



Gutes
besser
tun.

Auftragsverarbeitungsvertrag

zwischen

Auftragnehmerin (im Folgenden «ANT»)

Bitte ankreuzen, mit welcher Gesellschaft der Vertrag geschlossen werden soll. In Normalfall ist dies die Gesellschaft, mit der Verträge über Dienstleistungen, Softwarenutzung und Lizenzen bestehen.

Wir schließen folgenden Vertrag mit der **ANT-Informatik AG, Schweiz**

ANT-Informatik AG Hertistrasse 2c CH-8304 Wallisellen	www.ant-informatik.ch Handelsregister Nr. CH-270.3.000.253-6 MWST-Nr. CHE-106.496.539
---	--

Wir schließen folgenden Vertrag mit der **ANT-Informatik GmbH, Deutschland**

ANT-Informatik GmbH Wilhelmstrasse 56 D-53721 Siegburg	https://www.ant-informatik.de/ Handelsregister Ut. Amtsgericht Bonn HRB 22757
--	---

und **Auftraggeber**

Name/Organisation/Firma

Strasse/Postleitzahl

Ort/Land

ANT-Informatik AG +41 44 552 29 29
Hertistrasse 2c
CH-8304 Wallisellen
info@ant-informatik.ch
ant-informatik.ch

ANT-Informatik GmbH +49 2241 898 70 30
Wilhelmstrasse 56
D-53721 Siegburg
info@ant-informatik.de
ant-informatik.de

1. Zweck

Dieser Vertrag wird von und zwischen dem Auftraggeber und ANT abgeschlossen, um einen angemessenen Schutz von personenbezogenen Daten in Situationen zu gewährleisten, in denen diese Daten vom Auftraggeber an ANT als Verarbeiter zum Zwecke der Bearbeitung dieser Daten im Namen des Auftraggebers übermittelt werden.

Ferner unterstützt dieser Vertrag die Parteien bei der Einhaltung der in der Schweiz und der Europäischen Union geltenden Vorschriften über die Bearbeitung von personenbezogenen Daten, insbesondere der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016, die ab dem 25. Mai 2018 anwendbar ist ("DS-GVO").

Die Zwecke, welche mit der Übertragung von personenbezogenen Daten an ANT und der Verarbeitung durch ANT verfolgt werden, sind in Anlage 1 zu diesem Vertrag beschrieben. Anlage 1 ist integraler Bestandteil dieses Vertrages und kann von den Parteien von Zeit zu Zeit geändert werden.

2. Geltungsbereich

Dieser Vertrag gilt für alle personenbezogenen Daten, die sich auf Dritte beziehen, und die

- a) vom Auftraggeber an ANT übertragen (mit eingeschlossen ist hierbei der Zugriff auf solche Daten) wurden oder
- b) von ANT im Auftrag des Auftraggebers bearbeitet werden.

Der Katalog der zu übertragenden und zu bearbeitenden personenbezogenen Daten ist in Abschnitt 1 von Anlage 1 zu diesem Vertrag enthalten.

Die Parteien sind sich einig, dass sowohl die ANT Informatik AG als auch die ANT Informatik GmbH im Rahmen dieser Vereinbarung als Auftragnehmer auftreten. Zwischen der ANT Informatik GmbH und ANT Informatik AG besteht ein Vertrag, der die Datenverarbeitung im Unternehmensverbund regelt.

3. Definitionen

Sofern hierin nicht anders definiert, haben alle Begriffe die gleiche Bedeutung wie im schweizerischen Bundesgesetz über den Datenschutz (DSG). Es wird davon ausgegangen, dass die meisten Begriffe im DSG mit denjenigen in der DS-GVO übereinstimmen.

Für den Fall, dass es einen wesentlichen Unterschied zwischen der Definition eines Begriffs im DSG und der DS-GVO geben sollte, hat die Definition in der DS-GVO Vorrang, mit Ausnahme der Definition der personenbezogenen Daten.

Für die Zwecke dieses Vertrages:

bezeichnet der Begriff "Unterauftragnehmer" jeden von ANT (oder von einem anderen Unterauftragnehmer von ANT) beauftragten Bearbeiter, der sich damit einverstanden erklärt, von ANT (oder von einem anderen Unterauftragnehmer von ANT) personenbezogenen Daten zu erhalten, die ausschließlich für die Bearbeitung im Namen des Auftraggebers gemäß dessen Anweisungen und den Bedingungen des schriftlichen Untervertrags bestimmt sind.

