Anhang 1: Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen gemäß Art. 28 DSGVO **(„AVV“)**

Vereinbarung über Auftragsverarbeitung zwischen der payever GmbH, Rödingsmarkt 20, 20459 („**Auftragnehmer**“) und ihrem Geschäftskunden („**Auftraggebern**“)

1 Vertragsgegenstand

Im Rahmen der Leistungserbringung gemäß den Allgemeinen Geschäftsbedingungen Geschäftskunden (nachfolgend „**Hauptvertrag**“ genannt) ist es erforderlich, dass der Auftragnehmer personenbezogene Daten verarbeitet, für die der Auftraggeber Verantwortlicher im Sinne der datenschutzrechtlichen Vorschriften ist (nachfolgend „**Auftraggeber-Daten**“ genannt). Dieser AVV konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung des Auftragnehmers der Auftraggeber-Daten zur Durchführung des Hauptvertrags.

2 Umfang der Beauftragung

2.1 Der Auftragnehmer verarbeitet die Auftraggeber-Daten im Auftrag und nach Weisung des Auftraggebers i.S.v. Art. 28 DSGVO (Auftragsverarbeitung). Der Auftraggeber bleibt Verantwortlicher im datenschutzrechtlichen Sinn.

2.2 Die Verarbeitung von Auftraggeber-Daten durch den Auftragnehmer als Auftragsverarbeiter erfolgt in der Art, dem Umfang und zu dem Zweck wie in **Anhang 1** zu diesem AVV spezifiziert; die Verarbeitung betrifft die darin bezeichneten Arten personenbezogener Daten und Kategorien betroffener Personen.

2.3 Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.

2.4 Dem Auftragnehmer bleibt es vorbehalten, die Auftraggeber-Daten zu anonymisieren oder zu aggregieren, so dass eine Identifizierung einzelner betroffener Personen nicht mehr möglich ist, und in dieser Form zum Zweck der bedarfsgerechten Gestaltung, der Weiterentwicklung und der Optimierung des nach Maßgabe des Hauptvertrags vereinbarten Dienstes zu verwenden. Die Parteien stimmen darin überein, dass anonymisierte bzw. nach obiger Maßgabe aggregierte Auftraggeber-Daten nicht mehr als Auftraggeber-Daten im Sinne dieses AVVs gelten.

2.5 Der Auftragnehmer darf die Auftraggeber-Daten im Rahmen des datenschutzrechtlich Zulässigen und außerhalb des Anwendungsbereichs dieses AVVs für eigene Zwecke auf eigene Verantwortung verarbeiten und nutzen, wenn eine gesetzliche Erlaubnisvorschrift oder eine Einwilligungserklärung des Betroffenen das gestattet. Auf solche Datenverarbeitungen findet dieser AVV keine Anwendung.

2.6 Die Verarbeitung der Auftraggeber-Daten durch den Auftragnehmer findet grundsätzlich innerhalb der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Insbesondere befinden sich die relevanten Datenzentren innerhalb des EWR. Lediglich im Rahmen von technischen Wartungsleistungen kann im Einzel- und Ausnahmefall ein Datenzugriff aus den USA stattfinden. Ein solcher Zugriff findet aber nicht regelmäßig, sondern nur im Ausnahmefall statt. Es ist dem Auftragnehmer jenseits dessen gleichwohl gestattet, Auftraggeber-Daten unter Einhaltung der Bestimmungen

dieses AVVs auch außerhalb des EWR zu verarbeiten, wenn die Voraussetzungen der Art. 44–48 DSGVO erfüllt sind oder eine Ausnahme nach Art. 49 DSGVO vorliegt.

3 Weisungsbefugnisse des Auftraggebers

3.1 Der Auftragnehmer verarbeitet die Auftraggeber-Daten gemäß den Weisungen des Auftraggebers, sofern der Auftragnehmer nicht gesetzlich zu einer anderweitigen Verarbeitung verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.2 Die Weisungen des Auftraggebers sind grundsätzlich abschließend in den Bestimmungen dieses AVVs festgelegt und dokumentiert. Einzelweisungen, die von den Festlegungen dieses AVVs abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers und erfolgen nach Maßgabe des im Hauptvertrag festgelegten Änderungsverfahrens, in dem die Weisung zu dokumentieren und die Übernahme etwa dadurch bedingter Mehrkosten des Auftragnehmers durch den Auftraggeber zu regeln ist.

