# Auftragsverarbeitungsvertrag Planet Pop

in der Fassung vom 26. Mai. 2024

**Gemäß Art. 28 Abs. 3 S. 1 DSGVO**

– nachstehend bezeichnet als **AV-Vertrag** –

zwischen (der)

| | |
|---|---|
| Name/Fa.: | phase-6 GmbH (nachfolgend auch “phase6”) |
| Straße Nr.: | Neue Schönhauser Straße 16 |
| PLZ, Ort, Land: | 10178, Berlin, Deutschland |
| Handelsregister/Nr.: | HRB 214234 B |
| Geschäftsführer: | Hendrik Langner |
| Zuständige Person: | Andreas Kruse (DSB) |
| E-Mail-Adresse: | a.kruse@phase-6.de |

– nachstehend bezeichnet als **Auftragnehmer** –

und (der)

| | |
|---|---|
| Name/Schule/Fa.: | |
| Schulleitung/Geschäftsführer: | |
| Straße Nr.: | |
| PLZ, Ort, Land: | |
| Zuständige Person: | |
| E-Mail-Adresse: | |

– nachstehend bezeichnet als **Auftraggeber** –

– Auftragnehmer und Auftraggeber werden nachstehend auch als **Vertragsparteien** bezeichnet. –

**Anlagen**

- Anlage 1: “Technische und organisatorische Maßnahmen”
- Anlage 2: “Verzeichnis der Auftragsverarbeiter”

Aus Gründen der leichteren Lesbarkeit wird im Folgenden bei allen Bezeichnungen, die auf Personen bezogen sind, die grammatikalisch männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat rein redaktionelle Gründe und beinhaltet keine Wertung.
Sofern im Folgenden von "uns" die Rede sein sollte, so ist phase6 gemeint.

1. **Gegenstand des Auftrags, Datenkategorien, Betroffene, Art, Umfang und Zwecksetzung der Verarbeitung (Art. 28 Abs. 3, 30 Abs. 2 DSGVO)**

1.1. Der Gegenstand des AV-Vertrages, die im Rahmen des Auftrags verarbeiteten personenbezogenen Daten (Art, 4 Nr. 1 DSGVO; nachfolgend kurz „**Daten**“), die von der Verarbeitung betroffene Personen (nachfolgend kurz „**Betroffene**“) sowie Art, Umfang und Zwecke der Verarbeitung, werden durch die folgenden Rechtsbeziehung(en) zwischen den Vertragsparteien bestimmt (nachstehend bezeichnet als **Hauptvertrag**):

1.2. Art der Daten:
Vor- und Nachname (bei Lehrkräften)
E-Mail-Adressen (bei Lehrkräften)
Schulname und Schuladresse
Nutzungsdaten
IP-Adressen (im Rahmen der Aufbewahrungsrichtlinien unseres Rechenzentrumsbetreibers Scaleway)

1.3. Verarbeitung besonderer Kategorien von Daten (Art. 9 Abs. 1 DSGVO):
Es werden grundsätzlich keine besonderen Kategorien von Daten verarbeitet, außer diese werden durch den Auftraggeber/ seine Kunden, Nutzer oder Mitarbeiter, etc. der Verarbeitung zugeführt.

1.4. Kategorien der Betroffenen:
Schüler (ohne Account) und Lehrkräfte

1.5. Zweck der Verarbeitung:
Bereitstellung und Vertrieb von Planet Pop

2. **Verantwortlichkeit und Weisungsrecht**

2.1. Der Auftraggeber ist als **Verantwortlicher** gem. Art. 4 Nr. 7 DSGVO für die Einhaltung der datenschutzrechtlichen Vorgaben, insbesondere für die Auswahl des Auftragnehmers, die an diesen übermittelten Daten sowie erteilte Weisungen verantwortlich (Art. 28 Abs. 3 lit. a, 29 u. 32 Abs. 4 DSGVO).

2.2. Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrages sowie der Weisungen des Auftraggebers verarbeiten (was insbesondere auch für deren Berichtigung, Löschung oder Einschränkung der Verarbeitung gilt) und nur insoweit die Verarbeitung hierzu erforderlich ist, außer wenn der Auftragnehmer zu der Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist; 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 (Art. 28 Abs. 3 S. 2 lit. a DSGVO).

