VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG

Enterprise

Diese Vereinbarung zur Auftragsverarbeitung ("**AVV**") ist Bestandteil des Hauptvertrags (wie unten definiert) und spiegelt die Zustimmung der Parteien in Bezug auf die Verarbeitung personenbezogener Daten wider. Sollten sich die Bestimmungen dieser AVV und des Hauptvertrags widersprechen, so haben die Bestimmungen dieser AVV Vorrang. Diese AVV besteht aus dem Hauptteil der AVV und ihren Anlagen.

Diese AVV wird nicht gültig und rechtsverbindlich, wenn der Abonnent keine Partei der Hauptvereinbarung ist. Die Parteien vereinbaren, dass diese AVV alle früheren Vereinbarungen zur Auftragsverarbeitung ersetzt.

Wenn der Abonnent Dienste von Cyren indirekt über einen autorisierten Wiederverkäufer oder einen anderen Partner von Cyren abonniert (unabhängig davon, ob Cyren dem Abonnenten direkt Support und Wartung anbietet) und mit diesem Wiederverkäufer oder Partner eine Vereinbarung zur Auftragsverarbeitung in Bezug auf die Dienste abgeschlossen hat, ist diese AVV nicht auf den Abonnenten anwendbar.

Einleitung/Präambel

Cyren bietet dem Abonnenten Produkte und Dienste an wie im Hauptvertrag näher definiert (zusammen die "**Dienste**"), die die Sicherheit elektronischer Kommunikationssysteme des Abonnenten verbessern. Die Dienste sind dazu bestimmt, Sicherheitsbedrohungen, Massen-E-Mails und Betrugsversuche zu erkennen, zu verhindern und zu verwalten oder bei der Erkennung, Verhinderung und Verwaltung von Sicherheitsbedrohungen, Massen-E-Mails und Betrugsversuchen zu helfen, indem sie in oder gegen Systeme, Netzwerke, Geräte, Dateien und andere Daten eingesetzt werden. Zu diesem Zweck scannt/überprüft Cyren die elektronische Kommunikation des Abonnenten und ermöglicht es dem Abonnenten hierdurch, Angriffe auf seine Netzwerke durch bösartige Software und/oder betrügerische Kommunikation oder gefährliche E-Mails (Viren, Malware) oder Massenmailings (SPAM) zu erkennen.

Im Rahmen der Verarbeitung personenbezogener Daten durch Cyren in Übereinstimmung mit den Bestimmungen dieser AVV sind die personenbezogenen Daten des Abonnenten Gegenstand der folgenden grundlegenden Verarbeitungsaktivitäten:

1. Bereitstellung der Dienste, die der Abonnent gemäß dem Hauptvertrag erworben hat, und Ermöglichung der Nutzung dieser Dienste;

2. Erbringung von Kontoverwaltungsleistungen und technischen Unterstützungsdiensten für Kunden.

1. DEFINITIONEN

a. "**Verbundenes Unternehmen**" hat die gleiche Bedeutung wie im Hauptvertrag.

b. "**Verbindliche Unternehmensregeln**" sind verbindliche interne Datenschutzvorschriften im Sinne von Artikel 47 der Verordnung (EU) 2016/679 ("**DSGVO**"), die von der zuständigen Aufsichtsbehörde genehmigt wurden.

c. "**Cyren**" bezeichnet das Cyren Unternehmen, mit dem der Hauptvertrag unterzeichnet wurde.

d. "**Verantwortlicher**", "**Auftragsverarbeiter**", "**Betroffener**", "**Verletzung des Schutzes personenbezogener Daten**", **"Verarbeitung" und "verarbeiten"** haben jeweils die Definitionen und Bedeutungen, die ihnen in den anwendbaren Datenschutzgesetzen zugewiesen werden, und schließen alle gleichwertigen oder entsprechenden Begriffe ein, die in diesen anwendbaren Datenschutzgesetzen verwendet werden.

e. "**AVV"** bezeichnet diese Vereinbarung zur Auftragsverarbeitung.

f. "**Datenschutzgesetze**" bezeichnet alle Gesetze und Vorschriften, die auf die Verarbeitung personenbezogener Daten im Rahmen des Hauptvertrags anwendbar sind, einschließlich solcher Gesetze, wie beispielsweise und ohne Einschränkung die Datenschutz-Grundverordnung (DSGVO), der California Consumer Privacy Act (CCPA) und der Personal Information Protection and Electronic Documents Act (PIPEDA).

g. **"Hauptvertrag"** bezeichnet den Cyren Abonnementsvertrag für Endnutzer – Europa (oder einen anderen Verkaufs-, Lizenz-, Beta-, Evaluierungs- oder ähnlichen Vertrag, falls zutreffend) einschließlich aller damit verbundenen Aufträge, die zwischen Cyren und dem Abonnenten abgeschlossen wurden.

h. "**Malware**" bezeichnet Computersoftware oder Programmcode, der dazu bestimmt ist, die Leistung oder Sicherheit eines Computerprogramms oder von Daten zu beschädigen oder zu verringern.

i. "**Personenbezogene Daten**" sind alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen und die Cyren vom Abonnenten in Verbindung mit dem Hauptvertrag zur Verfügung gestellt wurden.

j. "**Standardvertragsklauseln**" sind Standarddatenschutzklauseln, die angemessene Garantien für die Übermittlung personenbezogener Daten in Drittländer bieten und von der Europäischen Kommission angenommen wurden. Sobald die Standarddatenschutzklauseln geändert oder ersetzt worden sind, bilden die geänderten bzw. ersetzenden Klauseln die Standardvertragsklauseln.

k. "**Dienste**" hat die gleiche Bedeutung wie im Hauptvertrag.

l. "**Spam**" bezeichnet eine große Anzahl unerwünschter E-Mail-Nachrichten mit ähnlichem Inhalt, die in einem einzigen Vorgang oder in einer Reihe zusammenhängender Vorgänge gesendet oder empfangen werden.

m. "**Unterauftragsverarbeiter**" bezeichnet einen Auftragsverarbeiter, der von einem anderen Auftragsverarbeiter als Unterauftragnehmer beauftragt wird.

n. "**Support-Dienstleistung"** bedeutet technische Support-Dienstleistungen in Übereinstimmung mit den geltenden SLAs.

o. "**Abonnent**" bedeutet die Partei des Hauptvertrags.

p. "**Drittland**" bedeutet jedes Land, das weder ein Mitgliedstaat der Europäischen Union (EU) noch ein Mitglied des Europäischen Wirtschaftsraums (EWR) ist.

q. "**Unterauftragsverarbeiter aus einem Drittland**" bezeichnet einen Unterauftragsverarbeiter oder einen Unter-Unterauftragsverarbeiter, der in einem Drittland ansässig ist oder anderweitig personenbezogene Daten in einem Drittland verarbeitet.