3.3 Der Auftragnehmer gewährleistet, dass er die Auftraggeber-Daten im Einklang mit den Weisungen des Auftraggebers verarbeitet. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen AVV oder das geltende Datenschutzrecht verstößt, ist er nach einer entsprechenden Mitteilung an den Auftraggeber berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen. Die Parteien stimmen darin überein, dass die alleinige Verantwortung für die weisungsgemäße Verarbeitung der Auftraggeber-Daten beim Auftraggeber liegt.

4 Verantwortlichkeit des Auftraggebers

4.1 Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der Auftraggeber-Daten sowie für die Wahrung der Rechte der Betroffenen im Verhältnis der Parteien zueinander allein verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund der Verarbeitung von Auftraggeber-Daten nach Maßgabe dieses AVVs Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen.

4.2 Ist der Auftragnehmer gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung von Auftraggeber-Daten zu erteilen oder mit diesen Stellen anderweitig zusammenzuarbeiten, so ist der Auftraggeber verpflichtet, den Auftragnehmer auf erstes Anfordern bei der Erteilung solcher Auskünfte bzw. der Erfüllung anderweitiger Verpflichtungen zur Zusammenarbeit zu unterstützen.

5 Anforderungen an Personal

Der Auftragnehmer hat alle Personen, die Auftraggeber-Daten verarbeiten, bezüglich der Verarbeitung von Auftraggeber-Daten zur Vertraulichkeit zu verpflichten.

6 Sicherheit der Verarbeitung

6.1 Der Auftragnehmer wird gemäß Art. 32 DSGVO erforderliche, geeignete technische und organisatorische Maßnahmen ergreifen, die unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der

Verarbeitung der Auftraggeber-Daten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Auftraggeber-Daten zu gewährleisten.

6.2 Die konkreten vom Auftragnehmer zu ergreifenden Maßnahmen sind in **Anhang 4** dieses AVVs festgelegt.

6.3 Dem Auftragnehmer ist es gestattet, technische und organisatorische Maßnahmen während der Laufzeit des AVVs zu ändern oder anzupassen, solange sie weiterhin den unter Ziffer 6.1 dieses AVVs aufgestellten Anforderungen genügen.

7 Inanspruchnahme weiterer Auftragsverarbeiter

7.1 Der Auftraggeber erteilt dem Auftragnehmer hiermit die allgemeine Genehmigung, weitere Auftragsverarbeiter hinsichtlich der Verarbeitung von Auftraggeber-Daten hinzuzuziehen. Die zum Zeitpunkt des Vertragsschlusses hinzugezogenen weiteren Auftragsverarbeiter ergeben sich aus **Anhang 3**. Generell nicht genehmigungspflichtig sind Vertragsverhältnisse mit Dienstleistern, die die Prüfung oder Wartung von Datenverarbeitungsverfahren oder -anlagen durch andere Stellen oder andere Nebenleistungen zum Gegenstand haben, auch wenn dabei ein Zugriff auf Auftraggeber-Daten nicht ausgeschlossen werden kann, solange der Auftragnehmer angemessene Regelungen zum Schutz der Vertraulichkeit der Auftraggeber-Daten trifft.

7.2 Der Auftragnehmer wird den Auftraggeber über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter informieren. Dem Auftraggeber steht im Einzelfall ein Recht zu, Einspruch gegen die Beauftragung eines potentiellen weiteren Auftragsverarbeiters zu erheben. Ein Einspruch darf vom Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden Grund erhoben werden. Soweit der Auftraggeber nicht innerhalb von 30 Tagen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Erhebt der Auftraggeber Einspruch, ist der Auftragnehmer berechtigt, den Hauptvertrag und diesen AVV entsprechend der im Hauptvertrag festgelegten regelmäßigen Kündigungsfrist zu kündigen.

7.3 Der Vertrag zwischen dem Auftragnehmer und dem weiteren Auftragsverarbeiter muss letzterem im Sinne des Art. 28 dieselben Pflichten auferlegen, wie sie dem Auftragnehmer kraft dieses AVVs obliegen. Die Parteien stimmen überein, dass diese Anforderung erfüllt ist, wenn der Vertrag ein diesem AVV entsprechendes Schutzniveau aufweist bzw. dem weiteren Auftragsverarbeiter die in Art. 28 Abs. 3 DSGVO festgelegten Pflichten auferlegt sind.

7.4 Unter Einhaltung der Anforderungen der Ziffer 2.6 dieses AVVs gelten die Regelungen in dieser Ziffer 7 auch, wenn ein weiterer Auftragsverarbeiter in einem Drittstaat eingeschaltet wird.

