Sicherheit & Zuverlässigkeit

Datenschutz und -sicherheit bei der LINK Mobility GmbH

link mobility

LINK Mobility GmbH
Am Sandtorkai 73
20457 Hamburg

Telefon: +49 40 88 88 08 – 0
Fax: +49 40 88 88 08 – 19
Internet: www.linkmobility.de

Inhalt

Datenschutz und Datensicherheit haben für uns oberste Priorität. Deswegen treffen wir stets alle notwendigen Vorkehrungen, um die höchste Sicherheit für unsere Systeme, angebotene Services und Ihre Daten zu gewährleisten. Im Nachfolgenden klären wir darüber auf, was wir als LINK Mobility dafür unternehmen, an wechen Standards und Zertifizierungen wir uns orientieren und welche Vorgaben für unsere Partner gelten.

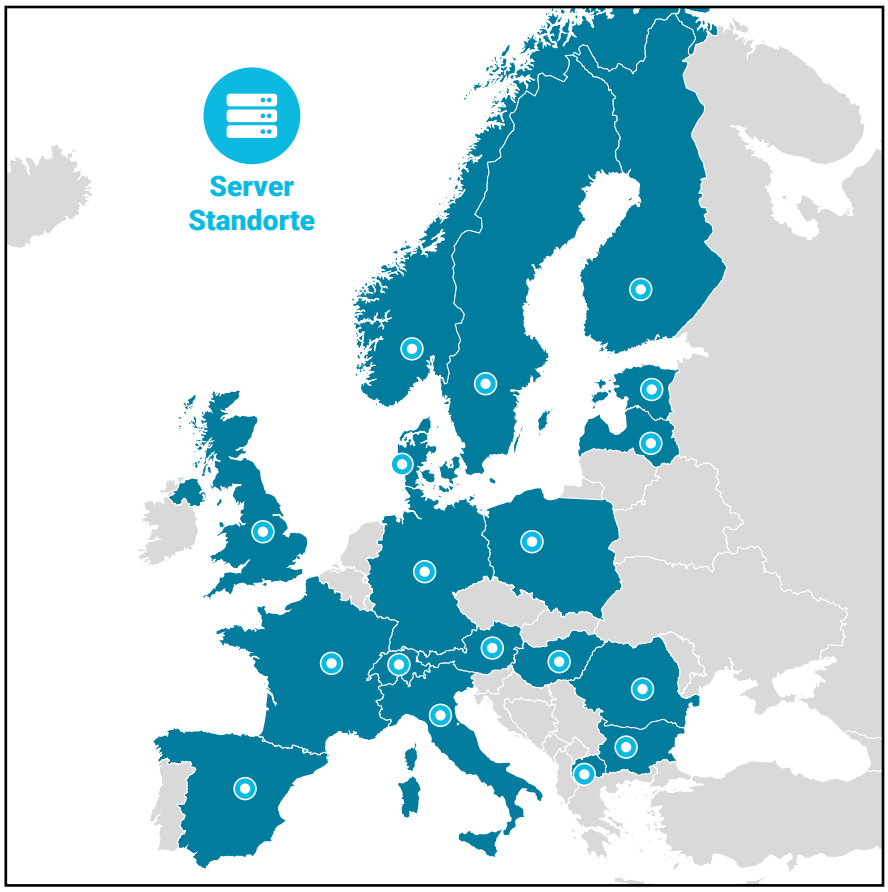
1. Rechtliche Rahmenbedingungen und geltende Gesetze

Als registrierter Telekommunikationsanbieter unterliegen wir neben der europäischen Datenschutzgrundverordnung (DSGVO) zusätzlich den hohen Datenschutz- und Sicherheitsanforderungen des deutschen Telekommunikationsgesetzes (TKG). Die Berücksichtigung und Achtung jeglicher rechtlicher Sicherheitsvorgaben wissen insbesondere unsere Kunden aus dem Versicherungs- und Finanzsektor zu schätzen. Dementsprechend verpflichten wir uns zusätzlich auf das Bankengeheimnis.

2. Unsere Rechenzentren

a. Standorte

Alle datenverarbeitenden Server der LINK Mobility GmbH und LINK Mobility Group befinden sich ausnahmslos in Europa. Damit unterliegen wir den höchsten Datenschutzgesetzen der Welt. Wir können Ihnen dadurch garantieren, dass Ihre Daten ausschließlich in Europa verarbeitet werden und dort bleiben.



