ERKLÄRUNG ZU KASPERSKY SECURITY NETWORK („KSN-Erklärung")

Alle Begriffe, die in dieser KSN-Erklärung verwendet werden, haben dieselbe Bedeutung wie im Endbenutzer-Lizenzvertrag (EULA) unter dem Abschnitt „Definitionen".

Bitte lesen Sie die Bestimmungen dieser KSN-Erklärung und die dort erwähnten Dokumente sorgfältig durch, bevor Sie ihr zustimmen. Falls die Software in einem Unternehmen oder auf einem von mehreren Personen genutzten Computer ausgeführt wird, müssen Sie sicherstellen, dass diese Personen die Bedingungen der KSN-Erklärung verstanden und ihnen zugestimmt haben, bevor die Datenverarbeitung stattfindet.

Datenschutz und Datenverarbeitung
Der Rechteinhaber behandelt die Daten, die er vom Endbenutzer im Rahmen dieser KSN-Erklärung erhalten hat, gemäß der Datenschutzrichtlinie für Rechteinhaber. Diese Richtlinie kann eingesehen werden unter: www.kaspersky.com/Products-and-Services-Privacy-Policy.

Zwecke der Datenverarbeitung
Die Verwendung des KSN kann die Reaktionsgeschwindigkeit der Software auf Informationen sowie auf Gefährdungen der Netzwerksicherheit beschleunigen. Dies wird erreicht durch:
- Ermittlung der Reputation untersuchter Objekte;
- die Identifizierung neuer und schwer zu erkennender Bedrohungen für die Informationssicherheit und deren Quellen;
- die Verringerung der Wahrscheinlichkeit von Fehlalarmen;
- Erhöhung der Leistungsfähigkeit von Softwarekomponenten;
- Verhinderung von Ereignissen, welche die Informationssicherheit bedrohen, und Untersuchung eingetretener Ereignisse;
- Leistungssteigerung für die Produkte des Rechteinhabers.

Verarbeitete Daten:
Bestimmte Daten, die im Rahmen dieser KSN-Erklärung verarbeitet werden, können entsprechend den Gesetzen einiger Länder als personenbezogene Daten eingestuft werden. Mit Ihrem Einverständnis werden im Rahmen dieser KSN-Erklärung regelmäßig die folgenden Daten automatisch an den Rechteinhaber geschickt:
1. Informationen über die Version des Betriebssystems (OS), das auf dem Computer installiert ist, und die installierten Service Packs des OS: Informationen über die Bitversion des OS, Kernelobjekte, Treiber, Dienste, Einträge in der hosts-Datei und der Systemregistrierung, Name des Computers im Netzwerk (lokale und Domänennamen), regionale Einstellungen des OS (Zeitzone, Standardtastaturlayout, Oberflächensprache), UAC-Einstellungen, Firewall-Einstellungen des OS, Einstellungen der Kindersicherung des OS, Daten und Einstellungen der Betriebssystemdienste.
2. Informationen zu allen installierten Anwendungen: Name und Version der installierten Anwendung, Versionen der installierten Aktualisierungen, Name des Herausgebers, Installationsdatum und vollständiger Installationsordnerpfad auf dem Computer.
3. Informationen über die installierte Software des Rechteinhabers und den Status des Antivirenschutzes des Computers: Softwareversion, Informationen über die Dateien der geladenen Module, deren Namen, Größe und Pfade, Prüfsummen (MD5, SHA2-256, SHA1), Herausgeber, Signatur und Integrität, IDs der Prozesse, in die die Module geladen wurden, die Ladereihenfolge der Module, Versionen der verwendeten Antiviren-Datenbanken und Zeitpunkt ihrer letzten Aktualisierung, Statistiken zu Updates und Verbindungen zu den Diensten des Rechteinhabers, individuelle ID der Software-Installation auf dem Computer und individuelle ID des Computers, Informationen über den Betriebsmodus der Software.
4. Informationen über die verwendete drahtlose Netzwerkverbindung des Computers: Name des drahtlosen Netzwerkes, Prüfsummen (MD5 und SHA256), MAC-Adresse des Zugangspunkts, Attribut des netz- oder akkubetriebenen Computers, Attribut der DNS-Verfügbarkeit, Computertyp, Informationen über die Art und das Sicherheitsniveau des drahtlosen Netzwerkes; individuelle IDs, bestehend aus der individuellen ID des Computers, der individuellen ID der Software-Installation auf dem Computer, dem Namen des drahtlosen Netzwerkes und der MAC-Adresse des Zugangspunkts; Informationen über verfügbare drahtlose Netzwerke: Netzwerkname, MAC-Adresse des Zugangspunkts, Informationen zur Netzwerksicherheit und Signalqualität; Attribut einer verwendeten VPN-Verbindung, Kategorie des in der Software konfigurierten drahtlosen Netzwerkes, DHCP-Einstellungen, Prüfsumme (SHA256) der IP-Adresse (IPv4 oder IPv6) des Computers, Domänenname und Prüfsumme (SHA256) des Pfads von der URL-Adresse des Internetzugangsdienstes; Parameter der WPS-Zugangspunkte: Prüfsummen des Namens und der Seriennummer des Geräts, Name und Nummer des Gerätemodells, Name des Geräteherstellers; Ortszeit des Beginns

