Impressum
Herausgeber: A1 Telekom Austria AG,
Lassallestraße 9, 1020 Wien,
www.A1.net

Vorbehaltlich Satz- und Druckfehler. Stand:Juni 2017.

1-400-002-435 (gültig ab Juni 2017)

(N678)

Du kannst sicher sein.

Wo viel kommuniziert wird, fallen auch viele sensible Daten an. Sie können darauf vertrauen, dass wir mit Ihren Daten sicher umgehen – das ist uns wichtig. Ein Teil davon ist, unsere Regelungen bezüglich des Datenschutzes für alle Betroffenen transparent zu machen. A1 hält sich dabei stets an aktuelle Richtlinien und Gesetze und garantiert Ihnen, dass Ihre Daten immer auf unseren Servern in Österreich gespeichert werden.

Mehr Schutz.

Du kannst Dich auf uns verlassen.

Zum Schutz Ihrer Privatsphäre im Internet hat der sichere und sensible Umgang mit Ihren Daten für uns hohe Priorität. Darum ist es uns ein Anliegen, Sie darüber zu informieren welche persönlichen Daten wir erfassen, wie diese von uns verwendet werden und was Ihr gutes Recht in puncto Datenschutz ist.

Zudem stellen sich im Zeitalter von Sozialen Netzwerken, Videoportalen und Internetnutzung über Smartphone, Tablet und Computer Fragen was man als User selbst machen kann, um seine Daten bestmöglich zu schützen.

Höchste Sicherheitsstandards.

Du kannst auf Nummer sicher gehen.

Wir setzen die gesetzlichen Regelungen zum Datenschutz konsequent um und orientieren uns an den internationalen Standards der Informationssicherheit. Außerdem passen wir uns immer an aktuelle Richtlinien, Gesetze, Gegebenheiten, wie das österreichische Datenschutzgesetz (DSG) an. Mit 25.05.2018 tritt die neue EU-Datenschutzgrundverordnung (EU-DSGVO) in Kraft. Bis dahin sind die aktuellen Datenschutzbestimmungen (DSG 2000) anwendbar.

Um die Sicherheit sensibler Daten zu gewährleisten, besitzt A1 ein eigenes Information Security Management System (ISMS). Dieses wird jährlich von externen und unabhängigen Institutionen überprüft und ist gemäß dem internationalen Standard ISO 27001:2013 zertifiziert.

Zudem bietet A1 Ihnen Cloud Services mit Datenschutz-Gütesiegel - denn die Sicherheit Ihrer Daten ist uns ein Anliegen.

Das Need-to-know-Prinzip.

Du kannst vertrauen.

Unsere Mitarbeiter arbeiten ausschließlich nach dem Need-to-know-Prinzip. Deshalb dürfen sie nur auf jene Daten zugreifen, die zur Erfüllung ihrer Aufgabe notwendig ist.

Alle Daten, die über die Erbringung unserer Dienstleistung hinausgeht, können ausschließlich mit Ihrer Zustimmung oder auf gesetzlicher Grundlage verarbeitet werden.

Und genau dafür holen wir uns von Ihnen selbstverständlich aktiv eine ausführliche Einwilligung oder Zustimmungserklärung.

Mehr Selbstkontrolle.

Du kannst Deine Rechte wahren.

Firewalls, Sicherheitssoftware und Codes bringen gar nichts, wenn man als User selbst fahrlässig mit sensiblen Daten umgeht.

Deshalb ist A1 besonders darum bemüht, Ihnen die potenziellen Gefahren und Risiken im Internet bewusst zu machen und Sie im kompetenten Umgang mit den Medien zu beraten.

Schützen Sie also Ihre Privatsphäre, verwenden Sie immer sichere Passwörter, glauben Sie nicht alles, was Ihnen versprochen wird und rüsten Sie Ihre Endgeräte mit einer entsprechenden Software auf. Und vergessen Sie nicht: Auch im Internet gilt das Urheberrecht. Mehr zum sicheren Umgang mit den Medien finden Sie auf **A1internetfüralle.at**

Was ist die Zustimmungs-erklärung?

Mit der Zustimmungserklärung können Sie folgenden Punkten zustimmen:

Zusendung von Produktinformationen und Angeboten.
Wir senden Ihnen aktuelle Produktinformationen und Angebote zu. Je nachdem, welche Kontaktdaten Sie uns bekannt gegeben haben, per Post, telefonisch, per SMS, per E-Mail oder über Social Media.