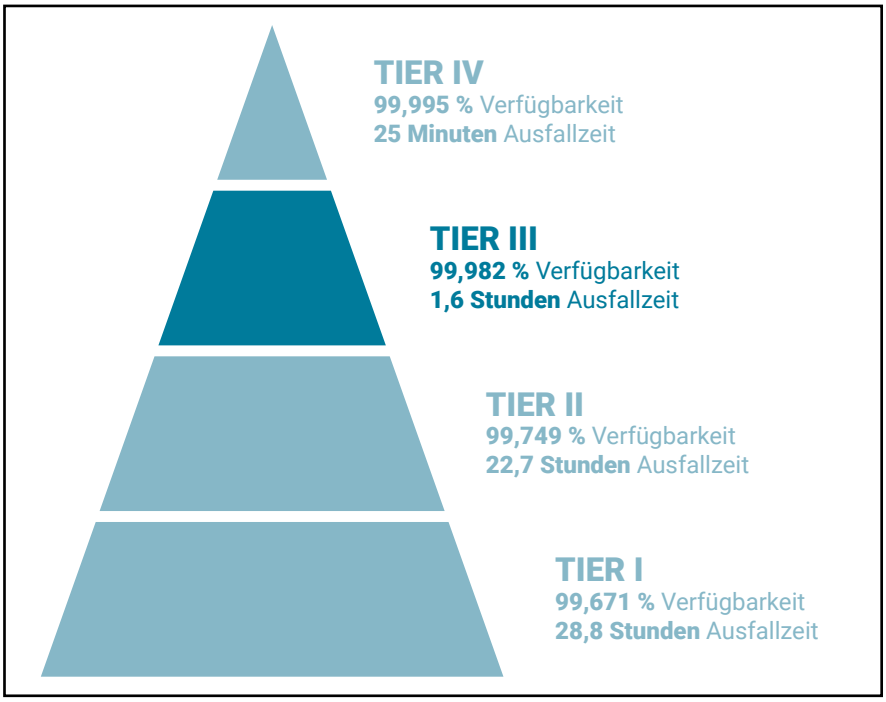
b. ISO 27001

Für den Betrieb unserer Rechenzentren arbeiten wir ausschließlich mit ISO 27001 zertifizierten Betreibern zusammen. Bei der ISO 27001 handelt es sich um eine internationale Norm für Informationssicherheits-Managementsysteme (ISMS). So erhalten Organisationen unterschiedlicher Art und Größe klare einheitliche Leitlinien für die Planung, Umsetzung, Überwachung und Verbesserung ihrer Informationssicherheit.

Gemäß den Vorgaben des ISO 27001 Standard stellen wir detaillierte Konzepte zur IT-Sicherheit, der Business Continuity sowie ein Disaster Recovery Concept bereit. Diese Konzepte beschreiben unsere technischen und organisatorischen Maßnahmen (TOM) zur Informationssicherheit. Die Wirksamkeit unseres Informationssicherheits-Managements wird regelmäßig durch interne und externe Audits, sowie durch Schwachstellen-, Disaster Recovery-, und Belastungstests überprüft.

c. Tier-Klassifizierung

Anhand der Einstufung in eine der vier Tier-Kategorien (Tier 1 = niedrigste Klasse, Tier 4 = höchste Klasse) lassen sich Rückschlüsse auf die Ausfallsicherheit eines Rechenzentrums ziehen. Die Klassifizierung unterscheidet Rechenzentren anhand der Anzahl von Versorgungswegen und der Möglichkeit zur Wartung im laufenden Betrieb sowie der Single Point of Failure (SPOFs), also Fehler in Systemkomponenten oder -pfaden, die zum Ausfall des Gesamtbetriebs führen. Ebenfalls berücksichtigt bei einer Beurteilung werden die Fehlertoleranz, die Anzahl von Brandabschnitten und die erforderliche Entwärmungsleistung.



Bei der Auswahl unserer Rechenzentren verlangen wir mindestens eine Verfügbarkeit pro Jahr die der Einstufung von Tier 3 entspricht.