2. UMFANG

2.1 **Rollen der Parteien.** Die Parteien erkennen an und vereinbaren, dass in Bezug auf die Verarbeitung von personenbezogenen Daten der Abonnent der Verantwortliche und Cyren der Auftragsverarbeiter ist.

2.2 **Einhaltung der Datenschutzgesetze.** Der Abonnent ist verpflichtet, während der Laufzeit dieser AVV in jeder Hinsicht alle anwendbaren Datenschutzgesetze einzuhalten, insbesondere alle Verpflichtungen in Bezug auf die Rechte der Betroffenen gemäß Art. 15-23 DSGVO und alle Informationspflichten gegenüber den Betroffenen gemäß Art. 12-14 DSGVO. Die Verantwortlichkeiten des Abonnenten in dieser Hinsicht umfassen, sind aber nicht beschränkt auf: (i) sicherzustellen, dass die Anweisungen, die er Cyren zum Zweck der Verarbeitung personenbezogener Daten erteilt, mit allen anwendbaren Datenschutzgesetzen übereinstimmen; (ii) sicherzustellen, dass es eine rechtmäßige Grundlage für die Verarbeitung personenbezogener Daten durch Cyren gibt; (iii) sicherzustellen, dass alle sensiblen personenbezogenen Daten entfernt werden, bevor Daten oder Anfragen an Cyren übermittelt werden; und (iv) sicherzustellen, dass alle erforderlichen Einwilligungen von den Betroffenen eingeholt wurden, um die Verarbeitung personenbezogener Daten durch den Abonnenten und Cyren zu ermöglichen (einschließlich, aber nicht beschränkt auf besondere Kategorien von Daten).

3. ANWEISUNGEN DES ABONNEMENTEN

3.1 Cyren wird personenbezogene Daten nur in dem Umfang verarbeiten, der gemäß den Anweisungen des Abonnenten und den Bestimmungen des Hauptvertrags erforderlich ist. Dies umfasst die Verarbeitung personenbezogener Daten im Rahmen der vom Abonnenten bestellten Dienste und zur Erbringung dieser Dienste gemäß des Hauptvertrags.
Der Abonnent weist Cyren an, personenbezogene Daten zu verarbeiten: (i) wenn die Verarbeitung für die Erbringung der Dienste und in Übereinstimmung mit dem Hauptvertrag erforderlich ist; (ii) als Teil einer Verarbeitung, die vom Abonnenten oder den Endnutzern des Abonnenten bei der Nutzung der Dienste veranlasst wird, und (iii) zur Erfüllung anderer angemessener Anweisungen des Abonnenten (z. B. per E-Mail oder über Supportanfragen), soweit diese mit den Bedingungen des Hauptvertrags und dieser AVV übereinstimmen.

3.2 **Individuelle Anweisungen.** Der Abonnent weist Cyren an, personenbezogene Daten wie in Ziffer 3.1 oben beschrieben zu verarbeiten. Darüber hinausgehende Einzelanweisungen sind zwischen den Parteien abzustimmen und durch Konfiguration der Dienste über die jeweiligen Kundenportale oder Supportprozesse zu dokumentieren (oder anderweitig schriftlich zu vereinbaren). Cyren wird den Abonnenten unverzüglich informieren, wenn es der Ansicht ist,

dass eine Anweisung gegen Datenschutzgesetze verstößt. Cyren ist in diesem Fall berechtigt, die Ausführung der Weisung bis zu ihrer Bestätigung oder Änderung durch den Abonnenten auszusetzen.

4. ARTEN VON PERSONENBEZOGENEN DATEN UND KATEGORIEN VON BETROFFENEN

4.1 **Arten von Daten.** Die Verarbeitung personenbezogener Daten im Geltungsbereich dieser AVV bezieht sich auf die folgenden Datenarten/Datenkategorien:

- Nutzerdaten (d.h. Daten, die im Rahmen des Registrierungsprozesses übermittelt werden);
- Inhaltsdaten (d.h. Inhalt der elektronischen Kommunikation);
- Nutzungsdaten (d.h. Informationen, die bei der Nutzung eines Dienstes anfallen);
- Kommunikations-Metadaten (d.h. Daten, die zum Zweck der Übertragung, der Verteilung oder des Austauschs von elektronischen Kommunikationsinhalten verarbeitet werden).

Die Daten können, je nach den genutzten Diensten, Folgendes umfassen:

- Name, E-Mail-Umschlag, E-Mail-Betreff
- Benutzerauthentifizierungsdaten wie z.B. Benutzer-IDs (d.h. aus dem Unternehmensverzeichnis des Kunden und/oder wie von Cyren zugewiesen);
- Transaktionsprotokolle;
- IP-Adressen;
- URLs;
- Telefonnummern;
- Inhalts- und Verbindungsdaten;
- vollständige E-Mail mit angehängten Dateien.

4.2 **Kategorien von Betroffenen.** Die Gruppe derjenigen Personen, die von der Verarbeitung personenbezogener Daten im Geltungsbereich dieser AVV betroffen sind, umfasst:

- Angestellte des Abonnenten oder andere autorisierte Benutzer;
- Personen, mit denen die Nutzer per E-Mail korrespondieren;
- Dritte, deren personenbezogene Daten im Inhalt der im Rahmen der Dienste zuzuordnenden E-Mails enthalten sind.

5. LAUFZEIT UND KÜNDIGUNG

Die Laufzeit dieser AVV, einschließlich ihrer Anlagen, entspricht der Laufzeit des Hauptvertrags. Die AVV (einschließlich ihrer Anlagen) und die Verarbeitung personenbezogener Daten gemäß ihren Bestimmungen enden gleichzeitig und automatisch mit der Beendigung des Hauptvertrags.

6. TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

6.1 Cyren setzt die in **Anlage 1** beschriebenen technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit um und hält diese aufrecht.

6.2 Die technischen und organisatorischen Maßnahmen sind dem technischen Fortschritt unterworfen. Cyren kann daher alternative, angemessene Maßnahmen ergreifen, die das Sicherheitsniveau der in **Anlage 1** beschriebenen Maßnahmen erreichen oder übertreffen. Cyren wird alle wesentlichen Änderungen dokumentieren.