2.3. Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen im Hinblick auf die Verarbeitung der Daten und die Sicherheitsmaßnahmen zu erteilen.

2.4. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen geltendes Datenschutzrecht verstößt, wird er den Auftraggeber unverzüglich darauf hinweisen. In diesem Fall ist der Auftragnehmer berechtigt, die Ausführung der Weisung bis zur Bestätigung der Weisung durch den Auftraggeber auszusetzen und im Fall offensichtlich rechtswidriger Weisungen abzulehnen.

2.5. Die Vertragsparteien können zum Erteilen und Empfangen von Weisungen berechtigte Personen benennen (insbesondere, wenn diese sich nicht bereits aus dem Hauptvertrag ergeben) und sind verpflichtet, deren Änderung unverzüglich mitzuteilen.

## 3. Sicherheitskonzept und diesbezügliche Pflichten

3.1. Der Auftragnehmer wird die innerbetriebliche Organisation in seinem Verantwortungsbereich entsprechend den gesetzlichen Anforderungen gestalten und wird insbesondere technische und organisatorische Maßnahmen (nachfolgend bezeichnet als „**TOMs**“) zur angemessenen Sicherung, insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit von Daten des Auftraggebers, unter Beachtung 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 der Betroffenen treffen sowie deren Aufrechterhaltung sicherstellen (Art. 28 Abs. 3 u. 32 - 39 i.V.m. Art 5 DSGVO). Zu den TOMs gehören insbesondere die Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, Trennungskontrolle und die Sicherung der Betroffenenrechte.

3.2. Die diesem AV-Vertrag zugrundeliegenden TOMs ergeben sich aus der **Anlage 1 „Technische und organisatorische Maßnahmen“**. Sie dürfen entsprechend dem technischen Fortschritt weiterentwickelt und durch adäquate Schutzmaßnahmen ersetzt werden, sofern sie das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschreiten und wesentliche Änderungen dem Auftraggeber mitgeteilt werden.

3.3. Der Auftragnehmer stellt sicher, dass die zur Verarbeitung der Daten des Auftraggebers befugten Personen auf Vertraulichkeit und Verschwiegenheit (Art. 28 Abs. 3 S. 2 lit. b und 29, 32 Abs. 4 DSGVO) verpflichtet und in die Schutzbestimmungen der DSGVO eingewiesen worden sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

3.4. Die im Rahmen des AV-Vertrages überlassene Daten verbleiben im Eigentum des Auftraggebers, sind durch den Auftragnehmer sorgfältig zu verwahren, vor Zugang durch unberechtigte Dritte zu schützen und dürfen nur mit Zustimmung des Auftraggebers, und dann nur datenschutzgerecht, vernichtet werden. Kopien von Daten dürfen nur erstellt werden, wenn sie zur Erfüllung der Leistungshaupt- und Nebenpflichten des Auftragnehmers gegenüber dem Auftragnehmer erforderlich sind (z.B. Backups).

3.5. Sofern durch die DSGVO oder ergänzende, insbesondere nationale Vorschriften, vorgegeben, benennt der Auftragnehmer eine/n den gesetzlichen Vorgaben entsprechende/n Datenschutzbeauftragte/n und informiert den Auftraggeber entsprechend (Art. 37 bis 39 DSGVO).

## 4. Informationspflichten und Mitwirkungspflichten

4.1. Betroffenenrechte sind gegenüber dem Auftraggeber wahrzunehmen, wobei der Auftragnehmer den Auftraggeber hierbei gem. Art. 28 Abs. 3 S. 2 lit. e. DSGVO unterstützt und ihn insbesondere über die bei ihm eingehenden Anfragen Betroffener informiert.

4.2. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er im Hinblick auf die Verarbeitung der Daten Fehler oder Unregelmäßigkeiten im Hinblick auf die Einhaltung der Bestimmungen dieses AV-Vertrages oder einschlägiger Datenschutzvorschriften feststellt.

