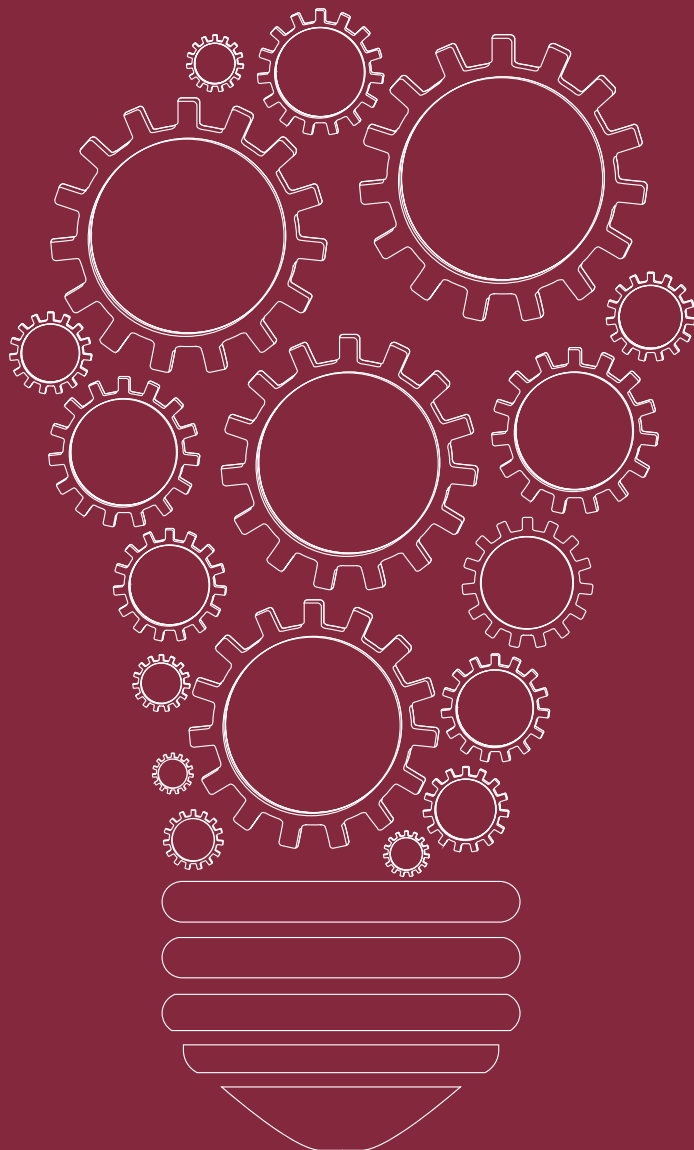


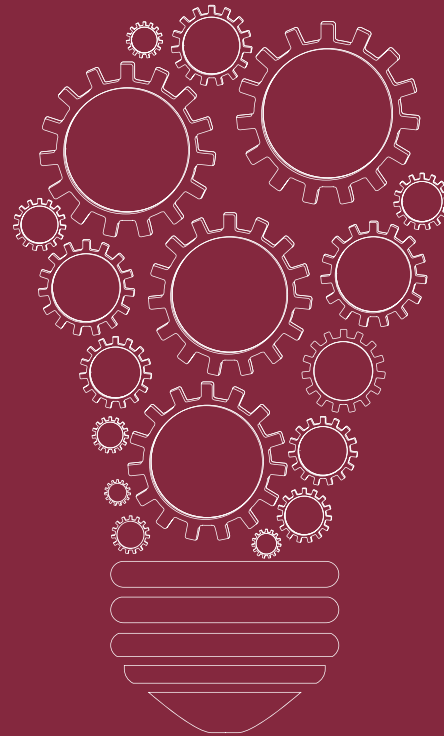
2/3|19

# News

**ispa**  
Internet Service Providers Austria



vielfältig  
Ideen skizzieren



### 03 Editorial

Von Maximilian Schubert

### 04 Digitale Ideen der österreichischen Parteien

ISPA Parteienbefragung anlässlich der Nationalratswahl 2019

### 15 DoH – Fluch oder Segen?

Das DNS over HTTPS Protokoll

### 18 »Ein neuer Besen, der ohne Struktur kehrt, ist eine riesige Staubwolke.«

Interview mit Dr. Klaus M. Steinmaurer

### 23 Digitalsteuer

Schutz für überholte Geschäftsmodelle

### 25 UN-Cybercrime-Konferenz

Zwischenstaatliche Zusammenarbeit von Behörden und ISPs

### 26 Weitreichende Umwälzungen

Der Europäische Kodex für die elektronische Kommunikation

### 28 Ausweispflicht wirkungslos gegen Hate Speech

Kritik am geplanten Gesetz über Sorgfalt und Verantwortung im Netz

### 29 SIM-Swapping

OLG lehnt Anordnung zur Duplizierung einer SIM-Karte ab

### 30 ISPA Forum 2019

Wie viel analoge Kompetenz benötigt die Digitalwirtschaft?

### 31 Rechtskonflikt zwischen DSGVO und CLOUD Act

Verhandlungen über ein transatlantisches Abkommen

### 34 CPC-Verordnung

Zukunftsweisende Umsetzung in Österreich

### 35 ISPA Academy

Breitbandförderung

### 35 »Der Online-Zoo«

ISPA Kinderbuch jetzt auch auf Portugiesisch verfügbar

### 36 Mitglieder

Stand August 2019

# Editorial



Von Maximilian Schubert

## »Erfahrung ist fast immer eine Parodie auf die Idee.«

JOHANN WOLFGANG VON GOETHE

5G ist in aller Munde und man gewinnt oftmals den Eindruck, dass dieser Begriff mehr oder weniger mit dem Begriff Infrastruktur gleichgesetzt wird. Doch 5G ist eine – ausgesprochen spannende – Technologie, die einen Ausbau der Glasfaserinfrastruktur voraussetzt. Dieser Ausbau braucht eine Vielfalt von Anbietern, Ideen und Technologien, mit einem Wort: Wettbewerb. Und zwar Wettbewerb auf allen Ebenen, nicht als Selbstzweck, sondern weil sonst schlichtweg beim Breitbandausbau nichts oder zumindest viel zu wenig passiert und wir in Bezug auf Infrastruktur weiter im lauen Mittelfeld bleiben oder noch weiter abrutschen.

Ein zweites brandaktuelles Thema ist der angeblich ›rechtsfreie‹ Raum im Internet. Ungeachtet dessen, dass dem keinesfalls so ist, diskutieren wir – manchmal recht emotional – darüber, was im Internet erlaubt sein soll und was nicht. Dabei verschwimmen jedoch im populistischen Diskurs oftmals die Grenzen zwischen Erlaubtem und Erwünschtem und ich halte diesen Trend für eine echte Gefahr für das Internet. Wenn wir alles verbieten, was uns (wen eigentlich?) irritiert oder unerwünscht erscheint, dann haben wir zwar irgendwann trotzdem die ersehnte Digitalisierung, aber eine ohne provokante Ideen und stimulierende Meinungsvielfalt. Stattdessen bekommen wir dann einen ziemlich faden Einheitsbrei, der die nationale Echokammer nährt und kontroverielle Meinungen effizient hintanhält.

Diese zwei Punkte haben wir auch in unseren 10 Fragen an jene acht Parteien, die österreichweit bei der Nationalratswahl Ende September kandidieren, thematisiert. Die vorgezogene Nationalratswahl am 29. September ist auch der Grund, warum Sie erstmals in der fast 20-jährigen Geschichte der ISPA News eine Doppelnummer unseres Magazins in Händen halten. Für die für Ende Juni geplante Ausgabe 2/19 wäre sich unsere in Vorwahlzeiten schon klassische Parteienbefragung auf keinen Fall mehr ausgegangen und die Ausgabe 3/19 wäre erst Ende September erschienen.

Die teilweise recht ausführlichen Antworten, ein Interview mit dem neuen Geschäftsführer der RTR-GmbH und viele weitere aktuelle Themen wie z. B. ›DNS over HTTPS‹ haben ein sehr umfangreiches Heft entstehen lassen. Ich wünsche Ihnen eine spannende Lektüre und freue mich darauf, Sie beim diesjährigen Internet Summit Austria am 12. September begrüßen zu dürfen, bei dem wir uns mit Künstlicher Intelligenz und Sprache beschäftigen werden.

Ihr

Maximilian Schubert

# DIGITALE IDEEN DER ÖSTERREICHISCHEN PARTEIEN

Wir haben anlässlich der bevorstehenden Nationalratswahl wie immer im Vorfeld die acht wahlwerbenden Parteien und Listen, die österreichweit kandidieren, gebeten uns durch die Beantwortung von zehn Fragen ihre Einstellungen, Meinungen und Pläne zu Digitalisierung und Internet zu verraten.

Hier eine Auflistung der Parteien, die Reihenfolge ergibt sich – auch bei den Antworten – aus der derzeitigen Anzahl an Abgeordneten im Nationalrat:

**Die neue Volkspartei**

Liste Sebastian Kurz – Die neue Volkspartei



Sozialdemokratische Partei Österreichs



Freiheitliche Partei Österreichs



Neos – Das Neue Österreich



JETZT – Liste Peter Pilz



Die Grünen – Die Grüne Alternative



Alternative Listen, KPÖ Plus, Linke und Unabhängige



Der Wandel

Auf den folgenden Seiten finden Sie die Fragen und alle Antworten dazu. Auch wenn diese teilweise sehr ausführlich ausgefallen sind, geben wir sie ungekürzt wieder.

## 1

## Das Thema Breitbandausbau beschäftigt Österreich seit Jahren. Mit dem Entstehen der ersten 5G Netze gibt es einen weiteren Technologiesprung. Was muss passieren, dass möglichst rasch viele Teile der Bevölkerung von der neuen Technologie profitieren können?

### Die neue Volkspartei

Eine moderne und leistungsfähige digitale Infrastruktur ist ein entscheidender Standortfaktor. Wir sind bereits ein führendes 5G Pilotland in Europa und wollen unsere 5G Vorreiterrolle weiter ausbauen. Die letzte Bundesregierung hat mit der neuen 5G-Strategie 34 konkrete Maßnahmen vorgelegt, um den Ausbau und die Einführung von 5G voranzutreiben. Mit höherer Kapazität, besseren und schnelleren Verbindungen und mehr Effizienz ist 5G der Schlüssel zu den digitalen Zukunftswelten. Diesen Weg wollen wir auch nach der Nationalratswahl gemeinsam mit Ländern, Gemeinden und Anbietern weitergehen.



Ziel muss sein, dass gigabit-fähige Anschlüsse bis 2030 flächendeckend angeboten werden. Dies kann nur durch die Errichtung eines engmaschigen Glasfasernetzes in Verbindung mit einer universell verfügbaren, mobilen Versorgung erreicht werden.

Bis Ende 2020, das heißt nach Vergabe der Frequenzbereiche 700/1500/2100 MHz, soll die Markteinführung von 5G in den Landeshauptstädten stattfinden.

Ende 2025 soll ein landesweites Angebot von 5G sowie Gigabit-Anschlüssen gegeben sein und bis 2030 soll eine flächendeckende Versorgung mit Gigabit-Anschlüssen erreicht sein.

Der enorme Investitionsbedarf für diese Vorhaben ist einerseits durch die weite Entwicklung der Fördermodelle (aus den Erträgen der Frequenzvergaben) sowie durch entsprechende Auflagen für Investitionen im Rahmen der Frequenzvergaben zu finanzieren.

Insbesondere in den ländlichen Gebieten wird eine Förderung mangels Rentabilität unumgänglich sein.



Die letzte Bundesregierung hat unter Federführung von Minister Norbert Hofer wichtige Weichenstellungen in Bezug auf Breitbandausbau und 5G vorgenommen. Unter anderem wurde das Telekommunikationsgesetz entsprechend geändert, um eine Versteigerung der Frequenzen in dem Sinne sicherzustellen, dass diese in einer guten Balance zwischen erzieltm Versteigerungserlös und Erhalt der Wettbewerbsfähigkeit stattfinden können. Darüber hinaus wurde auch die Breitbandstrategie erstellt, die sicherstellt, dass Österreich entsprechend wettbewerbsfähig bleiben kann.



Zwar verfügen mehr als 90 Prozent der österreichischen Haushalte über einen Internetzugang, aber der Ausbau der Infrastruktur geht nur schleppend voran. Die gesteckten Ziele sind unrealistisch, die Koordination mit den Bundesländern fehlt; die Nutzung der Transparenzdatenbank und die Evaluierung des Breitbandatlas sind mangelhaft. Es braucht beim Breitbandausbau ein höheres Tempo und eine bessere Koordination, damit derzeit unversorgte Regionen, v.a. der ländliche Raum, hier nicht zurückbleiben. Das 5G-Netz wird in Zukunft Teil der kritischen Infrastruktur des Staates sein. Wir fordern daher die Einrichtung eines gesamtgesellschaftlichen Lage- und Informationszentrums, das Gefährdungen und Risiken der kritischen Infrastruktur rasch erkennt und ihre Widerstandsfähigkeit erhöht.



5G kann, aber muss nicht die Schlüsseltechnologie des frühen 21. Jahrhunderts sein. Ein möglichst weitläufiger Ausbau von Breitband – und darum geht es – muss das Ziel sein. Wir wünschen uns hier einen klaren Wettbewerb der Technologien, statt der Fokussierung auf ein einziges System. Außerdem gilt auch hier, das Thema digitale Resilienz zu betrachten und das lässt sich nur durch ein Miteinander verschiedener Zugangstechnologien erreichen. Weiters steht die hohe Dichte an Sende- und Empfangseinrichtungen für uns in einem gewissen Widerspruch zu einer flächendeckenden Einführung. Und auch der dazu benötigte Energiebedarf darf nicht außer Acht gelassen werden. Deshalb kann nur der gezielte Einsatz, verbunden mit entsprechenden Standorten, 5G einen Durchbruch verschaffen.

Österreich war zu Beginn des Jahrhunderts ein digitales Vorzeigeprojekt, jetzt liegen wir abgeschlagen auf den hinteren Plätzen. Das gilt es zu ändern und dazu bedarf es mehrerer Ebenen und nicht nur der Einführung einer digitalen Funktechnologie. Was auf jeden Fall geschlossen werden muss, ist die digitale Lücke im Breitbandbereich in vielen ländlichen Gegenden. Hier könnten eventuell ausgesuchte 5G Pilotprojekte dazu führen, dass diese Gegenden einen gezielten Wettbewerbsvorteil erhalten und damit das Pendeln – und letztlich die Landflucht – eingedämmt werden kann. Auf jeden Fall gilt es die digitale Schere zu schließen und den Ausbau der Technologie in einen gesamtgesellschaftlichen Zusammenhang zu stellen. Das ist klar eine Aufgabe der Politik.



Die öffentliche Hand muss klare Ziele definieren und zu deren Erreichung Geld in die Hand nehmen. Bei Investitionen in Telekommunikationsinfrastruktur ist Österreich mit 0,17% des BIP Schlusslicht (unser Nachbar Slowenien beispielsweise liegt bei 0,53%) – zu diesem Schluss kommt sogar der Evaluierungsbericht ›Breitband in Österreich 2018‹ des BMVIT.

Das heißt nicht, dass blind per Gießkanne das Förderungsfüllhorn geöffnet werden soll. Angesichts der topographischen Herausforderungen Österreichs wird nicht überall die gleiche Technologie Sinn machen: Auf der Tiroler Alm sind 100 Mbit via Mobilfunk sinnvoller als ein Glasfaserkabel. In dicht besiedelten Gebieten ist ein Glasfaseranschluss bis zum Endverbraucher (FTTH – fibre to the home) anzustreben.

Die noch bestehenden Lücken in der Basisversorgung müssen zeitnah geschlossen werden, auch mit Förderungen. Dabei ist weniger relevant, welche Technologie für die ›letzte Meile‹ zum Einsatz kommt (ob Mobil- oder Leitungsnetz). In allen Fällen liegt der größte Druck auf dem unsichtbaren Rückgrat der Datenautobahnen: dem österreichischen Backbone und Backhaul. Diese sind für die Internet-Versorgungssicherheit genauso wichtig wie eine 380KV Leitung für Energie oder die Westbahnstrecke für den Bahnverkehr. Der Backbone braucht daher unsere Aufmerksamkeit, wie jede andere kritische Infrastruktur. Denn auch 5G Netze sind nur so leistungsfähig, wie der Backbone/Backhaul, an den sie angeschlossen sind.



Im städtischen Bereich klappt der Breitbandzugang schon relativ gut. Im ländlichen Bereich bedarf es wohl der Unterstützung durch die öffentliche Hand. Wichtig ist, dass diese öffentlichen Investitionen auch direkt den Menschen am Lande zugute kommen und nicht in den Taschen großer ISPs versanden. Insbesondere muss der Zugriff auch für die gemeinnützigen Kooperativen und Non-Profit ISPs wie Funkfeuer oder Aconet möglich sein.



Generell halten wir 5G für eine zukunftsweisende und förderungswürdige Technologie. Wir sehen aber die aktuellen Probleme eher in der Unter-versorgung des ländlichen Bereichs mit schnellen Breitbandanschlüssen. Viele österreichische Ballungsräume sind schon mit schnellen Glasfaser-, Kabel- oder zumindest breitbandigen DSL-Leitungen versorgt. Das Stadt-Land-Gefälle ist sehr hoch. Wir fordern daher eine staatliche Infrastrukturgesellschaft, die sich um den schnellst möglichen Glasfaser-Netzausbau kümmert – auch und gerade in ländlichen Gebieten. 5G halten wir gerade am Land nicht für den großen Heilsbringer, da die Reichweiten zumindest in den hochfrequenten Bändern stark beschränkt sind und daher das Sendernetz sehr engmaschig und dadurch teuer und langwierig zu errichten sein wird. Auch braucht es für einen folgenden großflächigen und engmaschigen Ausbau eines 5G-Netzes ein vernünftiges Glasfasernetz als Basis.

Bestehende Infrastrukturbetreiber sollen ihre Leitungen und Sendestandorte zu fairen Konditionen anderen Anbietern zur Verfügung stellen müssen. Die Kosten und somit die Endkundenpreise hielten sich in Grenzen. Geteilte Sendestandorte führen zu keinem weiteren ›Wildwuchs von Handymasten‹. Anstrebenswert ist eine verpflichtende Datenbank von Erdarbeiten auf öffentlichem Grund und Boden, um eine schnelle, unkomplizierte und günstige Verlegung von neuen Leitungen zu ermöglichen.

## 2

## Wie kann im Zuge dieser technologischen Entwicklungen der faire Wettbewerb sichergestellt werden und welche Rolle sollen dabei kleine bis mittlere Unternehmen mit lokaler Verortung einnehmen?

**Die neue Volkspartei**

Neben einem digitalen Hochleistungsnetz braucht Österreich auch umfassende Investitionen in Wirtschaft, Industrie und Infrastruktur. Die Digitalisierung bietet hier besondere Chancen, dass hochwertige Jobs auch in ländlichen Gegenden vermehrt ermöglicht werden. Gerade für den Erhalt und die Weiterentwicklung von Arbeitsplätzen oder die Neusiedlung von Betrieben in ländlichen Gegenden ist eine moderne und flächen-deckende Infrastruktur entscheidend. Deswegen muss sichergestellt werden, dass der Zugang zu schnellem Breitband- Internet überall in Österreich gewährleistet ist.



Grundsätzlich erscheint es zielführend, im Rahmen der Vergabe der Frequenzen sicherzustellen, dass einerseits die Ausgaben der Unternehmen für die Zuteilung der Frequenzen finanzierbar bleiben, andererseits aber die Versorgungsaufgaben ambitioniert gestaltet sind. Im Rahmen der Frequenz-Ausschreibung sind durch die RTR bzw. die Telekom-Control-Kommission Maßnahmen zu treffen, um den fairen Wettbewerb der Anbieter zu gewährleisten. Durch die TKG-Novelle, welche am 1.12.2018 in Kraft getreten ist, wurden diesbezüglich zahlreiche Anpassungen im Bereich Frequenzvergabe normiert.



Einerseits durch die Einführung einer digitalen Betriebsstätte (siehe Frage 3), andererseits durch eine gute Ausbildung in Österreich, die letztendlich den heimischen Betrieben – und das sind vor allem KMUs – zu Gute kommt. In diesem Sinne sind KMUs mit lokaler Verortung eine treibende Kraft und Motor der heimischen Wirtschaft.



