Anlage 1

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

--- Stand: 26. Mai 2024 ---

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 (mit Ausnahme von Planet Pop, siehe unten) nur über einen einzigen Unterauftragsverarbeiter, die Hetzner Online GmbH. Die Hetzner Online GmbH hat ihrerseits keine weiteren Unterauftragsverarbeiter, da phase6 nur Server am Standort Deutschland gemietet hat. phase6 betreibt in den eigenen Räumlichkeiten keine Server, auf denen personenbezogene Daten von Kunden verarbeitet werden. phase6 mietet bereits seit mehr als einem Jahrzehnt sogenannte “dedicated” Server bei Hetzner an. Diese Server werden gemeinsam durch eigenes Personal und einen externen Dienstleister gewartet. Der Dienstleister ist in besonderem Maße fachkundig und bereits seit ununterbrochen über 10 Jahren für unsere Systemsicherheit mitverantwortlich. Unser Dienstleister stimmt sich stets mit unserer eigenen IT ab, sofern Änderungen notwendig sind.
Adresse des Betreibers	Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen Deutschland
Standort der Server	Gunzenhausen
TOM des Betreibers	https://www.hetzner.com/AV/TOM.pdf

TOM des Rechenzentrumsbetreibers (für Planet Pop)	
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. 8 rue de la Ville l’Evêque 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. Mehr Informationen dazu sind hier zu finden: https://www.scaleway.com/en/security-and-resilience/ 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 Neue Schönhauser Str. 16 10178 Berlin Deutschland
Zutrittskontrolle Büroräume	– Ein Pförtnerdienst bzw. ständig besetzter Empfangsbereich existiert nicht. - 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. - Die Eingänge bzw. Türen zu den Betriebsstätten innerhalb der Gebäude sind ganztägig geschlossen. - 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. - 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 - Die Vergabe und Änderung der Zugriffsberechtigungen wird protokolliert - 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. - Sofern Passwörter vergessen oder gar ausgespäht werden, wird durch den Administrator ein neues Initialpasswort vergeben - Für die meisten der internen Dienste werden die Möglichkeiten des Single-Sign-Ons genutzt - Bei Bedarf kann zusätzlich auf einen VPN Dienst zurückgegriffen werden. Bestimmte Dienste sind entweder nur über eingetragene IP-Adressen oder VPN zugänglich. – Die Vergabe von Rechten wird ist formal geregelt und wird von dafür befugten Personen verwaltet – Die Arbeit mit personenbezogenen Daten erfolgt fast ausschließlich über den Browser über die Server der Hetzner Online GmbH. Sofern Daten auf Notebooks der Mitarbeiter verarbeitet werden, werden diese nach der Bearbeitung gelöscht. Sofern USB-Sticks verwendet werden, werden diese von der Firma gestellt. USB-Sticks dienen dabei als temporäre Transportmöglichkeit für Daten, bspw. zum Scannen eines Dokumentes und sind nicht verschlüsselt. Nutzerdaten werden nicht gespeichert. – 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. – Zugriffe auf technische Systeme werden stets protokolliert. - Die Verbindung zu den Betriebssystemen unserer Server erfolgt ausschließlich durch geschultes Personal, per SSH und passwortlos per Key/Token. Bei 6 erfolglosen Anmeldeversuchen wird der Zugang bzw. die IP-Adresse automatisch für 10 Minuten gesperrt. Wiederholt sich dieses Muster mehr als 6-Mal, so erfolgt eine Sperrung für 24h. Sofern Besucher unserer Webservices wiederholt Fehlermeldungen auslösen, wird eine solche Verbindung bzw. IP-Adresse automatisch für 20 Minuten gesperrt. Wiederholt sich dieses Muster mehr als 6-Mal, so erfolgt eine Sperrung für 24h. - Die eingehenden und ausgehenden Verbindungen werden durch unseren Serverbetreiber an den Netzwerkroutern hinsichtlich ungewöhnlichem Verhalten (z.B. Denial of Service Attacken) überwacht und im Bedarfsfall isoliert. - Die Firewalls unserer Server werden gemeinsam durch eigenes Personal und einen externen Dienstleister gewartet. Der Dienstleister ist in besonderem Maße fachkundig und bereits seit ununterbrochen über 10 Jahren für unsere Systemsicherheit mitverantwortlich. Unser Dienstleister stimmt sich stets mit unserer eigenen IT ab, sofern Änderungen notwendig sind. - Unsere Applikationsserver akzeptieren nur Verbindungen von einer Whitelist von IP-Adressen, die unseren VPN-Service einschließt und über einen limitierten Bereich von Ports. Externe Verbindungen zu unseren Servern werden nur über unsere Load Balancer oder Ingress-Cluster über https akzeptiert. Unsere Dienste kommunizieren untereinander ausschließlich über VPN (Wireguard). - Die Aufbewahrungszeit für Protokolldateien beträgt mindestens 1 Jahr und maximal 2 Jahre.