7. VERPFLICHTUNGEN VON CYREN

Zusätzlich zu den anderen Verpflichtungen, die sich aus dieser AVV ergeben, wird Cyren auch die folgenden Pflichten erfüllen:

7.1 **Datenschutzbeauftragter.** Schriftliche Benennung eines Datenschutzbeauftragten oder - sofern gesetzlich nicht vorgeschrieben - eines Datenschutzexperten;

7.2 **Verpflichtung auf Vertraulichkeit**. Sicherstellung, dass alle Mitarbeiter von Cyren, die im Rahmen dieser AVV Zugang zu personenbezogenen Daten haben, auf Vertraulichkeit und das Fernmeldegeheimnis verpflichtet wurden, sowie darauf, die personenbezogenen Daten streng vertraulich zu behandeln, und dass sie (i) über die sich aus dieser AVV ergebenden geltenden Datenschutzverpflichtungen und (ii) darüber informiert wurden, dass sie verpflichtet sind, die personenbezogenen Daten nur gemäß den Anweisungen des Abonnenten und für die angegebenen Zwecke zu verwenden;

7.3 **Unterstützung bei Anfragen von Betroffenen.** Befolgung der in Abschnitt 8 genannten Anforderungen für die Unterstützung des Abonnenten bei der Beantwortung von Anfragen Betroffener;

7.4 **Benachrichtigung im Falle von Ermittlungen.** Unverzügliche Benachrichtigung des Abonnenten über Überwachungsaktivitäten, Untersuchungen und andere Maßnahmen von Datenschutzaufsichtsbehörden oder anderen Behörden (z. B. Strafverfolgungsbehörden, Nachrichtendienste usw.), sofern dies gesetzlich zulässig ist;

7.5 **Überwachung der Umsetzung der AVV.** Überwachung der ordnungsgemäßen Umsetzung, Erfüllung und Durchführung dieser AVV;

7.6 **Verifizierung der TOM.** Überprüfung der Umsetzung und Aufrechterhaltung der technischen und organisatorischen Maßnahmen;

7.7 **Unterstützung bei Datenfolgenabschätzungen.** Gewährung der angemessenen Zusammenarbeit und Unterstützung auf Anfrage des Abonnenten gegenüber dem Abonnenten, die erforderlich ist, um die Verpflichtung des Abonnenten gemäß der DSGVO zur Durchführung einer Datenschutz-Folgenabschätzung in Bezug auf die Nutzung der Dienste durch den Abonnenten zu erfüllen, soweit der Abonnent nicht anderweitig Zugang zu den relevanten Informationen hat und soweit diese Informationen Cyren zur Verfügung stehen. Cyren unterstützt den Abonnenten in angemessener Weise bei der Zusammenarbeit oder vorherigen Konsultation mit den Aufsichtsbehörden bei der Erfüllung seiner oben beschriebenen Aufgaben; und

7.8 **Aufzeichnung der Verarbeitungstätigkeiten**. Führung eines Verzeichnisses aller Kategorien von Verarbeitungstätigkeiten, die im Auftrag des Abonnenten durchgeführt werden.

8. ANFRAGEN DER BETROFFENEN.

8.1 Cyren wird, soweit gesetzlich zulässig, den Abonnenten unverzüglich benachrichtigen, wenn Cyren eine Anfrage eines Betroffenen erhält, um das Recht des Betroffenen auf Auskunft, auf Berichtigung, auf Einschränkung der Verarbeitung, auf Löschung, auf Datenübertragbarkeit, auf Widerspruch gegen die Verarbeitung oder das Recht, keiner automatisierten Einzelentscheidung unterworfen zu werden, auszuüben ("Anfrage des Betroffenen").

8.2 Unter Berücksichtigung der Art der Verarbeitung wird Cyren den Abonnenten durch geeignete technische und organisatorische Maßnahmen unterstützen, soweit dies möglich ist, um die Verpflichtung des Abonnenten zur Beantwortung von Anfragen der Betroffenen gemäß den Datenschutzgesetzen zu erfüllen. Soweit der Abonnent bei der Nutzung der Dienste nicht in der Lage ist, eine Anfrage des Betroffenen zu beantworten, wird Cyren auf Anfrage des Abonnenten wirtschaftlich angemessene Anstrengungen unternehmen, um den Abonnenten bei der Beantwortung der Anfrage des Betroffenen zu unterstützen, soweit Cyren hierzu gesetzlich verpflichtet oder berechtigt ist und die Beantwortung der Anfrage des Betroffenen nach den Datenschutzgesetzen erforderlich ist. Soweit dies rechtlich zulässig ist, trägt der Abonnent die Kosten, die durch die Unterstützung von Cyren entstehen.

9. BENACHRICHTIGUNG IM FALLE VON VERLETZUNGEN DURCH CYREN

Cyren benachrichtigt den Abonnenten unverzüglich nach Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten per E-Mail an die vom Abonnenten schriftlich angegebenen Kontaktdaten. Diese Benachrichtigung enthält eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten und, soweit möglich, weitere Informationen, die nach den geltenden Datenschutzgesetzen erforderlich sind; sofern und soweit es nicht möglich ist, die Informationen gleichzeitig zu übermitteln, können die Informationen ohne unangemessene weitere Verzögerung schrittweise übermittelt werden.

In solchen Fällen wird Cyren in Absprache mit dem Abonnenten alle wirtschaftlich angemessenen Maßnahmen ergreifen, um die Daten zu sichern und mögliche schädliche Folgen für die Betroffenen zu minimieren.

10. UNTERAUFTRAGSVERGABE / UNTERAUFTRAGSVERARBEITER

10.1 **Zulässige Verwendung.** Der Abonnent erkennt an und erklärt sich damit einverstanden, dass (i) Cyren berechtigt ist, seine verbundenen Unternehmen als Unterauftragsverarbeiter zu beauftragen, und (ii) Cyren oder ein solches verbundenes Unternehmen von Zeit zu Zeit Dritte mit der Verarbeitung personenbezogener Daten in Verbindung mit der Erbringung von Diensten als Unterauftragsverarbeiter beauftragen kann. Cyren wird personenbezogene Daten nur an Unterauftragsverarbeiter weitergeben, die schriftliche Vereinbarungen mit Cyren

getroffen haben, die Verpflichtungen enthalten, die nicht weniger schützend sind als die Verpflichtungen dieser AVV.

10.2 Die derzeit von Cyren beauftragten und vom Abonnenten autorisierten Unterauftragsverarbeiter sind auf der Cyren-Webseite für Unterauftragsverarbeiter (die "Liste der Unterauftragsverarbeiter") unter www.cyren.com/legal/sub-processor-list aufgeführt.