8 Rechte der betroffenen Personen

8.1 Der Auftragnehmer wird den Auftraggeber angesichts der Art der Verarbeitung den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person nachzukommen.

8.2 Soweit eine betroffene Person einen Antrag auf Wahrnehmung der ihr zustehenden Rechte unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen zeitnah an den Auftraggeber weiterleiten.

8.3 Der Auftragnehmer kann für seine Unterstützungshandlungen nach Ziffer 8.1 und 8.2 dieses AVVs von dem Auftraggeber die Erstattung von Aufwänden und Kosten sowie eine angemessene Vergütung verlangen, sofern die Unterstützung nicht wegen eines Gesetzes- oder Vertragsverstoßes des Auftragnehmers erforderlich wurde.

9 Mitteilungs- und Unterstützungspflichten des Auftragnehmers

9.1 Soweit den Auftraggeber eine gesetzliche Melde- oder Benachrichtigungspflicht wegen einer Verletzung des Schutzes von Auftraggeber-Daten (insbesondere nach Art. 33, 34 DSGVO) trifft, wird der Auftragnehmer den Auftraggeber zeitnah über meldepflichtige Ereignisse in seinem Verantwortungsbereich informieren. Der Auftragnehmer wird den Auftraggeber bei der Erfüllung der Melde- und Benachrichtigungspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen unterstützen.

9.2 Der Auftragnehmer wird den Auftraggeber bei etwa vom Auftraggeber durchzuführenden Datenschutz-Folgenabschätzungen und sich gegebenenfalls anschließenden Konsultationen der Aufsichtsbehörden nach Art. 35, 36 DSGVO im Rahmen des Zumutbaren und Erforderlichen unterstützen.

9.3 Der Auftragnehmer kann für die Erfüllung seiner Mitteilungs- und Unterstützungsleistungen von dem Auftraggeber die Erstattung von Aufwänden und Kosten sowie eine angemessene Vergütung verlangen, sofern die Mitteilungs- oder Unterstützungspflicht nicht aufgrund eines Gesetzes- oder Vertragsverstoßes durch den Auftragnehmer erforderlich wurde.

10 Datenlöschung

10.1 Der Auftragnehmer wird die Auftraggeber-Daten nach Beendigung dieses AVVs nach Wahl des Auftraggebers löschen oder zurückgeben und vorhandene Kopien löschen, sofern nicht gesetzlich eine Verpflichtung des Auftragnehmers zur weiteren Speicherung der Auftraggeber-Daten besteht. Backups dürfen im Rahmen von marktüblichen Backuproutinen für den entsprechenden Zeitraum darüber hinaus erhalten bleiben.

10.2 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung von Auftraggeber-Daten dienen, dürfen durch den Auftragnehmer auch nach Vertragsende aufbewahrt werden.

11 Nachweise und Überprüfungen

11.1 Der Auftragnehmer wird dem Auftraggeber auf dessen Anforderung alle erforderlichen und beim Auftragnehmer vorhandenen Informationen zum Nachweis der Einhaltung seiner Pflichten nach diesem AVV zur Verfügung stellen.

11.2 Der Auftraggeber ist berechtigt, den Auftragnehmer bezüglich der Einhaltung der Regelungen dieses AVVs, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen, zu überprüfen; einschließlich durch Inspektionen.

11.3 Zur Durchführung von Inspektionen nach Ziffer 11.2 ist der Auftraggeber berechtigt, im Rahmen der üblichen Geschäftszeiten (montags bis freitags von 10 bis 18 Uhr) nach rechtzeitiger Vorankündigung gemäß Ziffer 11.5 auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers die Geschäftsräume des Auftragnehmers zu betreten, in denen Auftraggeber-Daten verarbeitet werden. Das Betreten der Räumlichkeiten des Auftragnehmers darf nur in ständiger Anwesenheit eines Vertreters des Auftragnehmers erfolgen. Dieser Vertreter ist befugt, Entscheidungen über den Verlauf der Inspektion zu treffen, soweit dies erforderlich ist, um Störungen des Geschäftsbetriebs des Auftragnehmers zu vermeiden und dessen Geheimhaltungspflichten gegenüber Dritten zu wahren. Der Auftraggeber ersetzt dem Auftragnehmer seine durch derartige physische Inspektionen entstehenden Kosten. Für das Hosting der Daten gelten die vom Hostinganbieter standardmäßig gewährten Überprüfungsmöglichkeiten.

