

An das  
 Bundesministerium für Verkehr, Innovation und Technologie  
 Radetzkystraße 2,  
 A-1030 Wien

E-Mail: [JD@bmvit.gv.at](mailto:JD@bmvit.gv.at), [begutachtungsverfahren@parlament.gv.at](mailto:begutachtungsverfahren@parlament.gv.at)

Wien, am 16. August 2016

**BETREFF: ISPA-STELLUNGNAHME ZUM ENTWURF EINES BUNDESGESETZES  
 BETREFFEND DIE MARKTÜBERWACHUNG VON FUNKANLAGEN (FUNKANLAGEN-  
 MARKTÜBERWACHUNGS-GESETZ – FMAG)**

Sehr geehrte Damen und Herren,

die ISPA erlaubt sich im Zusammenhang mit der öffentlichen Konsultation des Bundesministeriums für Verkehr, Innovation und Technologie zum Entwurf eines Bundesgesetzes betreffend die Marktüberwachung von Funkanlagen (Funkanlagen-Marktüberwachungs-Gesetz – FMAG) in Umsetzung der Richtlinie 2014/53/EU (Funkrichtlinie) wie folgt Stellung zu nehmen:

Die ISPA begrüßt die Bestrebungen des Gesetzgebers zur Harmonisierung der Nutzung von Funkfrequenzen um Gefahren für die Gesundheit und Funkstörungen zu vermeiden. Jedoch möchte sich die ISPA insbesondere kritisch zu jenen geplanten Maßnahmen, die eine nachträgliche Manipulation der Funkparameter in Funkanlagen verhindern sollen, äußern. Die ISPA möchte zunächst anmerken, dass Maßnahmen zur Verhinderung von nachträglichen Manipulationen der Funk-Firmware generell die Anwendung von alternativer Software verunmöglichen werden und daher abzulehnen sind. Ferner sollte jedenfalls sichergestellt werden, dass die vorgeschriebenen Konformitätsbewertungen nicht zu Lasten von unabhängigen Softwareanbietern durchgeführt werden. Zudem möchte die ISPA hervorheben, dass durch das Fehlen nachträglicher Software-Updates das Schließen von Sicherheitslücken verhindert wird sowie, dass es aufgrund der unverhältnismäßig stärkeren wirtschaftlichen Folgen für kleine und mittlere Provider zu einer Wettbewerbsverzerrung kommt. Darüber hinaus möchte die ISPA auf die Bedeutung der aus der Nutzung von alternativer Software auf WLAN Equipment resultierenden Innovationen hinweisen und sich jedenfalls gegen eine rechtliche Inanspruchnahme der Provider für Manipulationen durch Kunden sowie eine Abschottung des österreichischen WLAN-Marktes aussprechen. Außerdem spricht sich die ISPA dafür aus, dass sämtliche Gerätefunktionalitäten allen Wirtschaftsakteuren gleichermaßen offen stehen sollten, sowie dass die Möglichkeit der Weiterverwendung bereits bestehender Funkanlagen nicht eingeschränkt wird.

**1. Maßnahmen zur Verhinderung von nachträglichen Manipulationen der Funk-Firmware werden die Anwendung von alternativer Software verunmöglichen und sind daher abzulehnen.**

Zukünftig müssen Funkanlagen entsprechend konstruiert sein, um sowohl eine effiziente Nutzung von Funkfrequenzen zu gewährleisten als auch funktechnische Störungen zu verhindern. Jedoch kann durch die Integration von neuer Software oder durch Änderung bestehender Software die Konformität der Funkanlagen mit diesen Anforderungen beeinträchtigt werden. Daher verfügt der BMVIT über die Möglichkeit, durch Verordnung Klassen oder Kategorien von Funkanlagen zu bestimmen, für welche der Hersteller durch bestimmte Funktionen sicherzustellen hat, dass nur solche Software geladen werden kann, für die die Konformität ihrer Kombination mit der Funkanlage zuvor nachgewiesen wurde und diese nicht anschließend durch den Benutzer manipuliert werden kann. Hierzu haben die Hersteller von Funkanlagen für die beabsichtigte Kombination von Funkanlagen und Software jeweils eine Konformitätsbewertung gemäß § 11 Abs. 1 FMAG durchzuführen.

Aufgrund der Tatsache, dass sich auf modernen Geräten häufig alle wesentlichen Hardware-Komponenten auf einer einzigen Platine befinden, ist es in der Praxis kaum möglich, die Funkparameter von anderen Treiber- und Systemfunktionen abzuschotten. Für Hersteller von Funkanlagen ist es somit äußerst schwierig und weitaus kostenintensiver, lediglich eine nachträgliche Manipulation der Funk-Firmware zu verhindern und gleichzeitig die Änderung anderer Software weiterhin zu ermöglichen. Vielmehr ist zu befürchten, dass Hersteller, um sich gegen nachträgliche Haftung abzusichern, das Aufspielen von jeglicher Alternativsoftware für die zuvor keine Konformitätsbewertung eingeholt wurde, verhindern werden, anstatt sich darum zu bemühen, einen bestimmten Softwareteil abzusichern und entsprechende Vorkehrungen zu treffen.