und Endes der Verbindung des Computers mit dem drahtlosen Netzwerk, Modus für die Überwachung der Verbindungen des Geräts zum drahtlosen Heimnetzwerk, Liste der verfügbaren Zugangspunkte zum drahtlosen Netzwerk und ihrer Parameter;
5. Informationen über Aktivitäten auf dem Computer des Benutzers: Informationen über Prozesse, die im System ausgeführt werden (Systemprozess-ID (PID), Prozessname, Konto, unter dem der Prozess gestartet wurde, Anwendung oder Befehl, die bzw. der den Prozess gestartet hat, vollständiger Pfad zu Prozessdateien und Befehlszeichenfolge, die zum Starten des Prozesses verwendet wurde, Bezeichner, der angibt, dass sich die Prozessdatei in der Autorun-Liste befindet, Beschreibung des Produkts, zu dem der Prozess gehört (Produktname und Informationen zum Herausgeber), Informationen zu verwendeten digitalen Zertifikaten und Informationen zur Überprüfung deren Authentizität oder Informationen dazu, dass die Datei keine digitale Signatur aufweist), URL-Adressen der besuchten Websites und Zeitpunkt des Besuchs, Antwort vom DNS-Server und Dauer der Antwortpufferung, IP-Adressen (IPv4 oder IPv6) des DNS-Servers oder der Website-Domäne, Domänenname, Methode zur Erkennung des Domänennamens, Attribut, das angibt, dass der Domänenname gelistet ist, Name der Datei des Prozesses, der auf die Website zugreift, Größe und Prüfsummen (MD5 und SHA256) der Datei, Pfad zur Datei und Pfadvorlagencode, Ergebnis der Überprüfung der digitalen Signatur der Datei, User-Agent-Zeichenfolge, Dauer der Speicherung dieser Informationen vor der Übertragung an KSN, Suchabfragen, Parameter von HTTP-Abfragen, Zeit, die seit der letzten Benutzeraktivität auf dem Computer verstrichen ist, sowie Informationen über in Prozesse geladene Module: ihre Namen, Größe, Typen, Prüfsummen (MD5, SHA2-256, SHA1) und Pfade.
6. Informationen über alle untersuchten Objekte und Operationen: Name des untersuchten Objekts, Datum und Uhrzeit der Untersuchung, Name und Größe der untersuchten Dateien und Pfade zu diesen, Datum und Uhrzeit der Dateierstellung, Name des Packers (wenn die Datei gepackt war), Daten des PE-Headers der Datei, Version des Compilers, Anzahl, Größe und Daten der Dateiabschnitte, Dateientropie, ID des Dateityps und -formats, URL- und IP-Adressen, von denen aus das Objekt heruntergeladen wurde, ID des Downloadprotokolls und Nummer des Verbindungsports, Prüfsummen (MD5, SHA2-256, SHA1) des Prozesses, der das Objekt heruntergeladen hat, Prüfsummen des Objekts (MD5, SHA2-256, SHA1), Typ und Wert der zusätzlichen Prüfsumme des Objekts, Informationen über die digitale Signatur (das Zertifikat) des Objekts (Datum und Uhrzeit der Signatur, Name des Zertifikatsinhabers, Seriennummer des Zertifikats und Berechnungsalgorithmus für die Prüfsumme, Information über den öffentlichen Schlüssel des Zertifikats: Prüfsumme (SHA2-256) des öffentlichen Schlüssels, ID der Zertifikatsdatenbank, Name des Zertifikatsausstellers, Ergebnis der Zertifikatsprüfung), ID der Softwareaufgabe, die die Überprüfung durchgeführt hat, Datum und Uhrzeit der Überprüfung, Ergebnis der abgeschlossenen Überprüfung und Entscheidungen des Benutzers und des Produkts nach der Überprüfung, Informationen über Änderungen der Vertrauensgruppe.
7. Wenn eine Bedrohung oder Schwachstelle entdeckt wird, werden Informationen über das untersuchte Objekt mit Informationen über ID, Version und Typ des Eintrags der Antiviren-Datenbank ergänzt sowie über den Namen der Bedrohung nach der Klassifizierung des Rechteinhabers, Prüfsummen (MD5, SHA2-256, SHA1) der Datei der Anwendung, die den Zugriff auf die URL angefordert hat, wo die Erkennung erfolgt ist, die IP-Adresse (IPv4 oder IPv6) der erkannten Bedrohung, die ID des Verkehrstyps, bei dem die Erkennung erfolgte, die ID der Schwachstelle und ihre Gefahrenklasse, die URL-Adresse der Seite, auf der die Erkennung erfolgt ist, die Nummer des Skripts auf der Seite, die ID der Bedrohung, Typ und Status der Erkennung, Zwischenergebnisse der Objektanalyse, das Attribut, das angibt, dass es sich bei dem Objekt um einen Container handelt, und den Grad der Prozessintegrität.
8. Informationen über Netzwerkangriffe: IP-Adresse des angreifenden Computers und Nummer des Ports auf dem Computer des Benutzers, auf den der Netzwerkangriff gerichtet war, ID des Angriffsprotokolls, Name und Art des Angriffs.
9. URL- und IP-Adressen der Seite, auf der bösartiger oder verdächtiger Inhalt gefunden wurde, Name, Größe und Prüfsumme der Datei, die Zugriff auf diese URL angefordert hat, ID und Gewichtung der Regel, die das Untersuchungsergebnis zurückgab, und Angriffsziel.
10. Informationen zum Betrieb der URL-Advisor-Komponente: auf Untersuchungsergebnissen beruhende Entscheidungen des Benutzers darüber, ob Domains sicher oder bösartig sind, Prüfsummen (MD5) der URL und Referrer der untersuchten Domain, ID der URL-Advisor-Komponente.
11. Aggregierte Daten zu den Ergebnissen der Untersuchung mit lokalen und Cloud-KSN-Datenbanken während des Untersuchungszeitraums: Anzahl der einzelnen unbekannten Objekte, Anzahl der einzelnen vertrauenswürdigen Objekte, Anzahl der einzelnen nicht vertrauenswürdigen Objekte, Gesamtzahl der Einstufungen als "unbekannte Objekte", Gesamtanzahl der Einstufungen als "vertrauenswürdige Objekte", Gesamtzahl der Einstufungen als "nicht vertrauenswürdige Objekte", Anzahl der auf der Grundlage der Ergebnisse der Zertifikatsprüfung als vertrauenswürdig eingestuften Objekte, Anzahl der aufgrund der vertrauenswürdigen URL-Adresse als vertrauenswürdig eingestuften Objekte, Anzahl der aufgrund der Logik der Vererbung der Vertrauenswürdigkeit aus einem vertrauenswürdigen

Prozess als vertrauenswürdig eingestuften Objekte, Anzahl der unbekannten Objekte, für die keine Einstufung als vertrauenswürdig oder nicht vertrauenswürdig erfolgte, Anzahl der Objekte, die der Benutzer als vertrauenswürdig gekennzeichnet hat. Version der lokalen KSN-Datenbank auf dem Computer zum Zeitpunkt der Übermittlung der Statistik und ID der Einstellung für die Datenbankverwaltung der Software, Informationen über erfolgreiche/fehlgeschlagene Anfragen an KSN (Verbindungen und Operationen) und die Zeit für Operationen aufgewendete Zeit, Sitzungsdauer der KSN-Verbindung, Volumen der gesendeten und empfangenen Daten, Anfangs- und Endzeiten der Operation zur Sammlung von Informationen für die Weiterleitung an KSN, Gesamtzahl der Anfragen an KSN, die aus irgendeinem Grund fehlgeschlagen (der angegeben ist) sind.
12. Wurde ein potentiell schädliches Objekt erkannt, so enthält die Übertragung Informationen über Prozessspeicherdaten, Elemente der Systemobjekt-Hierarchie (ObjectManager), UEFI-BIOS-Speicherdaten, Namen von Registrierungsschlüsseln und deren Werte.
13. Informationen zu Systemprotokollereignissen: Ereigniszeit, Name des Protokolls, in dem das Ereignis erkannt wurde, Typ und Kategorie des Ereignisses, Name der Ereignisquelle und Ereignisbeschreibung.
14. Informationen über Netzwerkverbindungen: Version und Prüfsummen (MD5, SHA2-256, SHA1) Datei des Prozesses, der den Port geöffnet hat, Pfad zur Prozessdatei und deren Signatur, lokale und Remote-IP-Adressen, Nummern der lokalen und Remote-Ports, Verbindungsstatus, Zeitpunkt der Öffnung des Ports.
15. Informationen über die ausgeführte Datei: Prüfsumme, Format, Anzahl der Ausführungen der Datei, Version des Statistikpakets, Softwaredetails: Build-Nummer, IDs der Anwendung und ihre Version.
16. Informationen zum Abschluss des Rollbacks von Schadsoftware-Aktivitäten: Informationen über die Datei, deren Aktivitäten rückgängig gemacht wurden (Dateiname, vollständiger Dateipfad, Dateigröße und Prüfsummen (MD5, SHA2-256, SHA1)), Informationen zu erfolgreichen und fehlgeschlagenen Aktionen zur Löschung, Umbenennung oder Vervielfältigung von Dateien und zur Wiederherstellung von Werten in der Registrierung (Namen der Registerschlüssel und deren Werte), Informationen zu von Schadsoftware geänderten Systemdateien vor und nach dem Rollback, Name der erkannten Bedrohung gemäß der Klassifikation des Rechteinhabers, ID der Antiviren-Datenbanken und ID des Eintrags in den Antiviren-Datenbanken, auf deren Grundlage die Einstufung vorgenommen wurde.
17. Informationen zur Verwendung einer VPN-Verbindung: IP-Adresse des VPN-Servers, zu dem die Verbindung hergestellt wird, individuelle ID der Software-Installation auf dem Computer.