Personalisierte Angebote & Weiterentwicklung unserer Services.
Durch die Analyse Ihrer Kunden- und Nutzungsdaten können wir Angebote, Informationen und Services genau auf Ihre Bedürfnisse zuschneiden. Zusätzlich nutzen wir für die Weiterentwicklung unserer Produkte & Services sogenannte Big Data Analysen. Das heißt wir analysieren große Datenmengen, um die Bedürfnisse von möglichst vielen A1 Kunden zu berücksichtigen. Ihre Daten werden natürlich anonymisiert, ein Rück-schluss auf Ihre Person ist ausgeschlossen.

Personalisierte Angebote. Wir verwenden Ihre Kunden- und Nutzungsdaten, um Ihnen möglichst relevante und nützliche Angebote zu machen. Produktinformationen und Angebote sind so genau auf Ihre Bedürfnisse zugeschnitten. Beispielsweise bieten wir Ihnen dann ein neues Datenpaket an, wenn Ihre Frei-einheiten bald aufgebraucht sind.

Nutzung unserer Services. Wir verwenden Daten, die wir durch Nutzung unserer Dienste erhalten, um unsere Produkte & Services anhand Ihrer Bedürfnisse weiterzuentwickeln. Um Ihre Anforderungen an Produkte und Dienste besser zu verstehen, ist beispielsweise wichtig zu wissen, mit wie vielen Endgeräten Sie gleichzeitig das Internet nutzen oder mit wie vielen Personen Sie wann telefonieren. Ein Rückschluss auf Personen oder Kommunikationsinhalte ist natürlich ausgeschlossen.

Big Data Analysen. Wir entwickeln unsere Produkte, Services und unser Netz ständig weiter. Um dabei die Bedürfnisse von möglichst vielen A1 Kunden zu berücksichtigen, nutzen wir sogenannte Big Data Analysen. Das heißt wir analysieren große Datenmengen, um die Bedürfnisse von möglichst vielen A1 Kunden zu berücksichtigen. Ihre Daten werden natürlich anonymisiert, ein Rückschluss auf Ihre Person ist ausge-schlossen.

Weitergabe von Daten.
Ihre Daten können von Tochter- und Partnerunternehmen der A1 Telekom Austria AG und A1 Telekom Group verwendet werden. So können Ihnen unsere Partnerunternehmen relevante Produktinformationen zusenden (z.B. ein Mobilfunk-Angebot von Vipnet während Ihres nächsten Kroatien-Urlaubs).

Telekom Austria Group Tochterunternehmen und Vodafone Global Enterprise Limited.
Die Telekom Austria Group Tochterunternehmen und Vodafone Global Enterprise Limited dürfen Ihnen relevante Angebote und Informationen über deren Dienstleistungen zusenden (z.B. Mobilfunk-Angebot von Vipnet während Ihres nächsten Kroatien-Urlaubs). Dabei können die unter „Zusendung von Produkt-informationen & Angeboten" genannten Kommunikationskanäle verwendet werden.

Paybox. Als Tochterunternehmen der A1 Telekom Austria AG darf Ihnen die paybox Bank AG und paybox Service AG relevante Angebote und Informationen über deren Dienstleistungen zusenden. Zum Beispiel kann Paybox Sie bzgl. Neuigkeiten zum Handyparken informieren. Dabei können die unter „Zusendung von Produktinformationen & Angeboten" genannten Kommunikationskanäle verwendet werden.

Zustimmungserklärung

Was geschieht bei Widerruf? Wenn Sie Ihre Einwilligung widerrufen, verpflichten wir unsere Konzern-Unternehmen, die übermittelten Daten sofort wieder zu löschen.

Wer kann auf Ihre Daten zugreifen?

Das Need-to-know-Prinzip bei A1.

Unsere Mitarbeiter arbeiten ausschließlich nach dem Need-to-know-Prinzip. Das bedeutet, dass sie nur in dem Umfang auf Daten zugreifen dürfen, wie es zur Erfüllung ihrer Aufgabe notwendig ist.