11.4 Der Auftragnehmer ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Auftraggebers, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragnehmers sind oder wenn der Auftragnehmer durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Auftraggeber ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, zu Informationen hinsichtlich Kosten, zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragnehmers, die nicht unmittelbar relevant für die vereinbarten Überprüfungszwecke sind, zu erhalten.

11.5 Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens vier Wochen vorher) über alle mit der Durchführung der Überprüfung zusammenhängenden Umstände zu informieren. Der Auftraggeber darf eine Überprüfung pro Kalenderjahr durchführen. Weitere Überprüfungen erfolgen gegen eine angemessene Vergütung und nach Abstimmung mit dem Auftragnehmer, sofern die Überprüfung nicht wegen eines Gesetzes- oder Vertragsverstoßes durch den Auftragnehmer erforderlich wird.

11.6 Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Überprüfung, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund von dieser Ziffer 11 dieses AVVs gegenüber dem Auftragnehmer verpflichtet ist. Zudem hat der Auftraggeber den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber ihm die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Die entsprechenden Verpflichtungen müssen eine vertragliche Pflicht unmittelbar gegenüber dem Auftragnehmer begründen. Der Auftraggeber darf keinen Wettbewerber des Auftragnehmers mit der Kontrolle beauftragen.

12 Vertragsdauer und Kündigung

Die Laufzeit und Kündigung dieses AVVs richten sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses AVVs. Eine isolierte Kündigung dieses AVVs ist ausgeschlossen.

13 Haftung

13.1 Für die Haftung des Auftragnehmers nach diesem AVV gelten die Haftungsausschlüsse und -begrenzungen gemäß dem Hauptvertrag. Soweit Dritte Ansprüche gegen den Auftragnehmer geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftraggebers gegen diesen AVV oder gegen eine seiner Pflichten als datenschutzrechtlich Verantwortlicher haben, stellt der Auftraggeber den Auftragnehmer von diesen Ansprüchen auf erstes Anfordern frei.

13.2 Der Auftraggeber verpflichtet sich, den Auftragnehmer auch von allen etwaigen Geldbußen, die gegen den Auftragnehmer verhängt werden, in dem Umfang auf erstes Anfordern freizustellen, in dem der Auftraggeber Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

14 Schlussbestimmungen

14.1 Sollten einzelne Bestimmungen dieses AVVs unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und dabei den Anforderungen des Art. 28 DSGVO genügt.

14.2 Im Fall von Widersprüchen zwischen diesem AVV und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieses AVVs vor.

Anhänge:

Anhang 1: Einzelheiten zur Verarbeitung

Anhang 2: Weitere Auftragsverarbeiter

Anhang 3: Sicherheitsmaßnahmen

Datum [01.12.2025]

Anhang 1 - Einzelheiten zur Verarbeitung

1. Gegenstand der Verarbeitung

Der Gegenstand der Verarbeitung ist die Verarbeitung personenbezogener Daten im Kontext der Services des Auftragnehmers, insbesondere der Nachverfolgung von Verkaufs-, Zahlungs- oder Finanzierungsvorgängen.

2. Zweck und Art der Verarbeitung

Zweck der Verarbeitung

Die Datenverarbeitung findet im jeweils für den Service erforderlichen Umfang statt. Insofern gelten die Details der Servicebeschreibung. Die Datenverarbeitung findet statt, soweit der jeweilige Service beauftragt wurde.

Es sind zwei grundlegende Formen der Services bzw. Datenverarbeitungen zu unterscheiden:

Bestellungs- bzw. Zahlungsnachverfolgung: Datenverarbeitungen, die mit nachgelagerten Maßnahmen im Kontext der Bezahlung oder Finanzierung von Bestellungen oder Transaktionen online und im Ladengeschäft (z.B. Bezahlabwicklung, Bestellinformationen, Kundenverwaltung, Versandabwicklung, Analysen, etc.) zusammenhängen.

Marketing und Vertriebsunterstützung: Datenverarbeitungen für verkaufsfördernde Maßnahmen, also insbesondere Datenverarbeitungen im Rahmen der Marketing- und Vertriebsunterstützung (z.B. Kundensupport, Newsletter, E-Mail-Marketing).

Der Zahlungs- bzw. der Finanzierungsvorgang finden nicht im Auftrag des Auftraggebers, sondern im Auftrag des jeweiligen Zahlungs- bzw. Finanzierungsdienstleisters statt.