Wenn Software aus dem Speicher entladen wurde, werden die unter den Punkten 5, 6 und 7 genannten Daten nicht übertragen, sondern können in einem begrenzten Speicher auf dem Computer des Benutzers gespeichert werden. Solche Daten können nach dem Entfernen der Software nicht wiederhergestellt werden. Nach dem Laden der Software werden diese Daten für die oben genannten Zwecke an Kaspersky Lab übermittelt.

Objekte, die durch Eindringlinge zur Schädigung des Benutzer-Computers missbraucht werden können, können auch zur zusätzlichen Überprüfung an Kaspersky Lab übermittelt werden:
- Dateien oder Teile daraus.
- Name, Größe und Version der übermittelten Datei, ihre Beschreibung und Prüfsummen (MD5, SHA2-256, SHA1), Dateipfad, Format-ID, Name des Herausgebers der Datei, Name des Produkts, zu dem die Datei gehört.
- Start- und Enddatum der Gültigkeit des Zertifikats, wenn die gesendete Datei eine digitale Signatur aufweist, Datum und Uhrzeit der Signierung des Zertifikats, Name des Zertifikatsherausgebers, Informationen zum Zertifikatsinhaber, zur Abdruck und zum öffentlichen Schlüssel des Zertifikats und zu dem zu ihrer Berechnung verwendeten Algorithmus, Seriennummer des Zertifikats.
- Informationen über Datum und Uhrzeit der Erstellung und Änderung der Datei, Attribut, das angibt, ob das Datum und die Uhrzeit der Dateisignatur bei der Überprüfung der Signatur verwendet wird, Ergebnis der Integritätsprüfung der Datei.
- Unter schädlichen Links erkannte Objekte.
Solche Objekte können bis zu ihrer Übermittlung temporär auf dem Benutzercomputer gespeichert werden.

Darüber hinaus kann die Übermittlung zum Zwecke der Verhinderung und Untersuchung von Vorfällen auch ausführbare und nicht ausführbare vertrauenswürdige Dateien, Arbeitsspeicher-Segmente, Boot-Sektoren des Betriebssystems und Berichte über die Programmaktivität enthalten, die Folgendes beinhalten:
- Informationen über Prozesse und Dienste, die gestartet wurden: Prüfsummen (MD5, SHA2-256, SHA1) der Prozess- oder Dienstdatei, Dateiname und -größe, Dateipfad, Namen von und Pfade zu Dateien, auf die der Prozess zugreift, Namen und Werte der Registrierungsschlüssel, auf die der Prozess zugreift, Arbeitsspeicher-Segmente, URL- und IP-Adressen, auf die der Prozess zugreift oder aus denen die Datei stammt, die ausgeführt wurde.
- Name des Benutzerkontos, unter dem der Prozess ausgeführt wird, Name des Computers, auf dem er gestartet

wurde, Kopfzeilen von Prozessfenstern, ID der Antiviren-Datenbanken, Name der erkannten Bedrohung gemäß Klassifizierung des Rechteinhabers, individuelle ID der Lizenz, Ablaufdatum und Art der Lizenz, Version des Betriebssystems (OS) und der auf dem Computer installierten Service Packs sowie Ortszeit.

Zur Verbesserung der Produktqualität erklärt sich der Benutzer damit einverstanden, folgende Informationen an Kaspersky Lab zu übermitteln:
- Informationen über die auf dem Computer installierte Software des Rechteinhabers: Datum und Uhrzeit der Installation, Name und Version der Software, Versionen der installierten Updates, Informationen zur installierten Lizenz (ID und Typ), individuelle ID der Softwareinstallation auf dem Computer und individuelle ID des Computers, Lokalisierung der Oberfläche, Datum und Uhrzeit, die zum Zeitpunkt der Datenübermittlung an KSN auf dem Computer eingestellt waren, ID des Software-Rebrandings.
- Informationen über die auf dem Computer installierte Software: Name der Software und Name des Herstellers, Informationen über die Registrierungsschlüssel und ihre Werte, Informationen über die Dateien installierten Software-Komponenten (Prüfsummen (MD5, SHA2-256, SHA1) der Datei), Dateiname, Dateipfad auf dem Computer, Größe, Version und digitale Signatur), Art der an der Erkennung beteiligten Anwendung.
- Informationen über die auf dem Computer installierte Hardware: Informationen zur Größe des Arbeitsspeichers, zur Marke und Anzahl der Kerne des Prozessors (CPU), zur Marke der Festplatten (HDD), Typ, Name, Modell und Version der Firmware, Parameter von integrierten und Plug-in-Geräten.
- Wird eine Bedrohung erkannt, werden das Attribut, welches das Objekt als Container kennzeichnet, und der Grad der Prozessintegrität übermittelt.
- Informationen zu Fehlern bei Produktkomponenten: Typ und Uhrzeit des Fehlers, ID der Produktkomponente und Aufgabe, die den Fehler zurückgegeben hat.
- Informationen über die Untersuchung sicherer Verbindungen: verwendetes Zertifikat zum Herstellen der Verbindung und dessen Prüfsumme (MD5, SHA2-256, SHA1), DNS- und IP-Adresse (IPv4 oder IPv6) der Netzwerkressource, Nummer des Remote-Ports, Name und Version der Anwendung, mit der die sichere Verbindung hergestellt wurde, Pfad zu dieser Anwendung sowie Code des bei der Untersuchung der sicheren Verbindung aufgetretenen Fehlers (sofern ein Fehler zurückgegeben wurde).
- Informationen über die Qualität der Updates der installierten Produkte und Antiviren-Datenbanken: IP-Adresse (IPv4 oder IPv6) der verwendeten Update-Quelle, Art der Update-Aufgabe, ID des vorherigen und aktuellen Software-Updates, Anzahl und Gesamtgröße der während des Update-Vorgangs heruntergeladenen Dateien, durchschnittliche Downloadrate der Update-Dateien, durchschnittliche Geschwindigkeit der Netzwerkoperationen während des Update-Vorgangs, Status der Fertigstellung der Update-Aufgabe, Art des eventuell während des Update-Vorgangs aufgetretenen Fehlers, ID der Produktkomponente, die das Update ausführt, Wert des TARGET-Filters der Update-Aufgabe; Erstellungsdatum der Indexdateien der installierten und heruntergeladenen Updates, Datum und Uhrzeit der heruntergeladenen und installierten Updates.
- Informationen zu den Ressourcen, die von Produktkomponenten bei Objekt-Untersuchungen verwendet werden: tatsächliche und durchschnittliche Dauer der Untersuchung aufgeteilt nach Produktkomponenten, gesamte, minimale und maximale Untersuchungsdauer, Überwachung des Netzwerkverkehrs, Anzahl der Untersuchungsanfragen, ID des Untersuchungsvorgangs, Zeitpunkt des Starts und der Beendigung des Dienstprozesses und der Benutzeroberfläche des Produkts von Kaspersky Lab, Dauer der Erfassung von Daten über die Software von Drittanbietern, Anzahl der Ereignisse während dieser Zeit.
- Informationen über Interaktionen zwischen dem Produkt und My Kaspersky: ID und Name der Dienstdomäne, an die die Anfrage gesendet wurde, Anzahl der Anfragen und erfolgreiche/fehlgeschlagene Verbindungen zu jedem Dienst, Anzahl der Antworten von jedem Dienst, Anzahl der Anfragefehler und Timeouts, Zeitpunkt des Starts und der Beendigung des Prozesses für die Erfassung von Daten über die Anzahl der Anfragen und Verbindungen.
- Informationen über den Prozess, der die Selbstschutzkomponente des Produkts angegriffen hat: Name und Größe der Prozessdatei, ihre Prüfsummen (MD5, SHA2-256, SHA1), vollständiger Pfad zur Datei und Pfadvorlagencode, Datum und Uhrzeit der Erstellung und Kompilierung der Prozessdatei, Attribut einer ausführbaren Datei, Attribute der Prozessdatei, Informationen über das Zertifikat, mit dem die Prozessdatei signiert ist, Code des Kontos, unter dem der Prozess gestartet wurde, IDs der für den Zugriff auf den Prozess ausgeführten Operationen, Art der Ressource, mit der die Operation ausgeführt wird (Prozess, Datei, Registrierungsobjekt, Fenstersuche mit der FindWindow-Funktion), Name der Ressource, mit der die Operation ausgeführt wird, Erfolg oder Scheitern der Operation, Reputation der Prozessdatei und ihres Zertifikats gemäß KSN.
- ID des angegriffenen Software-Prozesses.
- ID des Ereignisses, das die auf dem Computer installierte Software oder Anwendung zum Absturz gebracht hat.
- Informationen über die Nutzung der Software auf dem Computer: Informationen über die Prozessornutzung (CPU-

