BOB
YOUR BUYOUT BUDDY

Allgemeine Geschäftsbedingungen

der EVERYDAY PEOPLE GmbH für Buyout Buddy

Präambel

Diese Allgemeinen Geschäftsbedingungen regeln die Nutzung der Software „Buyout Buddy“ (nachfolgend „Software“), welche von der EVERYDAY PEOPLE GmbH, Neusser Str. 467, 50733 Köln (nachfolgend „Bereitstellende Partei“) als Software as a Service (SaaS) über das Internet zur Verfügung gestellt wird. Der Geltungsbereich dieser Allgemeinen Geschäftsbedingungen beschränkt sich auf Unternehmen im Sinne von § 14 BGB. Eine Nutzung durch Verbrauchende im Sinne von § 13 BGB ist ausgeschlossen. Mit Vertragsabschluss wird versichert, dass ein Handeln als Unternehmen im Sinne von § 14 BGB vorliegt. Ein Vertragsschluss mit Verbrauchenden ist ausgeschlossen.

§ 1 Begriffsdefinitionen

(1) Nutzungsberechtigte Partei ist ausschließlich das vertragsschließende Unternehmen im Sinne von § 14 BGB für seine eigenen geschäftlichen Zwecke.
(2) Die Nutzungsberechtigung umfasst ausschließlich:

- Mitarbeitende in einem arbeitsvertraglichen Verhältnis zur nutzungsberechtigten Partei
- Geschäftsführende und andere vertretungsberechtigte Organe der nutzungsberechtigten Partei

(3) Eine Übertragung oder Erweiterung der Nutzungsberechtigung auf andere natürliche oder juristische Personen, insbesondere verbundene Unternehmen, ist ohne vorherige schriftliche Zustimmung der bereitstellenden Partei nicht gestattet.
(4) Die bereitstellende Partei ist berechtigt, die Nutzungsberechtigung einzelner Personen bei Vorliegen eines wichtigen Grundes zu widerrufen.

§ 2 Vertragsgegenstand

(1) Gegenstand ist die entgeltliche Bereitstellung der Software zur Nutzung über das Internet sowie die Bereitstellung von Speicherplatz für die durch Softwarenutzung erzeugten und zur Nutzung erforderlichen Daten.
(2) Die Software wird in ihrer jeweils aktuellsten Version am Routerausgang des Rechenzentrums („Übergabepunkt“) zur Nutzung bereitgestellt.

§ 3 Leistungsumfang

(1) Die Software wird in ihrer jeweils aktuellsten Version zur Nutzung über das Internet bereitgestellt. Die Bereitstellung erfolgt auf einem Server mit Internetzugang für die nutzungsberechtigte Partei.
(2) Der Funktionsumfang der Software sowie die technischen Anforderungen sind in der aktuellen Leistungsbeschreibung auf der Website aufgeführt.
(3) Die Dokumentation der wesentlichen Funktionen der Software steht in Form einer FAQ auf der Webseite zur Verfügung. Die Zugangsdaten legt die nutzungsberechtigte Partei bei der Erstregistrierung selbstständig fest.
(4) Die Software kann jederzeit aktualisiert und weiterentwickelt werden, insbesondere aufgrund geänderter Rechtslage, technischer Entwicklungen oder zur Verbesserung der IT-Sicherheit. Über wesentliche Änderungen erfolgt eine Information mit angemessener Frist.
(5) Es wird Speicherplatz im vereinbarten Umfang zur Verfügung gestellt. Die Abrufbarkeit der gespeicherten Daten wird im Rahmen der technischen Verfügbarkeit gewährleistet.

§ 4 Nutzungsrechte

(1) Die Nutzungsrechte an der Software werden nicht-exklusiv, zeitlich auf die Vertragsdauer beschränkt, nicht übertragbar und nicht unterlizenzierbar im vertraglich vereinbarten Umfang eingeräumt.
(2) Die Nutzung der Software ist auf eigene geschäftliche Zwecke durch das eigene Personal beschränkt.
(3) Eine physische Überlassung der Software erfolgt nicht.

