Wolkenwächter®

Auftragsverarbeitungs-vertrag (AVV)

Wolkenwächter (Managed Service)

1. Gegenstand und Dauer

1.1 Dieser AVV konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien im Rahmen des Hauptvertrags über „Wolkenwächter Managed Services“ (nachfolgend „Hauptvertrag“).

1.2 Gegenstand: Durch die Erbringung der definierten Leistungen erhält beyond expectations GmbH, Modecenterstraße 22/D40, 1030 Wien (im Folgenden der „Auftragsverarbeiter“) Zugriff auf personenbezogene Daten, die der Auftragsverarbeiter für den jeweiligen Kunden (im Folgenden „Verantwortlicher“) ausschließlich im Auftrag und nach Weisung des Verantwortlichen verarbeitet. Umfang und Zweck der Datenverarbeitung durch den Auftragsverarbeiter ergeben sich aus dem Hauptvertrag und etwaigen zugehörigen Leistungsbeschreibungen. Dem Verantwortlichen obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

1.3 Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten gilt mit Zeichnung des Hauptvertrages die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor. Sofern in diesem AVV jedoch nichts Abweichendes geregelt wird, bleiben die Bestimmungen des Hauptvertrags und der Allgemeinen Geschäftsbedingungen unberührt (das gilt insbesondere für die Bestimmungen zu Haftung, Rechtswahl und Gerichtsstand in den Allgemeinen Geschäftsbedingungen des Auftragsverarbeiters).

1.4 Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragsverarbeiter und seine Beschäftigten oder durch den Auftragsverarbeiter Beauftragte mit personenbezogenen Daten in

Berührung kommen, die vom Verantwortlichen stammen oder für den Verantwortlichen erhoben wurden.

1.5 Dauer: Die Laufzeit dieses AVV richtet sich nach der Laufzeit des Hauptvertrags, sofern sich aus den nachfolgenden Bestimmungen nicht darüber hinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

2. Weisungsrecht

2.1 Der Auftragsverarbeiter darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Verantwortlichen erheben, verarbeiten oder nutzen. Wird der Auftragsverarbeiter durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit.

2.2 Die Weisungen des Verantwortlichen werden anfänglich durch diesen Vertrag festgelegt und können vom Verantwortlichen danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Verantwortliche ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen im Hinblick auf die Berichtigung, Löschung und Sperrung von Daten.

2.3 Alle erteilten Weisungen sind vom Verantwortlichen zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

2.4 Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung des Verantwortlichen gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Verantwortlichen unverzüglich darauf hinzuweisen. Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis diese durch den Verantwortlichen bestätigt oder geändert wird. Der Auftragsverarbeiter darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen. Eine Pflicht zur Ablehnung besteht nicht. Der Auftragsverarbeiter haftet nicht für Schäden, die sich aus der Befolgung einer rechtswidrigen Weisung des Verantwortlichen ergeben.

3. Art der verarbeiteten Daten, Kreis der Betroffenen

3.1 Art der verarbeiteten Daten:

- Technische Identifikatoren (IP-Adressen, User-IDs, Hash-Werte).
- Protokolldaten (Logfiles, Audit-Logs, Zugriffszeiten).
- Kontaktdaten von Administratoren/Usern (Name, E-Mail-Adresse), soweit diese in den Systemen hinterlegt sind.
- Konfigurationsdaten (Berechtigungen, Rollen).

3.2 Kreis der Betroffenen:

- Mitarbeiter des Kunden (User, Administratoren).
- Externe Partner des Kunden (sofern im System angelegt).

4. Schutzmaßnahmen des Auftragsverarbeiters

4.1 Der Auftragsverarbeiter ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Verantwortlichen erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

4.2 Der Auftragsverarbeiter wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er hat die in Punkt 10 genannten technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Verantwortlichen gem. Art. 32 DSGVO getroffen, die der Verantwortliche als angemessen anerkennt. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragsverarbeiter vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte und gesetzlich vorgeschriebene Schutzniveau nicht unterschritten wird.

4.3 Eine Weitergabe personenbezogener Daten in ein Drittland (außerhalb des EWR) erfolgt nur unter den Voraussetzungen der Art. 44 ff. DSGVO.

4.4 Den bei der Datenverarbeitung durch den Auftragsverarbeiter beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragsverarbeiter wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (nachfolgend „Mitarbeiter"), entsprechend verpflichten (Verpflichtung

zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen.