Nutzung), Daten zur Speichernutzung (Private Bytes, nicht ausgelagerter Pool, ausgelagerter Pool), Anzahl der aktiven Protokolle und Anzahl der wartenden Threads, Dauer der Software-Nutzung bis zum Eintritt des Fehlers.
- Informationen über das System zum Erscheinen des BSOD: Name und Version des Treibers, der den BSOD verursacht hat, Code der Fehlerprüfung und dessen Parameter, Treiberfehler-Stack, ID für den Typ des erkannten Speichersegments, der während des Fehlers erstellt wurde, Attribut für eine Dauer der OS-Sitzung von mehr als 10 Minuten bis zum Erscheinen des BSOD oder bis zur unerwarteten Abschaltung, individuelle ID des OS-Speichersegments, Datum und Uhrzeit des BSOD, Berichte von Softwaretreibern aus dem Speichersegment (Fehlercode, Modulname, Name der Datei mit Quellcode und Zeichenfolge, in der der Fehler aufgetreten ist), vollständige Nummer des Builds des Betriebssystemkernels, Name, Lokalisierung und Version der Anwendung, in der der Fehler erkannt wurde, Fehlernummer und -beschreibung aus dem Systemprotokoll der Anwendung, für die der Fehler erkannt wurde, Informationen zu einem Ausnahmefehler in der Anwendung, Adresse des Anwendungsfehlers im Format eines Modul-Offsets, Name und Version des Anwendungsmoduls, in dem der Fehler aufgetreten ist, Attribut eines Anwendungsfehlers im Software-Plugin, Fehler-Stack, Dauer der Programmnutzung bis zum Fehler, Methode zur Erkennung des Softwarefehlers (Treiberüberwachung, Verarbeitung des Datenverkehrs oder Anzahl der wartenden Threads), Name des Prozesses der die Überwachung des Datenverkehrs initiiert hat oder Austausch, der zu dem Softwarefehler geführt hat.
- Name der Root-Index-Datei von Datenbanken, deren Datum und Uhrzeit, sekundäre Index-Dateien mit Datum und Uhrzeit für bestimmte Update-Kategorien, Namen bestimmter Dateien von aktualisierbaren Kategorien und deren Prüfsummen für Datenbanken, die heruntergeladen werden oder bereits heruntergeladen wurden.
- Informationen über die NativeImage-Datei: Typ, Name, Prüfsummen (MD5, SHA2-256, SHA1) der Datei, vollständiger Speicherpfad der Datei auf dem Computer, Dateipfadvorlagencode, ID der Dateimodul-Version, Prüfsumme (SHA256) der digitalen Signatur des Builds, durch den die untersuchte Datei erstellt wurde, und ID der Methode zur Ermittlung des Builds, IDs der Untersuchungsergebnisse bezüglich der Dateiintegrität.
- Informationen über die Aktivitätsmonitor-Komponente: vollständige Nummer der Komponentenversion, Versionsnummer, ID des aktuellen Komponentenereignisses, dessen Verarbeitung länger dauerte als das eingestellte Zeitlimit, Dauer der Ereignisverarbeitung, Gesamtzahl solcher Ereignisse, Name und Prüfsummen (MD5, SHA2-256, SHA1) der Datei des Prozesses, der das aktuelle Ereignis ausgelöst hat, Name und Code des Verzeichnisses, das die Datei auf dem Computer enthält, maximal zulässige Ereignisverarbeitungszeit, Ereigniscode, das einen Ereignis-Queue-Überlauf verursacht hat, und die Gesamtzahl solcher Ereignisse, Name der Datei, Verzeichnis und Code des Laufwerksverzeichnisses, das die Datei des Prozesses enthält, der das aktuelle Ereignis ausgelöst hat, das einen Überlauf der Ereigniswarteschlange verursacht hat, Prüfsummen (MD5, SHA2-256, SHA1) dieser Datei, Ereignis-ID, dessen Verarbeitung aufgrund von Timeout unterbrochen wurde, Überwachungsfilter-ID und Art des Überwachungsereignisses, Größe der Ereigniswarteschlange der Komponente zum Zeitpunkt der Übertragung von Statistiken, Differenz zwischen dem ersten und dem aktuellen Ereignis in der Warteschlange zum Zeitpunkt der Übertragung von Statistiken, Wahrscheinlichkeit der Übertragung von Statistiken, Erstellungs-ID von Statistiken, Art der Scanaufgabe, von der das Produkt das Datum der Installation der erkannten Anwendung erhielt, Pfad, Datum und Uhrzeit der Installation und der letzten Verwendung der erkannten Anwendung, Status der erkannten Anwendung, Datum und Uhrzeit des Betriebssystemstarts, Datum und Uhrzeit des empfangenen Ereignisses einer kontrollierten Aktion im OS, Datum und Uhrzeit der Produktinstallation, Datum und Uhrzeit des Startzeitpunkte von Aktivitätsmonitor, Anzahl der Neuinitialisierungen von Antiviren-Datenbanken nach deren Aktualisierung, Datum und Uhrzeit der letzten Neuinitialisierung von Antiviren-Datenbanken nach deren Aktualisierung, Verzögerungszeit der Verarbeitung eines Ereignisses einer Aktion im OS durch das Subsystem der permanenten Ereignisspeicherung, Verzögerungszeit der Verarbeitung eines Ereignisses einer Aktion im OS durch das Subsystem des proaktiven Schutzes, Verzögerungszeit der Verarbeitung eines Ereignisses einer Aktion im OS durch das Subsystem der Verhaltensanalyse, die Anzahl der synchronen Ereignisse in der Warteschlange der durchgeführten Aktionen im OS, die Anzahl der verarbeiteten Ereignisse der durchgeführten Aktionen im OS, die Anzahl der verarbeiteten synchronen Ereignisse der ausgeführten Aktionen im OS, die Anzahl der verzögerten Ereignisse des aktuellen Typs der ausgeführten Aktionen im OS, die zusammengefasste Verzögerungszeit aller Ereignisse des aktuellen Typs der ausgeführten Aktionen im OS, die zusammengefasste Verzögerungszeit aller Ereignisse der ausgeführten Aktionen im OS.
- Informationen zur Nutzung der Komponente Installationsassistent: Name der Setup-Datei von Fremdsoftware, Prüfsummen (MD5, SHA2-256, SHA1), Größe, Typ und Vollständiger Pfad der Setup-Datei, Pfadvorlagencode, zusätzliche Informationen zur Vorlagendatei (Dateibeschreibung und -version, Name und Version der von der Datei installierten Software, Name des Software-Herausgebers, interner Dateiname, ursprünglicher Dateiname, Copyright-Hinweis, Sprache der Softwarelokalisierung, Attribut der Verfügbarkeit einer digitalen Signatur, Name des Unternehmens oder der Organisation, die die Datei signiert hat), Datum und Uhrzeit der letzten Aktualisierung der auf dem Computer installierten Antiviren-Datenbanken, Name der Kategorie der Setup-Datei nach der Klassifizierung des