4.3. Für den Fall, dass der Auftragnehmer Tatsachen feststellt, welche die Annahme begründen, dass der Schutz der für den Auftraggeber verarbeiteten Daten verletzt worden ist, hat der Auftragnehmer den Auftraggeber unverzüglich und vollständig zu informieren, unverzüglich erforderliche Schutzmaßnahmen zu ergreifen, und bei der Erfüllung der dem Auftraggeber obliegenden Pflichten gem. Art. 33 und 34 DSGVO zu unterstützen.

4.4. Sollte die Sicherheit der Daten des Auftraggebers durch Maßnahmen Dritter (z.B. Gläubiger, Behörden, Gerichte, etc.) gefährdet sein (Pfändung, Beschlagnahme, Insolvenzverfahren, etc.) wird der

Auftragnehmer die Dritten unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich bei dem Auftraggeber liegen und nach Rücksprache mit dem Auftraggeber, sofern erforderlich, entsprechende Schutzmaßnahmen ergreifen (z.B. Widersprüche, Anträge, etc. stellen).

4.5. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde gegenüber dem Auftragnehmer tätig wird und deren Tätigkeit die für den Auftragnehmer verarbeiteten Daten betreffen kann. Der Auftragnehmer unterstützt den Auftraggeber bei der Wahrnehmung seiner Pflichten (insbesondere zur Auskunfts- und Duldung von Kontrollen) gegenüber Aufsichtsbehörden (Art. 31 DSGVO).

4.6. Der Auftragnehmer stellt dem Auftraggeber Informationen betreffend die Verarbeitung von Daten im Rahmen dieses AV-Vertrages, die für dessen Erfüllung von gesetzlichen Pflichten (zu denen insbesondere Anfragen Betroffener oder Behörden und die Einhaltung seiner Rechenschaftspflichten gem. Art. 5 Abs. 2 DSGVO, als auch die Durchführung einer Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO gehören können) notwendig sind, zur Verfügung, sofern der Auftraggeber diese Informationen nicht selbst beschaffen kann. Die Informationen müssen dem Auftragnehmer zur Verfügung stehen und müssen nicht von Dritten beschafft werden, wobei Mitarbeiter, Beauftragte und Subunternehmer des Auftraggebers nicht als Dritte gelten.

## 5. **Kontrollbefugnisse**

5.1. Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorgaben und der Regelungen dieses AV-Vertrages, insbesondere der TOMs beim Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren (Art. 28 Abs. 3 lit. h DSGVO).

5.2. Vor-Ort-Kontrollen erfolgen innerhalb üblicher Geschäftszeiten, sind vom Auftraggeber mit einer angemessenen Frist (mindestens 14 Tage, außer in Notfällen) anzumelden und durch den Auftragnehmer zu unterstützen (z.B. durch Bereitstellung von Personal).

5.3. Die Kontrollen sind auf den erforderlichen Rahmen beschränkt und müssen auf Betriebs- und Geschäftsgeheimnisse des Auftragnehmers sowie den Schutz von personenbezogenen Daten Dritter (z.B. anderer Kunden oder Mitarbeiter des Auftragnehmers) Rücksicht nehmen. Zur Durchführung der Kontrolle sind nur fachkundige Personen zugelassen, die sich legitimieren können und im Hinblick auf die Betriebs- und Geschäftsgeheimnisse sowie Prozesse des Auftragnehmers und personenbezogene Daten Dritter zur Verschwiegenheit verpflichtet sind.

5.4. Statt der Einsichtnahmen und der Vor-Ort-Kontrollen, darf der Auftragnehmer den Auftraggeber auf eine gleichwertige Kontrolle durch unabhängige Dritte (z.B. neutrale Datenschutzauditoren), Einhaltung genehmigter Verhaltensregeln (Art. 40 DSGVO) oder geeignete Datenschutz- oder IT-Sicherheitszertifizierungen gem. Art. 42 DSGVO verweisen. Dies gilt insbesondere dann, wenn Betriebs- und Geschäftsgeheimnisse des Auftragnehmers oder personenbezogene Daten Dritter durch die Kontrollen gefährdet wären.