4. Pflichten des Auftraggebers

Der Auftraggeber sichert zu, dass die personenbezogenen Daten gemäss den Anforderungen des DSGVO und der DS-GVO erhoben und bearbeitet wurden. Der Auftraggeber garantiert ferner, dass die Übertragung der personenbezogenen Daten und die Bearbeitung dieser Daten durch ANT, wie in dieser Vereinbarung festgelegt, nach dem DSGVO und der DS-GVO zulässig sind und der Auftraggeber verpflichtet sich, dass die Übertragung in Übereinstimmung mit dem DSGVO und der DS-GVO erfolgt.

Der Auftraggeber prüft, ob die technischen und organisatorischen Massnahmen, wie sie in Art. 7 Abs. 1 DSGVO sowie Art. 32 DS-GVO verlangt werden und wie sie von ANT gemäss Anlage 2 dieses Vertrags durchgeführt werden, angemessen sind, um die übermittelten personenbezogenen Daten vor jeglicher unbefugten Bearbeitung zu schützen. Anlage 2 ist integraler Bestandteil dieses Vertrags und kann von den Parteien von Zeit zu Zeit geändert werden.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmassnahmen von ANT vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Im Falle einer Geltendmachung von Ansprüchen gegenüber ANT durch eine betroffene Person aufgrund von Art. 82 DS-GVO verpflichtet sich der Auftraggeber, ANT bei der Abwehr der Ansprüche im Rahmen ihrer Möglichkeiten zu unterstützen.

5. Pflichten der ANT

ANT verpflichtet sich und garantiert, dass sie alle personenbezogenen Daten, die sie vom Auftraggeber erhält, die ihr vom Auftraggeber zur Verfügung gestellt werden oder sich aus diesen Daten ableiten,

- a) ausschließlich im Namen und für die Zwecke vom Auftraggeber, wie in Anlage 1 Abschnitt 2 dargelegt oder wie anderweitig ausdrücklich in dokumentierter Form vom Auftraggeber vorgesehen oder mit ANT vereinbart;
- b) in Übereinstimmung mit den Anweisungen des Auftraggebers; und
- c) in Übereinstimmung mit diesem Vertrag bearbeitet, sofern ANT nicht zu einer anderen Bearbeitung durch das Recht der Schweiz, der EU oder der EU-Mitgliedstaaten, dem ANT-Informatik AG unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungsbehörden); in einem solchen Fall teilt ANT dem Auftraggeber diese rechtlichen Anforderungen vor der Bearbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

ANT hat den Auftraggeber unverzüglich zu informieren, wenn sie der Ansicht ist, dass eine Anweisung gegen das DSGVO, die DS-GVO oder andere geltende Rechtsvorschriften der EU, der EU-Mitgliedstaaten oder der Schweiz, die den Datenschutz betreffen, verstösst. ANT-Informatik AG ist berechtigt, die Ausführung des Auftrages bis zur Bestätigung oder Änderung der Anweisung durch den Auftraggeber auszusetzen. Wenn ANT nach dem Schweizer Recht, dem EU-Recht oder dem Recht eines Mitgliedstaates, dem ANT unterliegt, verpflichtet ist, personenbezogenen Daten in ein Drittland oder an eine internationale Organisation zu übermitteln, hat ANT den Auftraggeber vor der Übermittlung über diese gesetzliche Verpflichtung zu informieren, es sei denn, das Gesetz verbietet solche Informationen aus wichtigen Gründen des öffentlichen Interesses.

ANT verpflichtet sich, vor jeder Bearbeitung geeignete technische und organisatorische Massnahmen im Sinne des DSGVO (insbesondere Art. 7 Abs. 1 und Art. 8 DSGVO) und der DS-GVO (Art. 32 DSGVO), und wie in Anlage 2 dieses Vertrags festgelegt, zu implementieren, um die personenbezogenen Daten vor unbefugter Bearbeitung zu schützen, einschliesslich jeglicher Bearbeitung, die nicht ausdrücklich durch diesen Vertrag genehmigt wurde, einschliesslich des zufälligen Verlusts oder der Zerstörung oder Beschädigung der personenbezogenen Daten. ANT hat Massnahmen zu treffen, welche die Vertraulichkeit, Integrität, Verfügbarkeit und Ausfallsicherheit von Systemen und Dienstleistungen im Zusammenhang mit der Bearbeitung von personenbezogenen Daten gewährleisten.