§ 5 Verfügbarkeit

(1) Die bereitstellende Partei gewährt eine Gesamtverfügbarkeit der Leistungen von mindestens 98,5% im Jahresmittel am Übergabepunkt. Der Übergabepunkt ist der Routerausgang des Rechenzentrums der bereitstellenden Partei.
(2) Als Verfügbarkeit gilt die Möglichkeit der nutzungsberechtigten Partei, die wesentlichen Funktionen der Software zu nutzen. Bei der Berechnung der Verfügbarkeit bleiben Wartungszeiten, Störungen aufgrund höherer Gewalt, Störungen im Verantwortungsbereich der nutzungsberechtigten Partei, geplante und angekündigte Wartungsarbeiten sowie Zeiten unerheblicher Störungen, die die Nutzung der Software nicht wesentlich beeinträchtigen, unberücksichtigt.
(3) Die bereitstellende Partei wird sich im Rahmen ihrer betrieblichen und technischen Möglichkeiten um eine angemessene Störungsbeseitigung bemühen.

§ 6 Nutzungspflichten

(1) Die zur Verfügung gestellten Zugangsdaten sind geheim zu halten und vor unberechtigtem Zugriff zu schützen.
(2) Bei der Nutzung der Software dürfen keine Rechte Dritter verletzt oder gegen geltendes Recht verstoßen werden.
(3) Für die regelmäßige Datensicherung ist selbst Sorge zu tragen.

BOB
YOUR BUYOUT BUDDY

§ 7 Vergütung und Preisanpassung

(1) Die Vergütung bestimmt sich nach der aktuellen Preisliste und dem gewählten Abomodell.
(2) Alle Preise verstehen sich zuzüglich gesetzlicher Umsatzsteuer.
(3) Eine Anpassung der Preise ist mit einer Ankündigungsfrist von 30 Tagen möglich. Die Ankündigung erfolgt per E-Mail an die hinterlegte E-Mail-Adresse.
(4) Bei Preiserhöhungen besteht ein Sonderkündigungsrecht. Die Kündigung muss innerhalb von 30 Tagen nach Mitteilung der Preiserhöhung erfolgen und wird zum Zeitpunkt des Inkrafttretens der Preiserhöhung wirksam.
(5) Unabhängig von Abs. 3 ist eine jährliche Preisanpassung in Höhe der Inflationsrate gemäß dem vom Statistischen Bundesamt festgestellten Verbraucherpreisindex für Deutschland möglich. Diese Anpassung ist mit einer Frist von 30 Tagen anzukündigen und löst kein Sonderkündigungsrecht aus.

§ 8 Zahlungsbedingungen

(1) Die Zahlung der Vergütung erfolgt ausschließlich im Voraus:
- bei monatlicher Zahlungsweise: zu Beginn jedes Vertragsmonats
- bei jährlicher Zahlungsweise: zu Beginn jedes Vertragsjahres

(2) Die Zahlungsabwicklung erfolgt über den Zahlungsdienstleister Stripe (Stripe Payments Europe, Ltd., 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, Irland). Es gelten zusätzlich die Nutzungsbedingungen von Stripe (abrufbar unter stripe.com/de/legal).
(3) Für die Zahlungsabwicklung werden die erforderlichen Zahlungsdaten an Stripe übermittelt und dort verarbeitet. Mit der Angabe der Zahlungsinformationen wird Stripe zur Einziehung der fälligen Entgelte ermächtigt.
(4) Die Zahlung ist nur über die von Stripe angebotenen Zahlungsmethoden möglich. Die Auswahl der jeweils verfügbaren Zahlungsmethoden obliegt Stripe.
(5) Die Abrechnung erfolgt automatisiert. Die Rechnungen werden elektronisch im Kundenbereich der Software bereitgestellt oder per E-Mail versandt.
(6) Im Fall einer fehlgeschlagenen Zahlung oder Rücklastschrift sind die dadurch entstehenden Bankgebühren zu erstatten. Zudem kann eine Bearbeitungsgebühr gemäß aktueller Preisliste erhoben werden.
(7) Bei Zahlungsverzug kann der Zugang zur Software nach vorheriger Ankündigung bis zum Ausgleich aller fälligen Beträge gesperrt werden. Die Zahlungspflicht für den Zeitraum der Sperrung bleibt unberührt.
(8) Eine Aufrechnung ist nur mit unbestrittenen oder rechtskräftig festgestellten Forderungen zulässig.