Die rasche technologische Entwicklung hat dazu beigetragen, die Aufmerksamkeit wieder vermehrt auf die kleinen und mittleren Betriebe zu lenken. Diese sind in beachtlichem Umfang Innovationsträger. Ihre hohe Flexibilität kommt ihnen bei der Umsetzung von Innovationen zugute. Sie eröffnet den mittelständischen Unternehmen besondere Chancen. Um diese nutzen zu können, sind allerdings Rahmenbedingungen notwendig, die es ihnen erlauben, sich die erforderlichen Technologie- und Marktinformationen zu beschaffen sowie das zur Finanzierung von Innovationsvorhaben unerlässliche Eigenkapital zu bilden. Die Frage, ob KMU die Digitalisierung nützen wollen, stellt sich aber gar nicht, es ist eine Notwendigkeit, um künftig wirtschaftlich im Wettbewerb mit Großbetrieben bestehen zu können. Klar ist aber auch, dass in Bereichen, wo das Verhältnis bereits aus der Balance geraten ist, es regulierende Eingriffe braucht – es sei ganz prominent die Sharing Economy genannt. Während Hotels unter immer strengeren Vorgaben wirtschaften, machen es sich Sharing-Hosts im gesetzlichen Graubereich gemütlich mit einem Back-up von internationalen Großplayern, die sich jeder Rechtsordnung entziehen. Hier braucht es ein level playing field. In diesem Fall wäre beispielsweise die Umsetzung einer bundesweit einheitlichen Registrierungspflicht für Hosts dringend geboten.



Da die digitalen Supermächte (Alphabet, Apple, Amazon, Microsoft, Facebook, etc) immer mehr Macht in der digitalen und realen Welt gewinnen, muss die Politik endlich erwachen und dieser Entwicklung etwas entgegensetzen. Es müssen politische Rahmenbedingungen und gesetzliche Grundlagen für eine Open Source Digitalwirtschaft geschaffen werden, die es gerade KMUs, abseits der Startup-Blase, erlauben wieder in einen vernünftigen und unabhängigen Wettbewerb zu treten. Diese Entwicklung wird von einer immensen gesellschaftlichen und wirtschaftlichen Bedeutung sein.



Es gilt – auch im Sinne der Kund\*innen – einen fairen Wettbewerb zwischen den Service Providern herzustellen. Besteht eine Auswahl zwischen mehreren attraktiven Angeboten unterschiedlicher Internet-Serviceprovider, erhöht sich auch die Nutzung von Hochgeschwindigkeits-Internetangeboten. Ein solcher Wettbewerb lässt sich nur durch rechtliche Rahmenbedingungen hinsichtlich der (fair bepreisten) Nutzung von Netzinfrastruktur (die »letzte Meile« zu den Kund\*innen steht in Österreich meist im Eigentum eines einzigen Anbieters – der teilstaatlichen A1 Telekom AG) ermöglichen – und der Unterbindung unfairer Wettbewerbsmethoden.



Wichtig ist für uns das Prinzip der Netzneutralität. Für die unmittelbare Zukunft begrüßen wir Rahmenbedingungen, die es auch kleinen ISPs ermöglichen, wirtschaftlich zu überleben, und die offen für Non-Profit ISPs und entsprechende gemeinnützige Kooperativen sind.



Fairen Wettbewerb gibt es nur, wenn für alle die gleichen Spielregeln gelten. Bestehende Netze müssen für alle Anbieter geöffnet und zu fairen Konditionen mitgenutzt werden können. Wenn Förderungen wie die Breitbandmilliarde nur wenigen Anbietern nutzen, ist das freie Spiel der Kräfte genauso in Gefahr. Deshalb fordern wir statt einzelnen Förderungsmaßnahmen die oben genannte staatliche Infrastrukturgesellschaft, die die entstehenden Kapazitäten allen Anbietern zu gleichen, günstigen Konditionen zur Verfügung stellt und somit auch kleinen und lokalen Anbietern den Markteintritt vereinfacht.

Ohne Wenn und Aber stehen wir zur Netzneutralität, um nicht größere, marktbeherrschende Unternehmen zu bevorzugen.

# DIGITALISIERUNG UND INTERNET

## 3

## Die Besteuerung von digitalen Unternehmen ist nicht nur in Österreich ein viel diskutiertes Thema. Welche Lösungen wären aus Ihrer Sicht erstrebenswert?

### Die neue Volkspartei

Wir sagen jeder Form der ungerechten Steuervermeidung und des Steuerbetrugs den Kampf an. Das gilt im Besonderen für multinationale Online-Konzerne, die sich oft durch Tricks ihren steuerlichen Pflichten entziehen. In Österreich hat die letzte Bundesregierung daher bereits mit der Einführung einer Digitalsteuer für Online-Werbung reagiert, die zusätzliche Einnahmen von 200 Mio. Euro einbringt. Gleichzeitig ist klar, dass faire steuerliche Rahmenbedingungen auch weiterhin durch gemeinsame Einigungen auf OECD- und EU-Ebene verfolgt werden müssen.



Internationale Onlinekonzerne sichern sich die weltweit höchsten Werbeumsätze, sie optimieren zugleich ihre nationalen Steuerleistungen. Soll Österreich hier Maßnahmen ergreifen und welche? (Ein Initiativantrag von ÖVP und FPÖ für Digitalbesteuerung liegt vor.)

Internationale Konzerne besitzen derzeit durch lückenhafte Regulierung (Datenschutz, Medienrecht, Steuerrecht etc.) einen großen Wettbewerbsvorteil gegenüber traditionellen Medienunternehmen. Hier wollen wir faire Spielregeln für alle schaffen. Es braucht regulatorische Maßnahmen und Beschlüsse gegen Steuervermeidung auf europäischer Ebene, insbesondere die Einführung einer sogenannten ›digitalen Betriebsstätte‹ im Steuerrecht, um Gewinne am Ort der Wertschöpfung (in dem jeweiligen Staat) besteuern zu können. Eine sogenannte ›Digitalsteuer‹ wäre eine Übergangslösung. Der Vorschlag der ehemaligen schwarz-blauen Regierung für eine nationale Digitalsteuer ist insofern unzureichend, als er lediglich die digitalen Werbeumsätze erfasst. Damit bleibt er weit hinter dem Vorschlag für eine europaweite Digitalsteuer zurück, hier wären auch der Verkauf von nutzergenerierten Daten und Vermittlungsdienstleistungen auf digitalen Plattformen steuerlich erfasst worden.



Das Ziel einer solchen Besteuerung kann nur sein, dass internationale Konzerne, die Gewinne mit Leistungen in Österreich erzielen, im selben Umfang Steuern in Österreich zahlen müssen wie hier ansässige Unternehmen.



Es kann nur eine europäische Lösung geben, um internationale Internetkonzerne fair zu besteuern. Steuerschlupflöcher müssen beseitigt und die zu versteuernden Gewinne einheitlich berechnet werden. Nationalstaatliche Lösungen sind in diesem Bereich absolut nicht sinnvoll. Österreich soll hier keinen Alleingang machen, sondern sich stattdessen auf europäischer Ebene für eine Abschaffung des Einstimmigkeitsprinzips in Steuerfragen einsetzen, damit die Union in dieser so zukunftsweisenden Frage endlich handlungsfähig wird und gerechte Steuern für Digitalriesen einheben kann.



Im Zentrum der Wertschöpfung der digitalen Supermächte stehen die Daten der Bürger\*innen. Es kann nicht sein, dass hier die User\*innen letztlich zu kurz kommen. Der Neoliberalismus hat alle Unternehmen dazu gebracht, ihre gesellschaftlichen Aufgaben nur mehr teilweise oder gar nicht wahrzunehmen. Gewinne werden in Steueroasen verschoben und entziehen sich dem Ort, an dem sie eigentlich generiert werden. Hier sind zumindest auf europäischer – oder multilateraler – Ebene, Systeme einzuführen, die einen Teil der digitalen Wertschöpfung auf der nationalen Ebene der User\*innen verorten. Damit würde automatisch eine Steuerpflicht für die transnationalen Konzerne entstehen. Der Firmensitz oder der physikalische Serverstandort kann in einer digitalen Welt nicht der Maßstab für die Besteuerung sein.



Wir setzen uns für die Einführung einer ›Digitalen Betriebsstätte‹ auf nationalstaatlicher Ebene ein. Damit wären auch digitale Unternehmen Körperschaftssteuerpflichtig. Nur die Erweiterung des Betriebsstättenbegriffs kann sicherstellen, dass digitale Konzerne faire Beiträge leisten. Ein weiterer wichtiger Schritt ist vollständige Transparenz. Wir treten für ein wirksames, kostenloses und öffentlich zugängliches System länderspezifischer Steuertransparenz (›country by country reporting‹) ein. Detaillierte Berichtspflichten getrennt für alle Staaten, in denen ein multinationaler Konzern Niederlassungen hat, sind unbedingt notwendig, damit die Gewinne nicht mehr ungesehen von einem Land zum nächsten geschoben werden können. Darüber hinaus braucht es eine gemeinsame Bemessungsgrundlage in der Körperschaftsteuer in Verbindung mit Mindeststeuersätzen, damit das schädliche Steuerdumping endlich beendet wird und multinationale Konzerne keinen Wettbewerbsvorteil gegenüber kleineren und mittleren Unternehmen haben.



Digitalkonzerne wie Amazon, die riesige Umsätze und Gewinne machen, zahlen in der Europäischen Union kaum Steuern. Wir fordern daher eine EU-weite Digitalsteuer.



Solange Konzerne wie Apple, Google, Amazon u.a. nur wenig bis keine Steuern zahlen, verzerren sie den Wettbewerb extrem und verunmöglichen dadurch bestehenden lokalen Anbietern das wirtschaftliche Überleben sowie Startups den Markteintritt. Hier muss endlich gehandelt werden. Gewinne müssen dort besteuert werden, wo die reale ökonomische Aktivität stattfindet. Da die notwendigen Änderungen im Steuerrecht auf internationaler Ebene durch die unterschiedlichen Interessenslagen der Akteure aber noch lange auf sich warten lassen werden, müssen wir auf nationaler Ebene Druck aufbauen. Möglich wäre dies beispielsweise durch die Erhebung einer Quellensteuer auf Finanzflüsse in Steueroasen. Ebenso wichtig ist unbedingte Transparenz. Wenn Konzernzahlen auf EU-Ebene entsprechend offengelegt werden müssen, wären die steuerschonenden Praktiken sofort ersichtlich und somit bekämpfbar.

Priorität müssen auch schlagkräftigere Antimonopolgesetze haben. Gerade digitale Riesenkonzerne verzerren den Markt und nutzen ihre Größe, um ihre Interessen in Gesetzen zu gießen.

## 4

## Die EU hat nach einem intensiven Diskurs die Urheberrechtsrichtlinie inklusive Leistungsschutzrecht und Upload-Filter beschlossen. Wie kann man bei der Umsetzung die negativen Auswirkungen auf die Meinungsfreiheit und Meinungsvielfalt im Netz möglichst gering halten?

### Die neue Volkspartei

Die Richtlinie zum Urheberrecht im digitalen Binnenmarkt soll das europäische Urheberrecht für die Herausforderungen der digitalisierten Welt stärken. Das ist wesentlich für den Schutz geistigen Eigentums und unabdingbarer Schritt im asymmetrischen Wettbewerb mit den Online-Giganten. Schutz geistigen Eigentums ist eine Frage der Gerechtigkeit und die Herstellung gleicher Rahmenbedingungen für alle Marktteilnehmer eine Notwendigkeit.

Derzeit machen digitale Plattformen oft Gewinne mit den Inhalten von anderen – ohne, dass die Urheber dafür gerecht entlohnt werden. Das muss sich ändern. Das Prinzip des Eigentums muss auch im Internet gelten und geschützt werden. Deshalb hat sich die ÖVP-Delegation im Europaparlament nach eingehenden Beratungen auch für die Urheberrechts-Richtlinie ausgesprochen. Die Urheberrechts-Richtlinie wird in den kommenden zwei Jahren auf nationaler Ebene umgesetzt. Im Rahmen der genauen gesetzlichen Ausgestaltung werden selbstverständlich Experten und involvierte Stakeholder eingebunden. Für uns steht aber fest, dass der Schutz geistigen Eigentums eine Frage der Gerechtigkeit ist und auch im digitalen Raum gelten muss.



Die SPÖ hat sich von Anfang an gegen Upload-Filter eingesetzt. Wenn Europa ein relevanter Player in der digitalen Welt sein will, darf der freie Raum im Internet nicht zerstört werden. Große Konzerne sollen nicht mittels Upload-Filter entscheiden dürfen, was ins Internet darf und was nicht. Nicht zuletzt tragen Upload-Filter auch zu einer weiteren Monopolisierung im Internet bei. Wir wollen die Informationsvielfalt im Netz erhalten und gerade kleine Digitalunternehmen unterstützen und werden uns daher bei der Umsetzung der Urheberrechtsrichtlinie dafür einsetzen, dass alle Spielräume der Richtlinie für den Schutz von Meinungsfreiheit und Meinungsvielfalt genutzt werden.



Die FPÖ ist strikt gegen diese ›Upload-Filter‹. Urheberrechtsverletzungen können mit dem bestehenden Regelwerk verfolgt werden. Bei einer Umsetzung der Richtlinie ist darauf zu achten, nur die notwendigsten Teile im nationalen Gesetz zu verankern. Meinungsfreiheit und Meinungsvielfalt sind ein zu hohes Gut, um diese dritten Interessen zu opfern.



Zunächst einmal sind wir für ein modernes und effektives Urheberrecht. Wir haben großen Respekt vor Kunstschaffenden und Verlegern, denen eine angemessene Vergütung ihrer Leistung zukommen muss. Aber wir sind klar gegen die von Konservativen betriebene Zensur des Internets. Wir stellen uns gegen Upload-Filter. Das Internet ist heute für jeden Einzelnen von uns extrem wichtig. Dort spielt sich ein essentieller Teil unseres Lebens ab. Wir arbeiten, lernen und lachen im Internet. Daher muss jeder Eingriff in das freie Internet mit äußerster Vorsicht abgewogen werden. Denn jeder Eingriff in die Freiheit des Internets ist ein Eingriff in die individuelle Freiheit jedes Bürgers und jeder Bürgerin.



Die gängige Praxis zeigt uns bisher, dass nicht so heiß gegessen wie gekocht wird. Was natürlich kein guter Grundzustand ist. Hier müssen andere Regeln her. Das moderne Urheberrecht geht auf die Gesetzgebung des 18. Jahrhunderts zurück. Der Urheberbegriff ist ein anderer geworden und wieder sind es die digitalen Supermächte, die sich den Markt unter den Nagel gerissen haben.

Die Meinungsfreiheit wird aber deutlich mehr von einer anderen Seite angegriffen: Von den digitalen Supermächten und von superreichen Menschen, die sich immer mehr Medien unter den Nagel reißen und damit in einem weiteren Sinne Politik machen. Diese Tatsache ist viel alarmierender als der Umstand von Upload-Filtern, auch wenn diese dazu führen werden, das Meinungsspektrum einzuschränken.



Uploadfilter sind aus unserer Sicht nicht das geeignete Mittel, um gegen Urheberrechtsverletzungen vorzugehen. Uploadfilter und Leistungsschutzrecht werden sich negativ auf das Internet auswirken. Sie gefährden unsere Demokratie und die Meinungsfreiheit und schützen nicht die Autor\*innen, sondern nur große Presseverlage. Wir haben daher im Europaparlament dagegen gestimmt. Da das Gesetz aber leider gegen unseren Widerstand beschlossen wurde, liegt es nun an der nationalen Gesetzgebung, hier sinnvolle Lösungen zu finden. Das nationale Gesetz darf keinesfalls sehr eng gefasst sein. In der nationalen Implementierung wird es wichtig sein, so viele Ausnahmen wie möglich für KMUs, Vereine und andere nicht-kommerzielle Betreiber von Plattformen zu schaffen. Unsere Befürchtung ist, dass eine weitreichende Ausnahmeregelung unter Umständen nicht EU-rechtskonform sein könnte und es daher vor dem EUGH ausjudiziert werden muss.



Wir sind gegen Upload-Filter. Weder ISPs noch Plattform-Betreiber sollen zu Hilfsheriffs bei der Durchsetzung der Profitinteressen der Content-Industrie gemacht werden. Wir sind gegen die Einführung des Leistungsschutzrechtes und auch gegen alle anderen Verschärfungen und Ausweitungen von so genannten ›Geistigen Eigentumsrechten‹. Im Falle des konkreten Problems wären Modelle, die mit einer öffentlichen Förderung von Contentproduktionen arbeiten und etwa über eine entsprechende Besteuerung von Werbung finanziert werden, denkbar und vernünftiger.



Wir sind strikt gegen jede Art von Zensur und werden gerade die Upload-Filter auf allen uns möglichen Ebenen bekämpfen. Wir sehen zwar, dass das europäische Urheberrecht noch aus der Offline-Zeit stammt und dadurch stark reformbedürftig ist, allerdings geht das Beschlossene in die falsche Richtung und wird von uns abgelehnt.

Prinzipiell diskussionswürdig sind die oftmals überlangen Laufzeiten von Patenten. Natürlich muss Leistung geschützt werden, dieser Schutz darf sich aber nicht langfristig innovationshemmend auswirken und zur reinen Gelddruckmaschine werden.



## 5

## Filter scheinen derzeit überhaupt sehr beliebt zu sein. So wird z. B. mehr oder weniger laut über Porno-Filter nachgedacht. Wie steht Ihre Partei zu Filtern im Netz?

### Die neue Volkspartei

Ein gleichberechtigter Zugang zu Informationen und Services im Internet ist uns ein wichtiges Anliegen. Gleichzeitig gibt es Inhalte, die klar gegen Gesetze verstoßen. Daher unterstützen wir Initiativen wie Stopline, um beispielsweise kinderpornografische oder nationalsozialistische Inhalte zu melden und vom Netz zu nehmen.



Die SPÖ will ein freies Internet für alle – im Internet muss Meinungs- und Informationsfreiheit gewährleistet sein. Die Etablierung von diverseren Filtern steht dem entgegen. Dabei besteht nicht nur die Gefahr des ›Overblocking‹ wie in Großbritannien, wo aufklärende Inhalte zu sexuellen Orientierungen oder Geschlechtskrankheiten gesperrt wurden. Sondern es besteht vor allem auch die Gefahr, dass eine Infrastruktur entsteht, die missbräuchlich zur Zensur verwendet werden könnte.

Wichtiger als die Etablierung von Filtern ist die Vermittlung von Internetkompetenz – vor allem für Kinder und Jugendliche. Daher ist es notwendig, dass in der Schule ein verantwortungsvoller Umgang mit Medien im Lehrplan verankert ist.



Grundsätzlich lehnen wir jeden Filter ab, da dieser automatisch zu einer Einschränkung der Meinungsfreiheit und Meinungsvielfalt führt. Ausnahmen könnten im Bereich Kinderpornografie gemacht werden.



Kinder- und Jugendschutz sind für uns sehr wichtig und wir fordern seit längerem eine bundesweite Vereinheitlichung, damit Kinder und Jugendliche in ganz Österreich die gleichen Möglichkeiten, Rechte und Pflichten haben. An den lauten Überlegungen zum Thema Jugendschutz im Netz und konkret Porno-Filter zeigt sich wieder einmal, dass viele Politiker\_innen wenig Ahnung haben, wie das Internet funktioniert und wie sich junge Menschen dort bewegen. Das automatische Filtern von Inhalten ist ein Modell, das einfach nicht funktioniert und über das Ziel hinausschießt. In Großbritannien wurden solche Filter eingeführt. Zeitweise war daraufhin jede fünfte Seite gesperrt, auch solche mit für Jugendliche wichtigen und relevanten Informationen, z.B. zum Thema Verhütung. Wir sind gegen Internetfilter jeglicher Art, weil sie erstens nicht treffsicher funktionieren und zweitens von technisch einigermäßen Versierten leicht umgangen werden können, gerade Jugendliche wissen das.



Filter sind keine Lösung. Es werden immer die Bürger\*innen auf der Strecke bleiben, die bei den Medienbesitzern unbeliebt sind. Die Beispiele China, Ungarn oder Russland zeigen deutlich, was passiert, wenn gefiltert wird. Damit gehen die Menschenrechte verloren.



Die Grünen lehnen Filter im Netz klar ab. Wir beziehen klar Stellung für eine offenes, neutrales und zensurfrees Netz.