## 6. **Unterauftragsverhältnisse**

6.1. Nimmt der Auftragnehmer die Dienste eines Unterauftragsverarbeiters (d.h. Unterauftragnehmer oder Subunternehmer) in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Auftraggebers auszuführen, dann muss er dem Unterauftragsverarbeiter im Wege eines Vertrags oder eines nach der DSGVO zulässigen anderen Rechtsinstruments dieselben Datenschutzpflichten zu denen sich der Auftragnehmer in diesem AV-Vertrag verpflichtet hat, auferlegen (insbesondere im Hinblick auf die Befolgung von Weisungen, Einhaltung der TOMs, Erteilung von Informationen und Duldung von Kontrollen). Ferner hat der Auftragnehmer den Unterauftragsverarbeiter sorgfältig auszuwählen, auf dessen Zuverlässigkeit zu prüfen und diese, als auch dessen Einhaltung der vertraglichen und gesetzlichen Vorgaben zu überwachen (Art. 28 Abs. 2 u. 4 DSGVO).
Der Auftraggeber erklärt sich unbeschadet etwaiger Einschränkungen durch den Hauptvertrag

ausdrücklich damit einverstanden, dass der Auftragnehmer im Rahmen der Auftragsverarbeitung Unterauftragsverarbeiter einsetzen darf.

6.2. Die diesem AV-Vertrag zugrundeliegenden Unterauftragsverhältnisse ergeben sich aus der **Anlage 2 „Verzeichnis der Auftragsdatenverarbeiter“**.

6.3. Der Auftragnehmer informiert den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Unterauftragsverarbeiters, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Der Einspruch darf nur aus wichtigem Grund erfolgen.

6.4. Die Inanspruchnahme der in **Anlage 2** zum Zeitpunkt der Vertragsunterzeichnung aufgeführten Unterauftragsverarbeiter gilt als genehmigt, sofern die in Ziffer 6.1 dieses Vertrages genannten Voraussetzungen umgesetzt werden. Optionale oder sonstige Optionale Auftragsverarbeiter kommen bei der Verwendung des strikten Modus gemäß Ziffer 1.6 nicht zum Einsatz.

6.5. Vertragsverhältnisse, bei denen der Auftragnehmer die Leistungen Dritter als reine Nebenleistung in Anspruch nimmt, um seine geschäftliche Tätigkeit auszuüben (z.B. Reinigungs-, Bewachungs- oder Transportleistungen) stellen keine Unterauftragsverarbeitung im Sinne der vorstehenden Regelungen dieses AV-Vertrages dar. Gleichwohl hat der Auftragsverarbeiter sicherzustellen, z.B. durch vertragliche Vereinbarungen oder Hinweise und Instruktionen, dass hierbei die Sicherheit der Daten nicht gefährdet wird und die Vorgaben dieses AV-Vertrages und der Datenschutzvorschriften eingehalten werden.

## 7. Verarbeitung in Drittländern

7.1. Alle Daten werden systematisch und regelmäßig nur innerhalb des Rechtsraumes der DSGVO verarbeitet.

7.2. Die Auftragsverarbeitung in einem Drittland, auch durch Unterauftragsverarbeiter, bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, außer wenn der Auftragnehmer zu der Verarbeitung im Drittland durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist; 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 (Art. 28 Abs. 3 S. 2 lit. a DSGVO).

7.3. Die Zustimmung des Auftraggebers zur Verarbeitung im Drittland, gilt im Hinblick auf die in **Anlage 2 „Verzeichnis der Auftragsdatenverarbeiter”** genannten Verarbeitungen als erteilt.

## 8. Dauer des Auftrags, Vertragsbeendigung und Datenlöschung

8.1. Dieser AV-Vertrag wird mit dessen Abschluss gültig, wird auf bestimmte Zeit geschlossen und endet spätestens mit der Laufzeit des Hauptvertrags.

8.2. Das Recht auf außerordentliche Kündigung bleibt den Vertragsparteien vorbehalten, insbesondere im Fall eines schwerwiegenden Verstoßes gegen die Vorgaben dieses AV-Vertrages und geltendes Datenschutzrecht. Der außerordentlichen Kündigung hat grundsätzlich eine Abmahnung der Verstöße mit angemessener Frist vorauszugehen, wobei sie nicht erforderlich ist, wenn nicht damit zu rechnen ist, dass die beanstandeten Verstöße behoben werden oder diese derart schwer wiegen, dass ein Festhalten am AV-Vertrag der kündigenden Vertragspartei nicht zuzumuten ist.