§ 9 Abomodelle und Testphase

(1) Es werden Abomodelle mit monatlicher oder jährlicher Zahlungsweise angeboten. Die Konditionen sind der aktuellen Preisliste zu entnehmen.
(2) Vor Abschluss eines kostenpflichtigen Abonnements kann eine kostenlose Testphase von 30 Tagen gewährt werden.
(3) Während der Testphase kann der Zugang jederzeit ohne Angabe von Gründen beendet werden.
(4) Nach Ablauf der Testphase erfolgt ohne ausdrücklichen Widerspruch die automatische Umwandlung in das gewählte kostenpflichtige Abonnement. Hierauf wird spätestens 7 Tage vor Ablauf der Testphase per E-Mail hingewiesen.
(5) Die Testversion kann in ihrem Funktionsumfang gegenüber der kostenpflichtigen Version eingeschränkt sein.
(6) Ein Wechsel in ein höherwertiges Abonnement (Upgrade) ist jederzeit möglich. Die Berechnung erfolgt anteilig ab dem Zeitpunkt der Umstellung.
(7) Ein Wechsel in ein niedrigerwertiges Abonnement (Downgrade) ist zum Ende der jeweiligen Vertragslaufzeit möglich. Die Ankündigung muss mit einer Frist von 14 Tagen erfolgen.
(8) Bei Upgrades oder Downgrades bleiben gespeicherte Daten und Einstellungen im Rahmen der technischen Möglichkeiten erhalten.
(9) Die Übertragung von Lizenzen auf andere Unternehmen bedarf der vorherigen schriftlichen Zustimmung.

§ 10 Datenschutz und Vertraulichkeit

(1) Die einschlägigen datenschutzrechtlichen Vorschriften sind einzuhalten.
(2) Soweit der Auftragnehmer im Rahmen der Softwarenutzung personenbezogene Daten im Auftrag der nutzungsberechtigten Partei verarbeitet, gelten die Regelungen der Auftragsverarbeitung gemäß Anlage 1 zu diesen AGB. Die Regelungen zur Auftragsverarbeitung werden mit Abschluss dieser AGB automatisch Vertragsbestandteil. Eine separate Unterzeichnung ist nicht erforderlich.
(3) Vertrauliche Informationen aus dieser Vereinbarung sind geheim zu halten.

§ 11 Vertragslaufzeit und Kündigung

(1) Die Mindestvertragslaufzeit richtet sich nach dem Abomodell:
- Monatliche Zahlung: ein Monat Mindestlaufzeit
- Jährliche Zahlung: ein Jahr Mindestlaufzeit

(2) Nach Ablauf verlängert sich der Vertrag automatisch um die jeweilige Laufzeit des gewählten Abomodells ohne fristgerechte Kündigung.
(3) Kündigungsfristen:
- Bei monatlicher Zahlung: 14 Tage zum Monatsende
- Bei jährlicher Zahlung: drei Monate zum Laufzeitende

(4) Die Kündigung kann über die Anwendung selbst, über das Zahlungsdienstleistungsunternehmen oder in Textform (z.B. per E-Mail) erfolgen.
(5) Das Recht zur außerordentlichen Kündigung bleibt unberührt.
(6) Mit Vertragsende erlöschen alle Nutzungsrechte an der Software.

§ 12 Gewährleistung

(1) Die Software wird in der jeweils verfügbaren Version bereitgestellt. Eine bestimmte Beschaffenheit der Software wird nicht garantiert.
(2) Die Gewährleistung für nur unerhebliche Minderungen der Tauglichkeit ist ausgeschlossen. Insbesondere stellen technische Störungen, die auf höherer Gewalt oder auf der technischen Infrastruktur des Kunden beruhen, keinen Mangel dar.
(3) Die verschuldensunabhängige Haftung gemäß § 536a Abs. 1 BGB für bereits bei Vertragsschluss vorhandene Mängel wird ausdrücklich ausgeschlossen.
(4) Mängel sind unverzüglich nach Entdeckung in Textform unter detaillierter Beschreibung der Fehlersymptome zu melden. Der Kunde hat im Rahmen des Zumutbaren die Maßnahmen zu treffen, die eine Feststellung und Analyse der Mängel ermöglichen.
(5) Die Behebung von Mängeln erfolgt nach Wahl der bereitstellenden

Partei durch kostenfreie Nachbesserung oder Ersatzlieferung.
(6) Ein Kündigungsrecht wegen Nichtgewährung des Gebrauchs nach § 543 Abs. 2 Nr. 1 BGB besteht erst dann, wenn die Nachbesserung wiederholt fehlgeschlagen und dem Kunden ein weiteres Abwarten unzumutbar ist.