Das Sperren von Inhalten ist kein geeignetes Mittel, um Probleme mit Pornografie, Gewaltverherrlichung oder Urheberrechtsverletzungen im Internet zu lösen. Daneben ist das ein Verstoß gegen das Prinzip der Netzneutralität. Mit der technischen Umsetzung von Filtern oder Sperren werden ISPs in eine schwierige Situation gebracht. Gerade kleinere Anbieter sind benachteiligt.

Ist die Infrastruktur für Sperren erst umfassend aufgebaut, wird der Druck immer weiter steigen, mit weiteren Inhalten so zu verfahren – vorangetrieben durch Interessen von Konzernen. Die Umgehung solcher Sperren bleibt dabei für technisch Versierte möglich.



Siehe Punkt 4. Wir lehnen Zensur jeglicher Art ab, Filter dementsprechend auch. Sie sind nur ein vordergründig einfacher Weg, um für Manche unliebsame Inhalte der Masse nicht zugänglich zu machen. Jedoch sind Filter technisch meist leicht zu umgehen, ebenso sind alle entsprechenden Inhalte schwer erfassbar. Prävention und Aufklärung statt Filtern und Verboten.

# DIGITALE IDEEN DER ÖSTERREICHISCHEN PARTEIEN

## 6

Laut DESI-Index liegt Österreich in Sachen Digitalisierung EU-weit im Mittelfeld und verliert im Vergleich zum Vorjahr einen Platz im Ranking, der Abstand zu den führenden Ländern hat sich vergrößert. Welche konkreten Maßnahmen schlägt Ihre Partei vor, um Österreich an die Spitze heranzuführen?

**Die neue  
Volkspartei**

Wir betrachten die Digitalisierung als Chance für Österreich. Digitalisierung hat für uns mehrere Dimensionen:

- Digitalisierung des Staates – sowohl was die Abläufe in der Verwaltung betrifft als auch die Interaktion mit den Bürgerinnen und Bürgern
- Infrastruktur für die Bürger sowohl Breitband als auch mobiler Zugang zum Internet
- Ausbildung und Vorbereitung der Bürgerinnen und Bürger auf die Anforderungen einer digitalisierten Welt
- Rechtliche Rahmenbedingungen und entsprechende Schwerpunktsetzung für eine digitale Wirtschaft

Um die Potentiale der Digitalisierung bestmöglich nutzen zu können, wollen wir den von der letzten Bundesregierung begonnenen Weg der gesamtstaatlichen Kraftanstrengung hin zu einer erfolgreichen digitalen Zukunft fortsetzen. Mit Digital Austria wurde eine erfolgreiche Initiative und Dachmarke für erfolgreiche Digitalisierung in Österreich geschaffen, die auf Basis eines strategischen Aktionsplans die Digitalisierung in unserem Land vorantreibt. Parallel dazu braucht es Anstrengungen etwa im Bildungsbereich: Mit dem neuen Schulfach ›Digitale Grundbildung‹ wird ein breites Spektrum von digitalen Kompetenzen vermittelt, aber auch die weitere Verbesserung digitaler Infrastruktur an Schulen oder ein IT-Schwerpunkt an Hochschulen ist zentral. Darüber hinaus sind der bereits erwähnte flächendeckende Breitbandausbau sowie der Ausbau der neuen Plattform oesterreich.gv.at für uns von großer Bedeutung.



Neben dem flächendeckenden Angebot von gigabit-fähigen Anschlüssen bis 2030 und der Erstellung und Umsetzung einer entsprechenden Breitbandstrategie ist es notwendig, die Forschungs- und Technologieförderung zu erhöhen und entsprechende Schwerpunkte (z.B. künstliche Intelligenz) zu setzen.



Grundlage dafür ist eine sehr gute Bildung. Die letzte Bundesregierung hat bereits Maßnahmen ergriffen, die auf Grund der Kürze noch kein messbares Ergebnis liefern können. Wenn der Weg entsprechend weiterbestritten wird – auch wieder mit einem positiven Bekenntnis zur Leistung – dann wird sich Österreich nicht nur in diesem Ranking verbessern.



Österreich kommt hier nur langsam voran. Der Abstand zu den besten Ländern wird immer größer, während andere Länder hier verstärkt Maßnahmen setzen und aufholen. Konkrete Maßnahmen sind in unterschiedlichen Bereichen vonnöten. Der Ausbau von Breitband/5G muss stärker vorangetrieben werden. Der Fachkräftemangel im IKT-Bereich muss bekämpft werden. Dafür braucht es eine MINT-Initiative, um den Zugang zu Berufen in diesem Bereich attraktiver und einfacher zu machen. Die Lehre soll in Module gegliedert und laufend evaluiert werden, damit unsere Jugend passgenaue und relevante Inhalte lernt und veraltete Techniken der Vergangenheit angehören. Im Bereich der Verwaltung sollen digitale Dienste für die Gründung von Unternehmen und für laufende Geschäftstätigkeit verbessert und weiter ausgebaut werden, um mühselige Behördengänge einzusparen.



Breitband flächendeckend ist zwingend erforderlich – wie auch immer die Technologie dahinter aussieht. Weiters erfordert es eine Digitalisierungsoffensive bei den KMUs. Der Ansatz der WKO in Verbindung mit dem Infrastrukturministerium war bisher einer der möglichen Ansätze. Leider wurde das Fördervolumen viel zu früh ausgeschöpft und bisher wurde wenig nachgereicht. Aber auch die großen Player am Markt sind gefordert hier Angebote zu schaffen, die auch aus rechtlicher Sicht, Stichwort DSGVO, KMU-gerecht sind. Open Source ist in diesem Zusammenhang ebenfalls ein Stichwort. Der IT-Sektor und die digitalen Angebote sind für KMU in vielen Fällen undurchschaubar, weil wichtige Entscheidungsgrundlagen fehlen. Hier ist der Bildungsbereich gefordert ebenfalls Angebote zu schaffen. Ein PC-Führerschein ist zu wenig für eine funktionierende Wirtschaft von Klein- und Mittelbetrieben.



Erstens ist jedenfalls die bereits genannte Schaffung eines geeigneten Biotops – also der Ausbau von Breitbandverfügbarkeit, Förderung von Breitbandnutzung und Sicherung der Netzneutralität – nötig. Zweitens hinkt Österreich vor allem bei der Adaption auf digitale Produkte und Abläufe hinterher, wie auch im DESI Index betont wird – etwa bei der schwachen Nutzung von Big Data oder Cloud-Diensten. Hier birgt die KMU-lastige Struktur der österreichischen Wirtschaft zusätzliche Herausforderungen. Anders als bei großen Unternehmen mit eigenen IT-Abteilungen fehlen in kleineren Betrieben für die Entwicklung digitaler Lösungen oft Ressourcen oder die Zeit. Um KMU dabei zu unterstützen, braucht es Fördergelder und einen niedrigschwiligen Ansatz. Der bis 2017 existente Kreativwirtschaftsscheck war beispielsweise ein unbürokratischer Einstieg für viele KMU für die erstmalige Anwendung neuartiger digitaler Technologien. Dieses Programm wird seit 2018 nicht mehr angeboten, stattdessen setzte die abgesetzte Regierung gerne auf Beratungsprogramme. Freilich ist ein Beratungsgespräch nett, aber im Jahre 2019 und bei brennendem Hut ist praxisnäheres Denken und Handeln angebracht. Als Nachfolge für den erfolgreichen Kreativwirtschaftsscheck wäre ein unbürokratischer Digitalscheck für KMU mit konkreten digitalen Problemstellungen anzubieten. Da kann man sich durchaus was beim Liechtensteiner Digitalscheck-Modell (der neben Beratungs- und Investkosten auch Trainings- und Schulungskosten fördert) oder der Wiener ›Wien Digital‹ Förderung anschauen.



Wir wollen die offene Architektur des Netzes bewahren und damit das Potential für Innovation und Entwicklung fördern. Dazu gehört auch der verstärkte Einsatz freier Software bzw. Open-Source-Software. Der Zugang zu Internet und Computern soll für alle als Teil des Existenzminimums bzw. der Teilhabe am kulturellen und politischen Leben gewertet werden. Die IT-Infrastruktur aller Schulen muss ausgebaut werden und digitale Kompetenz im Bildungssystem vermittelt werden.



Wir müssen mehr in Bildung investieren, statt unsere Bildungseinrichtungen auszuhungern. Das fängt bei Volks- und Mittelschulen an und endet bei Universitäten und Erwachsenenbildung. Alle Einrichtungen müssen mit breitbandigen Anschlüssen, moderner Hard- und Software ausgestattet werden. Das Lehrpersonal muss auch und umso mehr im digitalen Bereich fortgebildet und Lehrpläne müssen laufend evaluiert und den aktuellen Gegebenheiten angepasst werden. Gerade an Schulen erreicht man einen großen Teil der Bevölkerung und kann dort gezielt auf die umfangreichen Möglichkeiten und Chancen, aber auch auf die Gefahren des Internets hinweisen.

In ländlichen Gebieten hinkt Österreich bei der Breitbandversorgung noch massiv hinterher, das Stadt-Land-Gefälle ist hoch. Wir fordern, wie oben erwähnt, eine staatliche Infrastrukturgesellschaft, die sich um den schnellst möglichen Glasfaser-Netzausbau kümmert.

Der Digitalisierungsgrad der Wirtschaft lässt zu wünschen übrig. Unter anderem durch den schleppenden Breitbandausbau begründet braucht es aber auch ein faires Steuersystem mit gleicher Besteuerung aller Marktteilnehmer (siehe Punkt 3.). Die Bereitstellung von grundlegenden digitalen Services (wie bspw. Onlineshops) und die Unterstützung bei der Installation und Wartung durch die jeweiligen Interessensvertretungen oder direkt von staatlicher Seite würden die Situation verbessern.

Im Bereich der digitalen öffentlichen Dienste sind wir auf einem guten Weg. Eine weitere Integration der unterschiedlichen Systeme – unter Einhaltung des Datenschutzes – ist aber unumgänglich.

## 7

## Die ÖVP/FPÖ-Regierung hat sich bis zuletzt für eine digitale Ausweispflicht ausgesprochen. Halten Sie diese Bestrebungen für gerechtfertigt?

**Die neue Volkspartei**

Jüngste Fälle von herabwürdigenden Postings gegen Frauen zeigen die Notwendigkeit klarer Spielregeln im Netz auf. Denn klar ist: Hass und Gewalt im Netz dürfen nicht ohne Konsequenzen bleiben und das Internet kann und darf kein rechtsfreier Raum sein. In der digitalen Welt müssen die gleichen Prinzipien gelten wie in der realen Welt. Den Betroffenen soll Schutz und Prävention durch eine digitale Ausweispflicht geboten werden. Opfer im Netz müssen die Möglichkeit bekommen, bei Rechtsverletzungen die Identität der Täter zu kennen. Eine allfällige Lüftung der Identität würde jedoch nur im Rahmen eines Gerichtsverfahrens erfolgen. Daher stehen wir hinter dem eingebrachten Gesetz über Sorgfalt und Verantwortung im Netz.



Das Internet darf kein Platz von Gewalt und diskriminierenden, rassistischen oder frauenfeindlichen Hassbotschaften sein. Der beste Weg zur Qualitätssicherung von Debatten im Internet ist eine intensive Moderation. Nur dadurch kann unerwünschtes Verhalten im Internet verhindert werden. Plattform-Anbieter sind stärker in die Pflicht zu nehmen. Wir sprechen uns gegen eine Klarnamenpflicht oder Ausweispflicht bei der Registrierung aus, da die Erfahrung zeigt, dass Hassbotschaften in sehr vielen Fällen bereits jetzt mit Klarnamen gepostet werden. Daher braucht es andere Maßnahmen.



Es war das starke Bestreben der ÖVP, diese ›digitale Ausweispflicht‹ einzuführen. Die FPÖ hält die geltende Gesetzeslage für ausreichend. Denkbar wäre eine kleine Ergänzung im E-Commerce-Gesetz im § 18. Dort könnte analog dem ORF-Gesetz die Verpflichtung aufgenommen werden, Name und Adresse anzugeben. Den von Medienminister Blümel in Begutachtung geschickte Gesetzesentwurf halten wir für nicht durchdacht und überschießend.



Der Vorschlag der ehemaligen Regierungsparteien, einen Ausweiszwang im Internet einzuführen war nicht nur EU-rechtswidrig, sondern auch nicht dazu geeignet, einen respektvolleren Umgang in Onlineforen und eine bessere Durchsetzung von Rechtsansprüchen zu erreichen. Vielmehr brauchen wir die effektive Durchsetzung von bereits bestehendem Recht gegenüber internationalen Internetunternehmen. Es braucht eine Verankerung von psychischer Gewalt und verbaler sexueller Belästigung als Straftatbestand und die Justiz muss mit entsprechenden Mitteln für mehr Personal und spezialisierte Stellen ausgestattet werden, um eine schnelle Verfolgung zu gewährleisten. Außerdem brauchen wir mehr und bessere Maßnahmen zur Medienkompetenz, sowohl in der Schule als auch in der Erwachsenenbildung. Letztlich soll sich Österreich auf europäischer Ebene für eine vernünftige Ausgestaltung der E-Evidence-Verordnung einsetzen, anstatt auf nationale Alleingänge zu setzen.



Nein! Die BVT-Affäre hat uns gezeigt, was passiert, wenn Geheimdienste im Sinne der Politik agieren und gleichzeitig auch noch dilettieren. An diesem Punkt sind die Bürgerrechte in Gefahr. Jeder einzelne Österreicher und jede Österreicherin hinterlässt schon heute immense digitale Spuren und hat kaum Kontrolle darüber. Eine Ausweispflicht führt in letzter Konsequenz zu einem Kontrollstaat. China mit seinen ›erzieherischen‹ Maßnahmen muss uns hier ein warnendes Beispiel sein.



Nein, die vorgeschlagenen Maßnahmen sind im Gegenteil als demokratiegefährdend zu bewerten. Das Grundrecht auf Meinungsäußerungsfreiheit darf nicht an die Bedingung geknüpft werden, sich mit Klarnamen und privater Adresse zu registrieren. In Bezug auf Hass im Netz, den die ÖVP/FPÖ-Regierung angeblich damit bekämpfen wollte ist zu sagen, dass der größte Teil der Hasspostings unter Klarnamen verfasst wird. Jene, die tatsächlich anonym bleiben wollen, würden das auch mit der Klarnamenpflicht bewerkstelligen können. Für Plattform- und Forenbetreiber wäre die Registrierungspflicht ein enorm großer Aufwand mit entsprechenden Sicherheitsrisiken. Kleine Webseiten dagegen, zum Beispiel Fake-News-Plattformen, sind von dem Gesetz ausgenommen. Das führt dazu, dass rechte Hetz-Portale wie unzensuriert.at keine Registrierungspflicht treffen würde. Der Gesetzesvorschlag ist aus grüner Sicht in mehreren Punkten verfassungswidrig und klar abzulehnen.



Ein ›digitales Vermummungsverbot‹ ist unverhältnismäßig, schränkt das Recht auf Privatsphäre ein und schützt vor allem die Opfer nicht. Wir halten davon nichts.



In Österreich gibt es keine Ausweispflicht, also brauchen wir auch keine digitale Ausweispflicht. Unabhängig davon werden die vordergründig angestrebten Ziele nicht erreichbar sein, dafür aber eine Unzahl an Problemen auftauchen. Die digitale Ausweispflicht wäre ein massiver Eingriff in das Grundrecht auf Privatsphäre. Viele Randgruppen und Aktivisten würden aus Angst vor Repressionen und Verfolgung ihre Stimme im Internet nicht mehr erheben. Kinder und Jugendliche würden sich in einem für sie neuen Medium ohne Schutz eines Pseudonyms bewegen. Abgesehen von diesen Punkten wäre ein digitales Vermummungsverbot eine Schwächung des Wirtschaftsstandortes Österreich. Die Umsetzung ist aufwendig, die Einhaltung der Datenschutzbestimmungen schwierig und viele User würden schlicht und einfach zu ausländischen Anbietern wechseln.

# NATIONALRATSWAHL

## 8

## Wie kann die Rechtsdurchsetzung im Online-Bereich verbessert werden, ohne dabei die Grundrechte der Bürgerinnen und Bürger massiv zu beschneiden und einen Überwachungsstaat zu schaffen?

**Die neue Volkspartei**

Jede Maßnahme im Interesse der öffentlichen Sicherheit muss einer Güterabwägung unterliegen, sowie der Zielsetzung und rechtsstaatlichen Prinzipien entsprechen. Klar ist, in den letzten Jahren ist die terroristische Bedrohung in der Europäischen Union massiv angestiegen. Auch in Österreich spüren wir dies. Organisierte Banden oder terroristische Vereinigungen nutzen dabei ebenso die Möglichkeiten modernster Technologie. Daher müssen wir unseren Ermittlungsbehörden das notwendige Rüstzeug geben, damit sie diese auch bekämpfen können. Dies ist klar anlassbezogen und es muss durch Rechtsschutzmaßnahmen sichergestellt werden, dass kein Eingriff in die verfassungsrechtlich gewährten Grundrechte stattfindet.



Hass und Gewalt im Internet muss entschieden entgegengetreten werden. Strafbares Verhalten muss auf einfachem Wege zur Anzeige gebracht werden können. Hierzu braucht es eine Aufstockung und Schulung des Personals bei Polizei und Justiz.

Wir brauchen neben verbesserten Möglichkeiten zur Verbrechensbekämpfung klare und starke Schranken für den Eingriff der nationalen Staatlichkeit, einen starken Datenschutz und effektive Rechtsschutzmöglichkeiten für Betroffene. Gleichzeitig müssen wir überlegen, wie weit die Freiheit von Großkonzernen gehen darf, Unmengen von Daten zu sammeln.



Siehe Frage 7



Weniger Anonymität und mehr Überwachung führen nicht zu mehr Sicherheit oder einem zivilisierteren Umgang im Netz, sondern schränken unsere Freiheit ein und gefährden Demokratie und Rechtsstaat. Das bedeutet aber nicht, dass es keine Regeln geben soll. Wir fordern klare und einheitliche Gesetze, die online wie offline gelten und notfalls mit der nötigen Härte durchgesetzt werden. Es bringt nichts, ständig neue Gesetze auf den Weg zu bringen, wenn die bereits geltenden nicht durchgesetzt werden. Für eine effektive Durchsetzung von geltendem Recht im Internet braucht es eine bessere Ausstattung der Justiz. Zusätzlich braucht es eine Verankerung von psychischer Gewalt und verbaler sexueller Belästigung als Straftatbestand und entsprechend spezialisierte Stellen zur Verfolgung. Letztlich soll sich Österreich auf europäischer Ebene für eine vernünftige Ausgestaltung der E-Evidence-Verordnung einsetzen, damit die Rechtsdurchsetzung über nationale Grenzen hinweg einfacher wird.



Rechtsdurchsetzung wovon? Eines Urheberrechts mit den Wurzeln im 18. Jahrhundert? Löschung von Hasskommentaren? Wiederbetätigung? Auf diese Frage kann es keine pauschale Antwort geben. Zentrales Element müssen die Grundrechte sein. Hier bedarf es entsprechender Ausdifferenzierung bei den Gesetzen. Das wird sich nicht vermeiden lassen.



Die Staatsanwaltschaft muss dringend mit mehr Ressourcen für Ermittlungen im online Bereich ausgestattet werden. Das Internet ist kein rechtsfreier Raum – dieses Verständnis kann nur hergestellt werden, wenn Straftaten im Netz auch tatsächlich verfolgt werden können. Es braucht umfangreiche Schulungen für Polizei und Justiz, um die Funktionsweisen von Internetplattformen zu verstehen und Straftaten effizient verfolgen zu können. Zudem müssten Verfahren beschleunigt werden – unter den derzeitigen Rahmenbedingungen scheitert die Rechtsdurchsetzung immer wieder daran, dass die Anträge der Justiz zu spät bei den Plattformen eintreffen und beispielsweise IP-Adressen schon gelöscht sind. Jedenfalls notwendig ist, dass für Plattformen wie Facebook, Google und Twitter auch in Österreich Zustellungsbevollmächtigte eingesetzt werden.



Bei der Bekämpfung von Hass und Hetze im Netz muss es vor allem um den Schutz der Opfer gehen. Maßnahmen wie digitale Ausweispflichten, massives Speichern von Nutzerdaten, ein Verbot von Pseudonymen etc. sind unverhältnismäßig und unwirksam. Gleichzeitig gefährden sie freie Diskussion, bestehende Diskussions-Plattformen und können politische AktivistInnen gefährden.

