

Leistungsbeschreibung für das Sicher Shoppen Paket (LB Sicher Shoppen Paket)

Diese Leistungsbeschreibung gilt ab 31. Juli 2026. Eine Neubestellung ist ab 31. Juli 2026 nicht mehr möglich.

A1 Telekom Austria (A1) erbringt im Rahmen Ihrer technischen und betrieblichen Möglichkeiten das Paket „Sicher Shoppen“ nach den Allgemeinen Geschäftsbedingungen von A1 für Kommunikationslösungen (AGB Komm) in der jeweils gültigen Fassung. Sofern A1 bei der Leistungserbringung die personenbezogenen Daten des Kunden verarbeiten, gelten die Allgemeinen Geschäftsbedingungen für die Auftragsverarbeitung. Die Dokumente finden sich unter www.A1.net/agb oder auf Wunsch bei A1.

1. Allgemeine Bestimmungen

Dies ist eine rechtliche Vereinbarung zwischen dem Kunden als Lizenznehmer und A1 als Lizenzgeber. Sicher Shoppen besteht aus den Bestandteilen A1 Identitätsschutz, A1 Passwortschutz und A1 Netzwerkschutz.

Das Sicher Shoppen Paket wird in Zusammenarbeit mit den Subunternehmen Eyeonid Group AB („EyeonID“) und F-Secure Corporation („F-Secure“) angeboten und enthält:

- **A1 Identitätsschutz**

- Das Produkt A1 Identitätsschutz dient dazu festzustellen, ob Daten des Kunden unerlaubt im Internet veröffentlicht wurden. A1 Identitätsschutz identifiziert, sammelt und bewertet ständig riesige Datenmengen aus allen Ecken des Internets, inklusive Deep Web und Darknet. Die Daten werden sowohl automatisch als auch manuell gesammelt und analysiert. So kann schnell festgestellt werden, ob Benutzerinformationen unerlaubt veröffentlicht wurden.
- Die Verwaltung des Produktes A1 Identitätsschutz erfolgt durch den Kunden über den Mein A1-Bereich (App/ Web) wo der Kunde auf das A1 Identitätsschutz-Dashboard weitergeleitet wird.
- Um die Überwachung zu starten, gibt der Kunde seine E-Mail Adresse(n) und/oder seine Mobilrufnummer(n) im A1 Identitätsschutz-Dashboard bekannt. Der Kunde hat die Möglichkeit insgesamt bis zu fünf (5) Datensätze, nämlich E-Mail Adresse(n) und/oder Mobilrufnummer(n), überprüfen zu lassen. Die E-Mail-Adresse oder Mobilrufnummer dient hierbei als Identifikator für die damit zusammenhängenden, veröffentlichten Daten des Kunden. Die Identitätsschutzüberprüfung bezieht sich nur auf die vom Kunden bekannt gegebene E-Mail Adresse(n) und/oder Mobilrufnummer(n).
- Die Überprüfung einer neu zu überwachenden E-Mail-Adresse oder Mobilrufnummer kann einige Minuten in Anspruch nehmen, bevor das Resultat angezeigt wird.
- Auf Basis der vom Kunden angegebenen Identifikatoren (E-Mail-Adresse(n) und Mobilrufnummer(n)) werden persönliche Daten, welche in Kombination mit der E-Mail-Adresse oder Mobilrufnummer gefunden werden, identifiziert und dem Kunden im A1 Identitätsschutz Dashboard angezeigt.
- Folgende Datensätze werden über die E-Mail Adresse oder Mobilrufnummer aufgeteilt in 3 verschiedenen Kategorien überwacht:
 - **Zugangsdaten:** E-Mail Adresse, Passwort, Username und IP-Adresse
 - **Personenbezogene Daten:** Nachname, Vorname, Adresse, Land, Geschlecht, Alter, Stadt, Staat, Geburtsdatum, Sozialversicherungsnummer, Reisepassnummer, Personalausweisnummer und Führerscheinnummer