4.5 Der Auftragsverarbeiter hat einen Datenschutzbeauftragten benannt. Der Datenschutzbeauftragte des Auftragsverarbeiters ist heyData GmbH, Schützenstr. 5, 10117 Berlin, datenschutz@heydata.eu, www.heydata.eu.

5. Unterauftragsverarbeiter (Sub-Dienstleister)

5.1 Genehmigung: Der Kunde erteilt BE-X die allgemeine Genehmigung, weitere Sub-Dienstleister hinzuzuziehen.

5.2 Genehmigte Sub-Dienstleister: Zum Zeitpunkt des Vertragsschlusses sind folgende Unterauftragsverarbeiter genehmigt:

- Google Cloud EMEA Ltd., Gordon House, Barrow Street, Dublin 4, Irland; Standort: EU (Irland, Belgien, Niederlande). Zweck: Cloud-Infrastruktur und KI-gestützte Datenanalyse (Google Vertex AI) zur Erbringung des Monitoring- und Alarming-Service.
- Freshworks Inc., 2950 S. Delaware Street, Suite 201, San Mateo, California 94403, USA; Standort: USA. Zweck: Ticket-Management und -Support; Rechtsgrundlage: Angemessenheitsbeschluss gem. Art. 45 DSGVO.

5.3 Änderungen: BE-X informiert den Kunden über geplante Änderungen (Hinzufügung/Ersetzung) von Sub-Dienstleistern. Der Kunde kann innerhalb von 14 Tagen Einspruch erheben, wenn durch die Hinzuziehung eines neuen Unterauftragsverarbeiters geltende gesetzliche Bestimmungen verletzt würden oder dies zu einer Verschlechterung des Schutzniveaus für die Verarbeitung personenbezogener Daten führen würde. Der Einspruch ist schriftlich zu begründen. Erfolgt kein Einspruch, gilt die Änderung als genehmigt.

5.4 Falls der Verantwortliche gegen einen Unterauftragsverarbeiter rechtmäßig Einspruch erhebt und der Auftragsverarbeiter diesem Einspruch nicht Rechnung tragen kann, wird der Auftragsverarbeiter den Verantwortlichen entsprechend informieren. Der Verantwortliche und der Auftragsverarbeiter verpflichten sich, sich über die Hinzuziehung einvernehmlich zu einigen. Da der Service „Wolkenwächter“ technisch zwingend auf bestimmten Plattformen (z.B. Google Vertex AI) basiert, steht dem Kunden bei einem berechtigten Einspruch ein Sonderkündigungsrecht zu.

5.5 Vertragskette: BE-X stellt sicher, dass mit Sub-Dienstleistern Verträge geschlossen werden, die

mit diesem AVV vergleichbar sind und den Anforderungen des Art. 28 DSGVO entsprechen, bevor personenbezogene Daten des Verantwortlichen durch den Unterauftragsverarbeiter verarbeitet werden. Das Datenschutzniveau wird ggf. durch die Implementierung ergänzender technischer Maßnahmen sichergestellt.

6. Kontrollrechte des Kunden (Audit)

6.1 Der Kunde hat das Recht, die Einhaltung dieses AVV zu überprüfen.

6.2 Da BE-X die Services in Umgebungen der Sub-Dienstleister erbringt, erfolgt der Nachweis der Datensicherheit für die Rechenzentren und Cloud-Infrastruktur ausschließlich durch Vorlage aktueller Testate unabhängiger Dritter (z.B. SOC 2 Typ II Bericht, ISO 27001 Zertifikat) der Sub-Dienstleister. Direkte Vor-Ort-Prüfungen in den Rechenzentren der Sub-Dienstleister sind ausgeschlossen.

6.3 Für die eigenen Geschäftsräume und Prozesse von BE-X hat der Kunde das Recht, einmal im Jahr Prüfungen durch einen unabhängigen, zur Verschwiegenheit verpflichteten Auditor durchführen zu lassen. Prüfungen sind mit einer Vorlaufzeit von 30 Kalendertagen schriftlich anzukündigen und dürfen den Geschäftsbetrieb von BE-X nicht unangemessen beeinträchtigen. Die Kosten der Prüfung trägt der Kunde.

7. Datenschutzverletzung, Meldepflichten und Unterstützung

7.1 Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich informieren, wenn der Auftragsverarbeiter Kenntnis von einer Verletzung des Schutzes personenbezogener Daten in Bezug auf die Services erlangt.