Beratungsorganisationen wie ZARA oder die Opferschutzorganisation Weisser Ring halten die Maßnahmen für ungeeignet hinsichtlich des Opferschutzes. Es gibt eine Reihe von Alternativvorschlägen wie auch jene der ISPA, die zeigen, dass es keinen Überwachungsstaat braucht, um gegen Hass und Hetze im Netz vorzugehen und die Opfer zu schützen.



Ein mehr an Überwachung und Zensur ist zwar ein Wunschtraum vieler »Law and Order«-Politiker, bringt aber in der Realität wenig und beinhaltet ein hohes Missbrauchspotential.

Was wir brauchen sind mehr IT-Spezialisten und geschultes Personal bei Polizei, Staatsanwaltschaft, Gerichten und nicht zuletzt beim Gesetzgeber. Ein Mehr an internationaler Zusammenarbeit, klare, aber sinnvolle Regeln für Plattformbetreiber und präventive Maßnahmen wie Awareness-Bildung und Aufklärung der Bevölkerung.

# DIGITALISIERUNG

## 9

## Der Verfassungsgerichtshof (VfGH) beschäftigt sich gerade mit Teilen des Sicherheitspakets, u. a. dem Bundestrojaner. Wo sehen Sie die Stärken und Schwächen des von den Kritikern als Überwachungspaket bezeichneten Maßnahmenbündels?

### Die neue Volkspartei

Der rasante technologische Fortschritt erfordert eine Anpassung der gesetzlichen Ermittlungsmöglichkeiten, um die Handlungsfähigkeit der österreichischen Behörden sicherzustellen. Daher wurde im vergangenen Jahr das angesprochene Sicherheitspaket beschlossen. Wir müssen unsere Behörden mit maßvollen, aber notwendigen Instrumenten ausstatten, um Terror und schwerste Verbrechen aufklären zu können. Dazu zählte auch ein Schließen bisheriger Gesetzeslücken. Wenn Verbrecher vom Telefon auf verschlüsselte Kommunikation wie Skype oder WhatsApp umsteigen, dann kann die polizeiliche Überwachung nicht mehr stattfinden. Die Justiz muss auf diese Informationen im Anlassfall zugreifen können, etwa um diese Daten als Beweis für die Strafverfolgung nutzen zu können. Auch die Anlassedatenspeicherung ist nur auf Anordnung der Staatsanwaltschaft und nach richterlichem Beschluss ausschließlich bei Verdacht von besonders schweren Straftaten möglich und auf den Anschluss einer bestimmten Person beschränkt.



Die SPÖ hat sowohl den Bundestrojaner wie auch andere Bestimmungen dieses Pakets vor den Verfassungsgerichtshof gebracht, damit dieser die verfassungsrechtlichen Bedenken, die wir gegen diesen Gesetzesbeschluss haben, überprüft. Für die SPÖ ist insgesamt der Eingriff in das Recht auf Privatsphäre zu weitgehend, wobei aus datenschutzrechtlicher Sicht dabei zwei Maßnahmen hervorzuheben sind:

Eine verstärkte Videoüberwachung des öffentlichen Raums führt dazu, dass Privatheit im öffentlichen Raum kaum mehr möglich ist, da die Sicherheitsbehörden Zugriff zu allen von Rechtsträgern des öffentlichen oder des privaten Bereichs, sofern letzteren ein öffentlicher Versorgungsbereich zukommt, gespeicherten Ton- und Bilddaten erhalten (§ 53 Abs. 5 SPG). Ergänzend dazu erhalten die Behörden aber auch direkten Zugang zu den Aufnahmezentren und dürfen an Ort und Stelle diese Daten in Echtzeit streamen. Für den Datenzugriff genügt schon der Zweck der Vorbeugung wahrscheinlicher Angriffe.

Diese Maßnahmen kombiniert mit Gesichtserkennungsprogrammen führen zu einer beinahe lückenlosen Überwachung jeder Person im öffentlichen Raum und damit zu einer maßlosen Einschränkung des Grundrechts auf Privatheit.

Darüber hinaus werden in Zukunft aber auch Fahrzeuge und deren Lenker sowie die Beifahrer großflächig durch beispielsweise die Kameras der ASFINAG erfasst und die dabei entstandenen Daten gespeichert (§ 54 Abs. 4b SPG). Auch diese Daten stehen in Zukunft den Sicherheitsbehörden unter denselben Voraussetzungen zur Verfügung. An diesem Beispiel lässt sich deutlich zeigen, dass eine positive Überwachungsmaßnahme im Sinne der Verkehrssicherheit und des Schutzes von Menschenleben nunmehr auch für völlig andere Zwecke – nämlich die umfassende Überwachung der Bürgerinnen und Bürger – verwendet werden soll.



Man muss der Exekutive auch das notwendige Rüstzeug geben, um Kriminalität und Terrorismus effektiv bekämpfen zu können. Unbegründete Massenüberwachung ist aber strikt abzulehnen.



Diese Maßnahmen sind komplett unverhältnismäßig, daher haben wir sie vor den VfGH gebracht. Das Überwachungspaket hat die regelrechte Besessenheit der ÖVP-FPÖ-Regierung mit dem Sammeln von Daten, Überwachung und Bespitzelung der Bevölkerung gezeigt. Anstatt sich für die Sicherheit der Menschen einzusetzen, passiert genau das Gegenteil. Die in dem Sicherheitspaket enthaltene anlasslose Vorratsdatenspeicherung lehnen wir grundsätzlich ab. Der Bundestrojaner ist eine extrem teure und missbrauchsanfällige Maßnahme. Privatsphäre und Grundrechte der Bürgerinnen und Bürger dieses Landes dürfen nicht leichtfertig am Altar vermeintlicher Sicherheit geopfert werden. Bevor wir weiterhin in teure, technisch und ethisch fragwürdige Maßnahmen Geld pumpen, müssen wir uns anschauen, wie wirksam die aktuellen Maßnahmen sind. Wir NEOS werden auch weiterhin gegen exzessive Überwachung der Bürgerinnen und Bürger kämpfen.



Das Beispiel Martin Balluch hat uns gezeigt, wie Gesetze, die bewusst oder unbewusst falsch angewendet wurden, einen Menschen in seiner Existenz vernichten können. Der Bundestrojaner darf nicht zum willfährigen Werkzeug einer politisch gesteuerten Exekutive werden. Dessen Einsatz muss auf entsprechenden Rechtsgrundlagen basieren und der sogenannte Bundestrojaner darf ohne richterliche Genehmigung und Kontrolle nicht eingesetzt werden. Maximale Bürgertransparenz bei gleichzeitiger maximaler Amtsverschwiegenheit ist ein Zustand, der nicht hingenommen werden kann. Letztlich zielt das Überwachungspaket darauf ab, die Freiheit der Menschen in diesem Land einzuschränken.



Wir sehen das Überwachungspaket sehr kritisch. Bevor neue Überwachungsmaßnahmen eingeführt werden, ist es dringend notwendig, bereits bestehende Überwachungsmöglichkeiten auf ihre Wirksamkeit und Effektivität zu überprüfen. Es ist dringend davon abzuraten, neue Überwachungsmaßnahmen einzuführen, ohne die Überwachungsgesamtrechnung anzugehen. Die Einführung des Bundestrojaners stellt ein Sicherheitsrisiko für uns alle dar. Durch das Ausnutzen von Sicherheitslücken zur Aufklärung gewisser Straftaten hat der Staat ein Interesse daran, dass diese Sicherheitslücken von mobilen Geräten nicht geschlossen werden. Diese Sicherheitslücken können aber nicht nur vom Staat, sondern auch von Cyberkriminellen ausgenutzt werden und somit die Sicherheit von uns allen gefährden. Wir unterstützen daher den im Parlament liegenden Initiativantrag zur Rücknahme des Bundestrojaners.



Wir sehen in den sogenannten Sicherheitspaketen schwerwiegende Eingriffe in die Grundrechte. Abgesehen von der fragwürdigen Wirksamkeit haben wir Bedenken bei der technischen Umsetzung und deren Folgen für die IT-Sicherheit. Angesichts der heutigen technischen Möglichkeiten ist die Gefahr einer Gedankenpolizei à la George Orwells Roman ›1984‹ erschreckend konkret.



Wir sind grundsätzlich gegen die anlasslose Massenüberwachung der österreichischen Bevölkerung und lehnen daher das Überwachungspaket als Ganzes ab. Wir wollen nicht, dass Österreich in einen Polizei- und Überwachungsstaat umgebaut wird. Auch sehen wir die Sicherheit der IT-Infrastruktur gerade durch Maßnahmen wie den Bundestrojaner gefährdet. Immerhin werden existierende Schwachstellen aktiv ausgenutzt, anstatt sie dem Hersteller zur Behebung zu melden. Abgesehen von verfassungsrechtlichen Bedenken und der möglichen Unvereinbarkeit mit EU-Recht entstehen auch enorme Kosten durch die teils eingriffsintensiven Maßnahmen, ohne die Sicherheit tatsächlich zu erhöhen.

## 10

## Welche Schritte werden Sie nach einem erfolgreichen Einzug ins Parlament setzen, um das Internet und die digitale Wirtschaft zum Nutzen sowohl der Bürgerinnen und Bürger als auch der Unternehmen zu fördern?

### Die neue Volkspartei

Wir wollen Österreich zum digitalen Herzen Europas entwickeln. Zum Einem durch Weiterentwicklung der Verwaltung zu einer modernen Anlaufstelle für Bürger und Bürgerinnen. Zum Anderem wollen wir die digitalen Kompetenzen aller Altersgruppen fördern, um die Fachkräfte und Unternehmer von morgen auszubilden und gleichzeitig die digitale Kluft zu schließen. Diesen begonnen Weg wollen wir im Parlament und in der nächsten Regierung weiterführen.



Es bedarf einer klaren Schwerpunktsetzung im Bereich der Forschungs- und Technologieförderung durch ein Forschungsfinanzierungs-Gesetz, das einen Wachstumspfad vorsieht und langfristige Budgets der Förderagenturen sowie der Forschungseinrichtungen beinhaltet.



Sofern der Wähler der FPÖ ein ausreichendes Vertrauen schenkt und damit auch die Basis für eine Fortführung der erfolgreichen Regierungsarbeit 2018/19 liefert, werden wir den begonnenen richtigen Weg fortführen.



In vielen Bereichen herrschen außerdem nach wie vor Rechtsunsicherheit und Durchsetzungsdefizite von geltendem Recht. Die Politik steht oft wie gelähmt daneben und schafft es nicht, Antworten auf gegenwärtige und zukünftige regulatorische Herausforderungen zu finden. Das Recht muss online wie offline gelten, klar und nachvollziehbar sein, sowie angemessen durchgesetzt werden. Das betrifft sowohl die großen Plattformen als auch neue Technologien und disruptive Dienste. Die beste und wichtigste Digitalisierungspolitik ist aber Bildungspolitik. Es reicht nicht, Schulbücher durch Tablets zu ersetzen. Wie wir heute leben und vor allem in Zukunft leben werden, ist derzeit im Unterricht kaum abgebildet. Wir wollen Österreich zum Innovation-Leader machen und dafür braucht es nicht nur gute Informatiker und Mathematiker. Auch der kritische Umgang mit Software und Information will gelernt sein und ist wichtiges Rüstzeug für die Informationsgesellschaft.



Die Digitalisierung war bisher mit Ausnahme der Bürger\*innenüberwachung kein besonderes Thema in der Politik. Im Parlament gilt es zuerst ein breites Bewusstsein bei allen Fraktionen und Parlamentarier\*innen zu schaffen. Denn ohne klare Vorstellungen zur Digitalisierung wird Österreich früher oder später auf dem Abstellgleis landen. Dann können einige der bisher genannten Projekte in Angriff genommen werden. Solange Tempo 140 im Infrastrukturministerium wichtiger ist als die Datenautobahn, solange wird Österreich in den Rankings weiter zurückfallen.

Dabei ist auch die Zusammenarbeit, nicht die Lobbyarbeit, von Anbietern, Wirtschaft und Konsumentenschutz mit dem Parlament gefragt. Die Schaffung einer Bürger\*innenplattform zum Thema Digitalisierung wäre ebenfalls hier dringend notwendig.



Als erstes: Neben Bürger\*innen und Unternehmen kann die Digitalisierung uns auch helfen, die Klimakrise zu meistern. Für eine Konkurrenzfähigkeit der Bahnlogistik inklusive autonomen Transports auf der letzten Meile sind vollintegrierte digitale Lösungen genauso Voraussetzung wie für ein stabiles Stromnetz bei 100% Ökostrom-Einsatz. Darüber hinaus gilt es, zwei Ziele zu erreichen: Erstens, eine flächendeckende Versorgung Österreichs mit Breitbandinternet unter möglichst effizientem Einsatz öffentlicher Gelder. Und zweitens: da die beste Infrastruktur nur etwas bringt, wenn alle sie nutzen können, brauchen wir Grundregeln für den Sinn und Zweck des Internets in Österreich. Damit sind beispielsweise Netzneutralität, ein Nein zur Dauerüberwachung oder die unbedingte Durchsetzung der Pressefreiheit (Stichwort Uploadfilter und Leistungsschutzrecht) gemeint.



- Einsatz Freier Software/Open Source
- Besseres und mehr freies WLAN
- Breitbandförderung, vor allem für den ländlichen Raum
- Förderung gemeinnütziger Initiativen und Non-Profit Kooperationen
- Aktives Auftreten gegen den Überwachungswahn



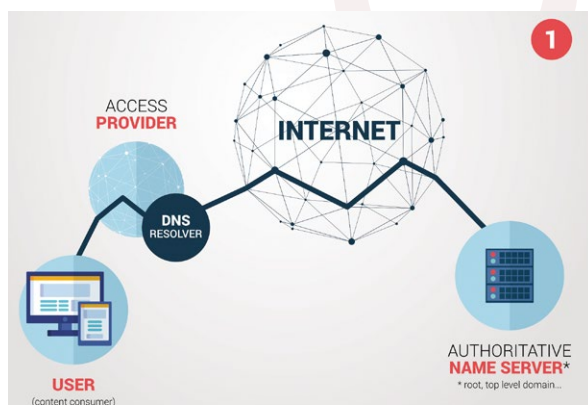
Hier möchten wir auf die unter Frage 6 beschriebenen Maßnahmen verweisen.

Ein weiterer wichtiger Punkt ist Open Data. Wissen vermehrt sich, wenn man es teilt. Wissen, das an staatlichen Institutionen generiert wird oder das der Staat direkt finanziert, muss für alle Marktteilnehmer unbeschränkt und kostenlos verfügbar sein. Freies Wissen steigert die Chancengleichheit und fördert die Wirtschaft im Ganzen.

Das Protokoll DNS over HTTPS (DoH) und seine Auswirkungen auf die fundamentalen Funktionsweisen des Internets werden unter Fachleuten bereits länger diskutiert. Durch eine durchaus unglückliche Einzelaktion eines nationalen Providerverbandes war das Thema zuletzt auch Gegenstand öffentlicher und durchaus polemischer Debatten. Da diese technische Entwicklung dennoch für viele noch relativ unbekannt ist, soll dieser Artikel über Funktionsweise und Auswirkungen von DoH informieren. Dieser Text basiert auf dem Issue Paper »DNS over HTTPS« von CENTR, dem internationalen Zusammenschluss von Top-Level-Domain-Registrierungsstellen mit Sitz in Brüssel<sup>1</sup>. Die Grafiken wurden uns freundlicherweise zur Verfügung gestellt.

### Was bedeutet DNS over HTTPS eigentlich?

Die Darstellung von Computernamen, auch Domain-Namen, wie beispielsweise [www.ispa.at](http://www.ispa.at) ist bekanntlich ein Hilfsmittel für Menschen, um sich die Adresse von Webseiten oder E-Mail-Adressen zu merken. Computer und andere Geräte können mit dieser Darstellung jedoch wenig anfangen, da sie numerische IP-Adressen (z. B. unter IPv4) verwenden, um miteinander zu kommunizieren. Deshalb findet im Internet jedes Mal, wenn ein Domain-Name aufgerufen wird, eine Übersetzung statt. Im Regelfall bedeutet dies, dass das Betriebssystem eines Geräts, z. B. eines Laptops oder eines Smartphones, die Anfrage »Wie lautet die IP-Adresse für [www.ispa.at](http://www.ispa.at)?« an einen sogenannten Resolver stellt, der sich um die Namensauflösung, also die Übersetzung in IP-Adressen, kümmert. Heutzutage ist es üblich, dass Internet Service Provider (ISP) ihren Nutzerinnen und Nutzern diese Übersetzungsleistungen zur Verfügung stellen.



Geregelt und aufgelöst werden diese Anfragen durch das Domain Name System (DNS), das wie ein Verzeichnis aller Webseiten fungiert. Dieses System ist ein bewährtes und stabiles Protokoll, bei dessen Erstellung vor

# DoH – FLUCH ODER SEGEN?

## Das DNS over HTTPS Protokoll

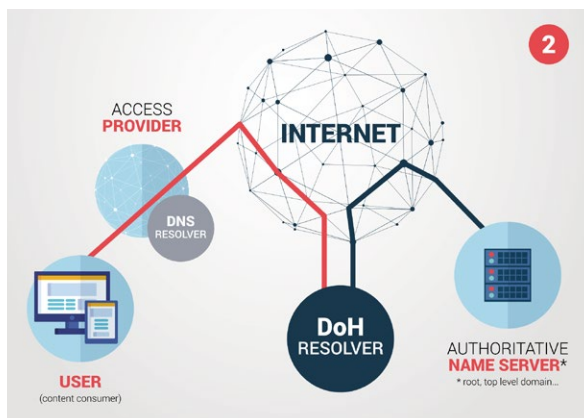
**Die technischen Neuerungen bieten zweifellos Werkzeuge für ein sichereres Internet. Gleichzeitig wollen die damit für viele Teile der Internetwirtschaft spürbaren Auswirkungen im Vorfeld gut durchdacht und abgewogen sein.**

über 30 Jahren allerdings zwei Aspekte nicht bedacht wurden, die heute von vielen als Schwächen wahrgenommen werden.

1. Die Anfragen, um einen Domain-Namen in eine IP-Adresse aufzulösen, werden im Klartext geschickt. Das bedeutet, dass beispielsweise der Betreiber des WLAN im örtlichen Café bei ausreichender technischer Expertise beobachten kann, welche Domain-Namen, ergo welche Webseiten, die Gäste des Cafés aufrufen.
2. Diese Transparenz birgt das Risiko, dass diese Anfragen abgefangen und falsche Antworten zurück an die Gäste des Cafés geschickt werden. Dies könnte auch dazu führen, dass die Gäste auf betrügerische Webseiten oder in weniger demokratischen Teilen der Welt auf regierungsfreundliche Webseiten fehlgeleitet werden.

Um diesen Schwächen des DNS zu begegnen, wurde DNS over HTTPS entwickelt und im Oktober 2018 von der Internet Engineering Task Force (IETF), freigegeben.

Im Kern stellt das DoH-Protokoll eigentlich eine leichtfüßige und elegante Lösung dar, denn es nützt bereits existierende Technologie, um die wahrgenommenen Schwächen zu beheben. Dabei werden die Anfragen über das weitaus sicherere HTTPS-Protokoll geschickt, das Teil des Browsers ist. Die Anfragen laufen also nicht mehr über das jeweilige Betriebssystem, sondern über den verwendeten Browser. Das hat den Vorteil, dass diese verschlüsselte Kommunikation (das »S« in HTTPS steht für »secure«, also »verschlüsselt«) weder durch den Provider noch den Betreiber des WLAN im Café aus obigem Beispiel beobachtet werden kann. Daraus ergibt sich, dass sogenannte »man-in-the-middle«-Attacken, bei denen Anfragen abgefangen (und die Gäste des Cafés, die Kunden eines bestimmten ISPs oder die Nutzer eines bestimmten Landes umgeleitet) werden, nahezu unmöglich sind.



So weit, so gut. DoH stellt somit aus technischer Sicht unter dem Gesichtspunkt der Sicherheit zweifellos eine Verbesserung dar, denn es behebt die zwei genannten Schwachpunkte.

Das verbesserte Protokoll gibt allerdings nicht vor, wer die Anfragen zur Namensauflösung, also zur Übersetzung in IP-Adressen, übernimmt. Dies kann nach wie vor durch den lokalen Provider erfolgen oder aber durch einen anderen Resolver. Und das ist der Punkt, an dem die Diskussion interessant wird.