- **Zahlungsdaten:** Kreditkartennummer, Debitkartennummer und Rechnungsadresse
 - Wird ein Datendiebstahl erkannt, so wird der Kunde wahlweise mittels E-Mail und/oder SMS benachrichtigt. Die Einstellungen hierzu können über das A1 Identitätsschutz Dashboard, welches via Mein A1 erreichbar ist, gewählt werden.
 - Wird ein Datendiebstahl identifiziert, werden dem Kunden am A1 Identitätsschutz Dashboard neben Details zur Quelle des Datendiebstahls auch Handlungsempfehlungen angezeigt, die er setzen sollte, um die Sicherheit seiner persönlichen Daten wiederherzustellen und das Risiko von Datendiebstahl in Zukunft zu minimieren.
- **A1 Passwortschutz**
 - Der A1 Passwortschutz ist ein Passwortmanager, der dazu dient, sichere Passwörter zu erstellen und zu speichern. A1 Passwortschutz erstellt Passwörter mit bis zu 31 Stellen aus zufälligen Kombinationen von Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen. Dem Kunden steht es auch frei selbst generierte Passwörter im Passworttresor zu speichern. Die Passwörter werden verschlüsselt im Passworttresor abgespeichert und können nur mit einem Masterpasswort, welches bei der ersten Nutzung erstellt wird, eingesehen werden. Dieses Masterpasswort wird verschlüsselt gespeichert und kann weder vom Subunternehmen F-Secure, noch von A1 eingesehen werden.
 - **Hinweis:** Das Masterpasswort kann nicht zurückgesetzt werden. Es wird deshalb empfohlen einen Wiederherstellungs-QR-Code bei der Erstnutzung des A1 Passwortschutz zu erstellen. Mit diesem kann im Falle des Vergessens des Masterpasswortes ein Neues angefordert werden. Dem Kunden steht es bei mobilen Endgeräten frei, ob er einen Zugriff mittels biometrischer Authentifizierung (FaceID oder Fingerabdruck – je nach Device) zulassen möchte.
 - Neben dem Erstellen und sicheren Speichern von Passwörtern bietet A1 Passwortschutz außerdem noch Informationen zur Stärke des eingegebenen Passwortes.
 - Die Verwaltung des Produktes A1 Passwortschutz erfolgt durch den Kunden über die A1 Sicherheit App. Diese kann sowohl auf mobilen Endgeräten (iOS & Android), als auch auf PCs/Laptops (Mac & Windows) installiert werden.
 - Der Kunde hat die Möglichkeit den A1 Passwortschutz über die A1 Sicherheit App auf insgesamt bis zu 5 Endgeräten zu nutzen.

A1 Netzwerkschutz

- Das Produkt A1 Netzwerkschutz ist ein Datenschutz-VPN zum anonymen und verschlüsselten Surfen im Internet. A1 Netzwerkschutz codiert nach Aktivierung am jeweiligen Gerät den darüber laufenden Datenverkehr im Internet durch Kapselung und Verschlüsselung der einzelnen Datenpakete. Dadurch kann der Datenverkehr durch keine Dritten ausgelesen werden. Darüber hinaus ändert A1 Netzwerkschutz nach Aktivierung die IP-Adresse des Kunden, sodass der Standort des Kunden nicht festgestellt werden kann.
- A1 Netzwerkschutz schützt den Datenverkehr nur nach Aktivierung in der A1 Sicherheit App. Das Datenschutz-VPN schützt ab diesem Moment auch nur das Gerät, auf dem die Nutzung über die A1 Sicherheit App aktiviert wurde.
- Neben dem Verschlüsseln des Datenverkehrs und dem Verändern der IP-Adresse enthält A1 Netzwerkschutz zusätzlich einen Schutz vor Tracking Cookies. Tracking Cookies sammeln beim Surfen auf eine Webseite Kundeninformationen wie Surfverhalten oder IP-Adresse und werden oft dazu verwendet personalisierte Werbung zu schalten.

- Darüber hinaus enthält A1 Netzwerkschutz einen Schutz vor unsicheren und gefährlichen Webseiten. Wird eine gefährliche Seite angesurft, erhält der Kunde einen Warnhinweis.
- A1 Netzwerkschutz bietet keine Möglichkeit einen virtuellen Standort außerhalb von Österreich einzustellen. Bei Aktivierung wird automatisch der virtuelle Standort auf eine IP-Adresse in Österreich eingestellt. Die Umgehung von Geosperren ist unzulässig.
- A1 Netzwerkschutz kann wie A1 Passwortschutz über die A1 Sicherheit App, welche sowohl auf mobilen Endgeräten (iOS & Android), als auch auf PCs/Laptops (Mac & Windows) genutzt werden kann, verwendet werden.
- Der Kunde hat die Möglichkeit den A1 Netzwerkschutz über die A1 Sicherheit App auf insgesamt bis zu 5 Endgeräten zu nutzen.

2. Technische Voraussetzungen

Um das Sicher Shoppen Paket nutzen zu können, benötigt der Kunde eine aufrechte Internetverbindung. Ein A1 Internet-, Mobilfunk-, oder Cube Internet-Vertrag ist keine Voraussetzung für die Nutzung des Paketes. Außerdem benötigt der Kunde ein Endgerät mit den Betriebssystemen iOS, Android, MacOS oder Windows & einer aktuellen Software-Version, um die A1 Sicherheit App installieren zu können. Die genauen technischen Voraussetzungen in Bezug auf Systemanforderungen können auf [A1.net/sicher-shoppen](https://a1.net/sicher-shoppen) eingesehen werden.