	- Patches für unserer Server werden täglich geprüft und abhängig von der Schwere manuell installiert. Das Mindestwartungsintervall beträgt einen Monat oder weniger. - Jeder Server verfügt über ein Intrusion Detection System, das den täglichen Zugriff auf Dateien, Konfigurationsänderungen oder offene Ports überwacht. Darüber hinaus gibt es eine permanente Überwachung (alle 5 Minuten) der Server-Ressourcen (Speichernutzung, CPU Load) - Direkte personenbezogene Daten werden ausschließlich auf Servern unseres Rechenzentrumsbetreibers gespeichert, weshalb Daten die bei unseren Unterauftragsverarbeitern durch die Nutzung der Apps anfallen stets pseudonymisiert sind. Eine Repersonalisierung dieser Daten ist theoretisch dann möglich, wenn der Algorithmus bekannt ist, voller Zugriff auf die Datenbank von phase6 auf den Servern bei Hetzner und die Daten des Unterauftragsverarbeiters besteht und erhebliche Ressourcen dafür eingesetzt werden. - Die Verschlüsselungsalgorithmen und Sicherheitsprotokolle werden regelmäßig überprüft und aktualisiert. Zum Beispiel: - Die Webserver Apache und Nginx unterstützen das neueste TLS v1.3. Zugleich werden keine Verbindungen mit TLS 1.1 oder kleiner akzeptiert. SSLv2 oder v3 werden ebenfalls nicht akzeptiert. - Bei SSH-Verbindungen wird das v2-Protokoll erzwungen. Es werden nur Schlüsselpaare mit einer Mindestlänge von 2048 Bit akzeptiert. - Die Verbindungen zwischen unseren Servern laufen über Wireguard VPN - Unsere Firewalls sind so eingestellt, dass erst einmal alles blockiert wird und dann die minimal notwendigen IPs und Ports freigegeben werden. - Die Dateiverschlüsselung erfolgt mit RSA mit einer Mindestschlüssellänge von 2048 Bit.
Eingabekontrolle	- Protokollierung von Dateneingaben-, Änderungen und Löschungen - Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind (sofern Teil des Requests) - Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
Auftragskontrolle	- Auswahl von Auftragnehmern unter Sorgfaltsgesichtspunkten - Schriftliche Festlegung der Weisungen - Kontrolle der Einhaltung bei Auftragnehmern, bspw. durch Stichproben der verarbeiteten (Roh-)Daten oder der Konfigurationsparameter. - Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

Verfügbarkeitskontrolle / Integrität	- Es besteht ein Notfallkonzept bei Hardware-Defekten samt SLA unseres Rechenzentrumsbetreibers. Fällt eine Festplatte aus, so wird ein Festplattentausch beantragt und der Server aus unserem System genommen. Sobald die Parität der Festplatten wiederhergestellt ist, wird der Server manuell wieder in die Produktivumgebung eingebunden. Startet ein Server nicht mehr, so besteht die Möglichkeit der Aufschaltung einer Remote Konsole. Aufgrund der Menge der von uns betriebenen Server und der eingespielten Abläufe in unseren Teams, sind diese Maßnahmen Teil der täglichen Arbeits und nichts Besonderes. - Alle Systeme, bei denen Daten persistent gespeichert werden, verfügen über eine Redundanz und Echtzeitspiegelung. Darüber hinaus gibt es tägliche Backups in verschlüsselter Form, die in getrennten Datenzentren am gleichen Standort gesichert werden. - Alle Business-kritischen Daten werden zusätzlich zu den normalen Backups auch in einem anderen System gespeichert, das über eine komplett unterschiedliche Authentifizierung verfügt. Die Backups werden je nach Dienst inkrementell, mindestens jedoch einmal täglich erstellt. Alle Backups sind verschlüsselt. Die Daten werden dabei für einen gewissen Zeitraum auf Festplattensystemen vorgehalten und später auf nicht magnetischen Datenträgern archiviert.
Gewährleistungs des Zweckbindungs- / Trennungsgebotes	- Trennung von Produktiv- und Testsystemen - Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten System. - Folgende Datenkategorien liegen pseudonymisiert vor: Gelöschte Daten, sofern eine Aufbewahrungsfrist besteht; Business Analytics Daten; personenbezogene Daten außerhalb der Serversysteme von Hetzner