ANT ist berechtigt, die getroffenen organisatorischen und technischen Massnahmen zu ändern. Es muss jedoch sichergestellt sein, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

ANT teilt dem Auftraggeber den Namen und die Kontaktdaten der Person mit, die bei ANT-Informatik AG für Datenschutzfragen zuständig ist.

ANT wird dem Auftraggeber im Rahmen des Zumutbaren bei der Erfüllung von Gesuchen und Ansprüchen der betroffenen Personen gemäss Kapitel III der DS-GVO sowie bei der Einhaltung der Anforderungen gemäss Art. 33 bis 36 DS-GVO unterstützen. ANT wird insbesondere den Auftraggeber unverzüglich informieren und mit ihm zusammenarbeiten:

- a) wenn sie der Ansicht ist, dass sie möglicherweise nicht mehr in der Lage ist oder sie tatsächlich nicht mehr in der Lage ist, den Pflichten gemäss diesem Vertrag nachzukommen, insbesondere wenn sie eine Anfrage oder Anordnung einer zuständigen Behörde erhält oder vernünftigerweise erwarten muss, die sie dazu auffordert, einige oder alle personenbezogenen Daten, auf die dieser Vertrag Anwendung findet, offen zu legen oder von einer weiteren Bearbeitung abzusehen;
- b) wenn ihr eine Verletzung des Schutzes der personenbezogenen Daten vom Auftraggeber bekannt wird; oder
- c) wenn ein unbeabsichtigter oder unbefugter Zugriff auf diese personenbezogenen Daten oder ein anderer Verstoss gegen die Datenschutzbestimmungen vorliegt. ANT hat den Auftraggeber unverzüglich nach Bekanntwerden der Datenschutzverletzung bzw. des unbefugten Zugriffs zu benachrichtigen. Die Meldung muss alle erforderlichen Unterlagen enthalten, die innert der Frist mit zumutbarem Aufwand erhältlich sind und es dem Auftraggeber ermöglichen, den Verstoss erforderlichenfalls der zuständigen Aufsichtsbehörde zu melden. Erforderliche Unterlagen, welche nicht unverzüglich übermittelt werden können, werden so rasch wie möglich nachgereicht. ANT wird mit dem Auftraggeber zusammenarbeiten und die vom Auftraggeber angeordneten angemessenen geschäftlichen Schritte unternehmen, um bei der Untersuchung, Eindämmung und Behebung jedes solchen Verstosses behilflich zu sein.

ANT unternimmt angemessene Schritte, um die Zuverlässigkeit aller Mitarbeiter oder Unterauftragnehmer zu gewährleisten, die Zugang zu den personenbezogenen Daten erhalten. Sie wird insbesondere sicherstellen, dass der Zugang strikt auf diejenigen Personen beschränkt ist, die die personenbezogenen Daten, für die in Anlage 1 genannten Zwecke kennen müssen. ANT sichert zu, dass es den betreffenden Personen untersagt ist, die Daten ausserhalb oder entgegen den Anweisungen des Auftraggebers zu bearbeiten.

Darüber hinaus sichert ANT zu, dass diese Personen einer Geheimhaltungsverpflichtung oder einer gesetzlichen Verschwiegenheitspflicht unterliegen. Die Geheimhaltungsverpflichtung gilt auch nach Beendigung dieses Vertrages. ANT gewährleistet ferner, dass diese Personen eine angemessene Schulung betreffend den Datenschutz erhalten.

ANT garantiert, dass sie ihre Pflichten gemäss Art. 32 Abs. 1 lit. d) DS-GVO durch die Einführung eines Verfahrens zur periodischen Überprüfung der Wirksamkeit der technischen und organisatorischen Datensicherheitsmassnahmen einhalten wird. ANT berichtigt oder anonymisiert die vertragsbezogenen Daten, wenn der Auftraggeber dies anordnet.

Ist eine datenschutzkonforme Beendigung oder eine entsprechende Einschränkung der Datenbearbeitung nicht möglich, so verpflichtet sich ANT, basierend auf einem separaten Auftrag vom Auftraggeber, zur datenschutzkonformen Vernichtung von Datenträgern und anderen Materialien oder sendet diese Datenträger an den Auftraggeber zurück, sofern dies nicht ohnehin bereits vertraglich vereinbart wurde.