§ 13 Haftung

(1) Die bereitstellende Partei haftet unbeschränkt nur für Vorsatz und grobe Fahrlässigkeit sowie für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit.
(2) Für leichte Fahrlässigkeit wird nur bei Verletzung wesentlicher Vertragspflichten (Kardinalpflichten) gehaftet. Die Haftung ist in diesem Fall begrenzt auf den vertragstypischen, vorhersehbaren Schaden und maximal auf die Höhe des jährlichen Nutzungsentgelts.
(3) Die Haftung für mittelbare und unvorhersehbare Schäden, Produktions- und Nutzungsausfall, entgangenen Gewinn, ausgebliebene Einsparungen und Vermögensschäden wegen Ansprüchen Dritter ist im Falle leichter Fahrlässigkeit ausgeschlossen.
(4) Die verschuldensunabhängige Haftung für anfängliche Mängel nach § 536a Abs. 1 Alt. 1 BGB wird ausgeschlossen.
(5) Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt.
(6) Eine Haftung für den Verlust von gespeicherten Daten besteht nicht, wenn der Schaden bei ordnungsgemäßer Datensicherung durch den Kunden nicht eingetreten wäre. Der Kunde hat seine Daten regelmäßig in anwendungsadäquaten Intervallen, mindestens einmal täglich, in geeigneter Form zu sichern.
(7) Soweit die Haftung nach den vorstehenden Vorschriften ausgeschlossen oder beschränkt wird, gilt dies auch für die persönliche Haftung der Organe, Erfüllungsgehilfen und Mitarbeitenden der bereitstellenden Partei.
(8) Die bereitstellende Partei haftet nicht für die Funktionsfähigkeit der Telekommunikationsverbindung (Internet-/Mobilfunkverbindung) zum Server, bei Stromausfällen sowie für die Funktionsfähigkeit der jeweiligen Zugangswege zu den Servern.
(9) Eine verschuldensunabhängige Garantiehaftung für bereits bei Vertragsschluss vorhandene Mängel wird ausdrücklich ausgeschlossen.
(10) Ansprüche auf Schadensersatz verjähren innerhalb von zwölf Monaten ab Kenntnis der anspruchsbegründenden Umstände.

§ 14 Schlussbestimmungen

(1) Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.
(2) Ausschließlicher Gerichtsstand ist Köln.
(3) Änderungen dieser AGB werden spätestens zwei Monate vor dem vorgeschlagenen Wirksamwerden in Textform mitgeteilt.
(4) Die Unwirksamkeit einzelner Bestimmungen berührt nicht die Wirksamkeit der übrigen Bestimmungen.

Stand: 7. Januar 2025

EVERYDAY PEOPLE GmbH
Neusser Str. 467
50733 Köln

BOB
YOUR BUYOUT BUDDY

Anlage 1 zu den AGB – Regelungen zur Auftragsverarbeitung

Präambel

Diese Anlage konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien, die sich aus der Nutzung der Software „Buyout Buddy“ gemäß den Allgemeinen Geschäftsbedingungen der EVERYDAY PEOPLE GmbH ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Software as a Service (SaaS) Vertrag in Verbindung stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

1. Allgemeines

(1) In dieser Anlage bezeichnet der Begriff „Auftragnehmer“ die EVERYDAY PEOPLE GmbH als bereitstellende Partei gemäß den AGB und der Begriff „Auftraggeber“ das vertragsschließende Unternehmen als nutzungsberechtigte Partei gemäß den AGB.
(2) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 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.
(3) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2. Gegenstand des Auftrags

Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen ergeben sich aus der nachfolgenden Festlegung:

1. Gegenstand und Zweck der Verarbeitung:

- Bereitstellung und Betrieb der Software „Buyout Buddy“ als SaaS-Lösung
- Speicherung und Verarbeitung von Daten zur Nutzung der Software gemäß den Funktionalitäten aus der aktuellen Leistungsbeschreibung
- Support und Wartung der Software

2. Art der personenbezogenen Daten:

- Bestandsdaten der Nutzer (Name, E-Mail, Zugangsdaten)
- Nutzungsdaten der Software
- Kundendaten, die im Rahmen der Softwarenutzung verarbeitet werden

3. Kategorien betroffener Personen:

- Mitarbeitende des Auftraggebers
- Kunden des Auftraggebers
- Auftraggeber als Einzelunternehmer
- Sonstige Personen, deren Daten durch den Auftraggeber in der Software verarbeitet werden

3. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 3 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.
(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.
(3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) erfolgen.
(4) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.
(5) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.
(6) 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.

