Apple Datenschutz - Sicherheitsüberblick – iCloud-Daten

Link zum Original Artikel: https://support.apple.com/de-de/102651

Sicherheitsüberblick – iCloud-Daten
iCloud nutzt starke Sicherheitsmethoden, wendet strikte Richtlinien zum Schutz deiner Daten an und ist branchenweit führend beim Einsatz von Sicherheitstechnologien, die die Privatsphäre schützen, wie z. B. der Ende-zu-Ende-Verschlüsselung deiner Daten.

Datensicherheit und Verschlüsselung in iCloud
Die Sicherheit deiner Daten in iCloud beginnt mit der Sicherheit deiner Apple-ID. Alle neuen Apple-IDs erfordern die Zwei-Faktor-Authentifizierung, um dich vor betrügerischen Versuchen zu schützen, Zugriff auf deinen Account zu erhalten. Die Zwei-Faktor-Authentifizierung ist auch für viele Funktionen im gesamten Apple-Ökosystem erforderlich, einschließlich der Ende-zu-Ende-Verschlüsselung.

Apple bietet zwei Optionen zum Verschlüsseln und Schützen der in iCloud gespeicherten Daten an:

Der standardmäßige Datenschutz ist die Standardeinstellung für deinen Account. Deine iCloud-Daten sind verschlüsselt, die Verschlüsselungsschlüssel sind in Apple-Rechenzentren gesichert, sodass wir dich bei der Datenwiederherstellung unterstützen können, und nur bestimmte Daten sind Ende-zu-Ende verschlüsselt.

Der erweiterte Datenschutz für iCloud ist eine optionale Einstellung, die das höchste Maß an Datensicherheit in der Cloud bietet. Wenn du den erweiterten Datenschutz aktivierst, behalten deine vertrauenswürdigen Geräte den alleinigen Zugriff auf die Verschlüsselungsschlüssel für den Großteil deiner iCloud-Daten. Auf diese Weise sind sie durch die Ende-zu-Ende-Verschlüsselung geschützt. Zu den zusätzlich geschützten Daten zählen iCloud-Backups, Fotos, Notizen und mehr.

Über Ende-zu-Ende verschlüsselte Daten

Ende-zu-Ende verschlüsselte Daten können nur auf vertrauenswürdigen Geräten entschlüsselt werden, auf denen du mit deiner Apple-ID angemeldet bist. Keine andere Person kann auf deine Ende-zu-Ende verschlüsselten Daten zugreifen – nicht einmal Apple –, und diese Daten bleiben selbst im Falle eines Datenmissbrauchs in der Cloud sicher. Wenn du den Zugriff auf deinen Account verlierst, kannst nur du diese Daten mithilfe deines Gerätecodes oder Passworts, Wiederherstellungskontakts oder Wiederherstellungsschlüssels wiederherstellen.

Standardmäßiger Datenschutz
Der standardmäßige Datenschutz ist die Standardeinstellung für deinen Account. Deine iCloud-Daten werden bei Übertragungen verschlüsselt und am Ablageort in einem verschlüsselten Format gespeichert. Die Verschlüsselungsschlüssel deiner vertrauenswürdigen Geräte sind in Apple-Rechenzentren gesichert, sodass Apple deine Daten bei Bedarf jederzeit in deinem Namen entschlüsseln kann, z. B. wenn du dich auf einem neuen Gerät anmeldest, ein Backup wiederherstellst oder deine Daten wiederherstellen möchtest, nachdem du dein Passwort vergessen hast. Solange du dich mit deiner Apple-ID erfolgreich anmelden kannst, hast du Zugriff auf deine Backups, Fotos, Dokumente, Notizen und mehr.

Für zusätzlichen Datenschutz und zusätzliche Sicherheit sind 15 Datenkategorien – einschließlich Gesundheitsdaten und Passwörter im iCloud-Schlüsselbund – durch die Ende-zu-Ende-Verschlüsselung geschützt. Apple verfügt nicht über die Verschlüsselungsschlüssel für diese Kategorien, und wir können dich nicht bei der Wiederherstellung dieser Daten unterstützen, wenn du den Zugriff auf deinen Account verlierst. Die folgende Tabelle enthält eine Liste der Datenkategorien, die immer durch Ende-zu-Ende-Verschlüsselung geschützt sind.

