Universität Erfurt
Rechtsamt
Nordhäuser Straße 63
99089 Erfurt
Fax: +49 361 737-5079

W I D E R S P R U C H

des Herrn Marcel Langner, [redacted]
wegen: Auskunftsversagen (Landesinformationsfreiheitsgesetz – LIFG)

1. Sachverhalt

Ihre Hochschule verweigert die Aussage darüber, ob Sie Störungen auf fremde WLAN Signale mithilfe von Deauthenticationpaketen vornehmen (https://fragdenstaat.de/a/170362).
Sie nennen als alleinigen Ablehnungsgrund § 7 Abs. 1 Nr. 6 ThürIFG.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit folgt Ihren Aussagen.

2. Rechtliche und technische Wertung

Sowohl technisch, als auch rechtlich kann ich den Aussagen nicht folgen. Vorangestellt sei zu bemerken, dass ich keine detaillierten Konfigurationsdetails der WLAN Infrastruktur angefragt habe, sondern lediglich wissen möchte, ob Sie mithilfe von Deauthenticationpaketen an Ihrer Hochschule andere WLAN Signale aktiv stören und so in die Frequenznutzung eingreifen. Ebenso sei auf die Widerspruchsfrist von einem Jahr hinzuweisen, aufgrund fehlender bzw. wirksamer Rechtsbehelfsbelehrung.
Zusätzlich zu den von mir bereits in der Anfrage genannten Aspekten möchte ich folgendes hinzufügen.

Befugnis zur (aktiven) Gefahrenabwehr („Hackback“)
Eine eventuelle Nutzung der Funktion eines Rogue Accespoint Containments mithilfe von Deauthenticationpaketen, stellt einen direkten Eingriff in die Nutzung einer Frequenz im Rahmen eine Allgemeinzuteilung dar. Ausübung von Macht dieser Art ist alleinig den Ordnungsbehörden vorbehalten.
Eine Hochschule hat zur Nutzung einer solchen Funktion keine Befugnis. Eine Hochschule kann daher eine Ablehnung auch nicht mit § 7 Abs. 1 Nr. 6 ThürIFG begründen, da ohne Befugnis gar kein Bezug herzustellen ist.

Gefahr im Sinne der öffentlichen Ordnung und Sicherheit
Zur Argumentation mit § 7 Abs. 1 Nr. 6 ThürIFG, ist auch eine Gefahr in einem Umfang erforderlich, die eine Argumentation in diesem Rahmen erlauben würde.
Selbst einer Argumentation mit einer im Rechtsrahmen gerade noch akzeptablen Grundlage einer abstrakten Gefahr, mangelt es an Substanz.
In der vielzitierten Entscheidung des VGH Mannheim zum Alkoholverbot in Teilen der Freiburger Innenstadt (Urteil vom 28.07.2009 – 1 S 2200/08) wird der Begriff der abstrakten Gefahr wie folgt definiert:

> *„[…] eine abstrakte Gefahr ist gegeben, wenn eine generell-abstrakte Betrachtung für bestimmte Arten von Verhaltensweisen oder Zuständen zu dem Ergebnis führt, dass mit*

> *hinreichender Wahrscheinlichkeit ein Schaden im Einzelfall einzutreten pflegt und daher Anlass besteht, diese Gefahr mit abstrakt generellen Mitteln, also einem Rechtssatz, zu bekämpfen.* ***Auch die Feststellung einer abstrakten Gefahr verlangt mithin eine in tatsächlicher Hinsicht genügend abgesicherte Prognose: es müssen – bei abstrakt-genereller Betrachtung – hinreichende Anhaltspunkte vorhanden sein, die den Schluss auf den drohenden Eintritt von Schäden rechtfertigen. Der Schaden muss regelmäßig und typischerweise, wenn auch nicht ausnahmslos, zu erwarten sein.*** *"*

Ihre Hochschule argumentiert mit einer nicht näher spezifizierten Gefahr:

> *..nach eingehender Prüfung Ihrer Anfrage teile ich Ihnen mit, dass eine Auskunft auf der Grundlage des zum Zeitpunkt Ihrer Anfrage geltenden Thüringer Informationsfreiheitsgesetzes (THürIFG) nicht erteilt werden kann, weil die Preisgabe der gewünschten Informationen nachteilige Auswirkungen auf die öffentliche Sicherheit haben kann (vgl. § 7 Abs. 1 Nr. 6 ThürIFG).*
> *Hintergrund ist, dass durch eine Offenbarung der technischen Einstellungen des WLAN-Netzes der Universität Erfurt das Risiko geschaffen wird, dass diese Informationen gezielt für Angriffe auf die IT-Infrastruktur der Universität genutzt werden.*