Mitarbeiter des technischen Betriebs benötigen beispielsweise Zugang zu Ihren Verkehrs- und Standortdaten, um Störungen oder Qualitätsprobleme beheben zu können. Auf alle weiteren Daten, wie Ihre Vertrags- und Rechnungsdetails dürfen sie allerdings nicht zugreifen. Über das für die Erbringung unserer Dienstleistungen hinausgehende Maß werden Daten nur mit Zustimmung des Betroffenen, oder auf gesetzlicher Grundlage verarbeitet.

So geben wir auf Grundlage von § 98 TKG Betreibern von Notrufdiensten auf deren Verlangen Name, Anschrift, und Kontaktinformationen von Teilnehmern sowie Standortdaten bekannt, wenn bei einem Notfall nur durch Bekanntgabe dieser Informationen rasch die notwendige Hilfe geleistet werden kann. Umfangreiche Dokumentationspflichten beugen hier einem möglichenDatenmissbrauch vor.

Weiters wird A1 durch § 18 TKG verpflichtet, ein auf den aktuellen Stand gehaltenes Teilnehmerverzeichnis („Telefonbuch“) zu führen und einen telefonischen Auskunftsdienst zu betreiben. Wir müssen unsere Teilnehmerdaten auch anderen Herausgebern von Teilnehmerverzeichnissen und Auskunftsdiensten auf Anfrage zur Verfügung stellen. Eine Ausnahme besteht nur dann, wenn eine Person der Aufnahme ihrer Daten in das Teilnehmerverzeichnis widersprochen hat.

Need-to-know-Prinzip

Können Sie widerrufen? Sie können an uns erteilte Einwilligungen natürlich widerrufen..In diesem Fall verwenden wir Ihre Daten nicht mehr für die genannten Zwecke.

Was tun wir für die Sicherheit Ihrer Daten?

Im Dienste des Datenschutzes und der Informationssicherheit.

Um die Sicherheit sensibler Daten zu gewährleisten, besitzt A1 ein eigenes Information Security Management System (ISMS). Dieses wird jährlich von externen und unabhängigen Institutionen überprüft und ist gemäß dem internationalen Standard ISO 27001:2013 zertifiziert.

Wir stellen in puncto Funktionalität und Effizienz die höchsten Qualitäts-Standards sicher. Mit zusätzlichen Schutzvorkehrungen gegen Schadprogramme, sowie modernen Vorbeugungsmaßnahmen gegen Datenverluste verstärken wir die Sicherheit Ihrer Daten. Überwacht werden all diese Systeme von einem zertifizierten Expertenteam, welches rund um die Uhr notwendige Maßnahmen ergreifen kann. Wir bewahren Ihre Daten absolut sicher auf: sicheres Rechenzentrum, das vor jeglichen Angriffen von Außen sicher ist. Ihre Daten sind bei uns sicher, weil wir zu jeder Zeit darauf achten. A1 garantiert, dass die Daten nur im Rahmen Ihrer Zustimmungserklärungen verarbeitet und verwendet werden.

Alle A1 Mitarbeiter sind durch ihren Arbeitsvertrag und durch das Gesetz (Telekommunikationsgeheimnis) zur Geheimhaltung verpflichtet. Die A1 Datenschutz-Richtlinie gibt genaue Vorgaben und regelt den Umgang mit allen personenbezogenen Daten. In wiederkehrenden Schulungen und Trainings sensibilisieren wir unsere Mitarbeiter für die Bedeutung des Datenschutzes und der Informationssicherheit.

Nutzen Sie unsere mit dem Datenschutz Gütesiegel ausgezeichneten A1 Cloud Services um sich zu vergewissern, dass Ihre Ideen, Daten, Fotos, etc. sicher sind.

Was tun wir, wenn doch einmal etwas passiert?

Ein Fall für die Datenschutzbehörde.

Leider kann man trotz aller Vorsichtsmaßnahmen niemals vollständig ausschließen, dass personenbezogene Daten einmal in die falschen Hände geraten könnten.

In einem solchen Fall ergreifen wir sofort alle notwendigen Maßnahmen, um einen drohenden Schaden zu verhindern oder – falls dies nicht mehr möglich ist – zu minimieren.

Durch das Telekommunikationsgesetz (TKG) sind wir verpflichtet, im Fall einer Verletzung des Schutzes personenbezogener Daten unverzüglich die Datenschutzbehörde zu benachrichtigen. Besteht die Annahme, dass dadurch Personen in ihrer Privatsphäre oder die personenbezogenen Daten selbst beeinträchtigt werden könnten, benachrichtigen wir unverzüglich die betroffenen Personen. Sie bekommen von uns alle erforderlichen Informationen zu Ursache und Ausmaß des Schadens, sowie über die nötigen Schritte und Maßnahmen zur Schadenbegrenzung.