Erweiterter Datenschutz für iCloud
Ab iOS 16.2, iPadOS 16.2 und macOS 13.1 kannst du den erweiterten Datenschutz aktivieren, um den größten Teil deiner iCloud-Daten zu schützen, selbst im Falle eines Datenmissbrauchs in der Cloud.

Mit dem erweiterten Datenschutz steigt die Anzahl der Datenkategorien mit Ende-zu-Ende-Verschlüsselung auf 25 an und umfasst auch iCloud-Backup, Fotos, Notizen und mehr. In der folgenden Tabelle sind die zusätzlichen Datenkategorien aufgeführt, die durch Ende-zu-Ende-Verschlüsselung geschützt sind, wenn du den erweiterten Datenschutz aktivierst.

Wenn du den erweiterten Datenschutz aktivierst und anschließend den Zugriff auf deinen Account verlierst, verfügt Apple nicht über die Verschlüsselungsschlüssel und kann dich bei der Wiederherstellung nicht unterstützen – in diesem Fall benötigst du deinen Gerätecode oder dein Passwort, einen Wiederherstellungskontakt oder einen persönlichen Wiederherstellungsschlüssel. Da der Großteil deiner iCloud-Daten durch die Ende-zu-Ende-Verschlüsselung geschützt ist, wirst du angeleitet, mindestens einen Wiederherstellungskontakt oder Wiederherstellungsschlüssel einzurichten, bevor du den erweiterten Datenschutz aktivierst. Du musst auch alle deine Apple-Geräte auf eine Softwareversion aktualisieren, die diese Funktion unterstützt.

Du kannst den erweiterten Datenschutz jederzeit deaktivieren. Dein Gerät lädt die erforderlichen Verschlüsselungsschlüssel sicher auf die Apple-Server hoch, und dein Account verwendet daraufhin wieder den standardmäßigen Datenschutz.

Hier erfährst du, wie du den erweiterten Datenschutz für iCloud aktivierst.

Datenkategorien und Verschlüsselung
Die folgende Tabelle enthält weitere Informationen dazu, wie iCloud deine Daten schützt, wenn du den standardmäßigen oder den erweiterten Datenschutz verwendest.

Datenkategorie

Standardmäßiger Datenschutz

Erweiterter Datenschutz

Verschlüsselung

Speicherung von Schlüsseln

Verschlüsselung

Speicherung von Schlüsseln

iCloud Mail (1)

Bei der Übertragung und auf dem Server

Apple

Bei der Übertragung und auf dem Server

Apple

Kontakte (2)

Bei der Übertragung und auf dem Server

Apple

Bei der Übertragung und auf dem Server

Apple

Kalender (2)

Bei der Übertragung und auf dem Server

Apple

Bei der Übertragung und auf dem Server

Apple

iCloud-Backup (umfasst Geräte- und Nachrichten-Backup) (3)

Bei der Übertragung und auf dem Server

Apple

Ende-zu-Ende

Vertrauenswürdige Geräte

iCloud Drive (4)

Bei der Übertragung und auf dem Server

Apple

Ende-zu-Ende

Vertrauenswürdige Geräte

Photos

Bei der Übertragung und auf dem Server

Apple

Ende-zu-Ende

Vertrauenswürdige Geräte

Notizen

Bei der Übertragung und auf dem Server

Apple

Ende-zu-Ende

Vertrauenswürdige Geräte

Erinnerungen (5)

Bei der Übertragung und auf dem Server

Apple

Ende-zu-Ende

Vertrauenswürdige Geräte

Safari-Lesezeichen

Bei der Übertragung und auf dem Server

Apple

Ende-zu-Ende

Vertrauenswürdige Geräte

Siri-Kurzbefehle

Bei der Übertragung und auf dem Server

Apple

Ende-zu-Ende

Vertrauenswürdige Geräte

Sprachmemos

Bei der Übertragung und auf dem Server

Apple

Ende-zu-Ende

Vertrauenswürdige Geräte

Wallet-Karten

Bei der Übertragung und auf dem Server

Apple

Ende-zu-Ende

Vertrauenswürdige Geräte

Freeform

Bei der Übertragung und auf dem Server

Apple

Ende-zu-Ende

Vertrauenswürdige Geräte

Passwörter und Schlüsselbund (6)