Im Falle einer Geltendmachung von Ansprüchen gegenüber dem Auftraggeber durch eine betroffene Person auf der Grundlage von Art. 82 DS-GVO verpflichtet sich ANT, den Auftraggeber bei der Abwehr der Ansprüche im Rahmen seiner Möglichkeiten zu unterstützen.

ANT sichert zu, dass sie bei ihren Arbeitsmitteln, Produkten, Anwendungen oder Dienstleistungen die Grundsätze des Data Privacy by Design und by Default berücksichtigt.

ANT erklärt, dass sie über alle Arten von Bearbeitungstätigkeiten, die im Auftrag vom Auftraggeber durchgeführt werden, ein schriftliches Verzeichnis führt, das den Namen und die Kontaktdaten von ANT, etwaige Subunternehmer und gegebenenfalls den Datenschutzbeauftragten, die Kategorien der im Auftrag des Auftraggebers durchgeführten Datenbearbeitungen, gegebenenfalls die Übermittlung von personenbezogenen Daten in Drittländer und die Kategorien der Empfänger von personenbezogenen Daten enthält.

Der Auftraggeber hat das Recht, jederzeit, in angemessener Weise und unter zumutbarer Mitwirkung von ANT, die Einhaltung des Vertrages durch ANT (und etwaige Subunternehmer) zu prüfen oder durch einen qualifizierten Dritten, der zur Verschwiegenheit verpflichtet ist, prüfen zu lassen. Die Kosten gehen zu Lasten des Auftraggebers.

ANT ist verpflichtet, dem Auftraggeber die Einhaltung der in diesem Vertrag festgelegten Verpflichtungen durch geeignete Massnahmen und Mittel nachzuweisen.

6. Unterauftragnehmer

Als Unterauftragnehmerverhältnisse 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 z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Massnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt.

ANT ist jedoch 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.

ANT darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

Der Auftraggeber stimmt der Beauftragung der nachfolgenden Subunternehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Massgabe des Art. 28 Abs. 2-4 DS-GVO:



Firma	Anschrift	Leistung
Atlassian. Pty Ltd	Level 6, 341 George Street Sydney NSW 2000 Australien	Jira-/Confluence-Cloud (Australien)
Microsoft Corporation	One Microsoft Way Redmond, WA 98052-6399 USA www.microsoft.com	Office 365: Server, Sharepoint, One-Drive, E-Mail (Deutschland Schweiz) Azure: Kaleido-Cloud (Deutschland)
Netrics AG	Tennisweg 6 CH - 2504 Biel/Bienne +41 (0)58 531 31 31 info@netrics.ch	Rechenzentrum für SEXTANT-Kunden, die gehostet werden bis 31.12.2023
Netrics AG	Tennisweg 6 CH - 2504 Biel/Bienne +41 (0)58 531 31 31 info@netrics.ch	JIRA Server Hosting bis 31.12.2023
Nexus-Schweiz AG	Hertistrasse 2c CH - 8304 Wallisellen info@nexus-schweiz.ch	Rechenzentrum für SEXTANT-Kunden die gehostet werden.
Nexus-Schweiz AG	Hertistrasse 2c CH - 8304 Wallisellen info@nexus-schweiz.ch	IT-Support
Nexus AG	Irmastraße 1 D - 78166 Donaueschingen +49 771 22960-0 info@nexus-ag.de	IT-Support
bitvoodoo GmbH	Hardturmstrasse 101 CH - 8005 Zürich +41 (0)44 533 38 00 info@bitvoodoo.ch	JIRA-Support

Die Auslagerung auf weitere Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers ist 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 DS-GVO zugrunde gelegt wird.