10.3 Cyren benachrichtigt den Abonnenten im Voraus, bevor ein neuer Unterauftragsverarbeiter personenbezogene Daten verarbeitet. Der Abonnent kann dem neuen Unterauftragsverarbeiter innerhalb von fünfzehn (15) Tagen nach dieser Benachrichtigung aus angemessenen Gründen in Bezug auf den Schutz personenbezogener Daten widersprechen, indem er die in der Liste der Unterauftragsverarbeiter aufgeführten Anweisungen befolgt. In diesem Fall hat Cyren das Recht, dem Widerspruch durch eine der folgenden Optionen abzuhelfen (die Cyren nach dem alleinigen Ermessen ausgewählen kann): (i) Cyren wird seine Pläne zur Nutzung des Unterauftragsverarbeiters in Bezug auf die Verarbeitung personenbezogener Daten stornieren oder eine Alternative zur Erbringung der Dienste ohne einen solchen Unterauftragsverarbeiter anbieten; oder (ii) Cyren wird die vom Abonnenten in seiner Widerspruchsmitteilung geforderten Abhilfemaßnahmen ergreifen (die den/die Widerspruch/e des Abonnenten aufheben) und die Nutzung des Unterauftragsverarbeiters fortsetzen; oder (iii) Cyren kann die Bereitstellung des bestimmten Aspekts oder der Funktion der Dienste, die die Nutzung eines solchen Unterauftragsverarbeiters beinhalten würde, einstellen oder der Abonnent kann sich damit einverstanden erklären, diese (vorübergehend oder dauerhaft) nicht zu nutzen. Wenn keine der oben genannten Optionen nach Cyrens vernünftigem Ermessen wirtschaftlich durchführbar ist und die Beanstandung(en) nicht innerhalb von dreißig (30) Tagen nach Eingang der Beanstandungsmitteilung des Abonnenten bei Cyren zur Zufriedenheit der Parteien gelöst wurde(n), kann jede Partei den Vertrag aus wichtigem Grund ohne Rückerstattung im Voraus gezahlter Gebühren kündigen. Dieses Kündigungsrecht ist das einzige und ausschließliche Rechtsmittel des Abonnenten, wenn der Abonnent Einwände gegen einen neuen Unterauftragsverarbeiter hat.

10.4 Unter Untervertragsverhältnissen im Sinne dieses Abschnitts sind solche Leistungen zu verstehen, die in direktem Zusammenhang mit der Erbringung der Hauptleistung stehen. Nicht dazu gehören Nebenleistungen, die Cyren z.B. als (Tele-)Kommunikationsdienste, Post-/Transportdienste, Wartungs- und Benutzerservice oder die Entsorgung von Datenträgern und sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungssystemen in Anspruch nimmt. Wartungs- und Prüfleistungen stellen ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die in unmittelbarem Zusammenhang mit der von der Cyren nach diesem Vertrag erbrachten Leistung stehen. Cyren ist jedoch verpflichtet, auch bei ausgelagerten Nebenleistungen angemessene und rechtsverbindliche vertragliche Regelungen einschließlich technischer und organisatorischer Maßnahmen zu treffen und geeignete Kontrollmaßnahmen zu ergreifen, um den Datenschutz und die Datensicherheit der Daten des Verantwortlichen zu gewährleisten.

10.5 **Haftung**. Cyren haftet für die Handlungen und Unterlassungen seiner Unterauftragsverarbeiter in demselben Umfang, in dem Cyren haften würde, wenn Cyren die Diensten des jeweiligen Unterauftragsverarbeiters direkt gemäß den Bedingungen dieser AVV erbringen würde.

11. DATENÜBERMITTLUNG

11.1 In Bezug auf die in **Anlage 2** aufgeführten Dienste verarbeitet Cyren personenbezogene Daten nur innerhalb des Europäischen Wirtschaftsraums (EWR) oder, wenn Supportleistungen erbracht werden, im Vereinigten Königreich (UK) auf der Grundlage des Angemessenheitsbeschlusses der Europäischen Kommission; der Abonnent erkennt an und stimmt zu, dass bestimmte personenbezogene Daten für die Erbringung von Supportleistungen, wie in **Anlage 2** näher beschrieben, in das Vereinigte Königreich übertragen werden können. Jede Übermittlung personenbezogener Daten an einen Ort außerhalb des EWR oder des Vereinigten Königreichs bedarf der vorherigen schriftlichen Zustimmung des Abonnenten und darf nur erfolgen, wenn die spezifischen Anforderungen der geltenden Datenschutzgesetze für eine Datenübermittlung in das jeweilige Drittland erfüllt sind.

11.2 In Bezug auf die in **Anlage 3** aufgeführten Dienste verarbeitet Cyren personenbezogene Daten nur innerhalb des Europäischen Wirtschaftsraums (EWR), es sei denn, die spezifischen Anforderungen nach den geltenden Datenschutzgesetzen für eine Datenübermittlung in das jeweilige Drittland sind erfüllt, weil (i) ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, (ii) Standardvertragsklauseln implementiert wurden, (iii) die Datenübermittlung verbindlichen Unternehmensregeln unterliegt oder (iv) andere Sicherheitsvorkehrungen getroffen wurden (jeweils auch als "Transfermechanismus" bezeichnet). In Bezug auf diese Dienste erkennt der Abonnent an und stimmt zu, dass bestimmte personenbezogene Daten in Drittländer übertragen werden können. Der Transfermechanismus, auf den sich Cyren bei jeder Übermittlung in ein Drittland stützt, ist in **Anlage 3** aufgeführt.

11.3 Um Zweifel auszuschließen, wird Cyren in die schriftlichen Vereinbarungen mit Drittland-Unterauftragsverarbeitern gemäß Abschnitt 10.1 dieser AVV Verpflichtungen aufnehmen, die nicht weniger schützend sind als die Verpflichtungen dieser AVV. Diese gelten zusätzlich zu den Verpflichtungen des Unterauftragsverarbeiters im Drittland als Datenimporteur gemäß den Standardvertragsklauseln. Im Falle eines Konflikts haben die Bestimmungen der Standardvertragsklauseln Vorrang vor den Verpflichtungen, die sich aus dieser AVV ergeben.

12. ÜBERWACHUNGSRECHTE DES ABONNENTEN

12.1 Der Abonnent kann die Einhaltung der Verpflichtungen von Cyren aus dieser AVV überwachen. Cyren stellt sicher, dass der Abonnent die Möglichkeit hat, sich vor Beginn der Verarbeitungstätigkeiten und während der Laufzeit dieser AVV durch Vor-Ort-Kontrollen von der Einhaltung der festgelegten technischen und organisatorischen Maßnahmen durch Cyren in angemessener Weise überzeugen zu können. Zu diesem Zweck wird Cyren auf Verlangen des Abonnenten einen Nachweis über die Umsetzung der in **Anlage 1** beschriebenen technischen und organisatorischen Maßnahmen erbringen.