8.3. Nach Abschluss der Erbringung der Verarbeitungsleistungen im Rahmen dieses AV-Vertrages, wird der Auftragnehmer alle personenbezogenen Daten und deren Kopien (sowie sämtliche im Zusammenhang mit dem Auftragsverhältnis in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände), nach Wahl des Auftraggebers entweder löschen oder zurückgeben, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht (Art. 28 Abs. 1 S. 2 lit. g DSGVO). Die Einrede

eines Zurückbehaltungsrechts, wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen. Im Hinblick auf die Löschung oder Rückgabe gelten die Auskunfts-, Nachweis- und Kontrollrechte des Auftraggebers entsprechend diesem AV-Vertrag.

8.4. Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten personenbezogenen Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, binnen 90 Tagen zu löschen. Der Nutzer wird über die Sperrung informiert und kann dieser widersprechen, indem er den Account in einen privaten Nutzungsaccount umwandelt. Dies ist insbesondere dann sinnvoll, wenn der Nutzer an einer Erhaltung des Lernstandes und einer weiteren Nutzung interessiert ist. Die Vorgänge sind in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt.

8.5. Im Übrigen bleiben die Verpflichtungen aus diesem AV-Vertrag im Hinblick auf die im Auftrag verarbeiteten Daten auch nach Beendigung des AV-Vertrages bestehen.

## 9. **Haftung**

9.1. Für den Ersatz von Schäden, die ein Betroffener wegen einer nach der DSGVO oder eines Landesdatenschutzgesetzes unzulässigen oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist der Auftragnehmer oder der Verantwortliche gegenüber der betroffenen Person verantwortlich. Der Auftragnehmer haftet nur dann, wenn er den ihm auferlegten Pflichten nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Weisungen oder gegen diese Weisungen gehandelt hat.

9.2. Die Vertragsparteien stellen sich jeweils von der Haftung frei, wenn eine der Vertragsparteien nachweist, dass sie für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, in keinerlei Hinsicht verantwortlich ist.

9.3. Der Auftragnehmer haftet für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung schuldhaft verursachen.

10. **Schlussbestimmungen, Rangfolge, Änderungen, Kommunikationsform, Rechtswahl, Gerichtsstand**

10.1. Änderungen, Nebenabreden und Ergänzungen dieses AV-Vertrages und seiner Anlagen bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieses AV-Vertrages handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

10.2. Dieser AV-Vertrag verpflichtet den Auftragnehmer nur insoweit, als dies zur Erfüllung der gesetzlichen Pflichten, insbesondere nach Art. 28 ff. DSGVO erforderlich ist und legt dem Auftragnehmer darüber hinaus keine weiteren Pflichten auf.

10.3. Vorbehaltlich einer Verpflichtung zur Schriftform in diesem AV-Vertrag und im Hauptvertrag, erfolgt die Kommunikation zwischen dem Auftragnehmer und Auftraggeber im Rahmen dieses AV-Vertrages (insbesondere im Hinblick auf Weisungen und Informationserteilung) zumindest in Textform (z.B. E-Mail). Eine geringere Form (z.B. mündlich) kann den Umständen nach statt der Textform zulässig sein (z.B. in Notfallsituation), muss jedoch unverzüglich zumindest in Textform bestätigt werden. Sofern die Schriftform verlangt wird, ist die Schriftform im Sinne der DSGVO gemeint.

10.4. Es gilt das Recht der Bundesrepublik Deutschland. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem AV-Vertrag ist der Sitz des Auftragnehmers (Berlin). Der Auftragnehmer behält sich vor, seine Ansprüche an dem gesetzlichen Gerichtsstand geltend zu machen.

.....

Ort, Datum, Unterschrift Auftraggeber

Berlin, 26.05.2024, ppa. .....

Ort, Datum, Unterschrift Auftragnehmer

Anlage 1

# Verzeichnis der Technischen und Organisatorische Maßnahmen (TOM) gemäß Art 32 Abs 1 DS-GVO

**Grundsätzliche Maßnahmen, die der Wahrung der Betroffenenrechte, unverzüglichen Reaktion in Notfällen, den Vorgaben der Technikgestaltung und dem Datenschutz auf Mitarbeiterebene dienen:**

Es besteht ein betriebsinternes Datenschutz-Management, dessen Einhaltung ständig überwacht und anlassbezogen mindestens jährlich evaluiert wird.