Für die Bedienung & Administration des A1 Identitätsschutz Dashboard benötigt der Kunde außerdem einen Webbrowser.

3. Sonstige Voraussetzungen

Voraussetzung für die Nutzung des Sicher Shoppen Paketes ist ein Wohnsitz in Österreich, die Volljährigkeit des Kunden und eine aufrechte Internetverbindung, unabhängig vom Anbieter. Außerdem ist der Download der A1 Sicherheit App und das Befüllen des A1 Identitätsschutz Dashboard erforderlich. Für die Nutzung von Sicher Shoppen können abhängig vom gewählten Tarif zusätzliche Kosten für die Datenverbindung anfallen. Diese notwendige Datenverbindung ist nicht im monatlichen Entgelt inkludiert.

4. Nutzungsrechte

Auf Grundlage dieser Leistungsbeschreibung wird dem Kunden ein nicht ausschließliches Recht zur Nutzung des Sicher Shoppen Paketes während aufrechter Vertragsbeziehung eingeräumt.

5. Änderung oder Beendigung von Funktionen sowie dieser Leistungsbeschreibung

Modifikation des Paketes Sicher Shoppen

Die Funktionen des Paketes „Sicher Shoppen“ entwickeln sich fort und können sich daher inhaltlich, technisch, optisch oder in sonstiger Weise verändern. Auch während eines aufrechten Vertrages ist A1 berechtigt die angebotenen Leistungsspezifikationen zu ändern. A1 ist berechtigt einzelne oder mehrere Funktionen zu erweitern, zu ändern oder zu entfernen. Sollten dadurch Anpassungsmaßnahmen in der Betriebsumgebung notwendig werden, so sind diese auf eigene Kosten vom Kunden zu tragen. Funktionen können zeitweilig oder auf Dauer aus sicherheitsrelevanten, technischen, wirtschaftlichen, rechtlichen oder regulatorischen Gründen abgeschaltet werden. A1 ist berechtigt, diese Leistungsbeschreibung unter Einhaltung einer

angemessenen Frist zu ändern, über diese Änderung wird der Kunde in geeigneter Art und Weise verständigt. Sofern die Änderung nicht ausschließlich begünstigend ist, kann der Kunde das Sicher Shoppen Paket mit sofortiger Wirkung kündigen, ohne dass dies mit zusätzlichen Kosten verbunden wäre. Weitere Rechte können daraus jedoch nicht abgeleitet werden.

Beendigung der Vereinbarung

Das Paket „Sicher Shoppen“ kann unter Einhaltung einer 1-monatigen Kündigungsfrist beendet werden.

Sollte eine Mindestvertragsdauer vereinbart werden, so kann der Kunde den Vertrag erst mit Ablauf dieser unter Einhaltung einer 1-monatigen Kündigungsfrist ordentlich kündigen.

6. Verfügbarkeit

Die Verfügbarkeit des Sicher Shoppen Paketes beträgt im Jahresmittel 95%. Ausgenommen sind davon jene Zeiten, in denen das Service aus technischen oder sonstigen Gründen, die nicht im Einflussbereich von A1 liegen (höhere Gewalt, Verschulden Dritter etc.), nicht verfügbar ist. Zeiten geplanter oder notwendiger Wartungsarbeiten, die zu Ausfallzeiten führen und vorher als Wartungsfenster kommuniziert wurden, gelten nicht als Beeinträchtigung der Verfügbarkeit. A1 ist jederzeit nach entsprechender Vorankündigung berechtigt, Wartungsfenster im erforderlichen Ausmaß durchzuführen. Werden Dienstleistungen ohne gesondertes Entgelt bereitgestellt, so ist A1 berechtigt, diese fristlos und ohne Vorankündigung wiedereinzustellen. Dadurch kann kein Minderungs-, Erstattungs- oder Schadensersatzanspruch begründet werden. Im Falle einer grundlegenden Änderung der rechtlichen oder technischen Standards im Internet ist A1 berechtigt, das Paket „Sicher Shoppen“ nach vorheriger schriftlicher Ankündigung einzustellen.

7. Entstörung

Anfragen und Anliegen von Kunden nimmt A1 Mo-Fr von 07:00 bis 22:00 Uhr (Feiertage ausgenommen) telefonisch über die A1 Serviceline (0800 664 100) entgegen. Diese Service Anfragen sind kostenlos.

