Häufig gestellte Fragen zu Geschäft, Produkten und Services von Kaspersky

- **Stellungnahme zur Entscheidung des US-Handelsministeriums**
- **Stellungnahme zur Aufnahme der Unternehmensleitung in die Sanktionsliste des Office of Foreign Assets Control (OFAC) des US-Finanzministeriums**
- **Globale Transparenzinitiative von Kaspersky**
- **Ausführliches FAQ auch hier**

Ist Kaspersky ein internationales Unternehmen?
Ja. Kaspersky ist ein internationales, privat geführtes Unternehmen mit Sitz in Großbritannien. Das Unternehmen ist in mehr als 200 Ländern und Regionen tätig und hat über 30 Niederlassungen weltweit. Fast 60 Prozent des Geschäfts von Kaspersky ist international und unsere lokalen Geschäfte werden von lokalen Einheiten effizient und unabhängig geführt.

Können Sie Kaspersky vertrauen?
Ja. Seit über 25 Jahren entwickelt Kaspersky erstklassige Cybersicherheitslösungen und stellt eine innovative Bedrohungsanalyse bereit. Unsere Kunden und Partner können sich auf die Integrität und Sicherheit unserer Produkte, Entwicklungspraktiken und Datenservices verlassen. Diese wurden durch unabhängige Bewertungen Dritter bestätigt: Kaspersky hat das SOC 2-Audit (Service Organization Control for Service Organizations) Typ 1 erfolgreich bestanden, das von einer der vier größten Wirtschaftsprüfungsgesellschaften durchgeführt wurde, und die ISO27001-Zertifizierung erhalten. Kaspersky schneidet häufig in unabhängigen Rankings am besten ab und hat angesehene, internationale Auszeichnungen in unabhängigen Tests führender Organisationen weltweit erhalten.

Wer vertraut Kaspersky?
Kaspersky trägt zur globalen und nationalen Sicherheit bei. Hunderte globaler Technologie- und OEM-Partnern vertrauen unseren Technologien, und wir arbeiten mit der globalen IT-Sicherheits-Community sowie mit Strafverfolgungsbehörden, einschließlich Interpol sowie Computer Emergency Response Teams (CERTs), weltweit zusammen.

Hat Kaspersky die Verpflichtung, der russischen Regierung Informationen bereitzustellen?
Kaspersky ist ein Privatunternehmen ohne jegliche Verbindung zur russischen Regierung. Darüber hinaus ist Kaspersky nicht verpflichtet, den russischen Behörden Informationen im Rahmen des russischen Systems operativer Ermittlungsmaßnahmen (SORM) (oder gemäß ähnlicher Gesetze) bereitzustellen, da das Unternehmen keine Kommunikationsdienste anbietet. Dies wurde durch eine unabhängige rechtliche Bewertung der russischen Gesetzgebung durch Dritte in Bezug auf die Datenverarbeitung bestätigt.

Kann Kaspersky von der russischen Regierung gezwungen werden, Malware zu ignorieren, die für Angriffe auf eine öffentliche Verwaltung verwendet wird?
Nein, Kaspersky kann von keiner Regierung dazu gezwungen werden. Alle derartigen Anfragen werden immer abgelehnt werden. Für weitere Transparenz und Rechenschaftspflicht werden Aktionen rund um die Malware-Erkennung von einem Team von Kaspersky-Experten weltweit, nicht nur in Russland, protokolliert und überprüft.
Das Grundprinzip von Kaspersky besteht darin, alle Formen schädlicher Bedrohungen zu erkennen und zu neutralisieren, unabhängig von deren Ursprung oder Zweck. Es spielt keine Rolle, welche Sprache die Bedrohung „spricht“, wir melden jede Art von Bedrohung, die wir entdecken. Neben Angriffen in

anderen Sprachen hat das Global Research and Analysis Team von Kaspersky auch zahlreiche Berichte über Angriffe, in denen die russische Sprache im Code gebraucht wurde, veröffentlicht.