12.2 Alternativ kann Cyren seinen Verpflichtungen aus diesem Abschnitt auch durch Vorlage aktueller Bescheinigungen, Berichte oder Berichtsauszüge unabhängiger Stellen (wie z.B. Wirtschaftsprüfer, Steuerberater, Datenschutzbeauftragte, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Bescheinigung im Rahmen eines IT-Sicherheits- oder Datenschutzaudits (z.B. nach dem

Zertifizierungsprogramm "IT-Grundschutz" des Bundesamts für Sicherheit in der Informationstechnik) nachkommen.

12.3 Für den Fall, dass der Abonnent vernünftigerweise der Ansicht ist, dass die von Cyren zur Verfügung gestellte Dokumentation eine weitere Prüfung erfordert, um die Einhaltung der Datenschutzgesetze und dieser AVV nachzuweisen, kann auf Antrag des Abonnenten, der mindestens dreißig (30) Tage im Voraus gestellt werden muss, eine (1) Vor-Ort-Prüfung pro Jahr (außer in Bezug auf außergewöhnliche Vorfälle oder Prüfungen, die von einer Aufsichtsbehörde gemäß dem Datenschutzgesetz verlangt werden) während der Laufzeit in den Einrichtungen von Cyren, die an der Erbringung der Dienste beteiligt sind, zu angemessenen Zeiten während der Geschäftszeiten und zu den dann geltenden Tarifen von Cyren durchgeführt werden. Der Umfang einer solchen Prüfung, einschließlich der Bedingungen für die Vertraulichkeit, wird vor Beginn der Prüfung einvernehmlich festgelegt.

13. DATENLÖSCHUNG UND RÜCKGABE VON DATENTRÄGERN

Nach Beendigung der vertraglich vereinbarten Leistungen (oder auf Wunsch des Abonnenten auch früher) - spätestens bei Beendigung der AVV - vernichtet Cyren alle im Rahmen dieser AVV erhaltenen oder erstellten personenbezogenen Daten, es sei denn, der Abonnent fordert Cyren mindestens vier (4) Wochen vor Beendigung schriftlich zur Übermittlung der personenbezogenen Daten auf. Auf Verlangen wird Cyren dem Abonnenten die Löschungsprotokolle vorlegen.

Dokumentationsunterlagen, die als Nachweis dafür dienen, dass personenbezogene Daten auf ordnungsgemäße Weise in Übereinstimmung mit den Bestimmungen dieser AVV verarbeitet wurden, müssen von Cyren nach Beendigung dieser AVV in Übereinstimmung mit den geltenden Aufbewahrungsfristen aufbewahrt werden. Cyren kann diese Dokumente nach Beendigung der AVV an den Abonnenten weitergeben, um nachzuweisen, dass die personenbezogenen Daten auf ordnungsgemäße Weise in Übereinstimmung mit den Bestimmungen dieser AVV verarbeitet wurden.

14. HAFTUNG

14.1 Cyren und der Abonnent haften gegenüber den Betroffenen gemäß Artikel 82 der Datenschutz-Grundverordnung.

14.2 Der Abonnent stellt Cyren von sämtlichen Ansprüchen Dritter (einschließlich Betroffener und Datenschutzbehörden) frei, die gegen Cyren aufgrund eines Verstoßes des Abonnenten gegen die Bestimmungen dieser Vereinbarung und/oder der Datenschutzgesetze erhoben werden und hält Cyren schadlos.

14.3 In keinem Fall übersteigt die Haftung von Cyren gegenüber dem Abonnenten im Zusammenhang mit Problemen, die sich aus oder in Verbindung mit dieser AVV ergeben, die Haftungsbeschränkungen von Cyren, die im Hauptvertrag festgelegt sind. Die im Hauptvertrag festgelegten Haftungsbeschränkungen von Cyren gelten insgesamt für den Hauptvertrag und diese AVV, so dass eine einzige Haftungsbeschränkungsregelung sowohl für den Hauptvertrag als auch für diese AVV gilt.

14.4 Ungeachtet des Vorstehenden schränkt keine der Bestimmungen dieser AVV die Haftung einer der Parteien für eine Haftung ein, die gesetzlich nicht ausgeschlossen oder beschränkt werden kann.

15. GELTENDES RECHT

Diese AVV unterliegt den Gesetzen derselben Gerichtsbarkeit, die im Hauptvertrag vereinbart wurde.

ANHANG 1

Technische und organisatorische Maßnahmen (TOM) im Sinne des Art. 32 DSGVO

Cyren gewährleistet ein angemessene Schutzniveau gemäß Artikel 32 der EU-Datenschutzgrundverordnung (DSGVO) für die Verarbeitung der in der AVV bezeichneten personenbezogenen Daten durch die nachfolgend beschriebenen technischen und organisatorischen Maßnahmen. Soweit nicht anders beschrieben beziehen sich die Informationen auf den Standort Heidestraße 10, 10557 Berlin, Deutschland.

Cyren erfüllt diese Anforderung durch die folgenden Maßnahmen:

1. Vertraulichkeit

1.1. Zugangskontrollen zu Datenverarbeitungsanlagen

Folgende Maßnahmen wurden ergriffen, um den Zugang Unbefugter zu den Datenverarbeitungsanlagen zu verhindern:

Physischer Zugang: Angemessene Sicherheitsvorkehrungen im Rechenzentrum, Zugangskontrollen und die Festlegung von autorisierten Personen werden genutzt, um zu verhindern, dass Unbefugte auf die Datenverarbeitungssysteme zugreifen.

Büro: Ein Zugangskontrollsystem verhindert den unbefugten Zutritt. Besucher werden am Empfang empfangen und persönlich durch das Büro geführt. Die Mitarbeiter benutzen Schlüsselkarten für den Zugang zum Büro.

Der interne Technikraum ist mit einem Sicherheitsschloss gesichert. Nur eine eng begrenzte Anzahl von Mitarbeitern des jeweiligen Dienstleisters (technische Verwaltung) hat Zugang zum Technikraum.