Als Tier 3 eingestufte Rechenzentren verwenden redundante Komponenten: Der Server ist in zweifacher Ausführung vorhanden und es gibt mehrfache Versorgungswege. Dadurch wird das System fehlertolerant und kann auch während des Betriebs gewartet werden. Die Ausfallsicherheit wird durch mehrere Brandabschnitte erhöht. Single Point of Failure kön-

nen in einem Tier-3-Rechenzentrum vorkommen, die Entwärmungsleistung liegt bei 1.070 bis 1.620 Watt pro Quadratmeter. Insgesamt erreicht ein Tier-3-Rechenzentrum bei einer maximalen Ausfallzeit von 1,6 Stunden im Jahr eine Verfügbarkeit von 99,98 Prozent.

3.Georedundanz und Systemverfügbarkeit

a. Georedundante Services

Um im Fall einer Störung abgesichert zu sein, bieten wir Kunden optional die Möglichkeit, sich georedundant an unseren Service anzubinden. Das bedeutet: Sollte unser Service einmal nicht erreichbar sein, weichen georedundant angebundene Kunden automatisch auf ein anderes Data Center aus und können so auch weiterhin ohne Einschränkungen Nachrichten ausliefern.

b. >99 Prozent Systemverfügbarkeit

Standardmäßig garantieren wir über das Jahr verteilt eine Systemverfügbarkeit von 99,45 %.

Bei georedundanter Anbindung garantieren wir eine Systemverfügbarkeit von 99,9 %.

4. Nachrichtenrouting: Smart und sicher

a. Intelligentes Routing

Unser intelligentes Routing wählt automatisch den besten Weg für jede einzelne SMS-Nachricht aus. Zusätzlich überwacht und analysiert unser technisches Experten-Team eine Vielzahl von Metriken, um alle Nachrichten so schnell wie möglich und in höchster Qualität auszuliefern. Dabei hilft uns unsere langjährige Markterfahrung und unser weltweites Partnernetzwerk.

- Anbindungen und Durchsatz zu den Netzbetreibern werden 24 / 7 überprüft
- Täglich wird das Routing von einem Experten-Team evaluiert und zusätzlich auf Anomalien untersucht
- Regelmäßiges SMS-Routen-Testing über unser eigenes Testnetzwerk REMOTE365

b. Testnetzwerk REMOTE365

In den vergangenen Jahren haben wir ein weltweit einzigartiges Testnetzwerk aufgebaut, das wir zur Überprüfung unserer Nachrichtenrouten und Versandqualität nutzen. In engmaschigen Abständen versendet unsere Ende-zu-Ende-Überwachung REMOTE365 Testnachrichten und stellt so sicher, dass alle Nachrichten zum richtigen Zeitpunkt und mit unverändertem Inhalt beim Nuzer ankommen. Bei abweichenden Ergebnissen werden Nachrichten automatisch über andere Wege verschickt, um Beeinträchtigungen zu vermeiden.

5. Verbände und Mitgliedschaften

a. Allianz für Cyber-Sicherheit

Wir sind Teilnehmer der Allianz für Cyber-Sicherheit, eine 2012 vom Bundesamt für Sicherheit in der Informationstechnik (BIS) ins Leben gerufene Vereinigung, die das Ziel verfolgt, die Widerstandsfähigkeit des Standortes Deutschland und hier ansässiger Unternehmen gegenüber Cyber-Attacken zu stärken.

Im Rahmen der Initiative engagieren sich IT-Dienstleister, -Beratungsunternehmen sowie -Hersteller gleichermaßen und fördern den Austausch von IT-Expertise und Erfahrungen untereinander.

b. Gesellschaft für Datenschutz und Datensicherheit

Wir sind ebenfalls Mitglied in der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD). Die GDD unterstützt als gemeinnütziger Verein einen sinnvollen, vertretbaren und technisch realisierbaren Datenschutz. Dafür pflegt die GDD die intensive Zusammenarbeit mit Wirtschaft, Verwaltung, Wissenschaft und Politik.

Sie vertritt die Belange von Datenverarbeitenden Stellen, Datenschutzbeauftragten und betroffenen Bürgern gegenüber Behörden und Gesetzgebungsorganen. Darüber hinaus unterstützt sie durch fachlichen Rat die politische Willensbildung.