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

Erbringt der Unterauftragnehmer die vereinbarte Leistung ausserhalb der EU/des EWR oder der Schweiz, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Massnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

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

Sämtliche vertragliche Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Rechte der betroffenen Personen

Der Auftraggeber ist dafür verantwortlich, dass die betroffenen Personen über ihr Recht auf Auskunft, Berichtigung, Sperrung, Beschränkung oder Löschung verfügen, wie sie durch das DSGVO und/oder die DS-GVO vorgeschrieben sind. ANT (und jeder Unterauftragnehmer) wird mit dem Auftraggeber in vollem Umfang und unverzüglich zusammenarbeiten und dem Auftraggeber die notwendigen Unterstützungsleistungen für die Erfüllung solcher Gesuche oder Anfragen von betroffenen Personen zur Verfügung stellen. ANT (und jeder Unterauftragnehmer) wird alle Gesuche oder Anfragen, die sie direkt erhält, unverzüglich an den Auftraggeber weiterleiten, ohne inhaltlich auf diese einzugehen.

8. Vertragsdauer und -beendigung

Dieser Vertrag ist zwischen den Parteien bei Unterzeichnung durch beide Parteien verbindlich und bleibt auf unbestimmte Zeit in Kraft. Er erlischt automatisch mit Beendigung der von ANT erbrachten Leistungen, für die dieser Vertrag abgeschlossen wurde. Jede Vertragspartei kann diese Vereinbarung auch jederzeit mit sofortiger Wirkung durch eine schriftliche Mitteilung kündigen. Der

Auftraggeber kann die Übermittlung von personenbezogenen Daten und deren Bearbeitung zudem jederzeit sistieren.

Bei Kündigung dieses Vertrages aus welchem Grund auch immer, ist ANT (und jeder Unterauftragnehmer) verpflichtet,

- a) unverzüglich alle personenbezogenen Daten und Kopien davon, für die dieser Vertrag gilt, einschliesslich der vom Auftraggeber übermittelten personenbezogenen Daten, zu retournieren und, soweit dies nicht möglich ist,
- b) diese personenbezogenen Daten und Kopien davon zu anonymisieren und dem Auftraggeber schriftlich zu bestätigen, dass er dies getan hat; oder,
- c) sofern die auf ANT anwendbare Gesetzgebung die Retournierung oder Anonymisierung der unter diesen Vertrag fallenden personenbezogenen Daten verbietet, den Auftraggeber hierüber zu informieren und die personenbezogenen Daten vertraulich zu behandeln und nicht mehr aktiv zu bearbeiten.

Nach Beendigung dieses Vertrags wird jede andere Vereinbarung, die zwischen ANT und Subunternehmern zum Zwecke der Bearbeitung und Übermittlung von personenbezogenen Daten, die unter diesen Vertrag fallen, abgeschlossen wurde, automatisch beendet. Dies gilt dagegen nicht für andere Vereinbarungen, die der Auftraggeber und ANT zu anderen Zwecken abgeschlossen haben.

9. Verschiedenes

Jede Partei stellt Gerichten oder Aufsichtsbehörden und der Auftraggeber stellt allen betroffenen Personen eine Kopie oder den Inhalt dieses Vertrags auf deren Anfrage, oder wenn dies gesetzlich vorgeschrieben ist, zur Verfügung. Die Rechte und Pflichten jeder Partei dieses Vertrages sind unpräjudizierend für und unbeeinflusst von allen anderen Rechten und Pflichten, die die Parteien aufgrund anderer Vereinbarungen haben oder nicht haben können. Dieser Vertrag regelt nicht die Folgen, die die Ausübung eines Rechts und die Erfüllung einer Pflicht aus diesem Vertrag im Rahmen eines anderen Vertragsverhältnisses zwischen den Parteien haben können.

Jede Partei wird die andere Partei im Falle von Ansprüchen Dritter oder anderen Schäden, die sich aus der fahrlässigen oder vorsätzlichen Nichteinhaltung dieses Vertrags und / oder der anwendbaren Datenschutzgesetze durch die zur Schadloshaltung verpflichtete Partei ergeben, schadlos halten.

Dieser Vertrag kann nur schriftlich abgeändert werden. Die Parteien dürfen diesen Vertrag oder irgendwelche Rechte oder Pflichten aus diesem Vertrag ohne vorherige schriftliche Zustimmung der anderen Partei nicht an Dritte abtreten.