4. Allgemeine Pflichten des Auftragnehmers

(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. 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. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.
(2) Der Auftragnehmer wird die Datenverarbeitung im Auftrag grundsätzlich in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchführen. Dem Auftragnehmer ist eine Datenverarbeitung auch außerhalb von EU oder EWR erlaubt, wenn entsprechende Unterauftragnehmer im Drittland unter Einhaltung der Voraussetzungen von Ziff. 9 eingesetzt werden

und die Voraussetzungen der Art. 44-48 DSGVO erfüllt sind bzw. eine Ausnahme i.S.d. Art. 49 DSGVO vorliegt.
(3) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

5. Datenschutzbeauftragter des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Der Auftragnehmer wird dem Auftraggeber den Namen und die Kontaktdaten seines Datenschutzbeauftragten gesondert in Textform mitteilen.
(2) Die Pflicht zur Benennung eines Datenschutzbeauftragten nach Absatz 1 kann im Ermessen des Auftraggebers entfallen, wenn der Auftragnehmer nachweisen kann, dass er gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu bestellen und der Auftragnehmer nachweisen kann, 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.

6. 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. 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 gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.
(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 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.

7. Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 12 dieses Vertrages.
(2) Der Auftragnehmer wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber mit. Er hat dem Auftraggeber die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.
(3) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

8. Regelung zu mobilen Arbeitsplätzen

(1) Der Auftragnehmer darf seinen Beschäftigten, die mit der Verarbeitung von personenbezogenen Daten für den Auftraggeber beauftragt sind, die Verarbeitung von personenbezogenen Daten an mobilen Arbeitsplätzen außerhalb der Geschäftsräume des Auftragnehmers erlauben.
(2) Der Auftragnehmer hat sicherzustellen, dass die Einhaltung der vertraglich vereinbarten technischen und organisatorischen Maßnahmen auch bei der Nutzung von mobilen Arbeitsplätzen der Beschäftigten des Auftragnehmers gewährleistet ist. Abweichungen von einzelnen vertraglich vereinbarten technischen und organisatorischen Maßnahmen sind vorab mit dem Auftraggeber abzustimmen und von diesem in Textform zu genehmigen.
(3) Der Auftragnehmer trägt insbesondere Sorge dafür, dass bei einer Verarbeitung von personenbezogenen Daten an mobilen Arbeitsplätzen die Speicherorte so konfiguriert werden, dass eine lokale Speicherung von Daten auf IT-Systemen ausgeschlossen ist. Sollte dies nicht möglich sein, hat der Auftragnehmer Sorge dafür zu tragen, dass die lokale Speicherung ausschließlich verschlüsselt erfolgt und andere am Ort des jeweiligen mobilen Arbeitsplatzes befindliche Personen keinen Zugriff auf diese Daten erhalten.
(4) Der Auftragnehmer ist verpflichtet, Sorge dafür zu tragen, dass eine wirksame Kontrolle der Verarbeitung personenbezogener Daten im Auftrag an mobilen Arbeitsplätzen durch den Auftraggeber möglich ist.
(5) Sofern auch bei Unterauftragnehmern Beschäftigte an mobilen Arbeitsplätzen eingesetzt werden sollen, gelten die Regelungen der Absätze 1 bis 4 entsprechend.

9. Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, 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 Auftrag-