Die ISPA betont, dass solche Maßnahmen, welche die Anwendung von alternativer Software unmöglich machen, jedenfalls abzulehnen sind und weit über die Zielsetzung der Gesetzesbestimmung, Funkstörungen zu verhindern, hinausgehen. Dieses Problem wurde vom Gesetzgeber, wie aus den Erläuterungen zu § 3 Abs. 3 FMAG hervorgeht, auch bereits erkannt. Daher ersucht die ISPA, dass der zuständige Bundesminister im Rahmen seiner Verordnungsermächtigung darauf Bedacht nimmt.

**2. Die vorgeschriebenen Konformitätsbewertungen dürfen nicht zu Lasten von unabhängigen Softwareanbietern durchgeführt werden.**

Aufgrund der damit verbundenen Kosten, ist zu erwarten, dass Hersteller von Funkanlagen eine Konformitätsbewertung zunächst nur mit der eigenen Firmware, sowie etablierter Drittsoftware durchführen werden. Da es gemäß § 11 FMAG lediglich dem Hersteller der Funkanlage obliegt, eine Konformitätsbewertung durchzuführen, ist zu befürchten, dass kleine Softwareunternehmen bzw Start-Ups benachteiligt werden und ihnen der Zugang zum Markt erheblich erschwert wird.

Die ISPA regt daher dazu an, den ersten Satz des Erwägungsgrundes 19 zur Funkrichtlinie, welcher bereits sinngemäß in die erläuternden Bemerkungen zu § 16 FMAG aufgenommen wurde und wie folgt lautet

*„Die Überprüfung der Konformität von Kombinationen aus Funkanlagen und Software durch die Funkanlagen selbst sollte nicht dazu missbraucht werden, die Verwendung der Anlagen mit Software von unabhängigen Anbietern zu verhindern. Durch das zur Verfügung stellen von Informationen über die Konformität beabsichtigter Kombinationen von Funkanlagen und Software soll der Wettbewerb gefördert werden.“*

als Text in das FMAG aufzunehmen und Hersteller von Funkanlagen dezidiert zur Konformitätsbewertung auch von Software von Drittanbietern aufzufordern<sup>1</sup>.

### 3. Das Fehlen nachträglicher Software-Updates verhindert das Schließen von Sicherheitslücken

Sofern ein Händler (bzw. ein Provider) eine bereits in Verkehr befindliche Funkanlage derart verändert, dass die Konformität im Sinne dieses Bundesgesetzes beeinträchtigt werden kann, unterliegt er gemäß § 8 FMAG den Pflichten des Herstellers. Aufgrund dessen hat er unter anderem selbst eine Konformitätsbewertung der neuen Software mit der Funkanlage einzuholen.

Dies kann mitunter weitreichende Folgen für den Fall mit sich bringen, dass ein Gerät eine Sicherheitslücke an einem Software-Bestandteil aufweist und diese vom Hersteller, oft aufgrund der kurzen Produktzyklen, nicht mehr behoben wird. Bisher konnten solche Sicherheitslücken durch die nachträgliche Ausführung von Open-Source Sicherheitsupdates, innerhalb kürzester Zeit geschlossen werden und somit die Lebensdauer des Equipments wesentlich verlängert und dadurch eine nachhaltige Wirtschaft gefördert werden. Gemäß der geplanten Regelung müsste für ein entsprechendes Update der Software durch den Provider, eine erneute Konformitätsbestätigung eingeholt werden. Dies ist diesem in der Praxis, da er nicht über alle notwendigen Unterlagen (Konstruktionszeichnungen, Schaltpläne etc.) verfügt, aber nicht möglich.