Im Anschluss der Freigabe von DoH durch die IETF erklärten Browser-Unternehmen, DoH zum Wohle ihrer Nutzerinnen und Nutzer einsetzen zu wollen, was für sie jedoch gleichzeitig auch zu größerer Kontrolle und somit Verantwortung über die Datennutzung ihrer Nutzerinnen und Nutzer führt. Es würde nun an ihnen liegen zu entscheiden, wohin (und auch in wessen Gerichtsbarkeit) sie die Milliarden von Anfragen schicken, die sie jeden Tag von Nutzerinnen und Nutzern auf der ganzen Welt bekommen. Der hier vorliegende Artikel geht von der Annahme aus, dass sich jedes Browser-Unternehmen für einen einzigen Resolver entscheiden würde und Anwenderinnen und Anwendern damit die Möglichkeit verwehrt bliebe, selbst einen Resolver zu bestimmen. Eine weitere Annahme lautet, dass die zum Einsatz kommenden Resolver in den USA angesiedelt wären. Diese Annahmen fußen auf ursprünglichen Statements mancher Browser-Hersteller und Resolver. Im Zuge der öffentlichen Debatte wurden mittlerweile mehr Details bekannt und die Browser-Unternehmen und Resolver haben ihre Absichten öffentlich zum Ausdruck gebracht (siehe Seite 17).

Für die Browser-Hersteller liegen die Vorteile auf der Hand: Sie erhöhen ihre Kontrolle über das gebotene Erlebnis beim Browsen, sie können ihre Nutzerinnen und Nutzer somit besser schützen und gleichzeitig auch entscheiden, wer die unzähligen Anfragen übersetzt. Mozilla erwägt zum Beispiel eine Zusammenarbeit mit Cloudflare.

Gleichermaßen würde eine Einführung von DoH und die damit einhergehenden Entscheidungen der Browser-Anbieter aber auch maßgebliche Konsequenzen für weite Teile der Internetwirtschaft nach sich ziehen, deren Tragweite bei der technischen Entwicklung des Protokolls vielleicht noch nicht in vollem Umfang bedacht wurde oder noch gar nicht absehbar ist.

### Auswirkungen auf die Nutzerinnen und Nutzer

Die meisten Userinnen und User des Internets haben weder technisches Verständnis noch großes Interesse daran, was sich im Hintergrund abspielt, während sie surfen oder E-Mails schreiben. Obwohl die Art und Weise, wie Anfragen an die Resolver gestellt werden, durch Nutzerinnen und Nutzer momentan mit nur wenigen Klicks geändert werden könnte, gibt es für die meisten von ihnen keine Veranlassung dies zu tun, und die wenigsten wissen, wo sich diese Einstellungen vornehmen lassen. Dennoch erfüllt diese Wahlmöglichkeit eine wichtige Rolle, denn sie ermöglicht im Bedarfsfall ein sichereres Browsen oder eine mehr oder weniger restriktive und zensurierte Nutzung. So ermöglicht sie durch die Auswahl besonderer DNS-Server schon jetzt beispielsweise elterliche Kontrolle und Vorsorge. Am wichtigsten ist aber die Möglichkeit, einen Resolver auswählen zu können, mit dessen Datenschutzbestimmungen man sich am wohlsten fühlt. Man kann sich für einen nationalen oder europäischen Resolver entscheiden, der der DSGVO unterliegt, oder für einen US-amerikanischen. In diesem Zusammenhang sei noch einmal betont, dass sämtliche Anfragen – also alle Webseiten, die man besucht, und alle E-Mail-Adressen, mit denen man kommuniziert – im Normalfall beim Resolver landen. Dadurch sind Rückschlüsse auf sensible Informationen möglich und man ist persönlich identifizierbar.

Ein weiterer relevanter Aspekt ist etwas, das oft als ›Universalität des Internets‹ bezeichnet wird. Dahinter steht die Logik des DNS, dass eine Anfrage immer die gleiche Antwort zutage fördert, gänzlich unabhängig von der Software, die man benutzt. Da die Anfragen innerhalb des DNS momentan durch das Betriebssystem gestellt werden, lautet die Antwort auf die zu Beginn des Textes gestellte Frage »Wie lautet die IP-Adresse für www.ispa.at?« auf jedem Gerät und in jedem Browser gleich. Es ist nicht gänzlich unrealistisch anzunehmen, dass nach einer Implementierung von DoH unterschiedliche Resolver, die aus anderen Gerichtsbarkeiten als ihre Nutzerinnen und Nutzer stammen, anders lautende Antworten auf die Frage liefern würden, wo die Webseite des österreichischen Betreiberverbandes zu finden ist. So könnte der Zugang zu Informationen durch die Obrigkeit am Standort des Resolvers eingeschränkt werden, obwohl die abgefragten Inhalte am Standort der Userin oder des Users völlig legal sind. Dies würde womöglich nur auf eine bestimmte Anzahl von Domains zutreffen, aber je nach Wahl des Browsers würde man ein unterschiedliches Internet angezeigt bekommen.

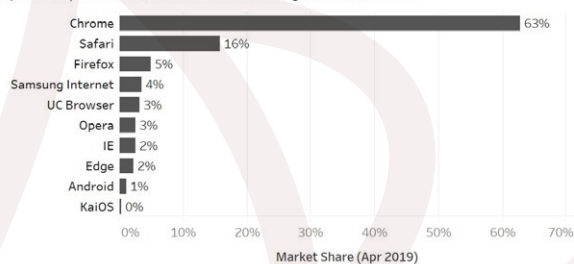


## Auswirkungen auf die Internetwirtschaft

Am deutlichsten wird die Tragweite einer allfälligen Einführung von DoH, wenn man die Marktverteilung unter den Browser-Herstellern betrachtet: Fünf Browser decken aktuell rund 90 Prozent des Weltmarkts ab, was die Auswahlmöglichkeiten der Kundinnen und Kunden deutlich einschränken könnte. Diese Zuspitzung auf wenige Anbieter wird noch verstärkt durch Kompatibilitätsanforderungen und Browser-Optimierungen, denn der überwiegende Teil der Webseitenbetreiber ist bemüht, die Entwicklungskosten gering zu halten, indem man den Wünschen der wenigen Browser-Unternehmen möglichst entspricht.

### Browser market share

April 2019 | Source: StatCounter Global Stats, gs.statcounter.com



Die Verdichtung von Marktmacht bei wenigen Browser-Herstellern und den Resolvieren, mit denen sie zusammenarbeiten, könnte einige Konsequenzen nach sich ziehen. Auch wenn es zunächst weit hergeholt erscheinen mag, könnten die Funktionsweise des DNS und die Art und Weise, wie es sich in Zukunft entwickelt, betroffen sein. Es lohnt sich in diesem Zusammenhang festzuhalten, dass die Autorität der Root Zone zu respektieren, aktuell auf freiwilliger Basis passiert. Die Root Zone beinhaltet die Namen und IP-Adressen aller Nameserver aller Top-Level-Domains. Jeder durch einen ISP bereit gestellte Resolver, der einen Domain-Namen auflösen möchte, fragt in der Root Zone an, respektiert die Antwort, die er von dort erhält, und zeigt Nutzerinnen und Nutzern das entsprechende Ergebnis an. Würde er sich nicht daran halten (und ein anderes Ergebnis anzeigen), würden die Kundinnen und Kunden des ISPs sich rasch einen anderen Dienstleister suchen. Gibt es allerdings nur noch wenige – dominierende – Marktteilnehmer, so ist unklar, ob sich dieses Prinzip aufrechterhalten lässt. Sollten diese einzeln oder gemeinsam zur Ansicht kommen, die aus der Root Zone erhaltenen Antworten nicht zu respektieren, gäbe es für sie dafür wenig bis keine Sanktionen. Stark betroffen wäre von einer solchen Entscheidung aber der Multi-Stakeholder-Ansatz unter der Federführung der Internet Corporation for Assigned Names and Numbers (ICANN), über den die

Identifikatoren festgelegt werden, anhand derer eine Adresse im Internet einzigartig, erkennbar und ansteuerbar wird. Theoretisch könnte eine Handvoll Resolver entscheiden Anfragen zu einer bestimmten Domain oder einer gesamten Top-Level-Domain zurückzuweisen, die sie für zu lasch im Umgang mit Missbrauch, Spam, Malware oder als problematisch erachtet.

Durch die Einführung von DoH würde sich zudem ein wichtiger ›Kontrollpunkt‹ verschieben. Im Moment kann der ISP den DNS-Datentransfer beobachten und so auch sein Netzwerk vor Missbrauch schützen. Das passiert z. B., wenn ISPs die Anfragen von Schadsoftware blocken, die die Geräte ihrer Kundinnen und Kunden befallen hat. Sie machen dadurch nicht nur ihr eigenes Netzwerk sicherer, sondern verhindern auch, dass sich Attacken und Schadsoftware auf andere Netzwerke ausbreiten. Mit DoH würde dies wegfallen, denn die ISPs könnten nicht mehr beobachten, welche Anfragen gestellt werden.

Dies hat noch weitere Konsequenzen. Nationale Gesetzgeber haben sich in der Vergangenheit dafür entschieden, ISPs zu verpflichten, den Zugang zu illegalen Inhalten durch Eingriff in die Resolver zu beschränken. Das hat sich ungeachtet des beständigen Widerstands der Provider als populärer, wenn auch ineffizienter und oftmals überzogener Weg herausgestellt, um den Zugang zu Inhalten zu unterbinden, die unter fremder Gerichtsbarkeit gehostet werden.

Mit DoH verschiebt sich der ›Kontrollpunkt‹ zu den Resolvieren, die von den Browsern mit der Übersetzung der Anfragen beauftragt werden. Weil diese Resolver in den USA ansässig sind, käme somit US-amerikanisches Recht zur Anwendung. Mit Cloudflare hat einer dieser Anbieter bereits öffentlich verlautbart, allfälligen Druck durch Behörden widerstehen zu wollen. Es bliebe allerdings abzuwarten, ob und wie lange Unternehmen in der Lage wären, einem solchen Druck standzuhalten.

## Position der Browser-Unternehmen

Mit Fortdauer der Debatte zum Thema DoH werden mehr und mehr Details bekannt und sowohl Browser-Hersteller als auch Resolver beziehen öffentlich Stellung zu ihren Vorhaben. Im Falle von Mozilla (und dem Resolver ihrer Wahl: Cloudflare) gehen die Aussagen in die Richtung, dass Userinnen und Usern eine beschränkte, von Mozilla auf Basis strikter Qualitätskriterien freigegebene Auswahl von Resolvieren zur Verfügung stehen soll. Google Chrome und sein eigener Resolver 8.8.8.8. haben angedeutet die Übersetzung von Anfragen weiter bei den ISPs zu lassen, sofern diese ihren Kundinnen und Kunden einen Resolver zur Verfügung stellen, der DoH-fähig ist. Die Standards zum Austausch zwischen Browser und ISP müssten aber noch festgelegt werden.

Die ISPA steht im Rahmen der EuroISPA im ständigen Kontakt mit Browser-Herstellern wie Mozilla und ist bemüht, in dieser Causa zu vermitteln, um eine für alle Seiten zufriedenstellende Lösung zu erreichen. ■

»Ein neuer Besen, der ohne Struktur kehrt, ist eine riesige Staubwolke.«



**Dr. Klaus M. Steinmaurer, Geschäftsführer des Fachbereichs Telekommunikation und Post der RTR-GmbH im Gespräch mit ISPA Generalsekretär Dr. Maximilian Schubert**

**ISPA: Sie sind seit Anfang Juli Geschäftsführer der Rundfunk und Telekom Regulierungs-GmbH im Fachbereich Telekommunikation und Post. Welches Bild haben Sie von der Behörde?**

**Klaus M. Steinmaurer:** Ich hatte auch schon vorher ein ungefähres Bild von außen. Aber es war gut, einen Abgleich zwischen Außenbild und Innenbild zu machen. Wir haben hier viele Topexpertinnen und -experten mit einer sehr hohen Arbeitsethik und auch dem Willen, nach Lösungen mit und für den Sektor zu suchen. Es werden die richtigen Fragen gestellt,

um die genauen Probleme zu identifizieren, um dann auf diese Antworten zu finden. Das habe ich mir schon in meiner Vorbereitungszeit gedacht, aber jetzt hat sich das noch verstärkt. Wenn man außerhalb ist, denkt man sich »Ah die Behörde! Die entscheiden da Dinge, die sind nicht branchenfreundlich und zu konsumentenfreundlich.« Der Wille, Lösungen zu finden, die für alle Stakeholder gut sind, ist jedoch stark ausgeprägt.

In der Behörde braucht man einen breiteren Fokus, denn man hat viele verschiedene Argumente zu berücksichtigen. Und wenn ich in der Behörde bin, muss ich alle Interessen der Stakeholder nehmen und versuchen eine Lösung zu finden, die für alle vertretbar ist. In meiner Aufgabe ist auch ein gesetzlicher Auftrag vorgegeben: Ich muss für den Wettbewerb sorgen, ich muss erschwingliche Preise für die Konsumenten sicherstellen und auf der anderen Seite muss ich auch die technische Weiterentwicklung unterstützen, damit investiert wird.

Um den Ausgleich zwischen diesen Aufträgen zu finden, muss man auch gewisse Kompromisse eingehen. Kompromisse finden bedeutet, dass nicht jeder zu 100 % bekommt, was er will. In Summe ist es aber die richtige Lösung. Und genau diesen Weg zu suchen, das ist der Wille und die Absicht von allen Expertinnen und Experten, die wir hier haben. Da geht es nicht um irgendwelche Bevorzugungen Einzelner. Das hat mich eigentlich sehr gefreut, weil das eine gute Basis ist, auf der man aufbauen kann. Da sehe ich auch bei mir ein entsprechendes Entwicklungspotential. Aus diesem Grund haben wir uns ja auch schon Gedanken gemacht, wie wir uns strategisch in der Zukunft aufstellen. Aber die Details, die bleiben noch offen.

**Sie waren also überrascht, weil in der Innenwahrnehmung doch viel mehr in die Richtung eines Konsenses – also zum Wohl der gesamten Branche – gearbeitet wird, als sie erwartet haben?**

Zum Wohl des Sektors. Der Sektor besteht nicht nur aus den Unternehmen und der Wirtschaft, die etwas verdienen wollen, der Sektor besteht aus viel mehr. Der Sektor besteht aus den Konsumenten, den Unternehmen, die hier tätig sind, investieren, für Wettbewerb am Telekom-Markt sorgen, Arbeitsplätze schaffen und die österreichische Wirtschaft voranbringen. Und aus den Dienstleistungen, die dieser Sektor hervorbringt, die wiederum Auswirkungen auf den Rest der Wirtschaft haben. Ich habe eher einen breiteren Sektorbegriff und für den müssen wir arbeiten. Nicht nur für die Infrastrukturbetreiber oder nur für die Internet Service Provider oder nur für die Konsumenten.

**Konsumentenschutz ist ein Reizthema bei uns in der Branche. Die RTR wurde in der Vergangenheit eher als Vollzugsbehörde und nicht als Enabler wahrgenommen. Wie sehen Sie das?**

Die Vollzugsbehörde ist nicht die RTR, sondern im Wesentlichen die TKK, die hier die Vollzugsaufgabe hat. Als RTR beraten wir einerseits die TKK und haben Eigenkompetenzen im Rahmen des Gesetzes. Unser Ziel ist hier aber, ganz stark in die Enabling-Funktion zu gehen. Wir wollen viel in die Branche hineinhorchen. Zurzeit gibt es einen sehr hohen Qualitätsstandard im Bereich der Netze. Als RTR müssen wir bestimmt enablen, um für weitere Investitionen ein Framework zu schaffen. Wir haben einen hochentwickelten Konsumentenschutz im Rahmen unserer Kompetenzen, der bei uns z. B. mit der AGB-Kontrolle einhergeht. Wir müssen evaluieren, was es schon gibt, und ich glaube, wir müssen diesen Standard dann auch halten. Wir

müssen schauen, wie wir mit dem auskommen, aber ich glaube, weniger Konsumentenschutz gibt's nicht. Ich sehe hier aber nicht die allerzentralste Funktion der RTR. Konsumentenschutz ist ein wichtiger Teil, aber er ist nicht wichtiger als alle anderen Aufgaben.

**Der EECC gibt einen gewissen Spielraum vor, welche Tätigkeiten die RTR übernehmen muss. Könnten die zur Verfügung stehenden Ressourcen nicht anders besser eingesetzt werden – Stichwort AGB-Kontrolle? Wollen Sie das tendenziell beibehalten, wie es ist?**

Ich will den Konsumentenschutz nicht schwächen. Es stellt sich aber schon die Frage, wer die Konsumentenschutzthemen am besten machen kann. Grundsätzlich denke ich, dass die Aufgaben des Konsumentenschutzes, die die RTR ausübt, für die Branche positiv und gut sind. Wir haben die technische Expertise, um einschätzen zu können, ob das Problem wirklich beim Betreiber liegt oder beim Service Provider oder beim Konsumenten. Durch die Streitschlichtungsfunktion kommen wir auf einer außergerichtlichen Ebene oft viel schneller zu Lösungen als über das normale Zivilgerichtsverfahren. Aber wie wir uns in dem Bereich aufstellen werden, kann ich jetzt noch nicht sagen, wahrscheinlich eher wie im TKG. Aber ich will mich da jetzt nicht im Detail auf Konsumentenschutzdiskussionen einlassen.

**Aus Sicht der Branche, kommt es ja relativ selten vor, dass Behörden Kompetenzen oder Tätigkeiten freiwillig abgeben, Ressourcen abbauen oder anders einsetzen. Können wir davon ausgehen, dass es eine kritische Überprüfung innerhalb der Behörde geben wird?**

Es wird alles hinterfragt. Ich komme nicht in dieses Haus und verschiebe sofort Kompetenzen und Aufgaben. Ich muss erst ganz sachlich alles anschauen und anhand dessen ein Bild bekommen. Dann muss ich überprüfen, was in der Branche in Zukunft stärker benötigt und was nicht mehr so wichtig sein wird. Dann kann ich die Ressourcen, die wir haben, richtig einsetzen. Es muss sichtbar werden, was der Output ist. Dafür werde ich mich einsetzen.

**Welche Ziele haben Sie innerhalb Ihrer ersten 100 Tage?**

Innerhalb der ersten 100 Tage schaut man sich an, was gibt es alles, spricht mit den Leuten, stellt Fragen und hört zu, beobachtet und versucht sich ein umfassendes Bild über das, was bereits da ist und das was man weiterentwickeln sollte, zu machen. Wenn man dann dieses gesamtheitliche Bild hat, wird man es in eine Strategie einarbeiten. Ich habe sicher bereits einige Ideen, wie wir uns ausrichten könnten und wohin der Weg gehen sollte. Wir sind derzeit in einem gemeinsamen Strategieprozess und diskutieren die Themen mit den Mitarbeiterinnen und Mitarbeitern. Das Ergebnis,

das wir dabei herausarbeiten, soll dann transparent an die Öffentlichkeit gelangen. Das Ergebnis dieses Prozesses werden wir dann im Frühherbst öffentlich machen und diskutieren. Es wird eine Strategie geben, an der man die RTR messen kann.

**Wird es eine Konsultationsphase für die Branche geben? Oder wird die Branche über diese Strategie informiert?**

Unsere Strategie ist UNSERE Strategie. Ich lasse meine Strategie nicht von denen, die ich regulieren soll, evaluieren. Die kann man kommentieren, aber die Strategie machen wir intern für unser Unternehmen. Natürlich bin ich im Vorfeld offen für Anregungen und es gibt genügend, die mit mir Gespräche führen. Aber jeder darf überall mitreden? Das wird nichts. Es wird eine Ausrichtung geben und zu der stehen wir dann auch. Mein Ziel muss sein, dass unsere Arbeit nachvollziehbar und sachlich ist, nicht populär. Dann habe ich nämlich die beste Lösung für dieses Land und für den Sektor erreicht. Ich mache diese Arbeit nicht, um von allen geliebt zu werden.

**Welche Vorhaben werden Sie zuerst in Angriff nehmen?**

Die Strategie, die wir intern ausarbeiten, ist für mich ein wichtiger Meilenstein. Das ist auch ein Novum für die Branche, dass man transparent zeigt, wie der grobe Arbeitsplan aussehen wird. Er beinhaltet, wie wir uns verstehen, was so unsere grundsätzlichen Zielsetzungen sind und wo wir hinwollen. Wenn ich das auch transparent mache, ist das – glaube ich – dann schon etwas Neues für die Branche. Daran kann man uns dann auch messen. Ich will sehr transparent in meiner Arbeit sein.