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit interpretiert daraus:

> *Die Universität Erfurt hat zum o. g. Sachverhalt Stellung genommen und dem TLfDI mitgeteilt, dass Ihnen der Antrag auf Informationszugang vom 13.11.2019 aufgrund des § 7 Abs. 1 Nr. 6 Thüringer Informationsfreiheitsgesetz (ThürIFG) abgelehnt wurde, da die Offenlegung der technischen Einstellungen des Wlan Netzes das Risiko begründet, dass potentielle Angreifer die offenbarten Informationen für Angriffe auf die IT Infrastruktur der Universität nutzen.*

ergänzt um eine Antwort auf die Frage, ob der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit die Nutzung einer solchen Funktion als Stand der Technik ansieht:

> *Der TLfDI sieht die Technik der De-Authentisierung als gültige Maßnahme zum Schutz der IT-Infrastruktur an. Dies umfasst auch, dass dies eine angemessene Maßnahme nach Art.32 DSGVO darstellen kann.*

Bereits der (Gefahren) Prognose mangelt es an hinreichenden Anhaltspunkten. Es ist unbestritten, dass ein möglicher Schaden eintreten kann (ebenso, wie ein Angriff von Aliens), erfolgt jedoch nicht mit der notwendigen Regelmäßigkeit oder typischerweise auftretender Häufigkeit. Die dafür notwendigen Nachweise haben Sie nicht erbracht. In einer gerichtlichen Prüfung werden diese Nachweise und die damit verbundene Intention des angeblichen Angreifers vorzulegen sein und den (auszugsweise) folgenden Argumenten entgegenstehen.
Als Nachweis meiner Argumentation sei auf meine noch nicht abgeschlossenen Forschungen (https://www.MeineHochschuleBehindertDasWLAN.de) verwiesen, bei denen ein überwiegender Anteil der deutschen Hochschulen (und damit der Experten) keine Bedenken sieht. Auch in Thüringen, sind Sie die einzige Hochschule bisher.
Ebenso sei verwiesen auf die Stellungnahme des Hessischen Landesbeauftragten für Datenschutz und Informationsfreiheit, der ebenso keine Bedenken hat und den Hochschulen eine entsprechende Auskunft anrät (siehe Anlage 1). Noch kritischer sieht es die Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (siehe Anlage 2).

Auch auf die Stellungnahme der Bundesnetzagentur (siehe Anlage 3) sei verwiesen, die die Maßnahme als nicht gültig im Rahmen gesetzlicher Maßgaben ansieht und damit dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit widerspricht.

Damit im Einklang steht die Einschätzung des Bundesverwaltungsgerichtes (Urteil vom 20.10.2016 - BVerwG 7 C 23.15) bezüglich der Relevanz einer Gefahr:

> *In Anwendung dieses Maßstabs ist eine Gefährdung der öffentlichen Sicherheit unter dem Gesichtspunkt ordnungsgemäßer Aufgabenerledigung nicht erst dann zu bejahen, wenn die informationspflichtige Stelle ihrer Funktion voraussichtlich überhaupt nicht mehr gerecht werden könnte, sondern schon dann, wenn die effektive Aufgabenerledigung gestört und die Arbeit der betroffenen Bediensteten beeinträchtigt werden kann. Bereits ein derartiger Geschehensablauf ist geeignet, sich nachteilig auf die Funktionsfähigkeit des Beklagten auszuwirken. Für eine Gefährdung von Individualrechtsgütern der Beschäftigten reichen - wie das Berufungsgericht zutreffend ausgeführt hat - nicht bereits fernliegende Befürchtungen aus;* ***vielmehr müssen konkrete Umstände oder allgemeine Erfahrungswerte eine hinreichende Wahrscheinlichkeit von Beeinträchtigungen begründen****.*

Ihre Hochschule argumentiert mit einer theoretisch möglichen Gefahr, für die Sie keine konkreten Umstände vorgelegt haben oder für die keine allgemein anerkanntem Erfahrungswerte existieren. Dies wird durch die Meinung der vielen anderen zuvor genannten Experten, die Auskunft erteilen, gestützt.
Letztlich kann man immer einen Fall konstruieren, wie eine Information dazu genutzt werden kann, um Schaden anzurichten. Selbst die Information über die Farbe der Gehäuse Ihrer Accesspoints ist nutzbar, um die Wellenlänge eines Lasers optimal bestimmen zu können, um damit die Elektronik im Gerät zerstören zu können, weil mit der gewählten Wellenlänge das Gehäuse am besten zu durchdringen ist.
Ich sehe keine hinreichenden Anhaltspunkte für eine substantielle Gefahr, die eine Ablehnung auf Basis der öffentlichen Sicherheit erlauben würden.