nehmer im erforderlichen Umfang zu kontrollieren.
(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.
(3) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören. Die Parteien gehen davon aus, dass eine Kontrolle höchstens einmal jährlich erforderlich ist. Weitere Prüfungen sind vom Auftraggeber unter Angabe des Anlasses zu begründen. Im Falle von Vor-Ort-Kontrollen wird der Auftraggeber dem Auftragnehmer die entstehenden Aufwände inkl. der Personalkosten für die Betreuung und Begleitung der Kontrollpersonen vor Ort in angemessenen Umfang ersetzen. Die Grundlagen der Kostenberechnung werden dem Auftraggeber vom Auftragnehmer vor Durchführung der Kontrolle mitgeteilt.
(4) Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen anstatt einer Vor-Ort-Kontrolle auch durch die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß Anlage 3 zu diesem Vertrag zu überzeugen. Sollte der Auftraggeber begründete Zweifel an der Eignung des Prüfdokuments i.S.d. Satzes 1 haben, kann eine Vor-Ort-Kontrolle durch den Auftraggeber erfolgen. Dem Auftraggeber ist bekannt, dass eine Vor-Ort-Kontrolle in Rechenzentren nicht oder nur in begründeten Ausnahmefällen möglich ist.
(5) 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.
(6) Die Parteien sind sich darüber einig, dass die Kontrollmaßnahmen bei einer Verarbeitung von personenbezogenen Daten an mobilen Arbeitsplätzen zur Wahrung der Persönlichkeitsrechte von weiteren Personen an diesen mobilen Arbeitsplätzen primär durch eine Kontrolle der Sicherstellung der vom Auftragnehmer nach Ziff. 8 Abs. 2 und 3 zu treffenden Maßnahmen erfolgt. Anlassbezogen ist dem Auftraggeber auch eine Kontrolle des mobilen Arbeitsplatzes von Beschäftigten durch den Auftragnehmer zu ermöglichen.

10. Unterauftragsverhältnisse

(1) Der Auftragnehmer ist berechtigt, die in der Anlage A zu diesem Vertrag angegebenen Unterauftragnehmer für die Verarbeitung von Daten im Auftrag einzusetzen. Der Wechsel von Unterauftragnehmern oder die Beauftragung weiterer Unterauftragnehmer ist unter den in Absatz 2 genannten Voraussetzungen zulässig.
(2) 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. Der Auftragnehmer wird den Auftraggeber im Falle eines geplanten Wechsels eines Unterauftragnehmers oder bei geplanter Beauftragung eines neuen Unterauftragnehmers rechtzeitig, spätestens aber 2 Wochen vor dem Wechsel bzw. der Neubeauftragung in Textform informieren („Information"). Der Auftraggeber hat das Recht, dem Wechsel oder der Neubeauftragung des Unterauftragnehmers aus wichtigem Grund unter Angabe einer Begründung in Textform binnen einer Woche nach Zugang der „Information" zu widersprechen. Ein wichtiger Grund liegt insbesondere vor, wenn objektive Anhaltspunkte dafür bestehen, dass der neue Unterauftragnehmer die datenschutzrechtlichen Anforderungen nicht erfüllen kann. Der Widerspruch kann vom Auftraggeber jederzeit in Textform zurückgenommen werden. Erfolgt kein Widerspruch innerhalb der Frist, gilt dies als Zustimmung zur Änderung bzw. Neubeauftragung. Im Falle eines berechtigten Widerspruchs kann der Auftragnehmer nach seiner Wahl entweder von der Änderung/Neubeauftragung absehen oder das Vertragsverhältnis mit einer Frist von einem Monat zum Monatsende kündigen.

11. Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet.
(2) Der Auftragnehmer hat seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut gemacht und zur Vertraulichkeit verpflichtet.
(3) Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Auftraggeber auf Anfrage nachzuweisen.

12. 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, 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 Auf-

tragnehmer entstehen, bleiben unberührt.

13. Haftung

(1) Für die Haftung des Auftragnehmers gelten die Haftungsbeschränkungen der AGB entsprechend. Die Haftung ist insbesondere:
a) bei leichter Fahrlässigkeit auf den vertragstypischen, vorhersehbaren Schaden begrenzt und maximal auf die Höhe des jährlichen Nutzungsentgelts beschränkt;
b) für mittelbare und unvorhersehbare Schäden, Produktions- und Nutzungsausfall, entgangenen Gewinn, ausgebliebene Einsparungen und Vermögensschäden wegen Ansprüchen Dritter im Falle leichter Fahrlässigkeit ausgeschlossen.
(2) Die verschuldensunabhängige Haftung für anfängliche Mängel wird ausgeschlossen.
(3) Die vorstehenden Haftungsbeschränkungen gelten nicht bei Vorsatz, grober Fahrlässigkeit, der Verletzung von Leben, Körper oder Gesundheit sowie bei Ansprüchen nach dem Produkthaftungsgesetz.

14. 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.