**Wie wird der Dialog mit den Stakeholdern ablaufen?**

Ich werde mit den Betreibern, der Wirtschaftskammer und sonstigen Stakeholdern meine offenen Gespräche und Jour fixes haben. Gerade auch mit der ISPA, den Internet Service Betreibern, die für uns wichtig sind, denn das Internet wird in Zukunft überhaupt wichtiger – speziell alles, was die Plattformen betrifft. Der Austausch und die Interaktion zwischen den Stakeholdern, der Branche und uns wird immer wichtiger, denn wir können ja nur wechselseitig voneinander lernen. Je besser wir erklären, was wir denken, warum wir zu gewissen Überlegungen und Entscheidungen kommen, desto leichter sind sie nachvollziehbar, und dann können wir einen gemeinsamen Weg gehen. Wenn wir hier im verschlossenen Kämmerchen zu irgendwelchen Entscheidungen

kommen und keiner versteht warum und wieso, dann ist es, auch wenn es eine gute Entscheidung war, schlecht, weil sie eben nicht transparent ist. Deswegen werde ich auch, so oft es möglich ist, für ein Gespräch zur Verfügung stehen.

**Die Strategie wird auf der Webseite veröffentlicht werden. Erwarten Sie dann auch, daran gemessen zu werden, ob die Ziele auch erreicht wurden? Wie konkret wird die Strategie sein?**

Es werden bestimmt ein paar konkrete Ziele drinnen sein, aber es wird auch viel offengelassen. Die einzelnen konkreten Maßnahmen werden daraus dann abgeleitet. Ich kann jetzt nicht alles festlegen, was ich in den nächsten fünf Jahren an Maßnahmen mache. Das haben Lenin und seine Nachfolger auch versucht, allerdings auch nur mit mäßigem Erfolg. Eine Strategie ist nur dann eine gute Strategie, wenn sie ausreichend flexibel ist, um auf geänderte Bedingungen rasch reagieren zu können, und Gestaltungsspielräume offenlässt.

**Also keine Planwirtschaft?**

Nein, keine Planwirtschaft der RTR. Und natürlich werden wir jetzt nicht eine komplett andere Strategie haben als das, was im Regulierungskonzept drinnen steht.

Es geht um einen fairen Wettbewerb mit einem angemessenen guten Preisniveau auf diesem Markt. Ein fairer Wettbewerb gibt möglichst vielen die Chance, auch die notwendigen Investitionen zu tätigen.

**Gibt es ein Leitbild für die Tätigkeit der RTR, dem Sie folgen?**

Das Leitbild der RTR heißt, wir stehen für Wettbewerb und Medienvielfalt. Und ich möchte eine Betonung machen, wir stehen für FAIREN Wettbewerb und Medienvielfalt. Wenn ich das Wort ›fair‹ betone, kommt damit auch zum Ausdruck, dass es einen Interessensausgleich für die vielen verschiedenen Interessen innerhalb des Sektors, innerhalb der Branche gibt.

Die großen und die kleinen Unternehmen sollen am Markt die gleichen Chancen haben, tätig zu sein und sich dabei zu bewähren. Die RTR und die TKK haben jedoch nicht die Aufgabe unternehmerisches Risiko abzuschaffen. Dann bräuchte sich keiner mehr anstrengen und es fände auch kein mehr Wettbewerb statt.

**Wir haben auch kleinere Access-Anbieter als Mitglieder, z. B. ein Kabelanbieter, der mir sagt, wenn man keine Hausnummer 35.000 Kunden hat, dann ist virtuelle Entbündelung uninteressant. Wie reagieren Sie darauf?**

Dann wird man darüber diskutieren müssen. Dazu gibt es uns. Wir werden uns die Argumente links und die Argumente rechts anhören und versuchen Lösungen zu finden. Am Ende wird in solchen Fällen die TKK entscheiden. Und wenn die TKK

hier Entscheidungen trifft, wird man ordentliche Entscheidungsgrundlagen für die Behörde entwickeln. Dazu sind wir da. Dass wir aber gleich von vornherein jeden Wettbewerb rausnehmen, das ist nicht unsere Aufgabe.

Das ist ein wichtiger Punkt. Es gibt kleinere ISPs, z. B. aus Oberösterreich und Salzburg, die auch Kabel und Glasfaser usw. anbieten, mit denen ich mich zu exakt solchen Themen unterhalten habe. Genau für sowas sind wir offen und horchen uns das an. Es gibt auch immer mehrere Zugangswege abgesehen von einem formalen Verfahren. Der erste ist, durch eine gewisse Art von Mediation oder Moderation einer Diskussion das Problem zu managen und zu Lösungen zu kommen.

**In der Vergangenheit war unsere Wahrnehmung teilweise, dass auch die RTR in ihren Möglichkeiten sehr begrenzt und vom Goodwill der großen Unternehmen abhängig war. Wie ist Ihre Einschätzung dazu?**

Wir haben als RTR und TKK zwei Dinge: Wir haben gesetzlich einige Werkzeuge in der Hand, die nur bestimmte Sachverhalte und Fälle lösen können. Zusätzlich haben wir in gewissen Themenbereichen eine Autorität, die es uns ermöglicht, Gespräche zu moderieren und zu versuchen, hier außerhalb eines Verfahrens auch Lösungen zu finden. Diese Vermittlerfunktion möchte ich durchaus wieder stärker ins Auge fassen. Wir haben die notwendigen Expertinnen und Experten, die das Know-how und Kenntnisse vom Markt haben, die sich auch Themen anschauen können. In diesen Bereichen habe ich jedoch nicht die gesetzliche Macht zu entscheiden, also einen Richterspruch zu fällen.



Im Rahmen des EECC könnte man sich anschauen, ob man der RTR an der einen oder anderen Stelle zusätzliche gesetzliche Werkzeuge in die Hand gibt. Dadurch könnten wir auch das eine oder andere Problem noch schneller lösen oder auch entscheiden. Zurzeit kann ich nur im Rahmen des gesetzlichen Auftrags und der gesetzlichen Möglichkeiten wirkliche Entscheidungen treffen. Der EECC gibt auch neuen Raum hier, gerade was Themen der digitalen Wirtschaft betrifft. Jetzt bin ich wieder beim großen Sektorbegriff. Um die Themen der digitalen Wirtschaft noch konsequenter und direkter anzugehen, möchte ich einen Appell an die Branche richten, sich zu überlegen, was hier sinnvoll ist.

**Es ist zu begrüßen, dass sich die RTR für mehr Rechtssicherheit im Kontext der Urheberrechtsnetzsperrern einsetzt. Angeblich gibt es jedoch auch Überlegungen, wonach sich Ihre Behörde in Zukunft auch mit Pornografie im Internet befassen wird. Wird die RTR-GmbH damit zum allumfassenden ›Zensur- und Wahrheitsministerium‹ aufgebläht?**

Das ist ein interessanter Aspekt – ich klammere jetzt meine persönliche Meinung aus, was alles, wie und wo gesperrt oder sonst etwas gemacht werden darf. Man muss hier eigentlich strukturiert an das Thema herangehen. Das erste ist, ich muss eine grundlegende Diskussion geführt haben, welche Eingriffe in die Freiheit des Internets es geben soll. Das war bis Ende der 1990er Jahre kein Thema. Die Diskussion hat begonnen, als das Internet groß geworden ist, Anfang der 2000er, u. a. in Folge von 9/11. Das ist der eine Faktor. Im Rahmen der Kommerzialisierung des Internets sind Musiktäuschbörsen und Streaming-Plattformen entstanden. Ich habe das oft nicht verstanden, warum plötzlich Betreiber verpflichtet werden sollten, Maßnahmen für kommerzielle Themen einzusetzen, die sonst den Überwachungsbehörden in gerichtlich zu behandelnden Sachverhalten – klaren gesetzlichen Vorschriften entsprechend – zugestanden sind. Die Frage ist, wollen wir das oder wollen wir das nicht? Soll hier die Möglichkeit einer Sperre gesetzt werden oder nicht? Das eine sind die kommerziellen Urheberrechtsthemen, das andere ist die Sicherheitsthematik, wobei diese aufgrund der Einbindung der Gerichte vielleicht noch ein bisschen außen vorsteht.

Soll man bei Pornografie vorab die Betreiber verpflichten, dass sie Zugänge vorsorglich sperren? Die Frage ist dann, wer ist die Prüfinstanz? Aber es ist eine generelle Frage, die mit dem zukünftigen Gesellschaftsvertrag,

den wir haben wollen, zusammenhängt. Das Internet – da bin ich jetzt schon fast in einer philosophischen Diskussion – ist Teil unseres Lebens. Da muss man überlegen, welche Eingriffe in unsere Freiheit wir zulassen wollen. Weil de facto ist ja der Eingriff in die Freiheit des Internets ein Eingriff in die persönliche Freiheit, zu entscheiden, was ich konsumieren will und was nicht. Das ist die Frage, welchen Gesellschaftsvertrag schließen wir in Europa oder auch weltweit ab?

**Wenn die Gesellschaft zu dem Schluss kommt, es soll derartige Maßnahmen geben, dann wäre unter Umständen auch Ihre Behörde dafür zuständig?**

Es stellt sich dann als nächste Frage, wer dann – unter Anführungszeichen – der Richter sein soll. Soll die Staatsanwaltschaft oder das Innenministerium das entscheiden, in einer Staats- und Behördenstruktur? Oder ist für die Durchführung und für den Vollzug dieser Angelegenheit eine unabhängige Regulierungsbehörde nicht die geeignetere, objektivere Lösung, vor allem auch aufgrund der internationalen Vernetzungen? Ich weiß ja, wie Regulierungsbehörden weltweit entscheiden. Wenn das überall die Regulierungsbehörden machen, dann gibt es dort auch einen Austausch, dann habe ich auch einen gewissen Standard, an dem man gemessen wird.

**So etwas wie einen europäischen Good-Practice-Standard?**

Wir haben dadurch auch die Kontrolle einer breiten Öffentlichkeit. Wenn aufgrund einer nationalgesetzlichen Ermächtigung von einem Ministerium – welcher Art auch immer – ein Beschluss gefasst wird, dann steht es gar nicht zur Diskussion, dass das europäisch auch quergecheckt wird. Also ich sehe die Funktion der Regulierungsbehörden, hier die Kontrolle und die Aufsicht zu übernehmen, durchaus als gegeben. Dabei kommt es auch immer auf die Ausführung an. Eine ›Durchstempelbehörde‹ ist natürlich nicht die gewünschte Sache. Ich muss Ressourcen für die Problematik entsprechend einsetzen. Mit dieser Thematik werden wir uns in Zukunft beschäftigen müssen, denn das Internet nimmt eine sehr wichtige Rolle ein. Aber da sage ich, nutzen wir doch unser Know-how, unsere Expertise, um das bestmöglich zu machen. Trotzdem müssen wir uns zuerst gesellschaftlich auf europäischer und dann auch auf einer nationalen Ebene einigen.

**Wenn Sie über den Sektor sprechen, dann meinen Sie die Digitalwirtschaft. Jetzt gibt es kaum einen Sektor, der nicht von der Digitalisierung betroffen ist. Ist der Einflussbereich Ihrer Behörde dadurch ein stetig wachsender, auch für die gesamte österreichische Wirtschaft?**

Wenn es nach dem Gesetz geht, nicht. Aber wenn man sich bei der Umsetzung des EECC ansieht, wie die Behörde in Zukunft aufgestellt wird, ja. Also jein. Themen, bei denen es sinnvoll ist, mit unserer Expertise reinzugehen, die werden mehr. Man muss aber schauen, was hinten wegfällt. Man muss sich

ansehen, wie man seine beschränkten Ressourcen bestmöglich für die neuen Herausforderungen aufstellt, das ist klar und deutlich mein Ziel. Die nächsten fünf Jahre werden auch ziemlich spannend. Bitte jetzt nicht glauben, dass im nächsten Halbjahr alles besonders und anders wird und die Regulierung sich ändert. Man muss Schritt für Schritt vorgehen.

**Aber kehrt ein neuer Besen nicht besser? Ist die Wahrscheinlichkeit, dass es noch große Änderungen in einer Behörde gibt, nicht geringer, wenn ein Jahr vorbei ist?**

Mit dem neuen Besen bin ich bei Ihnen, aber trotzdem muss der neue Besen eine Struktur haben und Raum für Raum entsprechend kehren. Ich bin ein wirklich sehr prozessorientierter, strukturierter Mensch. Ich bin keiner, der kommt, ›wusch‹ und jetzt machen wir alles neu. Ein neuer Besen, der ohne Struktur kehrt, ist eine riesige Staubwolke. Wichtig ist sich im ersten Halbjahr Ziele zu setzen, nach denen man messbar ist, die immer wieder überarbeitet werden, wenn es etwas Neues gibt. Wenn man am Anfang diesen Pflock eingerammt hat, dann kann man sehr strukturiert das ganze Haus auf den neuesten Stand der Technik bringen und saubermachen.

**Wie stehen Sie zum Thema DoH?**

Die Angst vieler ist, dass dies zu einem Monopol oder einem Oligopol wird. Die Security-Thematik ist eine wichtige, die DNS-Thematik in der unverschlüsselten Art und Weise ist unbefriedigend. Wir begrüßen grundsätzlich diese Möglichkeiten, hier in Zukunft verschlüsselte Lösungen zu übernehmen. Je mehr das machen und übernehmen, desto besser. DoT ist grundsätzlich schon relativ gut möglich, DoH geht nur, wenn du es über ein automatisiertes System hast, das der Betreiber zur Verfügung stellt. Es ist nicht so, dass ISPs dies grundsätzlich nicht machen können, es ist wahrscheinlich mit etwas Aufwand verbunden, das einzurichten. Um auf den Kritikpunkt der Zentralisierung einzugehen: Je mehr das machen – auch auf ihrer Netzebene – desto breiter ist das Angebot und desto weniger ist die Gefahr einer Monopolisierung bei Cloudflare und bei Google gegeben. Als Behörde begrüßen wir grundsätzlich die Möglichkeit von DNS-Verschlüsselungen.

**Vielen Dank für das Gespräch und wir sind sehr gespannt auf die Vorstellung Ihrer Strategie.**

(Das Gespräch fand Mitte Juli in den Räumlichkeiten der RTR statt.) ■

## Digitalsteuer schützt vor allem überholte Geschäftsmodelle



**Das Vorhaben könnte vom Parlament noch im September beschlossen werden und bringt überzogene Haftung für Vermittlerplattformen, eine Querfinanzierung österreichischer Medienunternehmen auf Kosten der heimischen Wirtschaft und nicht zuletzt die Gefahr eines Handelskonflikts mit den USA.**

**d**er Gesetzesentwurf zur Digitalsteuer, der bereits im September im Parlament beschlossen werden könnte, wirft mehr Fragen auf, wie die Internetwirtschaft gerecht besteuert werden kann, als er Antworten gibt. »Der österreichische Alleingang ist im Wesentlichen eine Querfinanzierung überholter Geschäftsmodelle und bringt überzogene Haftung für Vermittlerplattformen. Darüber hinaus ist die technische Umsetzung weiterhin unklar und eine gänzlich anonymisierte Erhebung der Daten in der Praxis daher fraglich. Im schlechtesten Fall provoziert das Gesetz einen Handelskonflikt mit den USA«, kritisiert ISPA Generalsekretär Maximilian Schubert das Vorhaben der ehemaligen Koalitionsregierung zwischen ÖVP und FPÖ, welches trotz Koalitionsende von beiden Parteien erneut ins Parlament eingebracht wurde.

### Intransparente Querfinanzierung der Medienunternehmen durch die heimische Wirtschaft

Anders als dargestellt wird die Steuer nicht von den im Entwurf als ›Internetgiganten‹ bezeichneten internationalen

Konzernen, sondern letztlich von österreichischen Unternehmen bzw. deren Kundinnen und Kunden zu tragen sein. Internationale Unternehmen werden die Steuerabgabe zwar leisten, diese aber wie in der Geschäftswelt üblich an die Auftraggeber der Werbung weiterverrechnen, die diese dann in ihre Dienstleistungen und Produkte einpreisen müssen.

Die Nutznießer der Digitalsteuer sind speziell österreichische Medienunternehmen. Von den Erträgen der Digitalsteuer sollen jährlich 15 Millionen Euro abgestellt werden, um den »digitalen Transformationsprozess österreichischer Medienunternehmen« zu fördern. Doch das Gesetz gibt keinerlei Anhaltspunkte, was als förderbar gilt und wie die Mittel aufgeteilt werden. »Das ist intransparent und legt nahe, dass lediglich veraltete Geschäftsmodelle österreichischer Verleger, die auf den Entwurfsprozess ja auch aktiv eingewirkt haben, künstlich am Leben gehalten werden. Es ergibt ein durchaus fragwürdiges Gesamtbild«, bemerkt Schubert.

Im Ergebnis handelt es sich bei der Digitalsteuer daher vor allem um eine Querfinanzierung österreichischer Verlagshäuser auf Kosten anderer heimischer Unternehmen. Gerade angesichts der Tatsache, dass viele österreichische Betriebe derzeit Digitalisierungsschritte durchlaufen und ihre Online-Präsenz etwa auch anhand verstärkter Online-Werbung ausbauen, ist eine solche Belastung wohl kritisch zu sehen.

### -----> **Datenschutzkonforme Umsetzung weiterhin fraglich**

Ein weiterer kritischer Aspekt des ursprünglichen Gesetzesentwurfs war die datenschutzkonforme Umsetzung. Denn um Werbeleistungen mit Österreichbezug zu bestimmen, ist die Erhebung der jeweiligen IP-Adresse des Endgeräts, auf welchem die Werbung aufscheint, notwendig. Durch die Kombination einer bestimmten IP-Adresse samt angezeigter Werbung sind jedoch sensible Rückschlüsse auf den Gesundheitszustand, die religiöse bzw. politische Zugehörigkeit oder die sexuelle Orientierung der Nutzerin oder des Nutzers möglich. Sollten diese Daten in die falschen Hände geraten, ist das Schadenspotenzial exorbitant.

Der Gesetzgeber ist auf die unter anderem von der ISPA deutlich geäußerte diesbezügliche Kritik jedoch kaum eingegangen. Es bleibt somit fraglich, wie die

dem Nationalrat nun vorgelegte Fassung, welche eine anonymisierte Erhebung der Daten anregt, in der Praxis umgesetzt werden kann, speziell wenn die jeweilige Werbeleistung auf der Webseite eines Drittanbieters erbracht wird. Denn eine Anonymisierung der IP-Adresse bereits bei deren Erhebung, etwa durch Löschung der letzten vier Stellen, müsste von sämtlichen Website-Betreibern, welche Werbeplatz zur Verfügung stellen, vorgenommen werden. Dies ist nicht nur in der Praxis schwer vorstellbar, sondern liegt auch außerhalb der Reichweite des österreichischen Gesetzgebers und zeugt von der Unausgereiftheit des Gesetzesentwurfs.

### **Überzogene Haftung für Vermittlerplattformen**

Das Gesetz sieht auch eine überzogene Haftung für Vermittlerplattformen der »sharing economy« vor.

Diese wird besonders kleine und mittelgroße heimische Betriebe in dieser aufstrebenden Branche hemmen, da das Haftungsrisiko und der Administrationsaufwand enorm sind. So sollen diese Unternehmen als Vermittler von Leistungen haften, falls der Erbringer einer Leistung z. B. die Umsatzsteuer nicht korrekt abführt. »Es erschließt sich nicht, weshalb Vermittlerplattformen für die Abgaben von durch sie vermittelte Leistungen haften sollen. Anstatt eine sinnvolle und gerechte Regulierung für einen aufstrebenden Industriezweig zu schaffen, wird in Österreich seine Entwicklung beinahe verunmöglicht«, erläutert Schubert.

### **Drohender Handelskonflikt mit den USA**

Die ersten erbosten US-amerikanischen Reaktionen auf ein ähnliches Gesetzesvorhaben aus Frankreich machen deutlich, wie sehr sich Staaten durch unkoordinierte nationale Alleingänge isolieren können. Ähnliche Reaktionen drohen auch Österreich, falls man ohne den geschlossenen Rückhalt aus der EU-Staatengemeinschaft in einen Handelskonflikt mit den USA tritt. »Für ein Exportland wie Österreich birgt das Vorgehen große Risiken«, gibt Schubert zu bedenken.