<u>Geheimnisbegriff</u>
Jeder kann mit trivialsten Mitteln ermitteln, ob Störungen vor Ort stattfinden. Dies kann im einfachsten Fall dadurch getestet werden, indem man mit seinem Mobilfunkgerät oder Laptop einen mobilen Accespoint (auch als Tethering bezeichnet) aktiviert. Diese Funktion ist in alle modernen Geräte eingebaut. Dann kann man sich mit einem zweiten Gerät verbinden und testet die Stabilität der Verbindung. Sollte diese Stabilität (je nach Einstellung der Rogue Accesspoint Funktion) früher oder später beeinträchtigt werden, was daran zu erkennen ist, dass man trotz geringer Entfernung immer wieder aus dem mobilen WLAN getrennt wird, ist von einer Störung auszugehen. Mit einem normalen Laptop und der freien Software Wireshark, lassen sich die Störpakete auch direkt nachweisen. Es soll auf den Geheimnisbegriff des GeschGehG verwiesen werden (der in Ermangelung einer Alternative jedoch nur für Geschäftsgeheimnisse gilt, jedoch trotzdem angemessen erscheint):

> *§ 2 Begriffsbestimmungen*
> *Im Sinne dieses Gesetzes ist*
> *1. Geschäftsgeheimnis eine Information*
> *a)* ***die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile*** *den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen,* ***allgemein bekannt oder ohne Weiteres zugänglich ist*** *und daher von wirtschaftlichem Wert ist und*

Wie dargelegt, kann die Erkenntnis darum, ob die Hochschule Störungen vornimmt oder nicht trivial ermittelt werden. Das Geheimnis ist daher keines, da die Information ohne Weiteres zugänglich ist. Nur noch ergänzend sei erwähnt, dass zur Ermittlung des Geheimnisses keinerlei rechtswidrige Handlungen nötig sind. Das inkludiert im Besonderen das Errichten eines Accesspoints, welches jedem freien Bürger erlaubt ist. Auch auf dem Gelände der Hochschule Erfurt.

3. ergänzende Angaben

Rogue Accesspoint
Gemeinhin wird ein Rogue Accesspoint nur dann so bezeichnet, wenn er den gleichen WLAN Namen ausstrahlt, wie das ursprüngliche WLAN Netzwerk. Uneinigkeit besteht darin, ob der Rogue erst dann zum Rogue wird, wenn dieser auch physisch mit dem Netzwerk des anzugreifenden Netzwerkes verbunden ist (z.B über ein Kabel). Ebenso unklar ist, ob auch ähnlich klingende Namen, die leicht verwechselt werden können, auch als Rogue angesehen werden. Unstrittig ist jedoch, dass die Aufstellung des Accesspoints mit rechtswidriger Intention, als Rogue zu bezeichnen ist.
Da WLAN Netzwerke Frequenzen im Rahmen einer Allgemeinzuteilung der Bundesnetzagentur nutzen, stehen diese Frequenzen jedem entsprechend dieser Allgemeinzuteilungen zur Nutzung zur Verfügung. Innerhalb dieser Regelungen ist keine Beschränkung für die Namensvergabe vorgesehen. Ein WLAN Netzwerk eines Besuchers vor Ort (z.B. durch einen LTE Hotspot), darf daher durchaus auch den gleichen (oder ähnlichen) Namen ausstrahlen, wie sie die Hochschule nutzt. Das impliziert jedoch keine rechtswidrige Intention.
Dieser Accesspoint eines Besuchers würde dann, sofern man der Argumentation der Hochschule folgt, aktiv durch die Hochschule angegriffen, obwohl die Intention des Aufstellenden ungeklärt ist.

Eine Ablehnung mit der Herstellung der öffentlichen Sicherheit und Ordnung muss angemessen und zielgerichtet sein. Das ist hier nicht gegeben.