Die ISPA möchte darauf hinweisen, dass Provider stets daran bemüht sind, ein höchstmögliches Niveau an Cyber-Sicherheit zu gewährleisten. Sollten derartige Updates in Zukunft jedoch nicht mehr möglich sein, müsste die Hardware vom Provider – sofern diese nicht in das Eigentum des Kunden übergegangen ist - aus dem Verkehr genommen und durch neue ersetzt werden. Da dies, insbesondere aus Kostengründen, in der Praxis nicht realistisch erscheint, besteht die Gefahr, dass die geplanten Beschränkungen negative Auswirkungen im Bereich der Cyber-Sicherheit nach sich ziehen. Eine solche Situation, in der zur Verbesserung der Störungsfreiheit von Funkanlagen,

<sup>1</sup> Hierbei möchte die ISPA zusätzlich auf die Probleme technischer Lösungen, ähnlich dem „Trusted computing“ hinweisen, welche einerseits die Einhaltung der Funkparameter garantieren und gleichzeitig Dritthersteller-Firmwares nicht aussperren. Durch die kryptografische Signierung von Software kann dabei der Hersteller zwar sicherstellen, dass nur von ihm freigegebene Software installiert werden kann. Bei vielen modifizierten Softwareanwendungen, welche insbesondere von KMU und Start-UPs verwendet werden, ist eine solche komplexe Signaturprüfung jedoch technisch äußerst schwierig und ihre Anwendung würde in der Praxis wiederum erheblich erschwert werden.

Sicherheit in anderen Bereichen abgeschwächt wird entspricht weder den Interessen der Wirtschaft noch jenen der Verbraucher und wird von der ISPA abgelehnt.

#### **4. Die nachteiligen Auswirkungen für kleine und mittlere Wireless Access-Provider führen zu einer Wettbewerbsverzerrung.**

Generell vertritt die ISPA die Ansicht, dass die beschränkte Nutzung von freier Systemsoftware auf WLAN Equipment, in erster Linie eine Belastung für KMU und Start-Ups darstellen würde. Bisher war es kleinen und mittleren Providern möglich, durch die Verwendung von freier Software von Drittanbietern auf WLAN Equipment auch auf kostengünstiger Hardware ein breites Funktionsspektrum zu aktivieren, welches ansonsten nur bei Geräten höherer Preisklassen desselben Herstellers genutzt werden kann. Die neue Rechtslage bringt Schwierigkeiten für KMU und Start-Ups, kostengünstig Hardware mit der für sie spezifischen Software zu beziehen wodurch sie in ihrer wirtschaftlichen Stellung geschwächt werden. Kleine und mittlere Wireless Access-Provider leisten einen essentiellen Beitrag zu einem aktiven und transparenten Wettbewerb und stellen aufgrund ihrer Spezialisierung insbesondere im ländlichen Bereich die Grundversorgung mit leistungsstarken Breitbandzugängen sicher. Dabei profitieren Verbraucher auch durch die stetigen Investitionen in neue Technologien bei gleichzeitig niedrigen Gebühren.

Wie aus Erwägungsgrund 26 zur Funkrichtlinie hervorgeht, soll diese insbesondere den Schutz der Gesundheit sowie ein angemessenes Niveau an elektromagnetischer Verträglichkeit und eine konkrete und effiziente Nutzung von Funkfrequenzen gewährleisten. Gleichzeitig soll jedoch ein fairer Wettbewerb auf dem Unionsmarkt bewahrt werden. Sofern es in Einzelfällen dazu kommt, dass durch Änderungen an der Software andere Funkdienste gestört werden muss dagegen vorgegangen werden. Aus diesem Grund jedoch Änderungen der Firmware zu verbieten und KMU und Start-Ups somit eine essentielle Voraussetzung ihrer wirtschaftlichen Tätigkeit zu entziehen ist nach Ansicht der ISPA eine überzogene Maßnahme und hemmt Innovationen in diesem Bereich. Die ISPA lehnt ausdrücklich die Schaffung solcher wettbewerbsverzerrender Strukturen ab und betont, dass diese jedenfalls nicht den Zielen der Funkrichtlinie entsprechen.

Aus diesem Grund regt die ISPA an, zuzüglich zur verpflichteten Einholung einer Konformitätsbewertung durch Hersteller, auch Betreibern von Funkanlagen die Möglichkeit zu verschaffen, selbst eine Konformitätsbewertung einzuholen oder eine solche anzufordern, ohne dabei den Pflichten des Herstellers gemäß § 8 gleichgestellt zu werden.

#### **5. Die restriktiven Auswirkungen der geplanten Regelung schaden der innovativen Nutzung von Wireless Access Technologien**

Das Betreiben von WLAN Equipment mit freier Software von Drittanbietern, brachte bereits in der Vergangenheit wesentliche Innovationen mit sich. Im Zuge der open-source Nutzung entstand eine Vielzahl an Projekten beispielsweise für Rettungsorganisationen und sogenannte Community Networks (Freifunknetze). Diese waren bisher vor allem deswegen so leicht aufzubauen, da

bereits günstige WLAN-Router mit der nötigen alternativen Systemsoftware dafür ausreichen. Der Nutzen solcher Netze wurde insbesondere während der Migrationswelle im vergangenen Jahr ersichtlich, als den Ankommenden auf diese Weise freier Zugang zum Internet bereitgestellt werden konnte. Sollte die Nutzung von alternativer Systemsoftware nicht mehr möglich sein, sind genau solche Projekte in Zukunft gefährdet, da es vom Wohlwollen des Hardwareherstellers abhängig sein wird, ob eine Konformitätsbewertung auch für die alternative Systemsoftware eingeholt wird.