Ende-zu-Ende

Vertrauenswürdige Geräte

Ende-zu-Ende

Vertrauenswürdige Geräte

Gesundheitsdaten

Ende-zu-Ende

Vertrauenswürdige Geräte

Ende-zu-Ende

Vertrauenswürdige Geräte

Journaldaten

Ende-zu-Ende

Vertrauenswürdige Geräte

Ende-zu-Ende

Vertrauenswürdige Geräte

Hausdaten

Ende-zu-Ende

Vertrauenswürdige Geräte

Ende-zu-Ende

Vertrauenswürdige Geräte

Nachrichten in iCloud (7)

Ende-zu-Ende (7a)

Vertrauenswürdige Geräte

Ende-zu-Ende

Vertrauenswürdige Geräte

Zahlungsdaten

Ende-zu-Ende

Vertrauenswürdige Geräte

Ende-zu-Ende

Vertrauenswürdige Geräte

Apple Card-Transaktionen

Ende-zu-Ende

Vertrauenswürdige Geräte

Ende-zu-Ende

Vertrauenswürdige Geräte

Karten (8)

Ende-zu-Ende

Vertrauenswürdige Geräte

Ende-zu-Ende

Vertrauenswürdige Geräte

Von der QuickType-Tastatur gelernte Wörter

Ende-zu-Ende

Vertrauenswürdige Geräte

Ende-zu-Ende

Vertrauenswürdige Geräte

Safari (9)

Ende-zu-Ende

Vertrauenswürdige Geräte

Ende-zu-Ende

Vertrauenswürdige Geräte

Screen Time

Ende-zu-Ende

Vertrauenswürdige Geräte

Ende-zu-Ende

Vertrauenswürdige Geräte

Siri-Daten (10)

Ende-zu-Ende

Vertrauenswürdige Geräte

Ende-zu-Ende

Vertrauenswürdige Geräte

WLAN-Passwörter

Ende-zu-Ende

Vertrauenswürdige Geräte

Ende-zu-Ende

Vertrauenswürdige Geräte

W1- und H1-Bluetooth-Tasten

Ende-zu-Ende

Vertrauenswürdige Geräte

Ende-zu-Ende

Vertrauenswürdige Geräte

Memoji

Ende-zu-Ende

Vertrauenswürdige Geräte

Ende-zu-Ende

Vertrauenswürdige Geräte

Weitere Hinweise
iCloud Mail: iCloud Mail verwendet keine Ende-zu-Ende-Verschlüsselung, da das Programm mit dem globalen E-Mail-System zusammenarbeiten muss. Alle nativen Apple-E-Mail-Clients unterstützen die optionale S/MIME-Verfahren für das Verschlüsseln von Nachrichten.

Kontakte und Kalender: Kontakte und Kalender basieren auf Industriestandards (CalDAV und CardDAV), die keine integrierte Unterstützung für die Ende-zu-Ende-Verschlüsselung anbieten.

iCloud-Backup (umfasst Geräte- und Nachrichten-Backup)

Standardmäßiger Datenschutz: Wenn iCloud-Backup aktiviert ist, werden die Schlüssel zu deinen Backups in den Apple-Datenzentren gesichert. Wenn du sowohl iCloud-Backup als auch Nachrichten in iCloud verwendest, enthält dein Backup eine Kopie des Verschlüsselungsschlüssels von „Nachrichten in iCloud“, damit du deine Daten wiederherstellen kannst.

Erweiterter Datenschutz: iCloud-Backup und alles, was sich darin befindet, ist Ende-zu-Ende verschlüsselt, einschließlich des Verschlüsselungsschlüssels für „Nachrichten in iCloud“.

iCloud Drive: Umfasst Pages-, Keynote- und Numbers-Dokumente, PDFs, Safari-Downloads und alle anderen Dateien, die manuell oder automatisch in iCloud Drive gespeichert werden.

Erinnerungen: Erinnerungen, die mithilfe von CalDAV synchronisiert werden, unterstützen die Ende-zu-Ende-Verschlüsselung nicht.

Passwörter und Schlüsselbund: Umfasst deine gespeicherten Konten und Passwörter.