Gewährt Kaspersky Regierungs- und Strafverfolgungsbehörden Zugriff auf Nutzerdaten?
Kaspersky gewährt Regierungs- und Strafverfolgungsbehörden niemals Zugriff auf Nutzerdaten oder die Unternehmensinfrastruktur. Wir stellen Informationen über solche Daten auf Anfrage bereit, aber keine externe Partei kann direkt oder indirekt auf unsere Infrastruktur oder Daten zugreifen, und alle Anfragen werden von Kaspersky-Mitarbeitern geprüft und bearbeitet. Zudem wird jede Anfrage, die wir erhalten, einer rechtlichen Prüfung unterzogen, um die Einhaltung der geltenden Gesetze und Verfahren sicherzustellen. Unser Verfahren zur überprüfung der Anfragen basiert auf fünf Kriterien und dient als Leitfaden, um zu entscheiden, ob diese Anfragen genehmigt, abgelehnt oder angefochten werden. Weitere Details finden Sie hier.
Kaspersky veröffentlicht regelmäßig seinen Transparenzbericht „Law Enforcement and Government Requests Report“. Der jüngste Bericht für das zweite Halbjahr 2023 ist hier verfügbar.

Sind die Geschäftsabläufe von Kaspersky stabil? Kann ich Kaspersky-Produkte weiter nutzen?
Der Geschäftsbetrieb von Kaspersky ist stabil. Das Unternehmen garantiert die Erfüllung seiner Verpflichtungen gegenüber seinen Partnern und Kunden, einschließlich der Lieferung von Produkten und Support sowie der Kontinuität finanzieller Transaktionen.

Garantiert Kaspersky die kontinuierliche Bereitstellung von Updates für seine Produkte?
Ja. Unsere internen Tests bestätigen, dass die globale Serverinfrastruktur des Unternehmens eine reibungslose Funktion der Kernprodukte von Kaspersky ermöglicht. Kaspersky ist ein internationales Unternehmen und unsere Cloud-Server sind über den ganzen Globus verteilt (beispielsweise in der Schweiz, in Deutschland, China, Kanada etc.). Dies ermöglicht eine schnellere Verarbeitung von Informationen und garantiert die Serververfügbarkeit, sollte einer der Server aus irgendeinem Grund ausfallen.

Wie schützt und gewährleistet Kaspersky die Sicherheit seiner Produkt-Update-Dienste?
Unsere Kunden können sich auf die Integrität und Sicherheit unserer Produkte, Entwicklungspraktiken und Datenservices verlassen. Diese wurden durch unabhängige Bewertungen Dritter bestätigt: Kaspersky hat das SOC 2-Audit (Service Organization Control for Service Organizations) Typ 1 erfolgreich bestanden, das von einer der vier größten Wirtschaftsprüfungsgesellschaften durchgeführt wurde. Das Audit bestätigt die ausreichend strengen Sicherheitskontrollen Kasperskys für die Entwicklungs- und Release-Prozesse von AV-Updates im Hinblick auf das Risiko von nicht autorisierten Änderungen. Der Abschlussbericht mit einer Beschreibung der Sicherheitskontrollen und des gesamten Ablaufs kann unseren Partnern auf Anfrage zur Verfügung gestellt werden.

Wie kann Kaspersky die Integrität und Vertrauenswürdigkeit seiner Produkte sicherstellen?
Die Sicherheit und Integrität unserer Datenservices und Entwicklungspraktiken wurden durch unabhängige Bewertungen Dritter – zwei externe unabhängige Prüforganisationen - bestätigt: durch das SOC 2-Audit (Service Organization Control for Service Organizations), das von einer der vier größten Wirtschaftsprüfungsgesellschaften durchgeführt wurde und die Sicherheit der Entwicklungs- und Release-Prozesse von AV-Updates bei Kaspersky im Hinblick auf das Risiko nicht autorisierter Änderungen bestätigt. Auch die Datenservices von Kaspersky wurden nach ISO/IEC 27001:2013 zertifiziert und erneut zertifiziert. Kaspersky stellt den Abschlussbericht seinen Partner auf Anfrage zur Verfügung.
Darüber hinaus betreiben wir weltweit Transparenzzentren, die es vertrauenswürdigen Partnern und Regierungsvertretern ermöglichen, den Code des Unternehmens, Software-Updates und Regeln zur Bedrohungserkennung zu überprüfen. Die Services der Transparenzzentren sind auf Anfrage auch per Fernzugriff verfügbar.

Wo werden die Lizenzen und Aktivierungsschlüssel für Kaspersky-Produkte erstellt?
Obwohl Lizenzen und Aktivierungscodes für Kaspersky-Produkte in Russland generiert werden, werden sie an Aktivierungsserver verteilt, die sich auf der ganzen Welt verteilt befinden. Für Europa haben wir beispielsweise lokale Aktivierungsserver in der Region, die die Produktaktivierungsanfragen der Kunden verarbeiten. Dieser diversifizierte Prozess ermöglicht es uns, sowohl die Integrität als auch die

Kontinuität der Produktlieferung an unsere Anwender sicherzustellen. Sollte es Risiken für den Ablauf der Erstellung von Lizenzen und Aktivierungscodes für unsere Produkte geben, bietet die globale Infrastruktur des Unternehmens die Möglichkeit, diesen zu verlagern.