15. Vergütung

Etwaige Regelungen zu einer Vergütung von Leistungen sind zwischen den Parteien gesondert zu vereinbaren.

16. Technische und organisatorische Maßnahmen zur Datensicherheit

(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 aus Art. 32 DSGVO.
(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als Anlage B zu diesem Vertrag beigefügt. 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 einmal jährlich oder bei begründeten Anlässen eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

17. Dauer des Auftrags

(1) Der Vertrag beginnt mit Vertragsschluss und läuft für die Dauer des zwischen den Parteien bestehenden Hauptvertrages (Nutzung der Software „Buyout Buddy“ gemäß den Allgemeinen Geschäftsbedingungen).
(2) 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, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.
(3) Die Verpflichtungen aus diesem Vertrag gelten über die Beendigung des Hauptvertrages hinaus fort, solange der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber überlassen wurden oder die er für diesen erhoben hat. Dies gilt insbesondere für:

- Die Geheimhaltungspflichten
- Die Pflichten zur Unterstützung des Auftraggebers bei der Erfüllung der Betroffenenrechte
- Die Pflichten im Zusammenhang mit der Löschung oder Rückgabe der Daten nach Beendigung der Verarbeitung
- Die Pflicht zur Aufbewahrung von Dokumentationen und Nachweisen gemäß den gesetzlichen Aufbewahrungspflichten

18. Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren.
(2) Der Auftragnehmer darf personenbezogene Daten, die im Zusammenhang mit dem Auftrag verarbeitet worden sind, über die Beendigung des Vertrages hinaus speichern, wenn und soweit den Auftragnehmer eine gesetzliche Pflicht zur Aufbewahrung trifft. In diesen Fällen dürfen die Daten nur für Zwecke der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht sind die Daten unverzüglich zu löschen.

19. 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.

20. Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.
(2) Für Nebenabreden ist die Schriftform erforderlich.
(3) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt

BOB
YOUR BUYOUT BUDDY

dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Anlage A - Unterauftragnehmer

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

1. Stripe Payments Europe, Ltd.
- Anschrift: 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, Irland
- Leistung: Zahlungsabwicklung für die Nutzungsentgelte
- Verarbeitung: Zahlungsdaten der nutzungsberechtigten Partei

2. Microsoft Ireland Operations Limited
- Anschrift: One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland
- Leistungen:
- Microsoft Azure: Cloud-Hosting der Software und Datenspeicherung
- Microsoft Entra: Identitäts- und Zugriffsmanagement
- Verarbeitung:
- Azure: Alle im Rahmen der Softwarenutzung verarbeiteten Daten
- Entra: Authentifizierungs- und Identitätsdaten der Nutzer

Anlage B - Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO. Die Maßnahmen unterscheiden sich nach den Verarbeitungsorten:
- Büroräume des Auftragnehmers: Hier finden Zugriffe auf die Daten statt
- Microsoft Azure Cloud: Hier werden die Daten gespeichert und verarbeitet

1. Vertraulichkeit

1.1 Zutrittskontrolle

Büroräume:
- Verschließbare Eingangstüren mit dokumentierter Schlüsselvergabe
- Besucherregelung (Besucher werden empfangen und begleitet)
- Verschließbare Büroräume
- Dokumentierte Schlüsselverwaltung

Azure-Rechenzentrum:
- Die physische Sicherheit wird durch Microsoft Azure gemäß ISO 27001 und weiterer Standards gewährleistet
- Details zu den Sicherheitsmaßnahmen der Azure-Rechenzentren sind dokumentiert unter: https://docs.microsoft.com/de-de/azure/security/fundamentals/physical-security

1.2 Zugangskontrolle

Büroräume/Arbeitsplätze:
- Persönliche Benutzerkonten für jeden Mitarbeiter
- Kennwortrichtlinie (min. 10 Zeichen, Komplexität erforderlich)
- Automatische Bildschirmsperre nach 10 Minuten
- Verschlüsselung von Laptops und mobilen Datenträgern
- Aktuelle Antivirensoftware auf allen Systemen
- Aktivierte Firewall auf allen Systemen

Azure-Cloud:
- Zugriff auf Azure-Ressourcen nur über verschlüsselte Verbindung (HTTPS/TLS)
- Multi-Faktor-Authentifizierung für Azure-Administratoren
- Zugangsdaten werden sicher verwahrt
- Regelmäßige Überprüfung der Azure-Berechtigungen