Rechteinhabers, ID, Version und Art des verwendeten Datensatzes der Antiviren-Datenbank, Attribut für die Erkennung der Setup-Datei im Debugging-Modus, Typ und Version der Vorlage für die Benutzeroberfläche der Setup-Datei, ihre Prüfsummen (MD5, SHA2-256, SHA1), Informationen über die Nutzung der Benutzeroberfläche der Setup-Datei: ID der Benutzeraktivität mit einem Element der Benutzeroberfläche, Name, Ort und Text des Elements der Benutzeroberfläche, Attribut für das Vorhandensein von Befehlszeilenparametern beim Start der Setup-Datei, ID des Komponentenszenarios, unter dem die Statistik übermittelt wird, Vollversion der Komponente.
- Wenn das Produkt eine URL-Adresse erkennt, die von einem Installationsprogramm zum Herunterladen von Inhalten verwendet wird, die Werbung oder Vorschläge zur Installation zusätzlicher Anwendungen enthalten können, umfasst die Übermittlung die erkannte URL-Adresse (Domänenname aus der URL-Adresse bei Zugriff über ein sicheres Protokoll). Name der URL-Adresskategorie gemäß der Klassifizierung des Rechteinhabers, Referrer und IP-Adresse (IPv4 oder IPv6) der erkannten URL-Adresse.
- Informationen zum letzten fehlgeschlagenen Neustart des Betriebssystems: Anzahl der fehlgeschlagenen Neustarts.
- Informationen über die Verwendung von adaptiven Schutzszenarien: Prüfsumme (SHA256), die auf Grundlage der individuellen ID der Softwareinstallation auf dem Computer und der ID der Statistik sowie der IDs der Attribute, die anzeigen, dass der Computer von einem Kind genutzt wird, ermittelt wird;
- Geräteinformationen: MAC-Adresse, Typ, Anzahl der Zeichen im Namen, Name des Herstellers, Methode zur Erkennung des Geräts in einem WLAN-Netzwerk; Version des Moduls zur Erkennung des Geräts in einem WLAN-Netzwerk; Typ, Hersteller, Name und Betriebssystem des in einem WLAN-Netzwerk erkannten Geräts, sowie weitere technische Angaben;
- Informationen über die Nutzung der Anwendung bei deaktiviertem Virenschutz: Name und Prüfsumme (MD5) der ausführbaren Datei der Anwendung, Dateipfad und Dateipfadvorlagencode, Informationen über den Grund und die Dauer der Deaktivierung des Virenschutzes.
- Informationen zu Festplattenparametern: ID des S.M.A.R.T-Parameters, Daten der S.M.A.R.T-Attribute, Modell, Seriennummer, Name und Version der Firmware, Größe, Status, Betriebszeit und Temperatur der Festplatte.
- Informationen zur Erkennung inkompatibler Treiberumgebungen: Prozessorarchitektur, Betriebssystemkernelversion, vollständige Betriebssystemversion mit erweiterten Optionen und Kernelversion, erweiterte CPU-Informationen, Name des inkompatiblen Treibers, Treiberintegritätsoptionen, Betriebszustand der Treiber, Vollversion der Treiber, Status des Hypervisor-Supports.

Mit der Teilnahme am KSN-Programm erklären Sie sich einverstanden, die folgenden Informationen für die oben genannten Zwecke zu übermitteln:
- Individuelle ID der Software-Installation auf dem Computer;
- Vollversion der installierten Software;
- ID des Softwaretyps;
- Individuelle ID des Computers, auf dem die Software installiert ist.

Im Sinne eines besseren Schutzes durch die Software kann der Rechteinhaber Objekte erhalten, die von Angreifern dazu missbraucht werden könnten, dem Computer und der Informationssicherheit zu schaden. Zu solchen Objekten gehören unter anderem:
• ausführbare und nicht ausführbare Dateien oder deren Teile;
• Teile des Arbeitsspeichers des Computers;
• Sektoren, die am Hochfahren des Betriebssystems beteiligt sind;
• Datenpakete des Datenverkehrs im Netzwerk;
• Webseiten und E-Mails mit verdächtigen und bösartigen Objekten;
• Beschreibung der Klassen und Klasseninstanzen des WMI-Repositorys;
• Aktivitätsberichte für die Anwendung.

Solche Anwendungsaktivitätsberichte enthalten die folgenden Daten zu Dateien und Prozessen:
- Name, Größe und Version der zum Senden vorgesehenen Datei, Beschreibung und Prüfsummen der Datei (MD5, SHA2-256, SHA1), ID des Dateiformats, Name des Dateilieferanten, Name des Produktes, zu dem die Datei gehört, vollständiger Pfad auf dem Computer, Vorlagencode des Dateipfads, Zeitstempel der Dateierstellung und -änderung;
- Datum und Uhrzeit für den Beginn und das Ende der Gültigkeit des Zertifikats (falls die Datei eine digitale Signatur besitzt), Datum und Uhrzeit der Signatur, Name des Zertifikatsherausgebers, Informationen über den Zertifikatsinhaber, Fingerabdruck, öffentlicher Zertifikatsschlüssel und entsprechender Algorithmus, und Seriennummer des Zertifikats;
– Name des Kontos, unter dem der Prozess läuft;

• Prüfsummen (MD5, SHA2-256, SHA1) des Namens des Computers, auf dem der Prozess läuft;
• Namen der Prozessfenster;
• ID der Antiviren-Datenbanken, Name der erkannten Bedrohung gemäß der Klassifizierung des Rechteinhabers;
• Informationen über die installierte Lizenz, deren ID, Typ und Ablaufdatum;
• Ortszeit auf dem Computer zum Zeitpunkt der Informationsbereitstellung;
• Namen und Pfade der Dateien, auf die durch den Prozess zugegriffen wurde;
• Namen der Registrierungsschlüssel und deren Werte, auf die durch den Prozess zugegriffen wurde;
• URL- und IP-Adressen, auf die durch den Prozess zugegriffen wurde;
• URL- und IP-Adressen, von denen die ausgeführte Datei heruntergeladen wurde.