Was können Sie selbst tun? Darüber hinaus haben Sie die Möglichkeit, weitere Fragen jederzeit direkt mit unseren Datenschutzexperten zu klären.

Was können Sie selbst für Ihre Datensicherheit tun?

So bewegen Sie sich sicher durchs Netz.

Surfen im Internet ist ein unverzichtbarer Bestandteil unseres Alltags geworden. Deshalb ist es besonders wichtig sich der potenziellen Gefahren und Risiken im Internet bewusst zu sein und sich im kompetenten Umgang mit den Medien zu schulen.

Die Initiative „A1 Internet für Alle" hat gemeinsam mit saferinternet.at die 10 wichtigsten Tipps für ein sicheres Surfen im Netz zusammengestellt:

1. Umsonst gibts nichts.
Wenn etwas auffällig günstig oder sogar gratis angeboten wird, seien Sie skeptisch – auch im Internet hat niemand etwas zu verschenken.

2. Erst lesen, dann kaufen.
Bevor Sie eine Bestellung aufgeben, lesen Sie immer genau die Produktbeschreibung und alle Kosten. Bei den meisten Einkäufen im Internet können Sie ohne Angabe von Gründen innerhalb von 14 Tagen zurücktreten.

3. Vorsicht bei der Datenweitergabe.
Wenn möglich, geben Sie keine persönlichen Daten wie Name, Adresse, Telefonnummer oder Passwörter im Internet bekannt.

4. Privatsphäre schützen.
Nutzen Sie in Sozialen Netzwerken die Einstellungen zur „Privatsphäre", schränken Sie Ihr Profil möglichst ein und überprüfen Sie regelmäßig die Wirksamkeit Ihrer Sicherheitseinstellungen. Auch mit Ihren persönlichen Daten und Fotos sollten Sie in diversen Social Media Kanälen bewusst und vorsichtig umgehen. Verwenden Sie in Foren und Chats einen Nickname (Spitznamen) anstelle Ihres echten Namens.

5. Sichere Passwörter verwenden.
Sichere Passwörter bestehen aus einer Kombination von mindestens acht Buchstaben, Zahlen und Sonderzeichen. Verwenden Sie unterschiedliche Passwörter für verschiedene Accounts. Halten Sie Ihre Passwörter geheim und ändern Sie diese regelmäßig.

Viele weitere Tipps sowie kostenlose Schulungen zum sicheren Umgang mit Medien finden Sie auf **A1internetfueralle.at**

6. Computer schützen.
Verwenden Sie ein Anti-Viren-Programm und aktualisieren Sie dieses regelmäßig. Erstellen Sie Sicherungskopien Ihrer Daten. Seien Sie sich bewusst, dass Sie bei Inanspruchnahme von Cloud-Diensten nicht mehr die alleinige Herrschaft über Ihre Daten haben. Achten Sie beispielsweise bei e-banking auf eine verschlüsselte Verbindung (https).

7. Phishing- (Betrüger-) E-Mails sofort löschen.
Seriöse Unternehmen fordern Sie niemals per E-Mail auf, Ihre Konto- oder Zugangsdaten auf einer Website einzugeben.

8. Urheberrechte beachten.
Jede Zurverfügungstellung von urheberrechtlich geschützten Werken im Internet, die ohne Zustimmung des Urhebers bzw. Rechteinhabers erfolgt, ist eine Urheberrechtsverletzung.

9. Nicht alles glauben.
Seien Sie misstrauisch bei Behauptungen, die Sie im Internet finden. Oft ist nicht klar, woher und von wem die Informationen stammen und ob die Person wirklich diejenige ist, die er/sie vorgibt zu sein. Überprüfen Sie Infos daher besser mehrfach!

10. Smartphone und Tablet schützen.
Sichern Sie Ihr Smartphone gegen unbefugten Zugriff (PIN-Code, Zugriffsschutz mit Passwort oder Entsperrmuster). Informieren Sie sich bevor Sie Apps installieren und erlauben Sie diesen nicht den Zugriff auf die Daten Ihres Geräts. Auf schlecht bewertete Apps verzichten Sie besser.