peer-Review von Konzepten und Implementierungen der technischen Maßnahmen innerhalb des Entwicklerteams.
- Regelmäßige Bewertung der Maßnahmen mit externem Datenschutzbeauftragten.

7. Verzeichnis von Verarbeitungstätigkeiten für Auftragsverarbeiter (Art. 30 Abs. 2 DSGVO)

- Verzeichnis von Verarbeitungstätigkeiten i. S. d. Art. 30 Abs. 2 DSGVO vorhanden.
- Die weisungsgemäße Verarbeitung personenbezogener Daten erfolgt beim Auftragnehmer durch eine Leistungsvereinbarung mit einem klar definierten Umfang für Art und Zweck der beabsichtigten Verarbeitung. Dies ist im Vertrag über Auftragsdatenverarbeitung nach Art. 28 DSGVO dokumentiert.

Stand: 01.08.2021