Der Rechteinhaber kann zur Vermeidung von Falschmeldungen außerdem vertrauenswürdige ausführbare und nicht ausführbare Dateien oder Teile davon erhalten.

Je nach der von Ihnen genutzten Software werden weitere Daten verarbeitet.

Wenn Sie Kaspersky Internet Security nutzen oder darauf wechseln, werden die folgenden Daten verarbeitet:
- Informationen über die Nutzung der Komponente Sicherer Zahlungsverkehr: Attribut ihres Betriebsmodus, Informationen über Änderungen der Liste der von der Komponente geschützten Websites durch den Benutzer: URL-Adresse und ggf. Referrer der Website, Attribut, das die Bearbeitung oder Löschung der Website kennzeichnet, Startmodus der Komponente für diese Website, Kontext der vorgenommenen Änderungen an der Liste der Websites; Informationen über den Browser, der zum Aufrufen der Website verwendet wurde: URL-Adresse und Referrer der Website, Name und Version des Browsers, Art des Browser-Starts, Startdauer und Attribut des erfolgreichen Starts, Informationen über die Schutzstufe und die Art der Nachricht über die Schutzstufe, Name und Version des Browsers, von dem aus der aktuell verwendete Browser gestartet wurde.
- Informationen über Updates von installierten Anwendungen: IDs der aktualisierten Anwendung und deren Updates, IDs der Lokalisierungssprache der Anwendung und ihrer Updates, Anwendungsversion vor dem Update, zum Herunterladen der Update-Setup-Datei verwendete URL-Adresse, ggfs. ID des Download-Fehlers der Setup-Datei, Attribut, das eine Verletzung der Integrität der Update-Setup-Datei anzeigt, ID der Benutzeraktion bei Verwendung der Liste der Ausnahmen, Art der Anwendung, die aktualisiert wird, Namen der Prozessdateien, welche die Installation des Updates verhindern, ID des Update-Ergebnisses, Parameter der Befehlszeile zum Starten der Setup-Datei des Updates, Attribut der erfolgreichen Update-Installation.
- Informationen über die Nutzung der Komponente Tool zum Entfernen unerwünschter oder überflüssiger Software: Datenbank-Version mit Informationen über installierte Anwendungen und deren Updates, Name und Version der untersuchten Anwendung, Registrierungsordner, der der betreffenden Anwendung zugeordnet ist, Ordner, in dem die Anwendung installiert wurde, Zeichenfolge mit dem Befehl zur Deinstallation der Anwendung, Lokalisierungssprache der Anwendung, ID des Ergebnisses der Untersuchung der Anwendung, Attribut der Anwendungsinstallation nur für den aktuellen Benutzer, Attribut der Untersuchung der Anwendung im Debugging-Modus, ID der Benutzeraktion bei Verwendung der Liste mit den Ausnahmen, empfohlene Arten von Anwendungen zur Deinstallation und deinstallierte Anwendungen, Namen von Prozessdateien, die die Deinstallation verhindern, ID des Ergebnisses der Deinstallation, Attribut der erfolgreichen Deinstallation, Informationen über die Suite, zu der die erkannte Software gehört: ID, Version, Name, Entwickler, Sprachen-ID, Typ der Hauptanwendung der Suite, Quelle von Informationen über das Installationsdatum, Datum und Zeitpunkt der Installation und der letzten Nutzung der Hauptanwendung der Suite sowie Installationspfad und gewährleistetes Schutzniveau;
- Informationen über die Nutzung der Komponente zum Schutz vor Datensammlung (Private Browsing): Referrer der HTTP-Tracking-Anfrage, Name des Dienstes oder der Organisation, welche die Tracking-Dienste zur Verfügung stellt, Kategorie des Tracking-Dienstes nach der Klassifizierung des Rechteinhabers, ID und Version des Browsers, mit dem die URL geöffnet wurde.
- Informationen über die von den Komponenten Kindersicherung und Web-Kontrolle blockierten Links: Grund für die Blockierung, Version der Komponenten Kindersicherung und Web-Kontrolle, URL und IP-Adresse des blockierten Links.
- Informationen zur Nutzung der Komponente Modus für vertrauenswürdige Programme: ID der Version ihrer Einstellungen, Attribut ihres Betriebsmodus, Ergebnis der Dateistatusüberprüfung und Quelle des Status der Vertrauenswürdigkeit, aggregierte Daten zur Anzahl der vertrauenswürdigen, nicht vertrauenswürdigen und unbekannten Objekte.
Wenn Sie Kaspersky Total Security nutzen oder darauf wechseln, werden die folgenden Daten verarbeitet:
- Informationen über die Nutzung der Komponente Sicherer Zahlungsverkehr: Attribut ihres Betriebsmodus, Informationen über Änderungen der Liste der von der Komponente geschützten Websites durch den Benutzer: URL-