Wo werden die Kaspersky-Websites gehostet?
Wir haben die GEO-DNS-Einstellung der Marketing- und Support-Websites von Kaspersky entsprechend den öffentlichen Informationen über die Geo-IP-Erkennung unserer Anwender angepasst, um sicherzustellen, dass nicht-russische Besucher an nicht-russische Front-End-Server weitergeleitet werden.

Was beinhaltet die ISO 27001-Zertifizierung?
Die Zertifizierung bescheinigt, dass Kaspersky ein Managementsystem gemäß der Norm ISO/IEC 27001:2013 für die Infrastruktur des Kaspersky Security Network (KSN) anwendet (im Weiteren – Data Service). Die im Jahr 2022 abgeschlossene erneute Zertifizierung umfasst Kaspersky Data Service, einschließlich:

- des KSN Systems für die sichere Speicherung und den Zugriff auf Dateien (genannt KLDFS);
- der KSN-Systeme zur Verarbeitung von Statistiken (genannt KSNBuffer-Datenbank).

Die Zertifizierungen sind hier verfügbar. Den Abschlussbericht mit Beschreibung stellen wir unseren Partnern auf Anfrage zur Verfügung.

Was für Kundendaten verarbeitet Kaspersky?
Die Informationen, die Kaspersky freiwillig von Anwendern zur Verfügung gestellt werden, umfassen cyberbedrohungsbezogene Daten und Statistiken. Um die höchste Sicherheit für unsere Anwender zu gewährleisten, wurden die Kaspersky-Datenservices nach IS027001 zertifiziert und 2022 erneut zertifiziert. Beide Zertifikate sind hier verfügbar. Kaspersky stellt seinen Partnern den Abschlussbericht auf Anfrage zur Verfügung.

Wo verarbeitet Kaspersky Nutzerdaten?
Im Rahmen unserer Globalen Transparenzinitiative (GTI) hat Kaspersky einen Teil seiner Datenverarbeitungsinfrastruktur in die Schweiz verlegt. Schädliche und verdächtige Dateien, die freiwillig von Anwendern von Kaspersky-Produkten in Europa, Nord- und Lateinamerika, dem Nahen Osten sowie in mehreren Ländern im asiatisch-pazifischen Raum geteilt werden, werden in zwei Datenzentren in Zürich in Übereinstimmung mit Industriestandards verarbeitet, um das höchste Sicherheitsniveau zu gewährleisten. Darüber hinaus gehört die Schweiz zu den wenigen Ländern, die einen Angemessenheitsbeschluss mit der EU haben, d. h. sie wurde von der EU-Kommission für einen angemessenen Schutz personenbezogener Daten anerkannt. Zudem können Statistiken, die von Anwendern an Kaspersky bereitgestellt werden, durch Services von Kaspersky Security Network verarbeitet werden, die sich in verschiedenen Ländern weltweit (Kanada, Deutschland, Russland usw.) befinden. Eine genaue Liste der Länder, in denen personenbezogene Daten, die von Anwendern Kaspersky bereitgestellt werden, verarbeitet werden können, finden Sie hier.

Wie behandelt Kaspersky Nutzerdaten?
Alle Daten, die über unsere Produkte verarbeitet und/oder übertragen werden, werden durch Verschlüsselung, digitale Zertifikate, getrennte Speicherung und strenge Datenzugriffsrichtlinien gesichert. Bei der Verarbeitung verdächtiger oder bisher unbekannter schädlicher Dateien entscheiden unsere Anwender, ob sie diese Daten zur automatisierten Malware-Analyse an das Kaspersky Security Network (KSN) weiterleiten. Kaspersky stellt immer Informationen zur Datenverarbeitung zur Verfügung – insbesondere die vollständige Liste der Daten, die verarbeitet werden – um sicherzustellen, dass unsere Kunden auf dem Laufenden gehalten werden und fundierte Entscheidungen treffen können. Außerdem veröffentlicht Kaspersky regelmäßig Informationen darüber, wie viele Datenanfragen von unseren Anwendern eingegangen sind und im Transparenzbericht verarbeitet wurden. Der jüngste Bericht für das zweite Halbjahr 2022 ist hier verfügbar.