Auftragsverarbeitungsvertrag nach Art. 28 DSGVO

zwischen

Ihnen
(nachfolgend “Auftraggeber”)

und

heylogin GmbH
Sophienstr. 40
38118 Braunschweig
(nachfolgend “Auftragnehmer“),

gemeinsam “Parteien“ genannt.

Präambel

Auftraggeber und Auftragnehmer haben einen Rahmenvertrag über die Nutzung der Passwortverwaltung heylogin geschlossen. Hierzu ist es notwendig, dass der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers verarbeitet.

Der Auftragnehmer hat einen externen Datenschutzbeauftragten bestellt:

Projekt 29 GmbH & Co. KG
Ostengasse 14
93047 Regensburg
E-Mail: privacy@heylogin.com

Dies vorausgeschickt schließen die Parteien hiermit die folgende Vereinbarung über Auftragsverarbeitung gemäß Art. 28 DSGVO (nachfolgend: “Vertrag“):

1 Gegenstand der Auftragsverarbeitung

1. Aus dem Rahmenvertrag und den – von den beauftragten Dienstleistungen abhängigen – Leistungsbeschreibungen ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Im Regelfall verarbeitet der Auftragnehmer folgende Daten für den Auftraggeber:

    - **Gespeicherte Daten in heylogin (z. B. Nutzernamen, Passwörter, Webseiten-URLs)**

  - **Art und Zweck der Verarbeitung:** Passwortmanagement. Die Daten werden ausschließlich Ende-zu-Ende-verschlüsselt übertragen und gespeichert. Eine Entschlüsselung oder inhaltliche Verarbeitung durch den Auftragnehmer ist technisch ausgeschlossen. Der Auftragnehmer beschränkt sich auf die sichere Synchronisation verschlüsselter Daten zwischen den Endgeräten des Auftraggebers. Eine detaillierte Auflistung der Ende-zu-Ende-verschlüsselten Daten findet sich im heylogin Security Whitepaper im Abschnitt “What we encrypt and how” (siehe https://www.heylogin.com/de/whitepaper).
  - **Kategorien betroffener Personen:** Nutzende von heylogin
- **Account- und Organisationsdaten**
  - **Art und Zweck der Verarbeitung:** Verwaltung von Accounts anhand der E-Mail-Adresse sowie Zuordnung zu einer oder mehreren heylogin-Organisationen. Diese Daten dienen ausschließlich der Authentifizierung und Lizenzverwaltung.
  - **Kategorien betroffener Personen:** Nutzende von heylogin
- **Protokoll- und Metadaten**
  - **Art und Zweck der Verarbeitung:** Verarbeitung von technischen Protokollen und Metadaten (z. B. Zeitstempel von Logins, technische Logs, IP-Adressen) ausschließlich zum Zweck der Systemsicherheit, Missbrauchserkennung und Fehleranalyse.
  - **Kategorien betroffener Personen:** Nutzende von heylogin
- **Support- und Gerätedaten**
  - **Art und Zweck der Verarbeitung:** Verarbeitung von Gerätedaten sowie von im Supportfall freiwillig übermittelten Inhalten (z. B. Screenshots, Anhänge, Textangaben) ausschließlich zur Fehlerbehebung und Unterstützung im Support. Eine weitergehende Nutzung oder Auswertung erfolgt nicht.
  - **Kategorien betroffener Personen:** Nutzende von heylogin

2. Die Dauer dieses Auftrags entspricht der Laufzeit des Rahmenvertrags.
3. Die Verarbeitung umfasst Erheben, Ordnen, Speichern, Auslesen, Verwenden, Übermitteln und Löschen personenbezogener Daten.

2 Anwendungsbereich und Verantwortlichkeit

1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Rahmenvertrag und in den dazugehörigen Leistungsbeschreibungen konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die

Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (”Verantwortlicher” im Sinne des Art. 4 Nr. 7 DSGVO).

2. Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

3 Rechte und Pflichten des Auftraggebers

1. Der Auftraggeber ist Verantwortlicher gemäß Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Als solcher hat er seine Mitarbeiter darüber zu informieren, welche Daten er erhebt und an den Auftragnehmer weiterleitet.
2. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
3. Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.
4. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

4 Pflichten des Auftragnehmers

1. 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 Artikel 28 Abs. 3 a) DSGVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.
2. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes

gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DSGVO) genügen und gewähren, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt sind. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

3. Eine aktuelle Liste der technischen und organisatorischen Maßnahmen liegt diesem Vertrag als **Anlage** bei.
4. Der Auftragnehmer kann diese Maßnahmen nach eigenem Ermessen ändern oder aktualisieren, sofern diese Änderungen oder Aktualisierungen dem jeweiligen Stand der Technik und den gesetzlichen Anforderungen entsprechen, und das bisherige, vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Der Auftragnehmer informiert den Auftraggeber über wesentliche Änderungen oder Aktualisierungen der Maßnahmen.
5. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er Grund zu der Annahme hat, dass die technischen und organisatorischen Maßnahmen nicht mehr ausreichend sind, um das vertraglich vereinbarte Schutzniveau zu halten und wird sich daraufhin mit dem Auftraggeber hinsichtlich weiterer technischer und organisatorischer Maßnahmen abstimmen.
6. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten.
7. Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten und wartet dessen Weisungen ab. Ohne entsprechende Einzelweisung wird der Auftragnehmer nicht mit der betroffenen Person in Kontakt treten.
8. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.
9. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.
10. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur

Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

11. Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.
12. Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.
13. Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.
14. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.
15. Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder vollständig und unwiderruflich zu löschen, sofern nicht eine gesetzliche Aufbewahrungsfrist dem entgegensteht. Dies gilt auch für Vervielfältigungen der Auftraggeberdaten beim Auftragnehmer, wie etwa Datensicherungen, nicht aber für Dokumentationen des Auftragnehmers, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung der Auftraggeberdaten dienen. Solche Dokumentationen sind vom Auftragnehmer für eine Dauer von zwei Jahren ab Beendigung aufzubewahren und auf Verlangen an den Auftraggeber zum Zwecke seiner Dokumentation herauszugeben. Der Auftragnehmer ist dadurch nicht gehindert, Dokumentationen unter den gesetzlichen Voraussetzungen länger aufzubewahren, maximal bis drei Monate nach Ablauf der gesetzlichen Verjährung etwaiger Ansprüche des Auftraggebers aus dem Vertragsverhältnis.
16. Auf Verlangen des Auftraggebers wird der Auftragnehmer dem Auftraggeber die Löschung schriftlich bestätigen.
17. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.
18. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, gilt § 3 (4) entsprechend.
19. Die Einrede des Zurückbehaltungsrechts im Sinne von § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten ausgeschlossen.

5 Nachweismöglichkeiten

1. Auf Anfrage weist der Auftragnehmer dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.
2. Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Die vorherige Anmeldung ist ausnahmsweise entbehrlich, wenn durch eine solche der Zweck der Kontrollmaßnahme nicht erreicht werden könnte. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.
3. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich (2) entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.
4. Der Auftragnehmer verarbeitet Daten durch mobiles Arbeiten oder in Privatwohnungen (Homeoffice). Die Maßnahmen nach Art. 32 DSGVO (”TOM“) stellt der Auftragnehmer auch in diesem Fall sicher.

6 Unterauftragsverarbeiter

1. Der Auftragnehmer setzt zur Datenverarbeitung im Rahmen dieses Vertrags geeignete Unterauftragsverarbeiter ein. Eine aktuelle Liste der eingesetzten Unterauftragsverarbeiter liegt diesem Vertrag als **Anlage** bei.
2. Der Auftragnehmer darf weitere und/oder andere Unterauftragsverarbeiter beauftragen, soweit der Auftragnehmer den Auftraggeber in Textform hierüber informiert und der Auftraggeber binnen einer Frist von vier Wochen ab Zugang der Information nicht wenigstens in Textform Einspruch gegen die beabsichtigte Beauftragung erhoben hat. Erfolgt innerhalb der genannten Frist kein Einspruch gegen die beabsichtigte Beauftragung, gilt dies als Zustimmung des Auftraggebers. Erhebt der Auftraggeber Einspruch, kann der Auftragnehmer nach eigener Wahl die Dienstleistungen ohne die beabsichtigte Beauftragung erbringen. Sofern die Erbringung der Dienstleistungen ohne die beabsichtigte Beauftragung

für dem Auftragnehmer nicht zumutbar oder möglich ist, hat er dies dem Auftraggeber unverzüglich mitzuteilen. Der Auftraggeber kann in diesem Fall den Hauptvertrag zwischen den Parteien innerhalb einer Frist von zwei Wochen ab Zugang der Mitteilung des Auftragnehmer schriftlich kündigen.