Adresse und ggf. Referrer der Website, Attribut, das die Bearbeitung oder Löschung der Website kennzeichnet, Startmodus der Komponente für diese Website, Kontext der vorgenommenen Änderungen an der Liste der Websites; Informationen über den Browser, der zum Aufrufen der Website verwendet wurde: URL-Adresse und Referrer der Website, Name und Version des Browsers, Art des Browser-Starts, Startdauer und Attribut des erfolgreichen Starts, Informationen über die Schutzstufe und die Art der Nachricht über die Schutzstufe, Name und Version des Browsers, von dem aus der aktuell verwendete Browser gestartet wurde.
- Informationen über Updates von installierten Anwendungen: IDs der aktualisierten Anwendung und deren Updates, IDs der Lokalisierungssprache der Anwendung und ihrer Updates, Anwendungsversion vor dem Update, zum Herunterladen der Update-Setup-Datei verwendete URL-Adresse, ggfs. ID des Download-Fehlers der Setup-Datei, Attribut, das eine Verletzung der Integrität der Update-Setup-Datei anzeigt, ID der Benutzeraktion bei Verwendung der Liste der Ausnahmen, Art der Anwendung, die aktualisiert wird, Namen der Prozessdateien, welche die Installation des Updates verhindern, ID des Update-Ergebnisses, Parameter der Befehlszeile zum Starten der Setup-Datei des Updates, Attribut der erfolgreichen Update-Installation.
- Informationen über die Nutzung der Komponente Tool zum Entfernen unerwünschter oder überflüssiger Software: Datenbank-Version mit Informationen über installierte Anwendungen und deren Updates, Name und Version der untersuchten Anwendung, Registrierungsordner, der der betreffenden Anwendung zugeordnet ist, Ordner, in dem die Anwendung installiert wurde, Zeichenfolge mit dem Befehl zur Deinstallation der Anwendung, Lokalisierungssprache der Anwendung, ID des Ergebnisses der Untersuchung der Anwendung, Attribut der Anwendungsinstallation nur für den aktuellen Benutzer, Attribut der Untersuchung der Anwendung im Debugging-Modus, ID der Benutzeraktion bei Verwendung der Liste mit den Ausnahmen, empfohlene Arten von Anwendungen zur Deinstallation und deinstallierte Anwendungen, Namen von Prozessdateien, die die Deinstallation verhindern, ID des Ergebnisses der Deinstallation, Attribut der erfolgreichen Deinstallation, Informationen über die Suite, zu der die erkannte Software gehört: ID, Version, Name, Entwickler, Sprachen-ID, Typ der Hauptanwendung der Suite, Quelle von Informationen über das Installationsdatum, Datum und Zeitpunkt der Installation und der letzten Nutzung der Hauptanwendung der Suite sowie Installationspfad und gewährleistetes Schutzniveau;
- Informationen über die Nutzung der Komponente zum Schutz vor Datensammlung (Private Browsing): Referrer der HTTP-Tracking-Anfrage, Name des Dienstes oder der Organisation, welche die Tracking-Dienste zur Verfügung stellt, Kategorie des Tracking-Dienstes nach der Klassifizierung des Rechteinhabers, ID und Version des Browsers, mit dem die URL geöffnet wurde.
- Informationen über die von den Komponenten Kindersicherung und Web-Kontrolle blockierten Links: Grund für die Blockierung, Version der Komponenten Kindersicherung und Web-Kontrolle, URL und IP-Adresse des blockierten Links.
- Informationen zur Nutzung der Komponente Modus für vertrauenswürdige Programme: ID der Version ihrer Einstellungen, Attribut ihres Betriebsmodus, Ergebnis der Dateistatusüberprüfung und Quelle des Status der Vertrauenswürdigkeit, aggregierte Daten zur Anzahl der vertrauenswürdigen, nicht vertrauenswürdigen und unbekannten Objekte.
Wenn Sie Kaspersky Security Cloud für Windows nutzen oder darauf wechseln, werden die folgenden Daten verarbeitet:
- Informationen über die Nutzung der Komponente Sicherer Zahlungsverkehr: Attribut ihres Betriebsmodus, Informationen über Änderungen der Liste der von der Komponente geschützten Websites durch den Benutzer: URL-Adresse und ggf. Referrer der Website, Attribut, das die Bearbeitung oder Löschung der Website kennzeichnet, Startmodus der Komponente für diese Website, Kontext der vorgenommenen Änderungen an der Liste der Websites; Informationen über den Browser, der zum Aufrufen der Website verwendet wurde: URL-Adresse und Referrer der Website, Name und Version des Browsers, Art des Browser-Starts, Startdauer und Attribut des erfolgreichen Starts, Informationen über die Schutzstufe und die Art der Nachricht über die Schutzstufe, Name und Version des Browsers, von dem aus der aktuell verwendete Browser gestartet wurde.
- Informationen über Updates von installierten Anwendungen: IDs der aktualisierten Anwendung und deren Updates, IDs der Lokalisierungssprache der Anwendung und ihrer Updates, Anwendungsversion vor dem Update, zum Herunterladen der Update-Setup-Datei verwendete URL-Adresse, ggfs. ID des Download-Fehlers der Setup-Datei, Attribut, das eine Verletzung der Integrität der Update-Setup-Datei anzeigt, ID der Benutzeraktion bei Verwendung der Liste der Ausnahmen, Art der Anwendung, die aktualisiert wird, Namen der Prozessdateien, welche die Installation des Updates verhindern, ID des Update-Ergebnisses, Parameter der Befehlszeile zum Starten der Setup-Datei des Updates, Attribut der erfolgreichen Update-Installation.
- Informationen über die Nutzung der Komponente Tool zum Entfernen unerwünschter oder überflüssiger Software: Datenbank-Version mit Informationen über installierte Anwendungen und deren Updates, Name und Version der untersuchten Anwendung, Registrierungsordner, der der betreffenden Anwendung zugeordnet ist, Ordner, in dem die Anwendung installiert wurde, Zeichenfolge mit dem Befehl zur Deinstallation der Anwendung, Lokalisierungssprache

der Anwendung, ID des Ergebnisses der Untersuchung der Anwendung, Attribut der Anwendungsinstallation nur für den aktuellen Benutzer, Attribut der Untersuchung der Anwendung im Debugging-Modus, ID der Benutzeraktion bei Verwendung der Liste mit den Ausnahmen, empfohlene Arten von Anwendungen zur Deinstallation und deinstallierte Anwendungen, Namen von Prozessdateien, die die Deinstallation verhindern, ID des Ergebnisses der Deinstallation, Attribut der erfolgreichen Deinstallation, Informationen über die Suite, zu der die erkannte Software gehört: ID, Version, Name, Entwickler, Sprachen-ID, Typ der Hauptanwendung der Suite, Quelle von Informationen über das Installationsdatum, Datum und Zeitpunkt der Installation und der letzten Nutzung der Hauptanwendung der Suite sowie Installationspfad und gewährleistetes Schutzniveau;
- Informationen über die Nutzung der Komponente zum Schutz vor Datensammlung (Private Browsing): Referrer der HTTP-Tracking-Anfrage, Name des Dienstes oder der Organisation, welche die Tracking-Dienste zur Verfügung stellt, Kategorie des Tracking-Dienstes nach der Klassifizierung des Rechteinhabers, ID und Version des Browsers, mit dem die URL geöffnet wurde.
- Informationen über die von den Komponenten Kindersicherung und Web-Kontrolle blockierten Links: Grund für die Blockierung, Version der Komponenten Kindersicherung und Web-Kontrolle, URL und IP-Adresse des blockierten Links.
- Informationen zur Nutzung der Komponente Modus für vertrauenswürdige Programme: ID der Version ihrer Einstellungen, Attribut ihres Betriebsmodus, Ergebnis der Dateistatusüberprüfung und Quelle des Status der Vertrauenswürdigkeit, aggregierte Daten zur Anzahl der vertrauenswürdigen, nicht vertrauenswürdigen und unbekannten Objekte.
Ihre Entscheidung zur Teilnahme
Sie können frei entscheiden, ob Sie im Rahmen dieser KSN-Erklärung regelmäßig Daten an den Rechteinhaber übermitteln. Sie können jederzeit Ihr Einverständnis widerrufen, indem Sie die Einstellungen der Software wie im Benutzerhandbuch beschrieben ändern.



ERKLÄRUNG ZU KASPERSKY SECURITY NETWORK („KSN-Erklärung")

Alle Begriffe, die in dieser KSN-Erklärung verwendet werden, haben dieselbe Bedeutung wie im Endbenutzer-Lizenzvertrag (EULA) unter dem Abschnitt „Definitionen".

Bitte lesen Sie die Bestimmungen dieser KSN-Erklärung und die dort erwähnten Dokumente sorgfältig durch, bevor Sie ihr zustimmen. Falls die Software in einem Unternehmen oder auf einem von mehreren Personen genutzten Computer ausgeführt wird, müssen Sie sicherstellen, dass diese Personen die Bedingungen der KSN-Erklärung verstanden und ihnen zugestimmt haben, bevor die Datenverarbeitung stattfindet.