Es besteht ein Konzept, welches die Wahrung der Rechte der Betroffenen (Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, Datentransfer, Widerrufe & Widersprüche) innerhalb der gesetzlichen Fristen gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren sowie die Benennung der für die Umsetzung zuständigen Personen.

Es besteht ein Konzept, das eine unverzügliche und den gesetzlichen Anforderungen entsprechende Reaktion auf Verletzungen des Schutzes personenbezogener Daten (Prüfung, Dokumentation, Meldung) gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren sowie die Benennung der für die Umsetzung zuständigen Personen.

Der Schutz von personenbezogenen Daten wird 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 der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen bereits bei der Entwicklung, bzw. Auswahl von Hardware, Software sowie Verfahren, entsprechend dem Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen berücksichtigt (Art. 25 DSGVO).

Die eingesetzte Software wird stets auf dem aktuell verfügbaren Stand gehalten, ebenso wie Virenscanner und Firewalls.

Mitarbeiter werden im Hinblick auf den Datenschutz auf Verschwiegenheit verpflichtet, belehrt und instruiert, als auch auf mögliche Haftungsfolgen hingewiesen. Sofern Mitarbeiter außerhalb betriebsinterner Räumlichkeiten tätig werden oder Privatgeräte für betriebliche Tätigkeiten einsetzen, existieren spezielle Regelungen zum Schutz der Daten in diesen Konstellationen und der Sicherung der Rechte von Auftraggebern einer Auftragsverarbeitung.

Die an Mitarbeiter ausgegebenen Schlüssel, Zugangskarten oder Codes sowie im Hinblick auf die Verarbeitung personenbezogener Daten erteilte Berechtigungen, werden nach deren Ausscheiden aus dem Unternehmen, bzw. Wechsel der Zuständigkeiten eingezogen, bzw. entzogen.

Das Reinigungspersonal, Wachpersonal und übrige Dienstleister, die zur Erfüllung nebengeschäftlicher Aufgaben herangezogen werden, werden sorgfältig ausgesucht und es wird sichergestellt, dass sie den Schutz personenbezogener Daten beachten.

Die von uns beauftragten Unterauftragsverarbeiter wurden sorgfältig ausgewählt und verarbeiten die übermittelten Daten vertraglich zugesichert nur in unserem Auftrag im dafür vorgesehenen Verwendungszweck. Durch geeignete Maßnahmen wird sichergestellt, dass die vertraglich zugesicherte Verarbeitung eingehalten wird. Zu diesen Maßnahmen zählen die Prüfung der übermittelten Daten, die Prüfung des Standorts der Verarbeitung, die Prüfung der Dokumentation und die Prüfung möglicherweise verwendeter Unterauftragsverarbeiter.

| TOM des Rechenzentrumsbetreibers | |
|---|---|
| Beschreibung | phase6 verarbeitet direkte personenbezogene Daten nur über einen einzigen Unterauftragsverarbeiter, Scalway S.A.S. phase6 betreibt in den eigenen Räumlichkeiten keine Server, auf denen personenbezogene Daten von Kunden verarbeitet werden. |
| Adresse des Betreibers | Scaleway S.A.S.<br>8 rue de la Ville l'Evêque<br>75008 Paris, Frankreich |
| Standort der Server | Niederlande, Frankreich, Polen |
| TOM des Betreibers | Scaleway beschreibt auf ihrer Seite zur Sicherheit und Resilienz ihre umfassenden Maßnahmen zum Schutz von Daten. Dazu gehören ISO/IEC 27001:2022-Zertifizierung, Einhaltung der GDPR, Tier 3 Uptime Institute-Zertifizierung und SWIPO-Compliance. Die physische Sicherheit wird durch überwachte Rechenzentren, Zugangskontrollen und Feuerprävention gewährleistet. Weitere Maßnahmen umfassen Risikomanagement für Naturkatastrophen und industrielle Risiken sowie ein Konzept der geteilten Verantwortung in der Cloud.<br>Mehr Informationen dazu sind hier zu finden:<br>https://www.scaleway.com/en/security-and-resilience/<br>Eine detaillierte öffentliche Dokumentation der ToM gibt es aktuell noch nicht, diese ist uns aber für Juni zugesagt worden (Stand 26.05.2024) |

