

WLAN und Sicherheit

Inhaltsverzeichnis

1. Technische Sicherheit
2. Abrechnungssicherheit
3. Datenschutz
4. Gesundheit

1. Technische Sicherheit

GANAG HotSpots bieten die größtmögliche technische Sicherheit, die für einen uneingeschränkten Zugang zum Internet möglich ist.

Alle Zugangsdaten und Anmeldeinformationen, einschließlich der Kreditkarteninformationen, sind über eine **128 Bit-SSL-Verschlüsselung** geschützt.

Die **interne Nutzerisolierung** über VLAN (Virtual Local Area Network) verhindert an besonders frequentierten Standorten, dass Anwender dort gegenseitig auf ihre Notebooks zugreifen können.

GANAG HotSpots verfügen über **HotSpot Firewalls**. Unbefugter Zugriff von außen wird so unterbunden. Um Anwendern einen uneingeschränkten Zugang zum Internet zu ermöglichen, werden Internetdienste nicht gefiltert. Allerdings können Seiten mit diskriminierenden oder Jugend gefährdenden Inhalten aufgrund regionaler gesetzlicher Bestimmungen gesperrt sein.

Für einen uneingeschränkten Zugang zum Internet verzichtet GANAG auf den Einsatz weiterer Sicherheitsprotokolle.

Um die sichere Übertragung Ihrer Daten zu gewährleisten und Ihren PC vollständig vor Angriffen von außen zu schützen, empfiehlt Ihnen GANAG den Einsatz aktueller Antiviren-Software, Personal Firewalls und VPN Lösungen.

Ein VPN bildet einen verschlüsselten, sicheren Tunnel vom Computer des Anwenders zum Unternehmensnetzwerk. Mittels spezieller Softwares von VPN-Anbietern wie z.B. Cisco, Check Point oder Computer Associates lassen sich VPNs einfach einrichten. GANAG HotSpots sind für die Nutzung von marktüblicher **VPN Lösungen** (Virtuelles Privates Netzwerk) optimiert, welche NAT-T (Network Address Translation Traversal) auf Client- und Serverseite unterstützen. NAT beschreibt die Umsetzungsmethode der (meist privaten) IP-Adressen in einem Netz auf andere (meist öffentliche) IP-Adressen eines anderen Netzes.

Als ganzheitliche Lösung für überregional oder international tätige Unternehmen mit hohem Reiseaufkommen empfiehlt GANAG den **GANAG iPass GlobalConnectivity** Zugang mit Integration der firmeneigenen Antiviren-, VPN- und Firewall-Software – die Dialer, Controller und Protector Lösung in einem.

2. Abrechnungssicherheit

Alle Zugangsdaten und Anmeldeinformationen, einschließlich der Kreditkarteninformationen, sind über eine **128 Bit-SSL-Verschlüsselung** geschützt.

Um sicher zu stellen, dass keine Dritten auf Ihre Kosten WLAN nutzen, indem sie Ihre Mobilfunknummer missbrauchen, erhalten Sie bei o2, Vodafone und Debitel für jede neue Nutzung ein Einmalpasswort via SMS auf Ihr Mobiltelefon. **Aus Sicherheitsgründen verfallen diese Zugangsdaten bei Nichtbenutzung nach ca. einer ¼ Stunde ohne Berechnung.** So ist gewährleistet, dass nur die Besitzer des Mobilfunktelefons die Zugangsdaten erhalten und nutzen können. Neue Zugangsdaten können jederzeit wieder angefordert werden.

Bei Excilan „Pay By Mobile Phone“ erhalten Sie einen Anruf mit den Zugangsdaten auf Ihr Mobiltelefon.

Bei der Zahlung mit Kreditkarte rät GANAG dringend, die **Autovervollständigung des Browsers** während des Zahlungsvorganges zu **deaktivieren** (z.B. im Internet Explorer unter Extras -> Internetoptionen -> Inhalte -> Autovervollständigen -> alle Haken entfernen) und **im Anschluss den Cache des Browsers zu löschen** (insbesondere bei öffentlich zugänglichen PCs).

GANAG empfiehlt Ihnen, sich in jedem Fall ordnungsgemäß über den Logout Button oder alternativ über die URL <https://login.hotels-on-air.de/logoutpda.html> auszuloggen, da ansonsten der Zugang für weitere Minuten (Leerlaufzeit = idle timeout) geöffnet bleibt. Diese Leerlaufzeit kann zu folgenden Unannehmlichkeiten für Sie führen:

- Bei Abrechnung über GANAG Minutenzugang (Minutentakt), o2 Mobilfunkrechnung (im 30 min Takt) und Excilan „Pay By Mobile Phone“ (im Minutentakt) kann dies ungewünscht zur Berechnung zusätzlicher Intervalle führen.
- Während dieser Zeit können Sie sich nicht mit einem anderen Endgerät (Internet Terminal, Notebook, PDA) einloggen.
- An öffentlich zugänglichen PCs kann der nachfolgende Anwender den Zugang weiter nutzen.
- Sollten Programme im Hintergrund aktiv sein, die die Internetverbindung aufrechterhalten, werden Sie **überhaupt nicht** ausgeloggt.

3. Datenschutz

Beim Umgang mit Daten hält sich GANAG an die geltende Gesetzgebung. GANAG erhebt, speichert und bearbeitet nur Daten, die für die Erbringung der Dienstleistungen, für die Abwicklung und Pflege der Kundenbeziehung, namentlich der Gewährleistung einer hohen Dienstleistungsqualität, für die Sicherheit von Betrieb und Infrastruktur sowie für die Rechnungsstellung benötigt werden.

GANAG trifft Vorkehrungen, um sein Netz vor Eingriffen Dritter zu schützen (siehe Punkt 1). Ein absoluter Schutz vor unerlaubten Zugriffen und unerlaubtem Abhören kann jedoch nicht gewährleistet werden. GANAG kann für solche Eingriffe nicht haften.

4. Gesundheit

Laut aktuellen Forschungsergebnissen ist die Strahlung der WLANs nicht gefährlich.

Die Sendeleistung der WLAN Adapter beträgt maximal 100 mW. Zum Vergleich: der Sender auf dem Fernsehturm Berlin Alexanderplatz strahlt mit 200 kW, eine Mobilfunk-Basisstation mit 20 W, ein Mobiltelefon mit 2 W, eine Mikrowelle arbeitet mit 1 kW und darf laut CE-Vorschrift bis zu 1 W Energie nach außen abstrahlen.

Die europäische Norm EN 60601-1-2 definiert die Anforderungen und Prüfungen, die speziell für die Elektromagnetische Verträglichkeit (EMV) von Geräten beim Einsatz im medizinischen Umfeld zutrifft. Mit bis zu 100 mW maximal ausgesendeter Energie sind WLAN Adapter im Gegensatz zu GSM, GPRS und UMTS in sensibelsten Bereichen wie z.B. in Kliniken oder Gesundheitszentren einsetzbar.