Digital Society.at
... changing the digital world together!

Digital Society | ·Graben 17/10 | A-1010 Wien

Digital Society
Graben 17/10
A-1010 Wien

+43 1 314 22 33-0
Info@DigiSociety.at

per E-Mail an
JD@bmvit.gv.at
begutachtungsverfahren@parlament.gv.at

Wien, 15.August 2016

**Betreff: Stellungnahme zum Entwurf des Bundesgesetz betreffend die Marktüberwachung von Funkanlagen (FunkanlagenMarktüberwachungs-Gesetz – FMAG)**

Sehr geehrte Damen und Herren,

Die Digitalisierung unserer Gesellschaft bringt umwälzende Veränderungen für die gesamte Gesellschaft, ob im privaten Umfeld oder für Unternehmen. Die **Digital Society** beschäftigt sich mit den Auswirkungen dieser Veränderungen auf die Gesellschaft, analysiert diese gemeinsam mit Experten und erarbeitet politische Lösungen für aktuelle gesellschaftliche Probleme.
Wir erlauben uns, im Sinne unserer Ziele im Folgenden zum Gesetzesentwurf Stellung zu nehmen.
Wir haben die in den Erläuterungen und im Gesetzestext festgehaltenen Vorgaben analysiert und hinsichtlich ihrer logischen Konsistenz und besonders ihrer technischen Machbarkeit und wirtschaftlichen Auswirkungen untersucht.

## Analyse des Störpotentials

Das FMAG bezweckt, dass Funkanlagen so konstruiert sein müssen, dass sie sowohl eine effiziente Nutzung von Funkfrequenzen gewährleisten als auch funktechnische Störungen verhindern.
Der Begriff Funkanlage ist sehr weit gesteckt. So fallen z.B. Wireless LAN Access Points, Notebooks mit WLAN oder UMTS Schnittstelle, Kraftfahrzeuge mit integrierter SIM Karte – oder in Zukunft alle IoT-fähigen Geräte vom Kühlschrank bis zum fernüberwachten Fahrstuhl in diese Kategorie.
Das BMVit hat die Möglichkeit, durch Verordnungen Klassen oder Kategorien von Funkanlagen festzulegen und für diese unterschiedliche Maßnahmen zur Erreichung der Störungsvermeidung vorzuschreiben.
Funkanlagen sind nach ihrer Sendestärke zu unterscheiden. Der Einfluss einer Funkanlage nimmt quadratisch mit der Entfernung ab ($1/r^2$-Gesetz). Für Funkanlagen mit geringer Sendestärke ergibt sich ein Einflussbereich von nur wenigen Metern. Selbst wenn so eine Funkanlage Störungen verursacht, so ist durch die geringe Reichweite davon auszugehen, dass

hauptsächlich andere Geräte des Besitzers der Funkanlage gestört werden und kaum Geräte anderer Personen.
Wir halten es wichtig, dass dieser Umstand bei der Kategorisierung der Funkanlagen berücksichtigt wird und schlagen daher vor, eine entsprechende Analyse bereits im Gesetz vorzuschreiben, beispielsweise "*Die Kategorisierung der Funkanlagen hat die technischen Gegebenheiten und besonders das effektive Störpotential der Funkanlage zu berücksichtigen.*"

## Maßnahmen zur Verhinderung der Manipulation der Funksoftware werden grundsätzlich Software Installationen auf diesen Geräten verhindern