Für Kunden der **ANT-Informatik AG (CH)** gilt:

Dieser Vertrag (und jede Vereinbarung, die von ANT-Informatik AG und einem Subunternehmer für die Zwecke der Bearbeitung und Übermittlung von personenbezogenen Daten im Rahmen dieses Vertrags unterzeichnet wurde) unterliegt dem materiellen Recht der Schweiz und wird in Übereinstimmung mit diesem ausgelegt. Jegliche Streitigkeiten, die sich aus oder im Zusammenhang mit diesem Vertrag (oder einer Subunternehmer-Vereinbarung, die von ANT-Informatik AG und einem Subunternehmer für die Zwecke der Bearbeitung und Übermittlung von personenbezogenen Daten im Rahmen dieses Vertrags unterzeichnet wurde) oder dessen Verletzung ergeben, werden ausschliesslich von den ordentlichen Gerichten am Sitz von ANT-Informatik AG in der Schweiz entschieden.

Für Kunden der **ANT-Informatik GmbH (DE)** gilt:

Dieser Vertrag (und jede Vereinbarung, die von ANT-Informatik GmbH und einem Subunternehmer für die Zwecke der Bearbeitung und Übermittlung von personenbezogenen Daten im Rahmen dieses Vertrags unterzeichnet wurde) unterliegt dem materiellen Recht der Bundesrepublik Deutschland und wird in Übereinstimmung mit diesem ausgelegt. Jegliche Streitigkeiten, die sich aus oder im Zusammenhang mit diesem Vertrag (oder einer Subunternehmer-Vereinbarung, die von ANT-Informatik GmbH und einem Subunternehmer für die Zwecke der Bearbeitung und Übermittlung von personenbezogenen Daten im Rahmen dieses Vertrags unterzeichnet wurde) oder dessen Verletzung ergeben, werden ausschliesslich von den ordentlichen Gerichten am Sitz der ANT-Informatik GmbH in Deutschland entschieden.

Auftraggeber/in:

Auftragnehmer/in:

Ort, Datum
Signatur

Wallisellen / Siegburg
Tobias Wunden, CEO



Anlage I: Beschreibung der Übermittlung und Bearbeitung

1. Katalog der zu übertragenden und zu bearbeitenden personenbezogenen Daten:

- Personenbezogene Daten wie Name, Adresse, E-Mail, Telefon, Fax, Geburtstag
- Kommunikations-Präferenzen, Kommunikationsdaten
- Zahlungsbezogene Daten wie Kontoverbindung, Spenden-Transaktionen, Dauer und Abbuchungsaufträge oder SEPA-Mandate.

2. Zweck der Übertragung und Bearbeitung

Art und Zweck der Verarbeitung personenbezogener Daten durch ANT-Informatik AG ergeben sich aus den geschäftlichen Beziehungen zwischen dem Auftraggeber und dem Auftragnehmer.

3. Kategorien der betroffenen Personen:

- Unterstützende (Spendende, Mitglieder, Förderer, Gönner, Paten, Spendensammelnde)
- Interessenten
- Mitarbeitende des Auftraggebers

4. Kontaktinformationen für Datenschutzanfragen:

Philipp Herold
Hafenstraße 1a
D - 23568 Lübeck
Tel: 49 451 160852 – 13
datenschutz@hub24.de
<https://www.mein-datenschutzbeauftragter.de/>

Anlage II: Technische und organisatorische Massnahmen

Technische und organisatorische Schutzmaßnahmen gemäß Art. 7 DSGVO

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft der Auftragsverarbeiter nachfolgend dargelegte technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten:

1. Vertraulichkeit

Zutrittskontrolle

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist. Technische und organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

- Festlegung befugter Personen inklusive Umfang der jeweiligen Befugnisse
- Existenz von Regelungen für Unternehmensexterne
- Umsetzung einer Schlüsselregelung
- Physische Maßnahmen vorhanden und regelmäßig überprüft:
 - Gesicherter Eingang (z. B. abschließbare Türen)

Zusätzliche Massnahmen

- Sorgfältige Auswahl von Reinigungspersonal

Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme und die unbefugte Systemnutzung sind zu verhindern.