Datenschutz und Datenverarbeitung
Der Rechteinhaber behandelt die Daten, die er vom Endbenutzer im Rahmen dieser KSN-Erklärung erhalten hat, gemäß der Datenschutzrichtlinie für Rechteinhaber. Diese Richtlinie kann eingesehen werden unter: www.kaspersky.com/Products-and-Services-Privacy-Policy.

Zwecke der Datenverarbeitung
Die Verwendung des KSN kann die Reaktionsgeschwindigkeit der Software auf Informationen sowie auf Gefährdungen der Netzwerksicherheit beschleunigen. Dies wird erreicht durch:
- Ermittlung der Reputation von WLAN-Netzwerken und Websites;
- Erhöhung der Leistungsfähigkeit von Softwarekomponenten;
- Leistungssteigerung für die Produkte des Rechteinhabers.

Verarbeitete Daten:
Bestimmte Daten, die im Rahmen dieser KSN-Erklärung verarbeitet werden, können entsprechend den Gesetzen einiger Länder als personenbezogene Daten eingestuft werden. Mit Ihrem Einverständnis werden im Rahmen dieser KSN-Erklärung regelmäßig die folgenden Daten automatisch an den Rechteinhaber geschickt:

- Informationen über die Software des Rechteinhabers: individuelle IDs der Softwareinstallation auf dem Computer; Typ, Version, Edition und Lokalisierung der installierten Software; Software-Betriebsmodus; Zustand der Software.

- Informationen über den Computer, auf dem die Software des Rechteinhabers installiert ist: individuelle IDs des

Computers, auf dem die Software installiert ist, Computertyp, Computername, Typ des Prozessors auf dem Computer, Verkäufer des Computers; Informationen über den geografischen Standort des Benutzercomputers.

- Informationen über den Typ, die Version und die Edition des auf dem Computer installierten Betriebssystems (OS) und der installierten Service Packs.

- Informationen über die Nutzung von Kaspersky Security Network durch die Software des Rechteinhabers: öffentliche IP-Adresse und Port, die für die Verbindung des Computers mit KSN verwendet werden, Anzahl der Verbindungsversuche, Kennzeichnung, ob die Verbindung erfolgreich war, Verbindungszeit; Protokoll zur Übermittlung der Statistiken; Gesamtanzahl der Anfragen mit zwischengespeicherten Antworten seit der vorherigen Generierung der Statistikmeldung; Anzahl der fehlgeschlagenen Anfragen an den Dienst seit der vorherigen Generierung der Statistikmeldung; Startzeit und Endzeit der Datensammlung für die aktuelle Statistikmeldung; Gesamtzahl der Anfragen an KSN seit der letzten Datenübermittlung; Informationen über fehlgeschlagene/erfolgreiche Anfragen an KSN, ID des Anfragetyps für die Anfrage an KSN, Dauer der Sitzung mit KSN, Volumen ausgehender und eingehender Daten, Start- und Endzeiten für die Datensammlung zur Übermittlung an KSN.

- Informationen über die aktuelle Verbindung des Computers mit dem drahtlosen Netzwerk: Name des drahtlosen Netzwerkes (SSID), Authentifizierungstyp des drahtlosen Netzwerkes, Prüfsummen (MD5 und SHA256) der MAC-Adresse des Zugangspunkts; individuelle IDs, generiert auf Basis der individuellen ID des Computers, der individuellen ID der Software-Installation auf dem Computer, dem Namen des drahtlosen Netzwerkes und der MAC-Adresse des Zugangspunkts; Kennzeichnung, die anzeigt, ob sich der Computer im Akkubetrieb befindet oder an ein Stromnetz angeschlossen ist, Ortszeit für den Beginn und das Ende der Verbindung des Computers mit dem drahtlosen Netzwerk, Einstellungen einer VPN-Sitzung für das drahtlose Netzwerk, Signalstärke des Netzwerks; URL (oder Teile davon) des Netzwerkdienstes, bei dem der Benutzer bestimmte Schritte für den Zugriff auf das Internet ausführen muss; Sicherheitsstufe des drahtlosen Netzwerks, Kategorie des drahtlosen Netzwerks, Kennzeichnung, die anzeigt, ob ein DNS-Name vorhanden ist. Informationen zu den DHCP-Einstellungen der Netzwerkverbindung: Prüfsumme (SHA256) der IP-Adresse (IPv4 und IPv6) der DNS-Server; Prüfsumme (SHA256) der lokalen IP-Adresse (IPv4 und IPv6), Prüfsumme (SHA256) der lokalen IP-Adresse (IPv4 und IPv6) des Gateways, Prüfsumme (SHA256) der Subnetzmaske und Netzwerkpräfixlänge.

- Informationen über drahtlose Netzwerke, die auf dem Computer verfügbar sind: Name des drahtlosen Netzwerks (SSID), Authentifizierungstyp des drahtlosen Netzwerks, vom drahtlosen Netzwerk verwendeter Verschlüsselungstyp, Prüfsummen (MD5 und SHA256) der MAC-Adresse des Zugangspunkts; individuelle IDs, generiert auf Grundlage der individuellen ID des Computers, der individuellen ID der Software-Installation auf dem Computer, des Namens des drahtlosen Netzwerks und der MAC-Adresse des Zugangspunkts; Signalstärke des Netzwerks.

- Informationen zur Verwendung der VPN-Funktionalität (Virtual Private Network) mit der Software des Rechteinhabers: Dauer der VPN-Sitzung, geografischer Standort des VPN-Servers, Volumen des eingehenden und ausgehenden Datenverkehrs, ID des Startvorgangs der VPN-Sitzung und Starttyp, ID der Aktion des Benutzers beim Start der VPN-Sitzung, Typ des Ereignisses, das die VPN-Sitzung beendet hat.

- Informationen über die Interaktion zwischen der Anwendung und My Kaspersky: ID und Domänenname des Dienstes, an den die Anfrage gesendet wird, Anzahl der Anfragen und erfolgreichen/fehlgeschlagenen Verbindungen zu jedem Dienst, Anzahl der Antworten von jedem Dienst, Anzahl und Arten von Anfragefehlern, Startzeit und Endzeit der Sammlung von Daten über die Anzahl der Anforderungen und Verbindungen.

- Informationen zur Qualität der Aufgaben zum Update installierter Software: IP-Adresse (IPv4 oder IPv6) der verwendeten Update-Quelle, Typ der Update-Aufgabe, Liste der aktualisierten Anwendungskomponenten; Anzahl und Gesamtgröße der während des Updates heruntergeladenen Dateien; durchschnittliche Download-Geschwindigkeit der Update-Dateien, durchschnittliche Geschwindigkeit von Netzwerkoperationen während des Updates, Status der Fertigstellung der Update-Aufgabe; Typ und Code des Fehlers während der Update-Aufgabe; ID und Version der aktualisierten Anwendungskomponente.

Ihre Entscheidung zur Teilnahme
Sie können frei entscheiden, ob Sie im Rahmen dieser KSN-Erklärung regelmäßig Daten an den Rechteinhaber

übermitteln. Sie können jederzeit Ihr Einverständnis widerrufen, indem Sie die Einstellungen der Software wie im Benutzerhandbuch beschrieben ändern.