7.2 Der Auftragsverarbeiter wird die Verletzung des Schutzes personenbezogener Daten unverzüglich untersuchen, sofern sich diese in der Infrastruktur des Auftragsverarbeiters oder in einem anderen Bereich, für den der Auftragsverarbeiter verantwortlich ist, ereignet hat, und wird den Verantwortlichen gemäß den folgenden Punkten unterstützen.

7.3 Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Möglichkeit bei der Erfüllung seiner Verpflichtungen zur Einhaltung der Betroffenenrechte und bei der Einhaltung seiner Verpflichtungen in Bezug auf die Sicherheit der Verarbeitung, die Mitteilung und Benachrichtigung

über eine Verletzung des Schutzes personenbezogener Daten und die Durchführung einer Datenschutz-Folgenabschätzung unter Berücksichtigung der dem Auftragsverarbeiter zur Verfügung stehenden Informationen.

7.4 Der Verantwortliche wird im Rahmen dieser AVV benötigte Unterstützung durch den Auftragsverarbeiter in Textform anfordern. Abweichend von den Regelungen des Hauptvertrages hat der Auftragsverarbeiter für seine im Rahmen dieser AVV erbrachten Leistungen, insb. bei der Erfüllung von Unterstützungsleistungen und ergänzenden Weisungen, Anspruch auf folgende Vergütung:

7.4.1 Die vom Auftragsverarbeiter erbrachten Leistungen werden grundsätzlich nach Zeithonorar auf Basis von Stundensätzen, zzgl. anfallender Sachkosten, verrechnet. Verrechnet wird die Gesamtzeit, die der Auftragsverarbeiter (und jeder seiner im Rahmen dieses AVV eingesetzten Mitarbeiter und/oder Sub-Auftragsnehmer) der vertragsgegenständlichen Tätigkeit widmet. Als Stundensatz werden EUR 150,- pro Beratungsstunde zuzüglich Umsatzsteuer vereinbart. Verrechnet wird nach tatsächlich geleisteter Echtzeit, wobei die abrechenbare Leistungszeit vom Auftragsverarbeiter in 15-Minuten-Schritten erfasst wird. Der Auftragsverarbeiter wird detaillierte Leistungszeitnachweise führen.

8. Anfragen und Rechte betroffener Personen

8.1 Soweit gesetzlich zulässig, informiert der Auftragsverarbeiter den Verantwortlichen über Anträge von betroffenen Personen, die ihre Betroffenenrechte direkt gegenüber dem Auftragsverarbeiter in Bezug auf personenbezogene Daten des Verantwortlichen geltend machen. Der Verantwortliche ist für die Beantwortung solcher Anträge zuständig.

8.2 Falls eine betroffene Person einen Anspruch aufgrund der Verletzung ihrer Betroffenenrechte direkt gegenüber dem Auftragsverarbeiter geltend macht, entschädigt der Verantwortliche den Auftragsverarbeiter für sämtliche Kosten, Gebühren, Schäden, Aufwendungen oder Verluste, die sich aus einem solchen Anspruch ergeben, sofern der Auftragsverarbeiter den Verantwortlichen über den Anspruch in Kenntnis gesetzt und ihm die Möglichkeit gegeben hat, in der Abwehr und Beilegung des Anspruchs mit dem Auftragsverarbeiter zusammenzuarbeiten.

8.3 Im Rahmen der im Hauptvertrag enthaltenen Bedingungen kann der Verantwortliche vom Auftragsverarbeiter Beträge einfordern, die er an eine betroffene Person gezahlt hat, deren Betroffenenrechte durch einen schuldhaft verursachten Verstoß des Auftragsverarbeiters gegen

seine Verpflichtungen aus der DSGVO verletzt wurden, sofern er den Auftragsverarbeiter über den Anspruch in Kenntnis gesetzt und ihm die Möglichkeit gegeben hat, in der Abwehr und Beilegung des Anspruchs mit dem Verantwortlichen zusammenzuarbeiten.

9. Löschung und Rückgabe

9.1 Nach Beendigung des Hauptvertrags löscht BE-X nach Wahl des Kunden entweder alle personenbezogenen Daten oder gibt sie in einem gängigen, maschinenlesbaren Format (z.B. CSV, JSON) zurück, sofern keine gesetzliche Aufbewahrungspflicht besteht. Die Rückgabe oder Löschung erfolgt innerhalb von 30 Kalendertagen nach Vertragsende. BE-X bestätigt die vollständige Löschung schriftlich.