Datenzentren: Durch den Einsatz von Sicherheitspersonal und der Nutzung eines Alarmsystems wird der unbefugte Zugang zu den Datenverarbeitungssystemen des Rechenzentrums verhindert. Der Zugang ist lediglich autorisierten Personen nach Vorlage eines Lichtbildausweises gestattet. Nur der Leiter des Servicebetriebs und der Leiter IT sind befugt zu bestimmen, wer autorisiert und damit zugangsberechtigt ist. Die Datenverarbeitungsanlagen werden mit Zahlenschlössern separat verschlossen, die Kombinationen sind nur den berechtigten Personen bekannt.

Die externen Rechenzentren in der EU sind nach ISO 27001 zertifiziert.

1.2. Datenträgerzugangskontrolle - Physische Sicherheit der Infrastruktur

Folgende Maßnahmen wurden ergriffen, um zu verhindern, dass Unbefugte Zugang zu Datenverarbeitungsanlagen erhalten:

Jeder Cyren-Mitarbeiter hat einen persönlichen, passwortgeschützten Anmeldenamen. Das Berechtigungskonzept wird über Active Directory Gruppenrichtlinien realisiert.

Der externe Zugang zu den Arbeitsplätzen wird durch Firewalls verhindert. Die Arbeitsplätze werden mit Anti-Virus-Software geschützt, die sich automatisch aktualisiert. Spam-Filter werden eingesetzt und regelmäßige Kontrollen durchgeführt.

Mobile IT-Systeme (Notebooks / iPhones) sind verschlüsselt und mit Anti-Virus-Software ausgestattet.

Die Kommunikation innerhalb von Cyren sowie zwischen den Arbeitsplätzen und den Datenverarbeitungssystemen in externen Rechenzentren erfolgt ausschließlich über sichere Kanäle (entweder verschlüsselt oder über Standleitungen). Zwischen den Büros von Cyren und den

Rechenzentren sowie zwischen den Rechenzentren selbst bestehen Standleitungen oder verschlüsselte Kanäle (VPN), auf die Dritte keinen Zugriff haben.

Der externe Zugriff auf das Firmennetzwerk (Außendienst, Mitarbeiter, die von zu Hause aus arbeiten) erfolgt ausschließlich über eine verschlüsselte VPN-Verbindung. Der Zugang zum VPN ist durch eine Multi-Faktor-Authentifizierung gesichert. Darüber hinaus ist ein separater VPN-Zugang für den Aufbau von VPN-Verbindungen zu Unternehmensstandorten und Rechenzentrumsumgebungen erforderlich.

1. 3. Speicherkontrolle

Folgende Maßnahmen wurden ergriffen, um sicherzustellen, dass die zur Nutzung eines Datenverarbeitungssystems berechtigten Personen ausschließlich auf die Daten entsprechend ihrer Zugriffsberechtigung zugreifen können und dass personenbezogene Daten während ihrer Verarbeitung und Nutzung und nach ihrer Speicherung nicht von Unbefugten gelesen, kopiert, verändert oder gelöscht werden können:

Arbeitsstationen: Eine Passwort-Policy inkl. Vorgaben zu Passwortlänge, verpflichtende Passwortänderung etc. ist vorhanden. Jeder Cyren-Mitarbeiter hat einen persönlichen, passwortgeschützten Login-Namen mit Wartezeiten für den Fall, dass ein falsches Passwort mehrfach eingegeben wurde. Die Mitarbeiter sind angewiesen, sichere Passwörter zu verwenden (ausreichend lange Kombinationen aus verschiedenen Zeichenarten, keine bekannten Wörter oder Namen) und ihre Passwörter geheim zu halten.

Anwendungen: Die Zugriffe auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten, werden protokolliert.

Ein Rollen- und Rechtemanagement mit differenzierten Zugriffsrechten und Genehmigungsroutinen wurde implementiert. Im Rahmen des Cyren-Berechtigungsmodells wird die Zugriffsberechtigung für Cyren-Mitarbeiter so eingeschränkt, dass jeder Mitarbeiter nur auf die für seine Arbeit notwendigen Datenverarbeitungsschritte Einfluss nehmen kann. Bei Ausscheiden aus dem Unternehmen werden den Mitarbeitern alle Zugriffsrechte entzogen.

Die Anzahl der Administratoren ist auf das notwendige Maß beschränkt. Die Administrationsrechte sind in System-Administration und Datenbank-Administration gestaffelt.

Es gibt Genehmigungsroutinen. Jeder Mitarbeiter, der Zugang zu einem System benötigt, muss eine Genehmigung bei seinem Vorgesetzten einholen. Der Vorgesetzte muss zu der Gruppe der Genehmigungsberechtigten gehören und befugt sein, die Genehmigung zu erteilen.

Der Fernzugriff auf Produktivsysteme erfordert die Nutzung des Firmen-VPN.

Der Zugriff auf das VPN wird protokolliert, so dass die Arbeit von Außendienstmitarbeitern und Heimarbeitern innerhalb des Firmennetzes nachvollziehbar ist.
Vor ihrer Wiederverwendung werden Datenträger gelöscht oder physikalisch vernichtet gem. DIN 32757.
Im Büro stehen Behälter für die Vernichtung von Papierdokumenten zur Verfügung.
Datenträger werden sicher im Technikraum aufbewahrt. Datenträgern werden im Einklang mit anerkannten Normen (z.B. DIN 32757) vernichtet und die Vernichtung protokolliert.

1.4. Trennungskontrolle

Die folgenden Maßnahmen wurden getroffen, um sicherzustellen, dass Daten, die für unterschiedliche Zwecke erhoben wurden, getrennt verarbeitet werden:

Die betroffenen Datenbanken sind nicht miteinander verbunden. Je nach Anwendungsfall wird die Trennung der Datensätze entweder durch eine physische Trennung gewährleistet, wenn Cyren seine eigenen Server in einem Colocation-DC nutzt, oder durch eine Trennung auf Anwendungsebene, wenn Cyrens Cloud Services nutzt.

Produktions- und Testumgebungen werden getrennt, und mit den Active Directory Gruppenrichtlinien wird ein Berechtigungskonzept realisiert.

2. Integrität

2.1. Übertragungskontrolle

Die folgenden Maßnahmen stellen sicher, dass personenbezogene Daten bei der elektronischen Übermittlung oder während des Transports oder der Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden und dass überprüft und festgestellt werden kann, wohin personenbezogene Daten durch Datenübertragungseinrichtungen übermittelt werden:

Die Übermittlung der Daten an den oder die betroffenen Empfänger erfolgt ausschließlich über das jeweilige Zielgerät zum Zwecke der Erbringung der vertraglichen Leistungen und der anschließenden Weitergabe der übermittelten Daten.
Die verschlüsselte Übertragung wird standardmäßig durchgeführt, sofern Cyren die Daten zuvor auf diese Weise vom Kunden erhalten hat.