Technische und organisatorische Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

- Konzeption und Implementierung eines Berechtigungskonzepts
 - Berechtigungskonzept für Endgeräte (Rechner)
 - Berechtigungskonzept für Software/Systeme
- Identifikation und Berechtigungsprüfung eines Benutzers
- Implementierung eines Systems zur Verwaltung von Benutzeridentitäten
- Festlegung und Kontrolle der Zugangsbefugnisse
- Verschlüsselung
- Angemessener Passwortschutz (Verhaltensregeln, verschlüsselte Archive)
- Spezielle Sicherheitssoftware (z. B. Anti-Malware, VPN oder Firewall)
- Existenz von Regelungen für Unternehmensexterne



Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern. Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung anhand:

- Berechtigungs- und Rollenkonzept für Applikationen
- Umsetzung von Regelungen zur Zugriffs- und Benutzerberechtigung
- Überprüfung der Berechtigungen
- Funktionsbegrenzung (funktional/zeitlich)
- Zugriffsbeschränkungen (gemäß „Need-to-Know“ und „Least Privilege“)
- Protokollierung
 - Protokollierung des lesenden Zugriffs
 - Protokollierung des schreibenden Zugriffs
 - Protokollierung von unberechtigten Zugriffsversuchen
 - Anlassbezogene Auswertung
- Umsetzung von Regelungen zur Löschung von Daten
- Umsetzung von Regelungen zum Umgang mit elektronischen Speichermedien
- Umsetzung von Regelungen zur Entsorgung von Speichermedien

Trennungskontrolle

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

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

- Mandantenfähigkeit:
 - Physische Trennung
 - Trennung auf Systemebene
 - Trennung auf Datenebene
- Trennung von Produktiv- und Testsystemen
- Vorhandensein von Richtlinien und Arbeitsanweisungen
- Vorhandensein von Verfahrensdokumentationen

Pseudonymisierung und Verschlüsselung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen:

- Softwarebasierte Verschlüsselung bei Datenspeicherung
- Hardwarebasierte Verschlüsselung bei Datenspeicherung



2. Integrität

Weitergabekontrolle

Aspekte der Weitergabe und Übertragung personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle.

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

- Für elektronische Übertragungen:
 - Verschlüsselung der Datenübermittlung (z. B. VPN, S/MIME)
 - Durchführung von Protokollierungen der Datenweitergabe oder Übermittlung
- Auflistung der Empfänger der Daten

Eingabekontrolle

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

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

- Protokollierung der Eingaben
- Organisatorisch festgelegte Zuständigkeiten für die Eingabe

Zusätzliche Maßnahmen:

- Protokollierung der Eingabe, Änderung von Daten auf Dateiebene
- Nachvollziehbarkeit von Eingabe und Änderung von Daten durch individuelle Benutzernamen
- Rechtevergabe auf Basis eines Berechtigungskonzepts
- Eingeschränkte Zugriffsrechte auf erstellte Protokolldaten

3. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Maßnahmen zur Datensicherung (physisch/logisch):

- Regelmäßige Kontrolle des Systemzustands (Monitoring)
- Kurzfristige Wiederherstellbarkeit des normalen Systemzustands
- Backup- und Wiederanlaufkonzept (regelmäßige Datensicherungen)
 - Offline
 - Online



- Onsite
- Offsite
- Vorhandensein von redundanten IT-Systemen (z. B. Server, Speicher)
- Replizierbarkeit virtueller Maschinen
- Funktionsfähige physische Schutzeinrichtungen (Brandschutz, Energie: USV, Klima)
- Meldewege und Notfallpläne

Belastbarkeitskontrolle

Die Verarbeitung der Daten soll tolerant gegenüber Störungen und Fehlern sein.

- Virenschutz/Anti-Malware/Anti-Ransomware
- Firewall

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Schriftlich fixierte Regelungen der Verantwortlichkeiten für Datenschutz
- Schriftlich fixierte Regelungen der Verantwortlichkeiten für Informationssicherheit
- Existenz eines angemessenen Informationssicherheitsmanagements
- Regelmäßige Aufklärung und Sensibilisierung der Mitarbeiter und Führungskräfte
- Datenschutzfreundliche Voreinstellungen
- Auftragskontrolle, um weisungsgemäße Auftragsverarbeitung zu gewährleisten:
 - Strikte Einhaltung der im vorliegenden Auftragsverarbeitungs-Vertrag festgeschriebenen Vereinbarungen und diesbezügliche Überprüfungen
 - Konzept dahingehend, wie die regelmäßige Kontrolle des Auftragsprozesses erfolgt (z. B. Vorlage von Self-Assessments, Vorlage der Verträge mit Unterauftragnehmern, Durchführung von Kontrollen bei Subunternehmern durch den Auftragnehmer)
 - Keine Auftragsdatenverarbeitung ohne entsprechende Weisung des Auftraggebers, z. B. anhand: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.