9.2 Der Kunde nimmt zur Kenntnis, dass bei Cloud-Diensten (z.B. Google Cloud) aus technischen Gründen (Backup-Zyklen, Disaster Recovery) eine vollständige Löschung aus allen Speichern bis zu 180 Tage dauern kann („Residual Data“). Der Zugriff auf diese Daten wird in der Zwischenzeit gesperrt.

10. Technisch-organisatorische Maßnahmen des Auftragsverarbeiters

Dieser Abschnitt fasst die technischen und organisatorischen Maßnahmen im Sinne von Art. 32 Abs. 1 DSGVO zusammen, die für Verarbeitungen in der Sphäre von BE-X gelten. Die Maßnahmen gliedern sich in zwei Verantwortungsbereiche:

a) Maßnahmen in der direkten Verantwortung von BE-X: Betrifft eigene Geschäftsräume, Endgeräte, Zugriffsmanagement auf Cloud-Dienste, Softwareentwicklung und betriebliche Prozesse.

b) Maßnahmen der Rechenzentrumsbetreiber: Die physische Infrastruktur wird in zwei professionellen, zertifizierten Rechenzentren betrieben. Die dort implementierten organisatorischen Sicherheitsmaßnahmen (Zutrittskontrolle, Brandschutz, Klimatisierung, Stromversorgung, Videoüberwachung) werden durch die jeweiligen Betreiber verantwortet und sind in den Abschnitten 10.1.1 und 10.3 entsprechend angeführt.

Für die technischen und organisatorischen Maßnahmen der Sub-Dienstleister Google Cloud und Freshworks wird auf Kapitel 11 verwiesen.

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

10.1.1 Zutrittskontrolle: Die folgenden Maßnahmen zur physischen Zutrittskontrolle werden durch die Betreiber der beiden Rechenzentren implementiert und aufrechterhalten:

- Alarmanlage
- Absicherung von Gebäudeschächten
- Automatisches Zugangskontrollsystem
- Biometrische Zugangssperren
- Chipkarten-/Transponder-Schließsystem
- Manuelles Schließsystem (z.B. Schlüssel)
- Sicherheitsschlösser
- Videoüberwachung der Zugänge
- Personenkontrolle beim Pförtner oder Empfang
- Protokollierung der Besucher (z.B. Besucherbuch)
- Sorgfältige Auswahl von Sicherheitspersonal
- Besucher nur in Begleitung durch Mitarbeiter

Für die Geschäftsräume von BE-X gelten: Manuelles Schließsystem, Sicherheitsschlösser, Besucher nur in Begleitung durch Mitarbeiter.

10.1.2 Zugangskontrolle: Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zugang zu den Datenverarbeitungssystemen haben:

- Authentifikation mit Benutzer und Passwort
- Einsatz von Anti-Viren-Software
- Einsatz von Firewalls
- Verschlüsselung von Datenträgern
- Automatische Desktopsperre
- Verschlüsselung von Notebooks / Tablets
- Verwaltung von Benutzerberechtigungen
- Erstellen von Benutzerprofilen
- Nutzung von 2-Faktor-Authentifizierung
- Allgemeine Unternehmens-Richtlinie zum Datenschutz oder zur Sicherheit
- Unternehmens-Richtlinie für sichere Passwörter
- Unternehmens-Richtlinie zur Verwendung mobiler Geräte
- Allgemeine Anweisung, bei Verlassen des Arbeitsplatzes Desktop manuell zu sperren

10.1.3 Zugriffskontrolle: Folgende implementierte Maßnahmen stellen sicher, dass Unbefugte

keinen Zugriff auf personenbezogene Daten haben:

- Vernichtung von Datenträgern mindestens nach DIN 66399
- Einsatz eines Berechtigungskonzepts
- Anzahl der Administratoren ist so klein wie möglich gehalten
- Verwaltung der Benutzerrechte durch Systemadministratoren

10.1.4 Trennungskontrolle: Folgende Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden:

- Mandantentrennung
- separate Datenspeicherung pro Kunde
- logische Isolation auf Applikationsebene
- Trennung von Produktiv- und Testsystem
- Erstellung eines Berechtigungskonzepts

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

10.2.1 Weitergabekontrolle: Es ist sichergestellt, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:

- TLS-Verschlüsselung der API-Kommunikation
- Verschlüsselung der Kundendaten at rest
- Secrets-/Credential-Management für die API-Keys und Zugangsdaten der Kundensysteme
- WLAN-Verschlüsselung (WPA2 mit starkem Passwort)
- Protokollierung von Zugriffen und Abrufen
- Bereitstellung von Daten über verschlüsselte Verbindungen wie SFTP oder HTTPS

10.2.2 Eingabekontrolle: Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat:

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit der Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

10.3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO): Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt

und für den Kunden stets verfügbar sind.