### **Neue Steuermodelle sollten wohlüberlegt sein**

Die Digitalisierung ist ein wichtiger Motor für das globale Wirtschaftswachstum. Daher sollte die Diskussion über die Besteuerung der digitalisierten Wirtschaft Wachstum, grenzüberschreitenden Handel und Investitionen fördern. Steuerliche Maßnahmen dürfen keine gravierenden Verzerrungen der Märkte und der globalen Wertschöpfungsketten zur Folge haben – nicht nur für die Digitalwirtschaft selbst, sondern auch für die traditionelle Wirtschaft. Jede Steueränderung sollte daher mit äußerster Vorsicht vorgenommen werden, sich in erster Linie an bewährten Grundsätzen wie Neutralität, Effizienz, Sicherheit und Einfachheit orientieren und jedenfalls ausgeglichene Bedingungen für alle Unternehmen garantieren. ■





## Vor internationalem Publikum erläuterte Maximilian Schubert in seiner Funktion als EuroISPA Präsident Möglichkeiten für einen effizienten Austausch zwischen ISPs und Behörden.

Im Rahmen der jährlichen Tagung der UN-Kommission für Verbrechensverhütung und Strafrechtspflege (CCPCJ) war Maximilian Schubert eingeladen in Wien an der Veranstaltung »How to Obtain Better Results in Transnational Corruption, Organized Crime and Terrorist Cases: UNODOC as a Global Facilitator for International Judicial Cooperation« teilzunehmen. Bei dem Termin am 23. Mai 2019 wurden nach Eingangstatements von Schubert und Vertreterinnen und Vertretern des Büros der Vereinten Nationen für Drogen- und Verbrechensbekämpfung (UNODC) verschiedene Beispiele für die zwischenstaatliche Zusammenarbeit von Behörden und Internet Service Providern (ISPs) im Rahmen von Workshops durchgespielt.

In seiner Funktion als EuroISPA Präsident zeigte sich Schubert hocherfreut über die Gelegenheit, vor Behördenvertreterinnen und -vertretern die Sicht von über 2500 Internetunternehmen auf das komplexe Verhältnis zwischen ISPs und Behörden darzulegen. Schubert betonte das gemeinsame Ziel aller Beteiligten, die digitale Welt als sicheren Raum zu schützen, und hob hervor, wie viele Beispiele für eine gelungene Zusammenarbeit es bereits gibt.

Das von allen Seiten geäußerte Bedürfnis nach Weiterentwicklung der Kooperation und den Ruf nach effizienteren Werkzeugen stellte Schubert außer Frage und strich dabei die Anstrengungen hervor, die bereits unternommen worden sind, um sowohl nationalen Gesetzgebungen, den Ansprüchen der Kundinnen und Kunden auf sorgfältigen Umgang mit ihren Informationen als auch den Erfordernissen

der Strafverfolgungsbehörden vollkommen gerecht zu werden. Ein wertvolles Instrument stellt in diesem Zusammenhang der »Practical Guide For Requesting Electronic Evidence Across Borders« dar, der im Auftrag der UNODOC erstellt und von Schubert lobend erwähnt wurde.

Der EuroISPA Präsident bot den Anwesenden einen aufschlussreichen und interessanten Perspektivenwechsel, indem er ganz konkrete und in einigen Fällen geradezu banal anmutende Herausforderungen beschrieb, denen sich ISPs im internationalen Austausch mit Behörden im Alltag stellen müssen:

- Die behördliche Anfrage ist in einer nicht geläufigen fremden Sprache verfasst.
- Die behördliche Anfrage geht an ein allgemeines Postfach, wie zum Beispiel office@isp.eu.
- Die Behörde weiß nicht, welche Daten sie abfragen kann und hat falsche Erwartungen.
- Die behördliche Anfrage ist unvollständig.
- Die Behörde kann verschlüsselt übermittelte Informationen nicht entschlüsseln.
- Auf Rechnern der Behörde ist die Webseite der Plattform gesperrt.

Schuberts Schilderungen sorgten bei den Teilnehmerinnen und Teilnehmern jedenfalls für ein gesteigertes Verständnis für die Position der Provider. Mit Hinblick auf das gut funktionierende und seit Jahren etablierte Zusammenspiel zwischen ISPs und Behörden in Österreich betonte Schubert neben der Bedeutung des fortlaufenden Dialogs vor allem jene der Schaffung von Werkzeugen wie Single Point of Contact oder Status des »Priority Flaggers«, der eine beschleunigte Behandlung durch den ISP ermöglicht. ■

# Weitreichende Umwälzungen:

## Der Europäische Kodex für die elektronische Kommunikation

**Der neue Rechtsrahmen wird im Telekommunikationsgesetz 2020 umgesetzt. Seine Ziele reichen von der Förderung von Glasfaser und 5G und das Vorantreiben des europäischen Binnenmarkts über die Schaffung eines Level-playing-fields unter den Diensteanbietern bis hin zu einer Teilharmonisierung der Rechte von Kundinnen und Kunden sowie der Aktualisierung der Universaldienste.**

**d**as Jahr 2020 bringt durch die Umsetzung des Europäischen Kodex für die elektronische Kommunikation (European Electronic Communications Code – EECC) weitreichende regulatorische Umwälzungen für große Teile der Internetwirtschaft mit sich. Der neue Rechtsrahmen für elektronische Kommunikationsdienste ersetzt die Rahmen-, Zugangs-, Genehmigungs- und Universaldienst-Richtlinie. Die nationale Umsetzung in Österreich hat bis zum 21. Dezember 2020 zu erfolgen, dies wird im Rahmen des Telekommunikationsgesetzes 2020 geschehen.

Die Hauptziele des EECC sind die Förderung von Glasfaserausbau und 5G-Technologie, das Vorantreiben des europäischen Binnenmarkts im Zusammenhang mit elektronischer Kommunikation, die Schaffung eines Level-playing-fields unter den Diensteanbietern unabhängig von der genutzten Infrastruktur, eine Teilharmonisierung der Rechte von Kundinnen und Kunden sowie eine Aktualisierung der Universaldienste.

Auch wenn zurzeit noch viele Detailfragen zu klären sind, lohnt sich ein Blick auf die anstehenden Änderungen und ihre Hintergründe. Erfreulich ist, dass der ISPA bereits erster Input durch Mitglieder übermittelt wurde, auf welche Aspekte bei der nationalen Umsetzung zu achten sein wird.

### Begriffsbestimmungen

Eine der wesentlichsten Änderungen ist die Erweiterung des Begriffs »elektronische Kommunikationsdienste«. Dieser wurde breiter gefasst und beinhaltet nun ebenfalls »interpersonelle Kommunikationsdienste«. Darunter fallen speziell auch Over-the-Top-Dienste (OTT), sofern sie einen direkten

interpersonellen und interaktiven Informationsaustausch ermöglichen, wie etwa Messenger Dienste oder Webmail. Nicht erfasst sind Kommunikationsdienste, die lediglich als Nebenfunktion dienen, wie etwa eine Chat-Funktion bei Videospielen. Noch herrscht allerdings Unklarheit darüber, wo genau die Grenze verläuft bzw. wann ein Kommunikationsdienst nur als Nebenfunktion vorliegt. Unterschieden wird zudem weiter zwischen nummerngebundenen Diensten, welche Verbindungen zu oder Kommunikation mit Nummern nationaler oder internationaler Nummerierungspläne erlauben, und nummernunabhängigen Diensten, mit welchen dies nicht möglich ist. In die erste Kategorie fällt als Beispiel etwa Skype Out, in die zweite WhatsApp oder Gmail.

Ein weiterer neuer Begriff ist »Netz mit sehr hoher Kapazität«. Es handelt sich dabei grundsätzlich um ein Kommunikationsnetz, welches ausschließlich aus Glasfaserkomponenten zumindest bis zum Verteilerpunkt am Ort der Nutzung besteht. Es ist allerdings noch nicht geklärt, ob hiervon lediglich FTTH umfasst ist oder ob damit auch FTTB oder sogar FTTC eingeschlossen ist. Das Gremium Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) wird zu dieser Frage bis Ende 2020 Leitlinien veröffentlichen.

### Infrastruktur und Zugang

Der EECC bringt in manchen Bereichen Neuerungen, greift gleichzeitig aber bei vielen Bestimmungen im Wesentlichen auf die bisherigen Richtlinien zurück. Eine interessante Neugierigkeit stellt im Zusammenhang mit Infrastruktur und Zugang der Umstand dar, dass nationale Regulierungsbehörden nunmehr auch nicht-marktbeherrschenden Unternehmen Zugangsverpflichtungen zu Verkabelungen und zugehörigen Einrichtungen aufbürden dürfen, selbst über den ersten Verteiler- bzw. Zugangspunkt hinaus, sofern die Replizierung der Netzbestandteile wirtschaftlich ineffizient oder praktisch unmöglich ist. Auch hierzu wird GEREK noch bis 2020 Leitlinien vorgeben.

Eine weitere Bestimmung lautet, dass Betreiber zur gemeinsamen Nutzung von passiver Infrastruktur oder zu nationalem Roaming verpflichtet werden können, sofern dies zur Bereitstellung lokaler frequenzgestützter Dienste erforderlich ist und keine tragfähigen alternativen Zugangswege zu Endnutzerinnen und -nutzern bei fairen und angemessenen Bedingungen verfügbar sind. Diese Möglichkeit muss jedoch

bereits im Zuge der Frequenzvergabe ausdrücklich vorgesehen worden sein.

Eine wesentliche Neuregelung in Bezug auf Infrastruktur ist das sogenannte ›Ko-Investment‹. Dabei handelt es sich entweder um Miteigentum an Netzanlagen, langfristige Risikoteilung durch Kofinanzierung oder Abnahmevereinbarungen zwischen Betreibern. Der neue Rechtsrahmen sieht vor, dass, sofern ein marktbeherrschendes Unternehmen eine entsprechende Vereinbarung in Bezug auf Netze mit sehr hoher Kapazität mit zumindest einem anderen Betreiber trifft, regulatorische Verpflichtungen hinsichtlich dieser Infrastruktur entfallen können. Hierzu ist es jedoch erforderlich, dass ein entsprechendes Angebot auch sämtlichen anderen Betreibern zu fairen, angemessenen und nicht-diskriminierenden Bedingungen während der gesamten Lebensdauer der Infrastruktur offensteht. In diesem Zusammenhang sind jedoch zahlreiche Fragen noch ungeklärt, etwa ob lediglich eine Vereinbarung getroffen oder diese auch umgesetzt werden muss oder ob sämtliche Regulierung tatsächlich für die gesamte Lebensdauer der Infrastruktur entfällt. Die ISPA wird sich aktiv in die Klärung diesbezüglicher Fragen einbringen, um zu vermeiden, dass dieses Modell zur Umgehung von Regulierung ausgenutzt werden kann.

Hinsichtlich der Marktanalyse wird der Ansatz fortgesetzt, dass zunehmend von ex-ante-Regulierung abgegangen werden soll, auch um Investitionen in neue Infrastruktur zu fördern. Darüber hinaus wird die Möglichkeit vorgesehen, auch länderübergreifende bzw. regionale Marktanalysen durchzuführen, und es werden die Marktanalysezyklen von drei auf fünf Jahre verlängert.

## **Frequenzen**

Die Bestimmungen zum Thema Frequenzen sollen grundsätzlich dem Ziel der Förderung des Ausbaus von 5G-Netzen dienen. Darüber hinaus sollen die Vergabe- und Nutzungsbedingungen auf europäischer Ebene im Sinne des Strebens nach einem europäischen Binnenmarkt nach Möglichkeit harmonisiert werden. Das konkrete Vergabesystem verbleibt jedoch weiterhin auf Ebene der Mitgliedstaaten. Diese sind verpflichtet die Frequenzbänder 3,6 GHz und 26 GHz für die Nutzung von 5G bis Ende 2020 zu vergeben. Der EECC sieht hinsichtlich der Frequenzvergabe eine Mindestvergabedauer von 15 Jahren vor, wobei die Verlängerung der Lizenz in der Regel möglich sein soll.

Zudem unterliegen Lizenzen einem ›use it or lose it‹-Prinzip. Demnach können diese auch wieder entzogen werden, sofern eine erworbene Lizenz nicht innerhalb einer angemessenen Frist genutzt wird.

## **Rechte der Kundinnen und Kunden**

Im Rahmen des EECC wird ein Teil der Rechte von Kundinnen und Kunden auf europäischer Ebene harmonisiert. Aufgrund dieser Harmonisierung ist es den Mitgliedstaaten nach Ablauf einer dreijährigen Frist nicht mehr erlaubt, strengere oder laschere Bestimmungen vorzusehen. Wesentlich ist darüber hinaus, dass diese Rechte auch gegenüber Klein- und Kleinstunternehmen sowie Organisationen ohne Gewinnerzielungsabsicht gelten. Die harmonisierten Rechte sollen zudem auch für Angebotsbestandteile gelten, welche grundsätzlich nicht dem EECC unterliegen, etwa bei kombinierten Angeboten von Internet und TV.

Eine wesentliche Neuerung ist die Notwendigkeit, den Kundinnen und Kunden zusätzlich zur Erfüllung der allgemeinen Informationspflichten vor Vertragsabschluss eine Zusammenfassung der wesentlichen Vertragsbestandteile in schriftlicher Form zur Verfügung zu stellen. Die EU-Kommission wird bis Ende 2019 eine entsprechende Mustervorlage zur Verfügung stellen. Die ISPA hat sich bereits zu Beginn dieses Jahres im Rahmen eines Workshops in Brüssel mit der EU-Kommission zu diesem Thema ausgetauscht.

Der EECC hält die Betreiber dazu an, ihre Kundinnen und Kunden einmal im Jahr über den ›besten Tarif‹ zu beraten. Im Zuge der Umsetzung des neuen Rechtsrahmens in Österreich wird zu bestimmen sein, was den ›besten Tarif‹ ausmacht und welche datenschutzrechtlichen Grundlagen zur Bestimmung dieses Tarifs erforderlich sind.

## **Universaldienst**

Universaldienste umfassen in Hinkunft sowohl Breitbanddienste als auch Sprachkommunikationsdienste, wobei letztere im Vergleich zur bisherigen Rechtslage nunmehr technologieneutral formuliert sind und etwa auch Skype Out erfassen. Darüber hinaus ermöglicht der EECC die Finanzierung der Universaldienste auch durch die öffentliche Hand.

## **Fortlaufende Diskussion**

Der EECC bietet die Gelegenheit, viele Weichenstellungen für die Zukunft vorzunehmen, um sowohl für Betreiber als auch für Kundinnen und Kunden möglichst ausgewogene Voraussetzungen zu schaffen. Die ISPA erarbeitet derzeit ihre Position zum neuen Rechtsrahmen und blickt der fortlaufenden Diskussion mit allen interessierten Stakeholdern im Zuge der nationalen Ausgestaltung gespannt entgegen. ■

# SVN-G: AUSWEISPFLICHT WIRKUNGSLOS GEGEN HATE SPEECH

Die ISPA kritisiert den Entwurf zum Bundesgesetz über Sorgfalt und Verantwortung im Netz scharf. Dieses eignet sich nicht zur Bekämpfung von Hass im Netz und senkt die Attraktivität des Digitalstandorts Österreich.

Der Gesetzesentwurf sieht eine Registrierungs- und Authentifizierungspflicht für sämtliche Nutzerinnen und Nutzer von Online-Plattformen vor. Die betroffenen Online-Foren müssen Namen und Adressen ihrer Userinnen und User erheben und speichern. Dies soll es ermöglichen, Verfasserinnen und Verfasser von rechtlich fragwürdigen Postings schneller auszuforschen und bei übler Nachrede, Beleidigungen oder Ehrverletzungen rechtlich zu belangen. Da der Großteil derartiger Postings unter Klarnamen veröffentlicht wird, schätzen Expertinnen und Experten die Wirksamkeit der Maßnahme als sehr gering ein. Der derzeit recht kontroversielle Gesetzgebungstrend, im nationalen Alleingang überschießende Regulierung für das Internet zu fordern, wird durch diese nicht zielführende Maßnahme nur verstärkt. Eine derartige Vorgehensweise widerspricht den Grundsätzen des gemeinsamen Binnenmarktes, bremst die Digitalisierung Österreichs und senkt damit die Attraktivität des Wirtschaftsstandorts.

## -----> Entwurf völlig unschlüssig

Der Gesetzesentwurf weist zudem auch eine Vielzahl inhaltlicher und formaler Schwächen auf. Die Anforderungen an die Online-Foren sind widersprüchlich und unklar. Wie die technische Umsetzung aussehen soll, erschließt sich nicht, wodurch auch Datenschutzfragen offen bleiben. Darüber hinaus ist der vorliegende Entwurf mit europäischen Rechtsgrundsätzen unvereinbar, verstößt er doch gegen das Datensparsamkeitsprinzip der Datenschutzgrundverordnung und ähnelt der bereits mehrfach vom europäischen Gerichtshof gekippten Vorratsdatenspeicherung. Darüber hinaus bergen derartige Datensammlungen über die Bevölkerung große Sicherheitsrisiken und sind aus Sicht der Internetwirtschaft schlicht fahrlässig.

## -----> Imageschaden für Tourismus-, Kongress- und Kulturland Österreich

Obwohl das Gesetz für auf Österreich ausgerichtete Online-Foren gelten soll, ist nicht klar, wie internationale Plattformen mit der Regelung umgehen werden. Denkbar wäre es, dass alle Nutzerinnen und Nutzer,

die den Standort ›Österreich‹ übermitteln, erst nach erfolgter Registrierung und Authentifizierung posten können. Touristinnen und Touristen, aber auch Personen, die an Kulturveranstaltungen oder Kongressen teilnehmen, würde dieses Gesetz ebenfalls treffen und deren Freiheit einschränken.

## Eingriff in die Grundrechte

Große Bedenken sieht die ISPA durch die Einschränkung der Anonymität im Internet in Bezug auf Datenschutz und Meinungsfreiheit. Die ganz überwiegende Anzahl von Postings im Internet sind positiver Natur und haben das Internet zu dem gemacht, was es heute ist – zu einer Erfolgsgeschichte. Durch die Anonymität im Netz können Nutzerinnen und Nutzer auch kontroversielle Themen ansprechen, ohne von ihrem Umfeld unter Druck gesetzt zu werden. Jedoch gibt es leider auch eine kleine Gruppe von Menschen, die das Internet zu illegalen Zwecken missbraucht. Mit dieser Maßnahme wird die Bevölkerung jedoch unter Generalverdacht gestellt. Denn diese Ausweispflicht stellt jedenfalls einen unverhältnismäßigen Eingriff in die Privatsphäre dar und widerspricht den Grundsätzen des Datenschutzes. Auch der Vorschlag, Daten zentral zu speichern, ist aufgrund des enormen Missbrauchspotentials klar abzulehnen.

## Rechtsdurchsetzung im Internet ist jetzt schon möglich

Die Rechtsdurchsetzung im Internet funktioniert gut, denn auch jetzt schon werden Straftaten, die online begangen wurden, erfolgreich rechtlich geahndet. Die Staatsanwaltschaft kann im Anlassfall die Internetunternehmen auffordern Daten der Userinnen und User herauszugeben. Dieser Gesetzesentwurf bringt dahingehend keine Verbesserung. »Wenn wirklich Interesse daran besteht, besser gegen Hass im Netz vorzugehen, wäre es ein Einfaches, bei bestimmten Delikten die Rolle der Staatsanwaltschaft zu erweitern. Diese könnte dann z. B. auch bei Beleidigungen im Internet Daten von den Betreibern verlangen«, erläutert Maximilian Schubert, Generalsekretär der ISPA. In Zukunft kann jeder, der sich in seinen Rechten verletzt fühlt, auf eine Auskunft bestehen. »Wir lehnen es ab, dass die Internetunternehmen zukünftig selbst entscheiden müssen, wem sie die Identität ihrer Nutzerinnen und Nutzer preisgeben sollen. Der Grundsatz der Rechtsstaatlichkeit im Sinne der Einbindung von Gerichten muss unbedingt hochgehalten werden«, betont Schubert.