Rechtmäßigkeit der Maßnahme
Die Bundesnetzagentur bestätigt die Rechtswidrigkeit der Maßnahme (siehe Anlage 3).

Das Aussenden von Deauthenticationpaketen kann nur deshalb überhaupt vereinzelt eine Wirkung zeigen, weil eine Designschwäche im WLAN Protokoll WPA2 ausgenutzt wird. Hier wäre eine mögliche Strafbarkeit nach § 303b StGB:

> *„Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er[...]Daten in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt[...]wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.“*

und § 202b StGB:

> *„Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.“*

einschlägig. Die Relevanz ergibt sich hier daraus, dass der Angriff auf ein anderes WLAN nur funktioniert, wenn dabei die MAC Adresse (eine eindeutige ID jedes WLAN Gerätes) des

Anzugreifenden erfasst wird und dann durch den Störenden selbst genutzt (und damit das Fälschen der eigenen MAC Adresse) wird.

Sofern man mit Belangen der öffentlichen Ordnung und Sicherheit argumentiert, können diese nur auf rechtskonforme Maßnahmen gestützt sein. Das ist beim Aussenden von Deauthenticationpaketen nicht der Fall.

Wirksamkeit der Maßnahme
Auch die technische Wirksamkeit der Maßnahme ist nicht gegeben. Hier vertritt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit eine andere Ansicht, sofern mit *„gültig“* der technische Aspekt gemeint war.

Der durch die Hochschule beschriebene Angriffsfall ist nicht auf die geografische Position der Hochschule beschränkt, sondern kann weltweit, also auch an anderen Hochschulen (die nachweislich keine Störungen durchführen) durchgeführt werden.

Ein eventueller Angreifer wird konsequenterweise davon ausgehen, dass die Hochschule sich an die Regelungen der Bundesnetzagentur hält und keine Störungen vornimmt. Dieser Angreifer wird doch dann nicht vermehrt (oder in besonderem Maße) angreifen, wenn die Hochschule bestätigt, sich an Recht und Gesetz zu halten, da dies ja bereits seine ursprüngliche Annahme war.

Ein Angreifer, der feststellt, dass auf dem Gelände mithilfe von Deauthenticationpaketen gestört wird, wird dann (sicherlich nicht erst dann) eine Funktion (PMF) in seinem Accesspoint aktivieren, die dafür sorgt, dass die durch eine Hochschule ausgesandten Störpakete keine Wirkung zeigen.
Weiterhin ist der neue WLAN Standard WPA3 bereits in der weltweiten Ausrollung (Nachrüstung durch Software Update). Innerhalb dieses Standards ist die Ausnutzung der zugrundeliegenden Schwachstelle nicht mehr möglich.

Auch aufgrund einer mangelnden (nicht existenten) Wirksamkeit der Maßnahme, kann daher nicht mit Belangen der öffentliche Sicherheit argumentiert werden, da diese ja dadurch nicht wirksam geschützt wird.

Nur noch zusätzlich nutzen Störungen bis zu 20% der verfügbaren WLAN Bandbreite, die dann anderen Nutzern (auch Ihrer Hochschule) nicht mehr zur Verfügung steht.

4. Ergebnis
Der Widerspruch ist zulässig und begründet.
Ihrer und der Auffassung des TLfDI scheint ein Großteil Deutschlands nicht zu folgen.
Ich bitte um technische und rechtliche Prüfung und rechtsmittelfähige Bescheidung in Schriftform bis zum 31.07.2020.

[redacted] 22.06.2020

[redacted]

Marcel Langner

Anlage 1: Stellungnahme des Hessischen Landesbeauftragten für Datenschutz und Informationsfreiheit

DER HESSISCHE BEAUFTRAGTE
FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT

DER HESSISCHE BEAUFTRAGTE
FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT
Postfach 31 63 · 65021 Wiesbaden

Herrn
Marcel Langner
[redacted]

Aktenzeichen *Bitte bei Antwort angeben* 90.19.35:0058-pi/bk
zuständig Durchwahl 14 08 - [redacted]
Ihr Zeichen
Ihre Nachricht vom 28.11.2019
Datum 17.02.2020