| TOM Allgemein | |
|---|---|
| Adresse der Hauptbetriebsstätte | phase-6 GmbH<br>Neue Schönhauser Str. 16<br>10178 Berlin, Deutschland |
| Zutrittskontrolle Büroräume | - Ein Pförtnerdienst bzw. ständig besetzter Empfangsbereich existiert nicht.<br>- Mechanische Sicherheitsschlösser sichern den Zugang zu sämtlichen Gebäuden, in denen Betriebsstätten unterhalten werden. Alle Schlüssel sind registriert und werden zentral ausgegeben und eingezogen. Dieser Vorgang wird protokolliert.<br>- Die Eingänge bzw. Türen zu den Betriebsstätten innerhalb der Gebäude sind ganztägig geschlossen.<br>- Unsere Hauptbetriebsstätte in Berlin verfügt zudem über ein elektronisches Zutrittssystem. Die elektronischen Schlüssel (RFID Transponder) werden gleichermaßen verwaltet wie die mechanischen Schlüssel. Der Zutritt wird elektronisch protokolliert und kann im Bedarfsfall ausgelesen werden. Es erfolgt keine regelmäßige Auswertung, allerdings werden die Protokolldaten nicht gelöscht. Darüber hinaus verfügt unsere Hauptbetriebsstätte über schwere Sicherheitstüren und ein Alarmsystem auf Basis von Bewegungsmeldern. Eine Weiterleitung eines Alarms an einen Wachdienst oder Mitarbeiter erfolgt nicht. Eine Videoüberwachung ist nicht vorhanden.<br>- Betriebsfremde Personen werden am Eingang vom Ansprechpartner abgeholt und während Ihrer Anwesenheit begleitet. Ein Besucherbuch wird nicht geführt, allerdings sind die Besucher und die Zeit im Kalender dokumentiert. |

| | |
|---|---|
| Zugangskontrolle / Zugriffskontrolle / Weitergabekontrolle | - Es existiert ein definierter Prozess zur Vergabe von Benutzerkennungen und Zugriffsberechtigungen bei der Neueinstellung oder dem Ausscheiden neuer Mitarbeiter<br>- Die Vergabe und Änderung der Zugriffsberechtigungen wird protokolliert<br>- Alle Personen / Mitarbeiter erhalten Ihr eigenes Benutzerkonto. Eine Firmenweite Passwort Policy gibt es nicht, stattdessen werden nur Passwörter ausgegeben, die mindestens 12-stellig sind und über Sonderzeichen verfügen. Je nach Dienst und Sensibilität gibt es unterschiedliche Mindestanforderungen an die Passwortsetzung oder eine 2-Faktor Authentifizierung. Eine Mindestgültigkeitsdauer kommt nicht zum Einsatz.<br>- Sofern Passwörter vergessen oder gar ausgespäht werden, wird durch den Administrator ein neues Initialpasswort vergeben<br>- Für die meisten der internen Dienste werden die Möglichkeiten des Single-Sign-Ons genutzt<br>- Bei Bedarf kann zusätzlich auf einen VPN Dienst zurückgegriffen werden. Bestimmte Dienste sind entweder nur über eingetragene IP-Adressen oder VPN zugänglich.<br>- Die Vergabe von Rechten wird ist formal geregelt und wird von dafür befugten Personen verwaltet<br>- Die Mitarbeiter nutzen für die Telearbeit die von der Firma gestellten Notebooks, deren Bildschirme nach 10 Minuten Inaktivität gesperrt werden. Auf privaten Geräten werden keine Nutzerdaten verarbeitet. |
| Eingabekontrolle | - Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts |
| Auftragskontrolle | - Auswahl von Auftragnehmern unter Sorgfaltsgesichtspunkten<br>- Schriftliche Festlegung der Weisungen<br>- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags |
| Verfügbarkeitskontrolle / Integrität | - Die von phase6 über Scalway S.A.S. betriebenen Services sind redundant ausgelegt und werden darüber hinaus in verschiedenen Regionen betrieben (z.B. in Frankreich und den Niederlanden). |
| Gewährleistungs des Zweckbindungs- / Trennungsgebotes | - Trennung von Produktiv- und Testsystemen |