Die folgenden physischen Maßnahmen werden durch die Betreiber der Rechenzentren sichergestellt:

- Feuerlöschgeräte in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Klimaanlage in Serverräumen
- Schutzsteckdosenleisten in Serverräume
- Unterbrechungsfreie Stromversorgung (USV)
- RAID-System / Festplattenspiegelung
- Videoüberwachung in Serverräumen
- Keine sanitären Anlagen im oder oberhalb des Serverraums

Die folgenden Maßnahmen verantwortet BE-X:

- Regelmäßige Backups
- Erstellung eines Backup- & Recoverykonzepts
- Kontrolle des Sicherungsvorgangs
- Erstellen eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)

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

10.4.1 Datenschutz-Management: Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

- Verwendung der heyData-Plattform zum Datenschutz-Management
- Bestellung des Datenschutzbeauftragten heyData
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Regelmäßige Schulungen der Mitarbeiter im Datenschutz
- Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO)

10.4.2 Incident-Response-Management: Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden:

- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)
- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO)

- Einbindung des Datenschutzbeauftragten in Sicherheitsvorfälle und Datenpannen
- Unverzügliche Information des Kunden bei Sicherheitsvorfällen, die dessen Daten betreffen

10.4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO): Die folgenden implementierten Maßnahmen tragen den Voraussetzungen der Prinzipien "Privacy by design" und "Privacy by default" Rechnung:

- Schulung der Mitarbeiter im "Privacy by design" und "Privacy by default"
- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.

10.4.4 Auftragskontrolle: Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten nur entsprechend der Weisungen verarbeitet werden können:

- Schriftliche Weisungen an den Auftragnehmer oder Weisungen in Textform (z.B. durch Auftragsverarbeitungsvertrag)
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags, z.B. durch Anfrage entsprechender Bestätigungen
- Bestätigung von Auftragnehmern, dass sie ihre eigenen Mitarbeiter auf das Datengeheimnis verpflichten (typischerweise im Auftragsverarbeitungsvertrag)

10.4.5 Technische Sicherheitsüberprüfung: Folgende Maßnahmen gewährleisten die regelmäßige Überprüfung der technischen Sicherheitsmaßnahmen:

- Patch-Management mit definierten Fristen für sicherheitskritische Updates

11. Technisch-organisatorische Maßnahmen der Sub-Dienstleister

11.1 Dieser Abschnitt fasst die von den Sub-Dienstleistern getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 Abs. 1 DSGVO für Verarbeitungen in der Sphäre der Sub-Dienstleister zusammen. BE-X gewährleistet, dass die Unterauftragsverarbeiter ein dem Risiko angemessenes Schutzniveau gemäß Art. 32 DSGVO aufrechterhalten, und weist dies auf Anfrage des Kunden durch die in Punkt 6.2 genannten Zertifizierungen und Berichte nach.

11.2 Für die in der Cloud-Infrastruktur von Google Cloud EMEA Ltd. verarbeiteten Daten gelten die von Google implementierten und aufrechterhaltenen technischen und organisatorischen Maßnahmen gemäß Anhang 2 des Google Cloud Data Processing Addendum, abrufbar unter https://cloud.google.com/terms/data-processing-addendum. Die aktuellen Zertifizierungen (ISO

27001, ISO 27017, ISO 27018, SOC 2/3) sind unter https://cloud.google.com/security/compliance/services-in-scope einsehbar.

11.3 Für die in der Infrastruktur von Freshworks Inc., 2950 S. Delaware Street, Suite 201, San Mateo, California 94403, USA, verarbeiteten Daten gelten die von Freshworks implementierten und aufrechterhaltenen technischen und organisatorischen Maßnahmen, abrufbar unter https://www.freshworks.com/technical-organisational-measures/.