3. Der Auftragnehmer trägt dafür Sorge, dass nur solche Unterauftragsverarbeiter eingeschaltet werden, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen bestehen, so dass die Verarbeitung der personenbezogenen Daten des Auftraggebers im Einklang mit den Anforderungen der DSGVO und anwendbaren nationalen Datenschutzgesetzen erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet ist. Der Auftragnehmer wählt einen Unterauftragsverarbeiter unter besonderer Berücksichtigung der Eignung der vom Unterauftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus und wird die Einhaltung der gesetzlichen und vertraglichen datenschutzrechtlichen Anforderungen durch den Unterauftragsverarbeiter regelmäßig überprüfen.
4. Der Auftragnehmer stellt sicher, dass die zwischen ihm und dem Unterauftragsverarbeiter getroffene Vereinbarung in einem schriftlichen Vertrag geregelt ist, der mindestens dieselben Datenschutzpflichten für den Unterauftragsverarbeiter enthält, die in diesem Vertrag für den Auftragnehmers festgelegt sind. Soweit auf den Auftraggeber anwendbar, wird der Auftragnehmer im Verhältnis zum Unterauftragsverarbeiter darüber hinaus die für den Auftraggeber geltenden gesetzlichen, berufsrechtlichen oder sonstigen besonderen Geheimhaltungs- und Verschwiegenheitspflichten vertraglich vereinbaren, insbesondere solche, die sich aus spezialgesetzlichen Vorschriften für Berufsgeheimnisträger ergeben (z. B. § 43e BRAO).
5. Die Offenlegung von personenbezogenen Daten gegenüber einem Unterauftragsverarbeiter ist nur zulässig, wenn sich der Auftragnehmer dokumentiert davon überzeugt hat, dass der Unterauftragsverarbeiter seine Verpflichtungen vollständig erfüllt und ein Vertrag gemäß Art. 28 DSGVO geschlossen worden ist.
6. Der Auftragnehmer bleibt gegenüber dem Auftraggeber für die Einhaltung der Pflichten aus diesem Vertrag verantwortlich und haftet gegenüber dem Auftraggeber, wenn der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nachkommt.

7 Übermittlung in Drittländer

Die Datenverarbeitung findet ausschließlich im Bereich der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung der Verarbeitung in ein sonstiges Land (“Drittland”), einschließlich durch Einschaltung etwaiger Unterauftragsverarbeiter, be-

darf der vorherigen Einwilligung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen für Datenexporte in Drittländer (insb. Art. 44 ff. DSGVO) erfüllt sind.

8 Haftung

Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen nach den gesetzlichen Bestimmungen des Art. 82 DSGVO. Eine Haftung des Auftragnehmers gegenüber dem Auftraggeber wegen Verletzung von Pflichten aus diesem Vertrag bzw. dem Rahmenvertrag bleibt hiervon unberührt.

9 Laufzeit

1. Dieser Auftragsverarbeitungsvertrag tritt automatisch mit dem Tag der Vertragsunterzeichnung des Rahmenvertrags in Kraft und bleibt bis zur Beendigung des Rahmenvertrags wirksam. Wenn gewünscht, kann er auch zusätzlich von beiden Parteien unterschrieben werden.
2. Ist der Rahmenvertrag ordentlich kündbar, gelten die Regelungen zur ordentlichen Kündigung entsprechend. Im Zweifel gilt eine Kündigung des Rahmenvertrags auch als Kündigung dieses Vertrags und eine Kündigung dieses Vertrages als Kündigung des Rahmenvertrages.
3. Der Auftraggeber ist jederzeit zu einer außerordentlichen Kündigung dieses Vertrages aus wichtigem Grund berechtigt. Ein wichtiger Grund liegt vor, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DSGVO vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will. Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Auftraggeber dem Auftragnehmer zunächst eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann. Nach fruchtlosem Ablauf dieser Frist steht dem Auftraggeber sodann das Recht zur außerordentlichen Kündigung zu.

10 Informationspflichten, Schriftformklausel, Rechtswahl

1. Sollten die Daten des Auftraggebers beim Auftragnehmer 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 schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
3. Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.
4. Anwendbares Recht und Gerichtsstand richten sich nach dem Hauptvertrag.

Anlagen

- Technische & Organisatorische Maßnahmen (TOMs)
- Liste der Unterauftragsverarbeiter