Anlage 2

# Verzeichnis der Auftragsverarbeiter

Vertragsverhältnisse, bei denen der Auftragnehmer die Leistungen Dritter als reine Nebenleistung in Anspruch nimmt, um seine geschäftliche Tätigkeit auszuüben (z.B. Reinigungs-, Bewachungs- oder Transportleistungen) stellen keine Auftragsverarbeitung im Sinne der vorstehenden Regelungen dieses AV-Vertrages dar. Gleichwohl hat der Auftragsverarbeiter sicherzustellen, z.B. durch vertragliche Vereinbarungen oder Hinweise und Instruktionen, dass hierbei die Sicherheit der Daten nicht gefährdet wird und die Vorgaben dieses AV-Vertrages und der Datenschutzvorschriften eingehalten werden.

Alle Daten, die durch phase6 oder Auftragsverarbeiter verarbeitet werden, werden **regelmäßig und systematisch nur im Rechtsraum der DSGVO verarbeitet.** Sofern nachfolgend vom **Europäischen Wirtschaftsraum (EWR)** die Rede ist, ist damit **stets der Rechtsraum der DSGVO gemeint.** Die Rechtsgrundlage der Verarbeitung basiert auf Verträgen mit unseren Auftragsverarbeitern. Details sind der nachfolgenden Tabelle zu entnehmen.

## Liste der Auftragsverarbeiter / externe Empfänger von Daten

| Auftrags-verarbeiter | Unterauftrags-verarbeiter | Firmen-hauptsitz | Daten-residenz | Zweck der Verarbeitung | PII? | Speicher-dauer |
|---|---|---|---|---|---|---|
| **Datenresidenz**: Vom Auftragsverarbeiter vertraglich zugesicherter Standort der Datenverarbeitung.<br>**PII**: Daten, die dem Auftragsverarbeiter die Rückverfolgung oder Identifikation einer Person ermöglichen. | | | | | | |
| Hetzner Online GmbH (DPA) | - | DE | DE | Versand von E-Mails (sofern erforderlich oder gewünscht) | JA | 90 Tage bis dauerhaft |
| Horizon Alpha GmbH & Co KG (DPA) | - | DE | - | Dienstleistungen im Bereich der Entwicklung | JA | 30 Tage |
| Scaleway S.A.S. (DPA) | Siehe: https://www.scaleway.com/en/subprocessorlist/ | FR | NL, FR, PL | Betrieb der Serversysteme zur Erbringung des Lernangebots von Planet Pop | JA | Dauerhaft |

## Datenschutzbezogene Einschätzung

Die Datenschutzbezogene Einschätzung befasst sich nachfolgend mit Auftragsverarbeitern oder Unterauftragsverarbeitern, die Verflechtungen außerhalb des EWR haben oder bei denen persönlich identifizierbare Informationen (PII) verarbeitet werden.
Es werden keine besonders sensiblen personenbezogenen Daten verarbeitet. (Art 35 DSGVO)

**Horizon Alpha GmbH & Co KG:** phase6 stellt sicher, dass keine Daten außerhalb des EWR verarbeitet werden.

**Hetzner Online GmbH**: phase6 stellt sicher, dass keine Daten außerhalb des EWR verarbeitet werden.

**Scaleway S.A.S.**: phase6 stellt sicher, dass keine Daten außerhalb des EWR verarbeitet werden. Zwar nutzt Scaleway insbesondere im Marketing und im Support auch Unterauftragsverarbeiter in unsicheren Drittländern, dies ist aber im Kontext von phase6 nicht der Fall. Scaleway hat uns auf Anfrage bestätigt, dass die als "Processor" verarbeiteten Daten (alle Daten, die phase6 im Konto hochlädt) nur in eigenen europäischen Rechenzentren oder mit europäischen Diensten gespeichert oder verarbeitet werden.