Art der Verarbeitung

Für diese Zwecke werden Daten auf folgende Art verarbeitet:

Bestellungs- bzw. Zahlungsnachverfolgung: Der Auftragnehmer stellt dem Auftraggeber diverse Informationen zum Bezahl- bzw. Finanzierungsstatus gemeinsam mit dem jeweiligen Bestell- und/oder Widerrufsstatus zentral bereit.

Marketing und Vertriebsunterstützung: Der Auftragnehmer verarbeitet für den Auftraggeber diverse persönliche Informationen wie Name, Anschrift, E-Mail-Adresse oder Telefonnummer.

3. Art der personenbezogenen Daten

- In Bestellungen enthaltene Daten (z.B. Name, Anschrift)
- Daten zu Bestellungen (z.B. Produktdaten, Preis).
- Informationen zum Bestellstatus
- Informationen zum Bezahl- oder Finanzierungsstatus

4. Kategorien der betroffenen Personen

- Kunden
- Interessenten
- Besucher der Website und Apps des Auftragsverarbeiter
- Lieferanten

- Partner des Auftragsverarbeiters

5. Ort der Verarbeitung

- Nürnberg, Deutschland
- Falkenstein/Vogtland, Deutschland
- Dublin, Irland
- Amsterdam, Niederlande

Anhang 2 - Unterauftragsverarbeiter

Name	Adresse	Land
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, L-1855	Luxemburg
Google Cloud EMEA Limited	70 Sir John Rogerson's Quay, Dublin 2	Irland
Hetzner Online GmbH	Industriestr. 25 91710 Gunzenhausen	Deutschland
Microsoft Ireland Operations Limited	Atrium Building Block A Carmen Hall Road, Sandyford Industrial Park, Dublin	Irland
One.com Group AB	Carlsgatan 3 211 20 Malmö	Schweden
Token GmbH	c/o Industrious Schicklerstraße 5 10179 Berlin	Deutschland
Twilio, Inc.	375 Beale Street, Suite 300 San Francisco, CA 94105	USA
Zendesk, Inc.	1019 Market Street San Francisco, CA 94103	USA

Anhang 3 - Sicherheitsmaßnahmen

Die in diesem Anhang dokumentierten technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO von payever (1) und den von payever in Anspruch genommenen Cloud Anbietern (2) betreffen den Schutz der Datenverarbeitung.

1 Sicherheitsmaßnahmen von payever

1.1 Vertraulichkeit (Art. 32 Abs. 1 lit b DSGVO)

1.1.1 Zutrittskontrolle

payever ergreift die folgenden technischen und organisatorischen Maßnahmen zur Zutrittskontrolle:

Technische Maßnahmen:

- Alarmanlage,
- Manuelles Schließsystem,
- Absicherung der Gebäudeschächte,
- Türen mit Knauf Außenseite,
- Videoüberwachung der Eingänge.

Organisatorische Maßnahmen:

- Schlüsselregelung / Liste,
- Besucherbuch / Protokoll der Besucher,
- Besucher in Begleitung durch Mitarbeiter,
- Sorgfalt bei Auswahl Reinigungsdienste.

1.1.2 Zugangskontrolle

payever ergreift die folgenden technischen und organisatorischen Maßnahmen zur Zugangskontrolle:

Technische Maßnahmen:

- Login mit Benutzername und Passwort,
- Anti-Viren-Software Server,
- Anti-Virus-Software Clients,
- Firewall,
- Intrusion Detection Systeme,
- Mobile Device Management,
- Einsatz VPN bei Remote-Zugriffen,
- Verschlüsselung von Datenträgern,
- Verschlüsselung Smartphones,
- Sperre externer Schnittstellen (USB),
- Verschlüsselung von Notebooks / Tablet.

Organisatorische Maßnahmen:

- Verwalten von Benutzerberechtigungen,
- Erstellen von Benutzerprofilen,
- Richtlinie „Sicheres Passwort“,
- Richtlinie „Löschen / Vernichten“,

- Richtlinie „Clean desk“,
- Allg. Richtlinie Datenschutz und / oder Sicherheit,
- Mobile Device Policy,
- Anleitung „Manuelle Desktopsperre“.

1.1.3 Zugriffskontrolle

payever ergreift die folgenden technischen und organisatorischen Maßnahmen zur Zugriffskontrolle:

Technische Maßnahmen:

- Aktenschredder (mind. Stufe 3, cross cut),
- Physische Löschung von Datenträgern,
- Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten.

Organisatorische Maßnahmen:

- Einsatz Berechtigungskonzepte,
- Minimale Anzahl an Administratoren,
- Verwaltung Benutzerrechte durch Administratoren.