Ihre WLAN-Anträge

Sehr geehrter Herr Langner,

den hessischen Hochschulen wird (so die Position unserer Technikabteilung) vorgeschlagen, Ihre Auskunftsanfrage generell so zu beantworten, dass die Nutzung der WLAN-Netze der Hochschule ausschließlich im Rahmen der Vorgaben der aktuell veröffentlichten Allgemeinzuteilungen erfolgt, § 55 Abs. 2 Telekommunikationsgesetz Gegebenenfalls kann mit der Antwort konkretisierend auf den in beiden Allgemeinzuteilungen gleichen Absatz Bezug genommen werden: Aussendungen, die absichtlich bestimmungsgemäße WLAN-Nutzungen stören oder verhindern, wie z.B. Aussenden von Funksignalen und/oder Datenpaketen, die die Abmeldung oder Beeinflussung von WLAN-Verbindungen anderer Nutzer gegen deren Willen zum Ziel haben, sind nicht gestattet und werden an der Hochschule nicht eingesetzt.

Mit freundlichen Grüßen
Im Auftrag
[redacted]

Anlage 2: Stellungnahme des Stellungnahme der Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz

Der Landesbeauftragte für den Datenschutz
und die Informationsfreiheit Rheinland-Pfalz

Internet: www.datenschutz.rlp.de
E-Mail: poststelle@datenschutz.rlp.de
Telefon: (06131) 208 2588
Telefax: (06131) 208 2497

Datum: 03.06.2020
Gesch.Z.: [redacted]

Ihr Zeichen:

[redacted]

Informationsfreiheitsrechtliche Beschwerde [redacted]

Ihre E-Mail vom 25. Mai 2020

Sehr geehrte [redacted]

in dem oben bezeichneten Beschwerdeverfahren habe ich die Antwort von [redacted] an [redacted] vom 19. Mai 2020 dieser E-Mail als Anhang beigefügt. Diese sowie die weitere Korrespondenz zu der Anfrage von [redacted] ist zudem öffentlich abrufbar unter https://fragdenstaat.de/anfrage/wlan-der-hochschule-mainz/. [redacted] hat im Rahmen seiner Antwort zwar ausdrücklich darauf hinwiesen, dass er einer Veröffentlichung dieser E-Mail nicht zustimme. Die Plattform FragDenStaat legt jedoch weder seinen Namen offen, noch ist die Antwort auf anderem Wege auf [redacted] bezogen oder beziehbar. Somit weist die Veröffentlichung keinen Personenbezug auf und ist damit datenschutzrechtlich nicht zu beanstanden.

Im Rahmen seiner Antwort erteilt [redacted] keine Auskunft und begründet seine Entscheidung damit, dass sich ihre Anfrage auf eine Konfigurationseinstellung beziehe, die im Rahmen der IT-Sicherheit eines Systems eingesetzt würde. Durch diese Antwort hat [redacted] den Antrag von [redacted] nach § 12 Abs. 4 S. 1 Landestransparenzgesetz Rheinland-Pfalz (LTranspG) vollständig abgelehnt. Nach meinem gegenwärtigen Kenntnisstand der Sachlage verwirklicht das Vorbringen von [redacted] jedoch keinen dem Antrag auf Informationszugang entgegenstehenden Belang nach § 14 ff. LTranspG.

Nach § 14 Abs. 1 S. 2 Nr. 7 LTranspG soll ein Antrag auf Informationszugang abgelehnt werden, soweit und solange das Bekanntwerden der Information der IT-Sicherheit oder der IT-Infrastruktur schaden könnte. Dokumentationen zur IT-Infrastruktur sowie IT-Sicherheitskonzepte stellen ein erhebliches Risiko für die Sicherheit der IT-Systeme der Landesverwaltung dar. Diese können wesentliche Hinweise auf eingesetze Hard- und Software, Netzstrukturen und Kommunikationsverbindungen geben, die gezielt Angriffe auf die IT-Systeme der Landesverwaltung ermöglichen würden (Gesetzesbegründung zum LTranspG, S. 44). Vorliegend ist jedoch nicht ersichtlich, dass die Beauskunftung der Anfrage von [redacted] das Risiko eines Angriffs auf die IT-Systeme der Hochschule Mainz hervorruft. [redacted]

erkundigte sich nach dem Vorhandensein einer Einstellung, womit z.B. durch eine Rogue Accesspoint Containment Funktion andere WLAN-Signale mithilfe von Deauth/Deassociationspaketen gestört werden. Da bei einer solchen Einstellung die Störung nicht von einem externen Angreifer, sondern von der Hochschule Mainz selbst ausginge, ist nicht ersichtlich, wieso die Bekanntgabe einer solchen Funktion geeignet wäre, einen Angriff auf die IT-Systeme der Hochschule zu ermöglichen.