Nachrichten in iCloud

Standardmäßiger Datenschutz: Nachrichten in iCloud ist Ende-zu-Ende verschlüsselt, wenn iCloud-Backup deaktiviert ist. Wenn iCloud-Backup aktiviert ist, enthält dein Backup eine Kopie des Verschlüsselungsschlüssels von „Nachrichten in iCloud“, damit du deine Daten wiederherstellen kannst. Wenn du iCloud-Backup deaktivierst, wird auf deinem Gerät ein neuer Schlüssel generiert, um künftige Nachrichten in iCloud zu schützen. Dieser Schlüssel ist zwischen deinen Geräten Ende-zu-Ende verschlüsselt und wird nicht von Apple gespeichert

Erweiterter Datenschutz: Nachrichten in iCloud ist immer Ende-zu-Ende verschlüsselt. Wenn iCloud-Backup aktiviert ist, ist alles, was sich darin befindet, Ende-zu-Ende verschlüsselt, einschließlich des Verschlüsselungsschlüssels für „Nachrichten in iCloud“.

Karten: Umfasst Favoriten, „Meine Reiseführer“ und den Suchverlauf.

Safari: Einschließlich Verlauf, Tabgruppen und iCloud-Tabs.

Siri-Daten: Umfasst Siri-Einstellungen und Personalisierung, und, falls du „Hey Siri“ eingerichtet hast, eine geringe Anzahl an Beispielen deiner Anfragen.

Verschlüsselung bestimmter Metadaten und Nutzungsinformationen
Einige in iCloud gespeicherte Metadaten und Nutzungsinformationen unterliegen weiterhin dem standardmäßigen Datenschutz, selbst wenn der erweiterter Datenschutz aktiviert ist. Beispielsweise werden Datum und Uhrzeit von Änderungen an einer Datei oder einem Objekt zum Sortieren deiner Daten verwendet und Prüfsummen von Datei- und Fotodaten werden genutzt, um Apple beim Entfernen von Duplikaten und Optimieren deiner iCloud und des Gerätespeichers zu unterstützen – dies erfolgt ganz ohne Zugriff auf die Dateien und Fotos. Repräsentative Beispiele sind in der folgenden Tabelle aufgeführt.

Diese Metadaten werden immer verschlüsselt, aber die Verschlüsselungsschlüssel werden weiterhin von Apple gespeichert. Während wir die Sicherheitsmaßnahmen für alle Benutzer weiter verstärken, verpflichtet sich Apple dazu, mehr Daten, einschließlich dieser Art von Metadaten, Ende-zu-Ende zu verschlüsseln, auch wenn die erweiterte Datensicherheit aktiviert ist.

Datenkategorie

Mit standardmäßiger Datenverschlüsselung geschützte Informationen

iCloud-Backup

Name, Modell, Farbe und Seriennummer des Geräts, das mit den einzelnen Backups verknüpft ist

Liste der Apps und Dateiformate, die im Backup enthalten sind

Datum, Uhrzeit und Größe der einzelnen Backup-Schnappschüsse

iCloud Drive

Die unformatierten Byte-Prüfsummen des Dateiinhalts und des Dateinamens

Dateityp, Zeitpunkt der Erstellung, der letzten Änderung und der letzten Öffnung

Ob die Datei als Favorit markiert wurde

Dateigröße

Signatur von App-Installationsprogrammen (.pkg-Signatur) und Bundle-Signatur

Ob es sich bei einer synchronisierten Datei um eine ausführbare Datei handelt

Fotos

Die unformatierte Byte-Prüfsumme des Fotos oder Videos

Ob ein Element als Favorit markiert, ausgeblendet oder als gelöscht markiert wurde

Zeitpunkt, an dem ein Objekt ursprünglich auf dem Gerät erstellt wurde

Zeitpunkt, an dem ein Objekt ursprünglich importiert und geändert wurde

Wie oft ein Objekt angezeigt wurde

Notizen

Datum und Uhrzeit, zu der eine Notiz erstellt, zuletzt geändert oder zuletzt angezeigt wurde

Ob eine Notiz angeheftet oder als gelöscht markiert wurde

Ob eine Notiz eine Zeichnung oder Handschrift enthält

Die unformatierte Byte-Prüfsumme des Inhalts einer importierten oder migrierten Notiz

Safari-Lesezeichen

Ob sich ein Lesezeichen im Ordner „Favoriten“ befindet

Zeitpunkt der letzten Änderung eines Lesezeichens

Ob ein Lesezeichen als gelöscht markiert wurde

Nachrichten in iCloud

Wann die letzte Synchronisierung abgeschlossen wurde und ob die Synchronisierung deaktiviert wurde

Datum der letzten Änderung von Inhalten

Fehlercodes

Nachrichtentyp, z. B. eine normale iMessage, SMS oder Tapback

Freigabe und Zusammenarbeit
Wenn der standardmäßige Datenschutz aktiv ist, sind iCloud-Inhalte, die du mit anderen Personen teilst, nicht Ende-zu-Ende verschlüsselt.