Technische Updates werden über verschlüsselte Verbindungen (SSL, VPN) bereitgestellt. Die Datenübertragung und Datentransporte werden protokolliert.

Cyren-Mitarbeiter müssen Dokumente und Datenträger mit personenbezogenen Daten sicher entsorgen, sobald sie nicht mehr aufbewahrt werden müssen.

2.2. Eingangskontrolle

Die folgenden Maßnahmen stellen sicher, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder gelöscht wurden:

Im Rahmen des Cyren-Berechtigungsmodells ist die Zugriffsberechtigung für Cyren-Mitarbeiter so eingeschränkt, dass jeder Mitarbeiter nur auf die für seine Arbeit notwendigen Datenverarbeitungsschritte Einfluss nehmen kann.

Um dies zu realisieren, werden die Cyren-Mitarbeiter nach Abteilungen und Aufgaben in Gruppen eingeteilt, deren Berechtigungen entsprechend den jeweiligen Anforderungen vergeben werden. Die Gruppenrichtlinien werden im Active Directory realisiert.

Cyren hält sich an den Grundsatz, dass die Berechtigungen auf der niedrigsten Ebene vergeben werden, die für die Erfüllung der jeweiligen Aufgaben erforderlich ist. Ändert sich der Tätigkeitsbereich eines Mitarbeiters, so ändert sich auch seine Zuordnung zu der jeweiligen Gruppe und damit die entsprechenden Berechtigungen.

Darüber hinaus setzt Cyren auch die bereits erwähnten Firewall-Systeme sowie Maßnahmen zur Benutzerautorisierung und -authentifizierung ein.

Der Zugriff auf das VPN wird protokolliert, so dass die Arbeit von externen Mitarbeitern und Heimarbeitern innerhalb des Firmennetzes nachvollziehbar ist.

Die Rückverfolgbarkeit von Eingaben, Änderungen und Löschungen von Daten über einzelne Benutzernamen (nicht über Benutzergruppen) wird, soweit einschlägig, umgesetzt.

3. Verfügbarkeit und Belastbarkeit

3.1. Verfügbarkeitskontrolle

Die folgenden Maßnahmen stellen sicher, dass personenbezogene Daten vor zufälliger Zerstörung oder Verlust geschützt sind:

Cyren nutzt Colocation-Anbieter (Housing) mit ISO 27001-Zertifizierung für den Betrieb seiner eigenen Infrastrukturen. Die Infrastruktur ist redundant. Kopien werden in geografisch getrennten DCs gespiegelt. (1 Master-3Salves).

Für bestimmte Cloud-Dienste nutzt Cyren die Infrastruktur und Dienste Dritter (Hosting).

Verarbeitete Daten: Cyren wird stets die notwendigen Maßnahmen ergreifen, um die höchstmögliche Verfügbarkeit des Dienstes zu gewährleisten. Personenbezogene Daten werden grundsätzlich auf redundanten Systemen verarbeitet.

Gespeicherte Daten: Daten, die über einen längeren Zeitraum gespeichert werden, werden durch die regelmäßige Erstellung von Backups gesichert. Der Sicherungsprozess ist zweistufig: Die Daten werden zunächst auf Festplatten im Rechenzentrum gespeichert (für eine schnelle Wiederherstellung) und dann auf Band (für eine sichere Aufbewahrung) gespeichert. Unter bestimmten Umständen werden die Bandsicherungen verschlüsselt und in einem anderen Gebäude aufbewahrt. Daten, die aufgrund ihres Umfangs nicht als normales Backup gespeichert werden können, werden dauerhaft in mehreren Kopien an verschiedenen geografischen Standorten gespeichert.

Die Datenzentren sind mit fortschrittlicher Technologie gegen Notfälle geschützt.

Cloud-Service-Anbieter: Cyren nutzt für seine Cloud-Services einen Cloud-Service-Provider, der verpflichtet ist, die Daten im EU-Raum zu speichern.

Die Betriebsbereitschaft durch unser eigenes Team besteht 24 Stunden am Tag. Für Software und IT-Anwendungen ist ein Sicherheitskonzept vorhanden.

3.2 Rechtzeitige Wiederherstellung

Die folgenden Maßnahmen stellen sicher, dass im Falle eines physischen oder technischen Zwischenfalls die Verfügbarkeit von und der Zugang zu personenbezogenen Daten rechtzeitig wiederhergestellt wird:

Siehe auch 3.1.

Büro: Ein Sicherheitskonzept für Software und IT-Anwendungen ist vorhanden.

Betriebliche Daten: Alle Verarbeitungssysteme sind redundant aufgebaut und können zeitnah wiederhergestellt werden. Nur in seltenen Fällen speichert Cyren überhaupt personenbezogene Daten seiner Kunden, z.B. für Konfigurationseinstellungen.

4. Wirksamkeitskontrollen - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1. Datenschutz-Management

Die folgenden Maßnahmen stellen sicher, dass die Datenschutz- und Informationssicherheitsorganisation des Auftragnehmers so gestaltet ist, dass sie den Anforderungen der beschriebenen Auftragsverarbeitung und den allgemeinen gesetzlichen Anforderungen entspricht:

- Die Cyren GmbH hat einen internen Datenschutzbeauftragten bestellt.
- Cyren verwendet eine Softwarelösung für die Verwaltung der Datensicherung.
- Die Mitarbeiter sind geschult und an Vertraulichkeits-/Datenschutzvereinbarungen gebunden.
- Es gibt ein formalisiertes Verfahren für die Bearbeitung von Auskunftsersuchen der betroffenen Personen.
- Eine Datenschutz-Folgenabschätzung (DPIA) kann gegebenenfalls durchgeführt werden.
- Cyren erfüllt die Informationspflichten nach Art. 13 und 14 DSGVO.
- Ein Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 Abs. 2 DSGVO wird geführt.
- Ein System für das Management von Vorfällen, einschließlich des Prozesses für den Umgang mit Datenschutzverletzungen, wird von einem speziellen Management Team betrieben.
- Es gibt ein Verfahren für den Umgang mit Anfragen von betroffenen Personen. Die beteiligten Abteilungen sind für den Umgang mit solchen Anfragen geschult.

4.2. Management von Vorfällen

Der Einsatz von Firewall, Spamfilter und Virenscanner ist für alle Nutzer, die nicht mit schädlichem Material arbeiten, obligatorisch. Firewall, Spamfilter und Virenscanner werden regelmäßig aktualisiert.