Zudem möchte ich Sie darauf hinweisen, dass § 14 Abs. 1 S. 2 LTranspG als Soll-Vorschrift ausgestaltet ist. Dies bedeutet, dass der Antrag auf Informationszugang bei Vorliegen der tatbestandlichen Voraussetzungen im Regelfall abzulehnen ist bzw. die Veröffentlichung zu unterbleiben hat. Im Ausnahmefall, nämlich bei einer atypischen Fallgestaltung oder besonderen Umständen, kann ein Informationszugang erfolgen, sofern keine anderen entgegenstehenden Belange vorliegen. Nach Maßgabe des § 17 ist jedoch immer eine Abwägung vorzunehmen, ob im vorliegenden Fall besondere Gründe ausnahmsweise für einen Informationszugang sprechen (Verwaltungsvorschrift zum LTranspG, Nr. 14.1.2). Die Antwort von [redacted] lässt nicht erkennen, dass die Hochschule Mainz das ihr durch diese Vorschriften eingeräumte Ermessen erkannt und hiervon Gebrauch gemacht hat.

Darüber hinaus möchte ich Sie darauf aufmerksam machen, dass [redacted] in der Vergangenheit bereits zahlreiche gleichlautende Anfragen an weitere Hochschulen sowohl aus Rheinland-Pfalz als auch aus anderen Bundesländern gerichtet hat. Die Antworten der transparenzpflichtigen Stellen sind öffentlich aufgelistet unter https://www.meinehochschulebehindertdaswlan.de/ Wie Sie dieser Aufstellung entnehmen können, haben fast alle Hochschulen [redacted] die erbetene Auskunft erteilt.

Ich bitte Sie, zu meinen vorgenannten Sach- und Rechtsausführungen bis zum **26. Juni 2020** Stellung zu nehmen. [redacted] erhält eine Kopie dieses Schreibens.

Mit freundlichen Grüßen
Im Auftrag

[redacted]

Anlage 3: Stellungnahme der Bundesnetzagentur (ohne die erwähnten Anlagen)

Bundesnetzagentur

Außenstelle Berlin

Bundesnetzagentur • DLZ8 • Seidelstraße 49 • 13405 Berlin

[redacted]

Herrn Marcel Langer

[redacted]

Ihr Zeichen, Ihre Nachricht vom	Mein Zeichen, meine Nachricht vom	☎ 030)	Berlin
	Berl8-11 D001/00658/18	43 74-14 00 oder -12 10	04.06.2019

Rechtsgrundlage von Frequenzen in lokalen Netzwerken

Sehr geehrter Herr Langer,

vielen Dank für Ihre Anfrage.

Als Rechtsgrundlage für die Verwendung von Frequenzen in lokalen Netzwerken (WLAN-Funkanwendungen) verweise ich auf die Verfügung 10/2013 (2,4 GHz), geändert mit Vfg. 64/2018 und Vfg. 7/2010 (5 GHz) mit Vfg 65/2018.

Beide enthalten den Absatz:

„Aussendungen, die absichtlich bestimmungsgemäße WLAN-Nutzungen stören oder verhindern, wie z.B. Aussendungen von Funksignalen und/oder Datenpaketen, die die Abmeldung oder Beeinflussung von WLAN-Verbindungen anderer Nutzer gegen deren Willen zum Ziel haben, sind nicht gestattet."

Damit verstoßen WLAN-Deauther bzw. die Nutzung bestimmter Funktionen von WLAN-Access-Points (z. B.: Cisco –> Rogue Management) gegen diese Allgemeinzuteilungen.

Dies gilt selbstverständlich auch für WLAN-Netze an Hochschulen.
Ich hoffe Ihnen hiermit ausreichend geholfen zu haben.

Mit freundlichen Grüßen
Im Auftrag

Anlagen:
2 Verfügungen

[redacted]

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

Behördensitz Bonn
Tulpenfeld 4
53113 Bonn
☎ (02 28) 14-0

Telefax Bonn
(02 28) 14-88 72

E-Mail
poststelle@bnetza.de
Internet
http://www.bundesnetzagentur.de

Kontoverbindung
Bundeskasse Trier
BBk Saarbrücken
BIC: MARKDEF1590
IBAN: DE81 5900 0000 0059 0010 20

Außenstelle Berlin
Dienstgebäude
Seidelstraße 49
13405 Berlin

Telefax Berlin
(0 30) 43 74-11 80