1.3 Zugriffskontrolle

Büroräume:
- Dokumentierte Benutzerberechtigungen
- Mindestberechtigungsprinzip
- Löschung/Änderung von Berechtigungen bei Personalwechsel
- Sichere Aktenaufbewahrung
- Datenschutzgerechte Vernichtung von Papierunterlagen (Shredder mind. Sicherheitsstufe P-4)

Azure-Cloud:
- Rollenbasierte Zugriffskontrolle (RBAC)
- Protokollierung aller administrativen Zugriffe
- Regelmäßige Überprüfung der Cloud-Berechtigungen
- Verschlüsselte Datenspeicherung

1.4 Trennungskontrolle

Büroräume:
- Logische Mandantentrennung in verwendeten Anwendungen
- Getrennte Ablagestruktur für verschiedene Projekte/Kunden

Azure-Cloud:
- Mandantentrennung durch Azure-Architektur
- Getrennte Speicherbereiche für verschiedene Kunden/Zwecke
- Separate Entwicklungs- und Produktivumgebungen

2. Integrität

2.1 Eingabekontrolle

Büroräume:
- Protokollierung von wesentlichen Datenbankänderungen
- Nachvollziehbarkeit durch personalisierte Benutzerkonten

Azure-Cloud:
- Umfassende Protokollierung durch Azure Monitor
- Audit-Logs für alle relevanten Änderungen

2.2 Weitergabekontrolle

Büroräume:
- Verschlüsselte E-Mail-Kommunikation (TLS)
- Richtlinien zur sicheren Datenübertragung

Azure-Cloud:
- Verschlüsselte Datenübertragung (HTTPS/TLS)
- Gesicherte API-Zugriffe
- Azure Private Link für sensitive Verbindungen

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Büroräume:
- Regelmäßige Updates von Systemen und Software
- Dokumentierte Backup-Strategie für lokale Daten
- Brandmelder in Büroräumen

Azure-Cloud:
- Automatische Skalierung der Ressourcen
- Redundante Datenspeicherung
- Georedundante Backups

- 99,9% Verfügbarkeits-SLA durch Azure
- Automatische Failover-Mechanismen

3.2 Wiederherstellbarkeit

Büroräume:

- Dokumentierte Wiederherstellungsprozeduren
- Regelmäßige Tests der Backup-Wiederherstellung

Azure-Cloud:

- Automatisierte Backup-Prozesse
- Point-in-Time-Recovery Möglichkeiten
- Disaster Recovery Plan
- Replikation zwischen Azure-Regionen

4. Verfahren zur regelmäßigen Überprüfung

4.1 Datenschutz-Management

- Bestellung eines externen Datenschutzbeauftragten
- Jährliche Datenschutzschulungen für alle Mitarbeiter
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Dokumentierte Datenschutzrichtlinien
- Führung eines Verarbeitungsverzeichnisses

4.2 Incident-Response

- Dokumentierter Prozess für Datenpannen
- Meldeketten für Sicherheitsvorfälle
- Zusammenarbeit mit Azure Security Center
- Einbindung des Datenschutzbeauftragten bei Vorfällen

4.3 Datenschutzfreundliche Voreinstellungen

- Datensparsamkeit als Grundsatz
- Regelmäßige Überprüfung der Sicherheitseinstellungen
- Dokumentation von Änderungen an Sicherheitsmaßnahmen

Der Auftragnehmer ist berechtigt, die technischen und organisatorischen Maßnahmen weiterzuentwickeln und an den technischen Fortschritt und rechtliche Entwicklungen anzupassen, solange das hier dokumentierte Sicherheitsniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber auf Anfrage zur Verfügung zu stellen. Unwesentliche Änderungen können ohne vorherige Abstimmung vorgenommen werden. Als unwesentlich gelten solche Änderungen, die die Sicherheit der Datenverarbeitung nicht negativ beeinflussen.
Der Auftragnehmer kann zur Erfüllung der technischen und organisatorischen Maßnahmen auch gleichwertige alternative Maßnahmen einsetzen, sofern diese ein mindestens gleichwertiges Schutzniveau gewährleisten. Eine vorherige Abstimmung mit dem Auftraggeber ist nur bei wesentlichen Änderungen erforderlich.

Stand: 7. Januar 2025