A1 ist bemüht die Dienstleistung so schnell wie möglich wieder fehlerfrei zur Verfügung zu stellen, falls es aufgrund von Reparatur, Wartung oder Verbesserungsmaßnahmen zu Unterbrechungen kommt.

8. Entstörungsfrist

Störungsmeldungen, die bei A1 eingehen und die technische Funktion des Produktes betreffen, werden innerhalb einer angemessenen Frist behoben.

9. Pflichten des Kunden

Diese Vereinbarung gewährt dem Kunden das persönliche, nicht exklusive und nicht übertragbare Recht (Werknutzungsbewilligung), das Paket für persönliche Zwecke zu nutzen. Alle darüberhinausgehenden Nutzungsrechte liegen bei A1 bzw. bei deren Masterlizenzgebern EyeonID und F-Secure und **werden ausdrücklich vorbehalten**, insbesondere allfällige Eigentums- und Urheberrechte sowie sonstige Immaterialgüterrechte.

Zugangsdaten und Passwörter sind geheim zu halten und der Kunde haftet für die unbefugte oder missbräuchliche Nutzung der Zugangsdaten, sofern er diese zu vertreten



hat. Darüber hinaus obliegt es der Verantwortung des Kunden sich das Masterpasswort für den Zugriff auf den A1 Passwortschutz zu merken (siehe Hinweis zum Passwortschutz). Besteht Verdacht auf Missbrauch der Zugangsdaten ist der Kunde verpflichtet A1 darüber zu informieren. Die Geltendmachung von Ansprüchen gegen A1 und die Subunternehmen EyeonID und F-Secure wird in diesem Zusammenhang ausdrücklich ausgeschlossen. Marken von A1 und jene der Subunternehmen EyeonID und F-Secure dürfen nicht für eigene Zwecke verwendet werden.

Der Kunde ist verpflichtet im Rahmen der vertraglichen Leistungspflicht A1 kostenfrei und in angemessenem Umfang zu unterstützen. Der Kunde wird in diesem Zusammenhang insbesondere:

- bei Fehlermeldungen die aufgetretenen Symptome detailliert beobachten und A1, oder den beauftragten Subunternehmern den Fehler unter Angabe von zweckdienlichen Informationen zur Kenntnis bringen.
- im Umfang seiner Möglichkeiten und nach besten Kräften A1 oder die beauftragten Subunternehmer bei der Suche nach Fehlern unterstützen.

10. Haftung des Kunden

Der Kunde haftet für die Vollständigkeit und die Richtigkeit seiner Angaben. **Wenn er durch missbräuchliche Nutzung der gegenständlichen Lösung Inhalte- oder Schutzrechte der A1, der Subunternehmen EyeonID und F-Secure oder sonstiger Dritter verletzt, wird er hinsichtlich allfälliger daraus entstehender Ansprüche Dritter, A1 schad- und klaglos halten.** Der Kunde haftet für sämtliche Nachteile, die durch missbräuchlich Verwendung von Zugangsdaten bei A1 und den Subunternehmen EyeonID und F-Secure entstehen und hält A1 diesbezüglich schad- und klaglos.

Gewährleistung/Haftung A1

Die zur Verfügung gestellten Produktausprägungen entsprechen dem verfügbaren Stand der Technik bei der Bekämpfung von Datendiebstahl und dem Schutz von persönlichen Daten bzw. Accounts im Internet. Dennoch ist es weder möglich, über ein Identitäts-Monitoring Tool alle unerlaubt veröffentlichten Daten im World Wide Web zu überwachen, noch durch einen Passwortmanager bzw. einem Datenschutz-VPN jegliche Form von Internet-Kriminalität zu unterbinden.

Die A1 Telekom Austria leistet – außer bei Mängeln im Sinne des Gewährleistungsrechtes - keine Gewähr und haftet - außer bei Vorsatz oder grober Fahrlässigkeit - dem Kunden gegenüber nicht für Schäden, die durch Datendiebstähle oder andere Formen von Internet-Kriminalität auftreten können. Weiters übernimmt A1 - außer bei Vorsatz oder grober Fahrlässigkeit - keine Haftung noch leistet sie - außer bei Mängeln im Sinne des Gewährleistungsrechtes - Gewähr dafür, dass Identitäts-Monitoring Produkte in der Lage sind, sämtliche Datendiebstähle zu entdecken.

Der Kunde trägt die Verantwortung für eine ausreichende Datensicherung sowie die Setzung von Schutzmaßnahmen gegenüber unberechtigtem Zugang. Dies gilt auch für den unberechtigten Zugang über Telekommunikationsmittel.