Es gibt ein spezielles Team für das Management von Vorfällen. Sicherheitsvorfälle werden dokumentiert. Ein formelles Verfahren zur Ursachenanalyse (RCA) wird auf relevante Sicherheitsvorfälle angewandt.

Sicherheitsvorfälle und Datenschutzverletzungen werden dokumentiert. Es gibt ein dokumentiertes Verfahren für den Umgang mit Sicherheitsvorfällen und Datenschutzverletzungen.

Der Datenschutzbeauftragte und das Datenschutzteam werden über Sicherheitsvorfälle informiert, die zu Datenschutzverletzungen führen könnten oder geführt haben.

4.3. Privacy by Design / Privacy by Default

Die folgenden Maßnahmen stellen sicher, dass standardmäßig nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen spezifischen Verarbeitungszweck erforderlich ist:

Die Cyren GmbH verfolgt einen Privacy-by-Design-Ansatz und "baut" per Code spezifische Maßnahmen zur Pseudonymisierung und Löschung/Überschreibung von Daten ein.

Cyren erhebt nicht mehr personenbezogene Daten, als diejenigen, die zur Erreichung des jeweiligen Zwecks erforderlich sind, und verarbeitet personenbezogene Daten nur so lange, wie es zur Erfüllung des jeweiligen Zwecks erforderlich ist.

Die Parameter wurden so codiert, dass nicht mehr benötigte Daten zurückgewiesen werden.

Automatisierte Überschreibungsroutinen der Verarbeitungssysteme sind implementiert. Diese werden nach Ende der Verarbeitung und nach dem Wegfall des Verarbeitungszwecks eingesetzt.

Das jeweilige Personal, insbesondere die Mietarbeiter der Detections- und Engineering-Teams, wird insbesondere im Hinblick auf den Datenschutz geschult.

Personenbezogene Daten werden in der Regel vom Kunden selbst verwaltet oder vom Kunden an Cyren übermittelt.

4.4. Kontrolle der Verarbeitung (Auslagerung an Dritte)

Die folgenden Maßnahmen stellen sicher, dass personenbezogene Daten, die im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet werden, nur gemäß den Anweisungen des für die Verarbeitung Verantwortlichen verarbeitet werden. Dieser Abschnitt umfasst auch die Durchführung von Wartungs- und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne der Verarbeitung personenbezogener Daten nach Art. 28 DSGVO einsetzt, sind mit diesen stets folgende Punkte geregelt:

Cyren gibt personenbezogene Daten nur an Unterauftragsverarbeiter weiter, die mit Cyren einen schriftlichen Vertrag abgeschlossen haben, der Verpflichtungen enthält, die nicht weniger schützend sind als die Verpflichtungen aus dieser AVV. Dazu gehört die Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragsverarbeiter sowie die Verpflichtung der Mitarbeiter des Auftragsverarbeiters zur Wahrung des Datengeheimnisses.

ANHANG 2

Verarbeitung nur innerhalb des Gebiets des EWR und des Vereinigten Königreichs: Verarbeitung personenbezogener Daten nur innerhalb des Gebiets des Europäischen Wirtschaftsraums (EWR) oder des Vereinigten Königreichs (UK), einschließlich der Kontoverwaltung und der technischen Unterstützungsdienste, wie im Datenblatt der Cyren Support Services auf www.cyren.com/legal beschrieben.

Produkt	Standort der Dienste	Standort der Unterstützungs-dienste	UK-Transfer-Mechanismus	UK Auftragsverarbeiter oder Unterauftragsverarbeiter
Cyren Email Security (my.Eleven - Single Engine)	DE	UK	Angemessenheits-beschluss	Cyren UK Ltd.
Cyren DNS- Security	DE	UK	Angemessenheits-beschluss	Cyren UK Ltd.
Cyren Cloud Sandboxing (EU Region)	DE	UK	Angemessenheits-beschluss	Cyren UK Ltd.
Cloud Threat Lookup (EU Region)	DE	UK	Angemessenheits-beschluss	Cyren UK Ltd.
CES Inhouse	DE	UK	Angemessenheits-beschluss	Cyren UK Ltd.

ANHANG 3

A. In Bezug auf die in der nachstehenden Tabelle aufgeführten Produkte werden personenbezogene Daten nur dann an Länder außerhalb des EWR übertragen und/oder von dort abgerufen, wenn dem Kunden Support- oder Wartungsdienste der Stufe 3 oder 4 gemäß der nachstehenden Tabelle bereitgestellt werden.

Produkt	Standort	Mechanismus der Übertragung	Auftragsverarbeiter oder Unterauftragsverarbeiter
Cyren Cloud Security - Email (Single Engine)	Israel/ UK	Angemessenheitsbeschluss	Cyren Ltd./ Cyren UK Ltd.
Cyren Email Archiving	Israel/ UK	Angemessenheitsbeschluss	Cyren Ltd./ Cyren UK Ltd.
Cyren Inbox Security	Israel/ UK	Angemessenheitsbeschluss	Cyren Ltd./ Cyren UK Ltd.

B. In Bezug auf die in der nachstehenden Tabelle aufgeführten Produkte werden personenbezogene Daten auch an Länder außerhalb des EWR übermittelt und/oder von dort abgerufen, wie in der nachstehenden Tabelle angegeben.

Produkt	Standort	Mechanismus der Übertragung	Auftragsverarbeiter oder Unterauftragsverarbeiter
Cyren Cloud Security - Email (Dual Engine)	Israel/ UK Vereinigte Staaten	Angemessenheitsbeschluss Standardvertragsklauseln [1]	Cyren Ltd./ Cyren UK Ltd. Cyren Inc.
Cyren Email Security (my.Eleven - Dual Engine)	Israel/ UK Vereinigte Staaten	Angemessenheitsbeschluss Standardvertragsklauseln	Cyren Ltd./ Cyren UK Ltd. Cyren Inc.
Cyren Cloud Sandboxing (US Region)	Israel/ UK Vereinigte Staaten	Angemessenheitsbeschluss Standardvertragsklauseln	Cyren Ltd./ Cyren UK Ltd. Cyren Inc.
Cloud Threat Lookup (US Region)	Israel/ UK Vereinigte Staaten	Angemessenheitsbeschluss Standardvertragsklauseln	Cyren Ltd./ Cyren UK Ltd. Cyren Inc.
Incident Response Service für Cyren Inbox Security	Ukraine	Standardvertragsklauseln	Cyren. Ltd.

[1] Durchführungsbeschluss (EU) 2021/914 der EU-Kommission vom 4. Juni 2021