Eine mögliche Maßnahme zur Störungsverhinderung ist, dass der Hersteller (bzw. in Verkehrbringer) sicherzustellen hat, dass nur solche Software geladen werden kann, für die die Konformität in Verbindung mit der Funkanlage im Vorhinein nachgewiesen wurde und die nicht im Nachhinein durch den Benutzer manipuliert werden kann. Hierzu haben die Hersteller dieser Funkanlagen (die Kombination aus Hardware und Software) jeweils eine Konformitätsbewertung nach §11 Abs. 1 FMAG durchzuführen.
Da viele Geräte in diesem Segment (in Zukunft vermutlich noch viel mehr im Bereich des Internet of Things) vor allem aus Einplatinencomputern bestehen, ist eine Trennung der Software für den Mobilteil von der generellen Betriebssoftware des Gerätes kaum machbar. Die Hersteller werden daher nur die Gesamtheit des Systems einer Konformitätsbewertung zuführen können.
Auch werden Hersteller schon aus dem Grunde sich vor befürchteten Haftungen abzusichern jegliche Softwareänderungen an den Geräten verbieten, statt Gefahr zu laufen eine Hintertüre offen zu lassen. So eine Softwareänderung wäre beispielsweise ein Update für neue Funktionalitäten oder die Behebung von erkannten Sicherheitsmängel, die wiederum Konfigurationsänderungen der Funkanlage mit sich bringen.
Dies hat zur Folge, dass es für den Eigentümer der Funkanlage juristisch, aber möglicherweise auch technisch unmöglich wird, eine Alternativsoftware aufzuspielen, selbst wenn diese über eine Konformitätsbewertung verfügt. Eine solche Einschränkung stellt einen schweren Eingriff in die Eigentumsfreiheit des Besitzers der Frunkanlage dar, hat darüber hinaus aber noch weitere Auswirkungen.

## Eine Einschränkung der Änderung an Geräten führt zur Verhinderung von Innovation und schädigt dadurch den Wirtschaftsstandort.

Die Praxis zeigt: In vielen Bereichen sind innovative Lösungen durch das Einspielen alternativ entwickelter Router-Software entstanden. So ist beispielsweise der Betrieb des Funkfeuer-Netzwerkes in Wien nur durch den Betrieb mit Routern mit einer solchen alternativen Software möglich geworden. Derartige innovative Lösungen werden in Zukunft durch das Abdrehen der Möglichkeit zur Softwareänderung, die  dieses Gesetz wie oben argumentiert impliziert, verunmöglicht.
Gerade der Themenbereich Internet of Things ist ein riesiger Wachstumsbereich, der vor allem aus intelligenten über Funknetzwerke verbundene Mikrocomputer bestehen wird. Die Hemmnisse bei der Verwendung alternativer Software auf solchen Geräten werden nachhaltig der Innovationskraft in Österreich und Europa schaden.

## Maßnahmen zur Verhinderung nachträglicher Manipulation werden die Freiheit von Konsumenten einschränken.

Die geplanten Maßnahmen zur Verhinderung der nachträglichen Manipulation werden die Verwendung alternativer Firmware für die Geräte verhindern. Daher können von Konsumenten – wie bisher gewohnt – keine alternativen Softwaresysteme auf Routern mit WLAN Funktionalität oder UMTS Routern mehr eingesetzt werden, da die Einspielung dieser Software in Zukunft vom Hersteller verhindert werden muss.
Diese alternativen Softwaresysteme stellen in vielen Bereichen wesentlich mehr Funktionalität zur Verfügung als die Software der Hersteller. Konsumenten haben daher in Zukunft nicht mehr die Freiheit, diese Funktionalitäten zu nutzen.

## Konformitätsbewertung von Alternativsoftware

Es ist davon auszugehen, dass Hardwarehersteller keinerlei Anreiz haben, eine Konformitätsbewertung für Drittsoftware durchzuführen, da diese kostenintensiv ist und für den Hersteller relativ wenig Nutzen hat. Im Gegenteil könnte aus der Konformitätsbewertung der Softwarekombination eventuell auch eine Haftung oder Garantie des Herstellers für die Funktionsfähigkeit dieser Software in anderen Bereichen abgeleitet werden. Auch dies schränkt die Nutzung alternativer Software ein und führt zu weniger technischen Vielfalt und weniger Innovation.

## Benachteiligung im Markt für kleine Unternehmen und Startups

Die gefordeten Konformitätsbewertungen werden durch die hohen Kosten - die bei jedem Software Update durch die neuerliche Konformitätsbewertungen anfallen - verhindern, dass kleine Unternehmen und Startups in diesem Bereich in Österreich tätig werden können. Dies reduziert die Vielfalt am Markt und ist innovationshemmend.