Der erweiterte Datenschutz wurde entwickelt, um die Ende-zu-Ende-Verschlüsselung für freigegebene Inhalte beizubehalten, solange bei allen Teilnehmer der erweiterte Datenschutz aktiviert ist. Diese Schutzstufe wird von den meisten iCloud-Freigabefunktionen unterstützt, einschließlich der freigegebenen iCloud-Fotomediathek, freigegebenen Ordnern in iCloud Drive und freigegebenen Notizen.

Die iWork-Zusammenarbeit, die Funktion „Geteilte Alben“ in der Fotos-App und das Freigeben von Inhalten mit der Option „Jeder mit dem Link“ unterstützen den erweiterten Datenschutz nicht. Wenn du diese Funktionen verwendest, werden die Verschlüsselungsschlüssel für die freigegebenen Inhalte sicher in die Apple-Rechenzentren hochgeladen, sodass iCloud die Zusammenarbeit in Echtzeit und die Webfreigabe erleichtern kann. Das bedeutet, dass die freigegebenen Inhalte nicht Ende-zu-Ende verschlüsselt sind, selbst wenn der erweiterter Datenschutz aktiviert ist.

Um die Freigabe oder Zusammenarbeit einzuleiten, werden die Namen und Apple-IDs der Teilnehmer an die Apple-Server gesendet, und der Titel und eine repräsentative Miniaturansicht des freigegebenen Objekts werden verwendet, sodass die Teilnehmer eine Vorschau anzeigen können.

iCloud.com und Datenzugriff im Internet
iCloud.com bietet Zugriff auf deine iCloud-Daten über einen beliebigen Webbrowser. Alle Sitzungen unter iCloud.com werden bei der Übertragung zwischen den Apple-Servern und dem Browser auf deinem Gerät verschlüsselt. Wenn der erweiterter Datenschutz aktiviert ist, ist der Zugriff auf deine Daten über iCloud.com standardmäßig deaktiviert. Du hast die Möglichkeit, den Datenzugriff unter iCloud.com zu aktivieren. Dadurch können der von dir verwendete Webbrowser und Apple vorübergehend auf datenspezifische Verschlüsselungsschlüssel zugreifen, die von deinem Gerät bereitgestellt werden, um deine Daten zu entschlüsseln und anzuzeigen. Hier erfährst du mehr über den Webzugriff über iCloud.com.

Daten von Drittanbieter-Apps
In iCloud gespeicherte Daten von Drittanbieter-Apps werden immer verschlüsselt – sowohl bei der Übertragung als auch auf dem Server. Wenn du den erweiterten Datenschutz aktivierst, werden Daten von Drittanbieter-Apps, die in verschlüsselten Feldern und Assets in iCloud-Backup und CloudKit gespeichert sind, Ende-zu-Ende verschlüsselt.

Informationen zu Rechenzentren von Drittanbietern
Zur Speicherung und Verarbeitung deiner Daten können Rechenzentren sowohl von Apple als auch von Drittanbietern genutzt werden. Bei der Verarbeitung von Daten, die in einem Rechenzentrum eines Drittanbieters gespeichert sind, hat nur die Apple-Software, die auf sicheren Servern läuft, Zugriff auf die Verschlüsselungsschlüssel, und das auch nur bei der Durchführung der erforderlichen Verarbeitung. Die Schlüssel werden immer in Apple-Rechenzentren gespeichert und gesichert. Apple greift nicht auf Ende-zu-Ende verschlüsselte Daten zu und speichert diese auch nicht.

Informationen zu nicht von Apple hergestellten Produkten oder nicht von Apple kontrollierten oder geprüften unabhängigen Websites stellen keine Empfehlung oder Billigung dar. Apple übernimmt keine Verantwortung für die Auswahl, Leistung oder Nutzung von Websites und Produkten Dritter. Apple gibt keine Zusicherungen bezüglich der Genauigkeit oder Zuverlässigkeit der Websites Dritter ab. Kontaktiere den Anbieter, um zusätzliche Informationen zu erhalten.

Veröffentlichungsdatum: 18. Dezember 2023