Die ISPA möchte darauf hinweisen, dass um solche innovative Nutzung von WLAN Technologie auch in Zukunft weiterhin zu ermöglichen, es essentiell ist, den Nutzern weiterhin ein gewisses Maß an technischem Spielraum – durch Anwendung freier Software - zu bewahren.

## **6. Keine rechtliche Inanspruchnahme der Provider für Manipulationen durch Kunden**

Die ISPA möchte festhalten, dass Provider jedenfalls immer gesetzeskonform tätig sind, dies auch deswegen um Funkstörungen zu vermeiden, und - sofern sie nicht ausnahmsweise den Pflichten des Herstellers gemäß § 8 FMAG unterliegen - keinesfalls für die nachträgliche Manipulation der Geräte durch die Kunden (Besitzer) verantwortlich gemacht werden können.

## **7. Abschottung des österreichischen Marktes soll vermieden werden**

Gemäß § 4 FMAG hat der Hersteller dafür zu sorgen, dass Funkanlagen nur dann in Verkehr gebracht werden, wenn sie so konstruiert sind, dass sie in mindestens einem Mitgliedstaat der EU betrieben werden können. Sofern Geräte nun für den österreichischen Markt produziert werden und die Funkbausteine physisch dementsprechend konstruiert sind, dass nur die hierorts zulässigen Funkbereiche genutzt werden können, ist zu befürchten, dass dies auch zu einem Rückgang beim Wettbewerb und zu höheren Preisen der Geräte führt.

Die ISPA möchte betonen, dass jedenfalls eine Abschottung des österreichischen WLAN-Marktes durch Gebundenheit an bestimmte Hersteller bzw. umgekehrt die geographische Gebundenheit des WLAN-Equipments vermieden werden soll.

## **8. Sämtliche Gerätefunktionalitäten sollten allen Wirtschaftsakteuren gleichermaßen offen stehen**

Die ISPA möchte ferner darauf hinweisen, dass einzelne Hersteller von Funkanlagen ihre Geräte derzeit so konfigurieren, dass bestimmte Gerätefunktionen, welche zur Erfüllung gesetzlicher Vorgaben notwendig sind (z.B. Empfang und Anzeige von SMS bzw. Roaming SMS auf Grundlage des § 4 Abs. 1 KostbeV) zusätzlicher bilateraler vertraglicher Vereinbarungen bedürfen, welche in der Regel mit zusätzlichen Kosten verbunden sind.

Aus diesem Grund regt die ISPA an, eine entsprechende Bestimmung in den Gesetzesentwurf aufzunehmen (z.B. im Rahmen von § 3 des Entwurfes welcher die grundlegenden Anforderungen für Funkanlagen enthält). Hierdurch soll sichergestellt werden, dass Funkanlagen so gebaut und konfiguriert werden, dass alle Gerätefunktionalitäten allen Wirtschaftsakteuren gleichermaßen offen stehen.

## 9. Die Weiterverwendung bereits bestehender Funkanlagen darf nicht eingeschränkt werden

Die ISPA begrüßt, dass gemäß § 36 Abs. 2 des Entwurfes, Funkanlagen die mit der bisherigen Rechtslage im Einklang stehen und die vor dem 13. Juni 2017 in Verkehr gebracht werden, weiterhin auf dem Markt bereitgestellt werden dürfen. Die ISPA spricht sich dafür aus, dass diese Bestimmung keinesfalls eingeschränkt werden sollte um weiterhin ein maximales Maß an Flexibilität bei der Nutzung von Funkanlagen zu gewährleisten.

Die ISPA ersucht um die Berücksichtigung ihrer Bedenken und Anregungen bei der Gestaltung des Gesetzesentwurfes.

Für Rückfragen oder weitere Auskünfte stehen wir jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen,

ISPA - Internet Service Providers Austria


 A handwritten signature in black ink, appearing to read "Schubert".

Dr. Maximilian Schubert

Generalsekretär

Die ISPA – Internet Service Providers Austria – ist der Dachverband der österreichischen Internet Service-Anbieter und wurde im Jahr 1997 als eingetragener Verein gegründet. Ziel des Verbandes ist die Förderung des Internets in Österreich und die Unterstützung der Anliegen und Interessen von über 200 Mitgliedern gegenüber Regierung, Behörden und anderen Institutionen, Verbänden und Gremien. Die ISPA vertritt Mitglieder aus Bereichen wie Access, Content und Services und fördert die Kommunikation der Marktteilnehmerinnen und Marktteilnehmer untereinander.