## Probleme für Internet Provider wenn der Hersteller keine Updates zur Verfügung stellt.

Wenn ein Internet Service Provider (ISP) in seinem Netz eine große Anzahl gleichartiger Geräte einsetzt – bei denen eine Software Lücke (Sicherheitsproblem) auftaucht – und der Hersteller keine Updates mehr zur Verfügung stellt (wegen der immer kürzer werdenden Produktzyklen) – so hat der Provider nur die Möglichkeit die gesamte Hardware auszutauschen. Dies führt mit Sicherheit zu höheren Kosten für den Konsumenten, aber auch zu einem schwer kalkulierbaren finanziellen Risiko für den Provider.
Es ist auch unwahrscheinlich, dass ein ISP in einem solchen Falle eine Konformitätserklärung für eine alternativ eingespielte Software beibringen könnte. Selbst wenn es ihm technisch möglich wäre eine solche Software zu entwickeln, hätte er jedoch in der Regel nicht den notwendigen Zugriff auf technische Unterlagen (Schaltpläne, Konstruktionszeichnungen, etc.) um eine solche Konformitätsbescheinigung zu beantragen.

## Folgeprobleme für den Konsumenten

Wenn der Hersteller also eine vorhandene Sicherheitslücke eines z.B. WLAN Routers nicht schließen will, und ein ISP eine solche nicht schließen kann, hat der Kunde kaum Alternativen. In vielen Fällen ist es einem Endkunden nämlich nicht möglich sein vom ISP zur Verfügung

gestelltes Modem durch ein eigenes zu ersetzen. Letztlich kann der Kunde nur entweder mit der Sicherheitslücke leben oder den Provider wechseln. Da das Wechseln zu einem anderen Provider mit nicht unerheblichem Aufwand verbunden ist, wird sich der Kunde hauptsächlich für das Ignorieren der Sicherheitslücke entscheiden.
Ein Gesetz jedoch, das durch seine indirekten Auswirkungen zu einer weiteren Verschlechterung der Sicherheitslage beiträgt, ist aus unserer Sicht abzulehnen.

## Lösungsvorschlag

Diese Probleme könnten relativ leicht entschärft werden, indem Funkanlagen mit geringer Leistung (dazu sollten WLAN-Router und andere Haushaltsapplikationen zählen), bei denen das Potiential zur Störung - wie anfangs argumentiert - relativ gering ist, dezidiert von der Notwendigkeit einer Konformitätsbescheinigung der Software (nicht aber der Hardware, Stichwort maximale Sendeleistung) und damit von einer Sperrpflicht für Software-Updates ausgenommen werden.

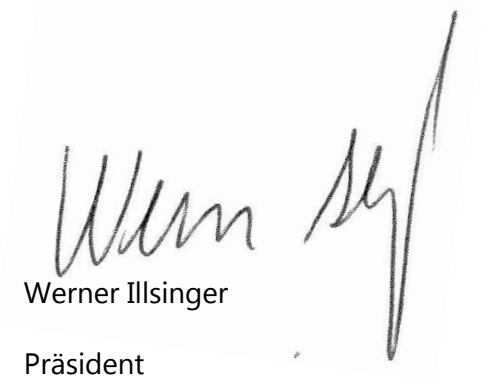
## Fazit

Aus all den obenstehenden aufgeworfenen Fragen kann nur der Schluss gezogen werden dass es weiterer Analysen der Auswirkungen des Gesetzesvorschlags bedarf. Die aufgelisteten Problempunkte zeigen deutlich, wie komplex die Thematik ist und wie viele Details noch zu klären sind.

Wir hoffen, mit diesen Kommentaren einen wertvollen Beitrag geliefert zu haben und stehen für Rückfragen gerne zur Verfügung.

Mit freundlichen Grüßen,

Roland Giersig
Vizepräsident
**Digital Society**



Werner Illsinger
Präsident
**Digital Society**