1.1.4 Trennungskontrolle

payever ergreift die folgenden technischen und organisatorischen Maßnahmen zur Trennungskontrolle:

Technische Maßnahmen:

- Trennung von Produktiv- und Testumgebung,
- Physikalische Trennung (Systeme / Datenbanken / Datenträger),
- Mandantenfähigkeit relevanter Anwendungen.

Organisatorische Maßnahmen:

- Steuerung über Berechtigungskonzept,
- Festlegung von Datenbankrechten.

1.1.5 Pseudonymisierung Art. 32 Abs. 1 lit. a DSGVO, Art. 25 Abs. 1 DSGVO

payever ergreift die folgenden technischen und organisatorischen Maßnahmen zur Pseudonymisierung:

Technische Maßnahme:

- Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesichertem System (mögl. verschlüsselt).

Organisatorische Maßnahme:

- Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren.

1.2 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

1.2.1 Weitergabekontrolle

payever ergreift die folgenden technischen Maßnahmen zur Weitergabekontrolle:

- Email-Verschlüsselung (S/MIME / PGP),

- Einsatz von VPN,
- Sichere Transportbehälter,
- Bereitstellung über verschlüsselte Verbindungen wie sftp, https,
- Nutzung von Signaturverfahren.

1.2.2 Eingabekontrolle

payever ergreift die folgenden technischen und organisatorischen Maßnahmen zur Eingabekontrolle:

Technische Maßnahmen:

- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten,
- Manuelle oder automatisierte Kontrolle der Protokolle.

Organisatorische Maßnahme:

- Klare Zuständigkeiten für Löschungen.

1.3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

payever ergreift die folgenden technischen und organisatorischen Maßnahmen hinsichtlich der Verfügbarkeit und Belastbarkeit:

Technische Maßnahmen:

- Feuer- und Rauchmeldeanlagen,
- Feuerlöscher Serverraum,
- Serverraum klimatisiert,
- Videoüberwachung Serverraum,
- Alarmmeldung bei unberechtigtem Zutritt zu Serverraum.
- Organisatorische Maßnahmen:Backup & Recovery-Konzept (ausformuliert),
- Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse,
- Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums,
- Keine sanitären Anschlüsse im oder oberhalb des Serverraums,
- Existenz eines Notfallplans (z.B. BSI IT Grundschutz 100-4).

1.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

1.4.1 Datenschutz-Management

payever ergreift die folgenden technischen und organisatorischen Maßnahmen für das Datenschutz-Management:

Technische Maßnahmen:

- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet …),
- Anderweitiges dokumentiertes Sicherheitskonzept,
- Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mindestens jährlich durchgeführt.

Organisatorische Maßnahmen:

- Einsatz eines externern Datenschutzbeauftragtern,
- Schulung und Verpflichtung der Mitarbeiter zu Vertraulichkeit / Datengeheimnis,
- Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich,
- Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt,
- Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach,
- Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden.

1.4.2 Incident-Response-Management

payever ergreift die folgenden technischen und organisatorischen Maßnahmen für das Incident-Response-Management:

Technische Maßnahmen:

- Einsatz von Firewall und regelmäßige Aktualisierung,
- Einsatz von Spamfilter und regelmäßige Aktualisierung,
- Einsatz von Virenscanner und regelmäßige Aktualisierung,
- Implementierung eines Intrusion Detection Systems (IDS),
- Implementierung eines Intrusion Prevention Systems (IPS).

Organisatorische Maßnahmen:

- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde),
- Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen,
- Einbindung von ISB in Sicherheitsvorfälle und Datenpannen,
- Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem,
- Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen.

1.4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

payever ergreift die folgende technische Maßnahme für eine datenschutzfreundliche Voreinstellungen:

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweckerforderlich sind.

1.4.4 Auftragskontrolle

payever ergreift die folgenden organisatorischen Maßnahmen zur Auftragskontrolle:

- Vorherige Prüfung der vom Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen und deren Dokumentation,
- Auswahl des Auftragsverarbeiters unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit,
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln,
- Schriftliche Weisungen an den Auftragsverarbeiter,
- Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf Datengeheimnis,
- Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragsverarbeiter,
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags,
- Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus.

2 Sicherheitsmaßnahmen der Cloud Anbieter

payever nimmt etablierte Cloud Anbieter in Anspruch. Deren Sicherheitsmaßnahmen sind über die folgenden Links abrufbar:

- Azure
- Hetzneri
- Google Cloud
- AWS