## Zweifelhafte Wirksamkeit der Maßnahme

Viele Hasspostings in den sozialen Medien werden jetzt schon unter Klarnamen veröffentlicht. Das Problem ist hier eher ein mangelndes Unrechtsbewusstsein als die Anonymität im Internet. Die angedachte Maßnahme wird die Verbreitung von Hasspostings nicht verhindern, sondern dazu führen, dass die Nutzerinnen und Nutzer, die sich bislang innerhalb des rechtlichen Rahmens an Diskussionen beteiligt haben, die Plattformen nicht mehr nutzen.

### Bessere Maßnahmen

Während die Abschaffung von Anonymität im

Internet nicht zu einer besseren Netzkultur führen wird, zeigen Maßnahmen zur Bewusstseinsbildung und zur Förderung von Medienkompetenz klare Wirkung. Es braucht keine neuen Gesetze, sondern Aufklärungsarbeit und die beständige Weiterentwicklung der Meldemechanismen. Das bestehende Meldesystem funktioniert in vielen Bereichen bereits gut, es bedarf jedoch klar weiterer Verbesserungen. Als besonders wertvoll bei der Eindämmung von Hasspostings haben sich sogenannte Flagging-Partnerschaften – z. B. zwischen den Plattformen und NGOs – herausgestellt. Dabei werden Meldungen in einem beschleunigten Verfahren behandelt, was zu einer umgehenden Entfernung sowie einer effizienten Verfolgung illegaler Inhalte führt. ■

# OLG LEHNT ANORDNUNG ZUR DUPLIZIERUNG EINER SIM-KARTE AB

ISP setzt sich für Privatsphäre seiner Kundinnen und Kunden ein und scheut dafür auch Rechtsstreitigkeiten nicht.

**E**in Mobilfunkbetreiber, der von der Staatsanwaltschaft dazu aufgefordert wurde, alle gespeicherten Daten zu einer bestimmten Rufnummer, inklusive einer duplizierten SIM-Karte und Daten zu einem Messenger-Dienst, zu beauskunften, hat erfolgreich Beschwerde beim OLG Wien eingereicht. Denn weder eine Überwachungsanordnung noch eine Anordnung zur Beauskunftung bietet eine gesetzliche Grundlage, um vom Betreiber die Duplizierung einer SIM-Karte oder den Zugang zu Daten, die bei Drittanbietern gespeichert sind, anzufordern.

Die Staatsanwaltschaft beantragte Einsicht in alle gespeicherten Daten und sämtliche Nachrichten, die in einem bestimmten Zeitraum getätigt wurden. Dadurch hätte speziell auf Nachrichten eines Messenger-Dienstes zugegriffen werden sollen. Da die SIM-Karte mit der entsprechenden Rufnummer zuvor zerstört worden war, verlangte die Staatsanwaltschaft die Duplizierung der SIM-Karte durch den Netzbetreiber samt PIN- und PUK-Code, um auf diese Weise Zugang zu den Daten zu erhalten. Die Staatsanwaltschaft begründete dies damit, dass eine Beauskunftungsanordnung sämtliche beim Betreiber gespeicherten Daten beinhalte, inklusive der zu duplizierenden SIM-Karte, welche als Schlüssel den Zugang zu diesen Daten gewähren sollte. Das OLG Wien folgte der Beschwerde

des Betreibers gegen diese Anordnung und wies den Antrag auf Bewilligung der Anordnung ab.

Begründet hat das OLG diese Entscheidung damit, dass sich eine Beauskunftungsanordnung nur auf bestimmte Daten, die beim Betreiber vorliegen, bezieht. Die Staatsanwaltschaft kann zwar eine Überwachung von Nachrichten, die über das Kommunikationsnetz des Betreibers übertragen werden, anordnen. Das schließt aber nicht bereits empfangene Nachrichten ein. Wenn die Staatsanwaltschaft auf bereits zugestellte Inhalte zugreifen möchte, stehen ihr zwei Wege offen: Entweder wird das Endgerät, auf dem die Nachrichten gespeichert sind, sichergestellt oder die Staatsanwaltschaft muss eine Beauskunftungsanordnung an den Betreiber des Kommunikationsdienstes, in diesem Fall des Messenger-Dienstes, tätigen.

Die ISPA setzt sich dafür ein, dass ein breiter Diskurs über die vorherrschende Rechtsunsicherheit geführt wird. Die bisherigen Ermittlungsbefugnisse müssen unter Wahrung der Verhältnismäßigkeit an die Gegebenheiten des 21. Jahrhunderts angepasst werden. Zu bedenken ist dabei, dass die Durchsuchung eines Smartphones oft sensiblere Bereiche der Privatsphäre offenbart als eine Hausdurchsuchung. ■

### Gefahren von SIM-Swapping

SIM-Swapping ist ein Prozess, bei dem ein Telekommunikationsanbieter eine Telefonnummer auf eine andere SIM-Karte überträgt. Dadurch kann nicht nur auf gespeicherte Daten zugegriffen werden, sondern auch Zugang zu verschiedenen Konten, die mit der Telefonnummer gesichert sind, erlangt werden. Ein solcher Zugang würde einen massiven Eingriff in die digitale Identität bedeuten. Die Telefonnummer dient z. B. bei der Zwei-Faktor-Authentifizierung als weiteres Sicherheitsmerkmal zusätzlich zum Passwort. Beim Online Banking wird die Transaktionsnummer oft per SMS versandt.

Mit der Telefonnummer kann bei vielen Accounts ein vergessenes Passwort zurückgesetzt werden. Auch auf Messenger-Dienste kann ohne weitere Verifizierung zugegriffen werden. Dadurch kann nicht nur in fremdem Namen kommuniziert, sondern es können auch alte Chats eingesehen werden.



# Wie viel analoge Kompetenz benötigt die Digitalwirtschaft?

**Expertinnen und Experten identifizieren beim ISPA Forum strukturiertes Denken und Medienkompetenz als zentrale Voraussetzungen.**

**d**ie aktuelle Bildungsdebatte zielt grösstenteils darauf ab, wie Schülergenerationen bestmöglich auf ihr Berufsleben vorbereitet werden sollen. Einerseits geht es dabei um neue, oftmals digitale Methoden der Wissensvermittlung und andererseits auch um konkret benötigtes Wissen und erforderliche Kompetenzen. Da der Bedarf der Wirtschaft an IKT-Fachkräften steigt, wird von verschiedenen Seiten gefordert, dass bereits die Kleinen möglichst früh mit Grundzügen des Programmierens vertraut gemacht werden. Im Rahmen des diesjährigen ISPA Forums am 9. Mai diskutierten Expertinnen und Experten darüber, welches Wissen und welche Kompetenzen die Heranwachsenden brauchen, um ihr Potential optimal in der digitalen Arbeitswelt entfalten zu können.

## Lebenslanges Lernen

In seinem Impulsreferat unterstrich der Schweizer Internetunternehmer Jörg Eugster, dass in einer zunehmend digitalisierten Welt das lebenslange Lernen, in kleinsten, aber beständigen Einheiten, immer mehr an Bedeutung gewinne, da Kompetenzen von heute bereits morgen schon obsolet sein könnten. »Letztlich ist für den Erfolg nicht das Wissen selbst, sondern die Denkweise, das Mindset, entscheidend. Nur wer den Veränderungen offen und vorurteilsfrei begegnet, wird die Herausforderungen der Digitalisierung bewältigen können«, betonte Eugster.

## Die Digitalwirtschaft braucht Empathie und logisches Denkvermögen

Die beiden Unternehmerinnen am Podium waren sich einig, dass die Jugendlichen neben Medienkompetenz vor allem Kommunikationsfähigkeiten und logisches Denkvermögen brauchen. »Abstraktes, strukturiertes Denken, das auf die Problemlösung abzielt, bringt mich immer weiter«, stellte Eva Tatschl-Unterberger, Geschäftsführerin der DigiTrans GmbH fest. Für Annette Mossel, CEO von Frameless, bleiben neben Programmierkenntnissen vor allem Softskills ausschlaggebend: »Self-Leadership, Kommunikation und Empathie sind gefragt: Analoge Kompetenzen sind ein Schlüsselfaktor in der Digitalwirtschaft, da agile Teams Selbstorganisation benötigen, digitale Prozesse wenig Grauwerte kennen und Algorithmen – noch – keinen Humor verstehen.«

## Kein Erfolg ohne Medienkompetenz

Die Expertinnen und Experten sehen grossen Bedarf bei der Förderung der Medienkompetenz, jedoch nicht immer mit demselben Ziel. »Zwischen klassischen Bildungsidealen und modernen Informations- und Kommunikationstechnologien besteht im Grunde keinerlei Widerspruch. Gerade deshalb stellt sich aber angesichts des öffentlichen Bildungssystems die Frage, inwiefern das Konzept der Medienkompetenz der privaten Wirtschaft dienen oder aber kritische Staatsbürgerinnen und Staatsbürger heranbilden soll«, erläuterte Bildungswissenschaftler Alessandro Barberi. Medienpädagogin Elisabeth Eder-Janca betonte, dass die Lebensrealität der Kinder nicht in eine virtuelle und eine reale Welt geteilt werden könne: »Die digitale Welt ist eine Erweiterung zur realen Welt. Wie die Technik funktioniert, wissen schon junge Kinder. Wie man Inhalte kritisch hinterfragt und vor allem auch reflektiert, müssen sie lernen.« ■

# Ein transatlantisches Abkommen zur Lösung des Rechtskonflikts zwischen der

**DATENSCHUTZ-  
GRUND-  
VERORDNUNG**

und  
dem

?

**CLOUD  
ACT**

Unternehmen sehen sich derzeit einem Rechtskonflikt zwischen der Datenschutzgrundverordnung (DSGVO) sowie dem US-amerikanischen CLOUD bzw. Stored Communications Act (SCA) ausgesetzt, in welchem rechtskonformes Verhalten mit beiden Gesetzen nicht möglich erscheint. Ein derzeit verhandeltes transatlantisches Abkommen bietet die Chance, dieses Problem zu beheben und eine zukunftsweisende Lösung zu schaffen.

Die weltweite Vernetzung durch das Internet ermöglicht es heute Nutzerinnen und Nutzern in einem Land, ohne größere Umstände die elektronischen Kommunikationsdienste eines Unternehmens in einem anderen Land in Anspruch zu nehmen. Die dabei anfallenden Daten können wiederum aus sicherheitstechnischen oder wirtschaftlichen Gründen in einem dritten Land gespeichert werden. Einhergehend mit den zahlreichen positiven Möglichkeiten, welche hierdurch geschaffen werden, entstehen jedoch sowohl rechtliche als auch praktische Herausforderungen, mit welchen sich die ISPA bereits seit geraumer Zeit befasst. Eine solche ist es, wie Strafverfolgungsbehörden grenzüberschreitend auf diese Daten zugreifen können und gleichzeitig bestehende (Grund-)Rechte gewahrt bleiben.

Der grenzüberschreitende Zugang zu Nutzerdaten im Rahmen der Strafverfolgung beschäftigt nicht nur ISPs im unternehmerischen Alltag, sondern ist auch der Anlass für derzeit geführte Verhandlungen sowohl auf europäischer als auch internationaler Ebene. Zum einen soll durch eine Verordnung auf EU-Ebene Strafverfolgungsbehörden die Befugnis zu grenzüberschreitenden Auskunftsanordnungen an ISPs gegeben werden.<sup>1</sup> Zum anderen befindet sich die EU aktuell in

Verhandlungen mit den USA hinsichtlich eines bilateralen Abkommens, welches grenzüberschreitende Auskunftsanordnungen auch im transatlantischen Kontext ermöglichen soll.

Der Ansporn, ein solches transatlantisches Abkommen zu schließen, existiert speziell seit dem Beschluss des CLOUD Acts durch den US-Senat im März 2018. Mit diesem wurde der Stored Communications Act (SCA) novelliert, welcher die freiwillige und die verpflichtende Beauskunftung von Nutzerdaten durch herkömmliche Telekomunikations- und Access-Anbieter sowie auch durch Anbieter von Messaging-, E-Mail-, oder Hosting-Diensten regelt. Dieser schafft die Grundlage für ein bilaterales Abkommen zwischen den USA und anderen ›qualifizierten‹ Staaten, welches Strafverfolgungsbehörden beider Seiten direkte grenzüberschreitende Auskunftsanordnungen an Unternehmen im anderen Staat gewähren würde.

Die hierdurch geschaffene Rechtslage würde dem Grunde nach jener entsprechen, welche derzeit auf EU-Ebene im Rahmen des Verordnungsentwurfs angestrebt wird. Die Initiative hierfür geht insbesondere von Strafverfolgungsbehörden in Europa aus. Diese erachten ein Abkommen als notwendig, um Nutzerdaten direkt von US-amerikanischen Diensteanbietern wie Google oder Facebook abfragen zu können, da dies auf dem herkömmlichen Weg im Rahmen von Rechtshilfeersuchen (den sogenannten ›MLAT-Verfahren‹)<sup>2</sup> of sehr viel Zeit in Anspruch nimmt.

<sup>1</sup> Einen detaillierten Artikel zu den zahlreichen Kritikpunkten am Entwurf der „Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen“ finden sie in den ISPA News 3/18

<sup>2</sup> Mutual legal assistance treaties. Dabei handelt es sich um bilaterale Abkommen, unter welchen der Datenaustausch zwischen den zuständigen Behörden in den jeweiligen Staaten erfolgt und Unternehmen die Daten lediglich an nationale Behörden beauskunften.

### -----> Extraterritorialer Effekt des Stored Communications Act

Der CLOUD Act beinhaltet jedoch noch einen zweiten, kontroversiellen Abschnitt. Dieser sollte ursprünglich dazu dienen, einen Rechtsstreit zwischen den USA und Microsoft Inc. aufzulösen, in welchem US-Strafverfolgungsbehörden auf E-Mail-Daten eines Outlook-Nutzers zugreifen wollten. Dessen Account wurde jedoch von deren Tochterunternehmen Microsoft Ireland betrieben, weshalb ein Teil der Daten auf irischem Territorium gespeichert wurde. Nach Worten des US-Gesetzgebers wurde im Rahmen des CLOUD Act lediglich »klargestellt«, dass ein Anbieter eines Dienstes, der unter den SCA fällt, sämtliche Nutzerdaten offenlegen muss, die sich in dessen Besitz oder unter dessen Kontrolle befinden. Dies schließt auch Daten mit ein, die von Tochtergesellschaften im Ausland aufbewahrt werden, unabhängig vom jeweiligen Speicherort der Daten. Während die USA argumentieren, dass diese Änderung lediglich den bereits gelebten Status quo nach US-Recht festschreibt, wird gerade von europäischer Seite argumentiert, dass dies eine extraterritoriale Durchsetzungsmaßnahme darstellt, welche im Widerspruch zu etablierten Prinzipien des Völkerrechts steht und eine wesentliche Abkehr von den traditionellen Rechtshilfeverfahren ist.

### -----> Konfliktpotential mit der DSGVO

US-amerikanische Unternehmen mit Tochterunternehmen in der EU, welche eine entsprechende Auskunftsanordnung erhalten, sehen sich nun widersprüchlichen Verpflichtungen hinsichtlich der Offenlegung solcher Daten gegenüber US-amerikanischen Strafverfolgungsbehörden ausgesetzt. Denn diese Daten können ebenfalls nach der DSGVO geschützt sein, speziell wenn sie im Rahmen der wirtschaftlichen Tätigkeit des Tochterunternehmens auf EU-Territorium verarbeitet werden. Aufgrund der strikten Vorgaben der DSGVO in Bezug auf die Übermittlung von personenbezogenen Daten an Drittstaaten ist es fraglich, inwiefern die Übermittlung von Daten an eine US-Strafverfolgungsbehörde ausschließlich aufgrund einer rechtlichen Verpflichtung unter US-Recht zulässig ist.

Denn die Übermittlung von personenbezogenen Daten an Drittstaaten erfordert als eigenständiger Verarbeitungsprozess, dass sämtliche Prinzipien der

DSGVO eingehalten werden. In dieser Hinsicht ist speziell die Rechtmäßigkeit der Verarbeitung fraglich. Schließlich entspricht die Offenlegung von Daten lediglich auf Grundlage der rechtlichen Verpflichtung in einem Drittstaat wohl keiner der in der DSGVO aufgelisteten Rechtsgrundlagen. Ebenso kann nicht davon ausgegangen werden, dass im Regelfall ein berechtigtes Interesse des Unternehmens an der Datenverarbeitung besteht, selbst wenn dieses andernfalls mit Strafen nach US-Recht rechnen muss. Darüber hinaus wird in Artikel 48 der DSGVO deutlich festgehalten, dass die Übermittlung von personenbezogenen Daten aufgrund einer rechtlichen Verpflichtung durch einen Drittstaat außerhalb eines MLATs oder einem anderen internationalen Abkommen grundsätzlich unrechtmäßig ist. Dieser Artikel wurde gerade als Reaktion auf rechtliche Vorstöße in anderen Staaten geschaffen, durch welche Unternehmen auf EU-Territorium zur Offenlegung von Daten verpflichtet werden sollten.

Als einziger Ausweg aus Sicht der Unternehmen erscheint derzeit daher die Möglichkeit, sich auf einen der Ausnahmetatbestände zur Übermittlung von Daten an Drittstaaten zu berufen.<sup>3</sup> Deren genauer Umfang ist bislang jedoch noch nicht abschließend geklärt. Während sich der Europäische Datenschutzausschuss stets für eine möglichst enge Auslegung ausgesprochen hat, wonach deren Anwendung jeweils im Einzelfall zu beurteilen sei und diese nicht als Grundlage für regelmäßige Datenübermittlungen verwendet werden können, haben sich gerade auch Vertreter der US-Regierung auf diese Ausnahmetatbestände berufen, um Datenübermittlungen durch Tochterunternehmen von US-Betreibern zu rechtfertigen. Dies schafft aktuell eine äußerst unbefriedigende Situation für Unternehmen, welche nicht nur mit widersprüchlichen Interpretationen konfrontiert sind, sondern darüber hinaus auch im Einzelfall nachweisen müssten, dass die Voraussetzungen zur Anwendung des Ausnahmetatbestandes erfüllt sind. Sofern tatsächlich keine Rechtsgrundlage gegeben ist, sehen sich die Unternehmen wiederum einer Situation ausgesetzt, in welcher die gleichzeitige Achtung sowohl US-amerikanischen als auch europäischen Rechts nicht möglich ist. Dies kann zu unausweichlichen Strafen führen, die insbesondere unter der DSGVO erheblich ausfallen können.

### Lösung verlangt einen ganzheitlichen Ansatz

Auch wenn dieses Dilemma auf den ersten Blick als ein Nischenthema für einzelne US-amerikanische Unternehmen mit Tochterunternehmen in der EU erscheint, ist die zugehörige Diskussion hinsichtlich des Konfliktpotentials zwischen dem SCA und der DSGVO weitaus größer. Denn auch die DSGVO selbst hat einen extraterritorialen Anwendungsbereich, der

<sup>3</sup> Artikel 49 DSGVO



einen entsprechenden Konflikt hervorrufen kann. Bekanntlich unterliegen auch Unternehmen in Drittstaaten wie den USA den Regeln der DSGVO, sofern diese Dienstleistungen oder Waren an Personen im Unionsgebiet anbieten oder deren Verhalten überwachen. Diese Unternehmen unterliegen jedoch aufgrund ihres Standorts gleichzeitig auch den Bestimmungen des SCA.

Nach dem Wortlaut der DSGVO ist es derzeit unklar, inwiefern auch diese Unternehmen die Bestimmungen zur Übermittlung von personenbezogenen Daten an Drittstaaten einzuhalten hätten, da nicht hinreichend geklärt ist, ob es notwendig ist, dass das übermittelnde Unternehmen sich auf EU-Territorium befindet. Sofern dies nicht der Fall ist, wären die bereits ausgeführten Fragen in Bezug auf die Konformität mit den Anforderungen der DSGVO an die Übermittlung von personenbezogenen Daten an Drittstaaten jedoch die gleichen. Es wäre daher wünschenswert, dass in dieser Hinsicht im Rahmen von Leitlinien des Europäischen Datenschutzausschusses Klarheit und Rechtssicherheit gleichermaßen für Nutzerinnen und Nutzer und Unternehmen geschaffen wird.

Unabhängig davon zeigt sich, dass der zunehmende Versuch, durch extraterritoriale Anwendung von nationalem oder regionalem Recht Online-Dienste zu regulieren, unausweichlich zu Rechtskonflikten führt, die am Ende die Unternehmen zu lösen haben. Angesichts der immanenten Interkonnektivität des Internets stellt sich die Frage, inwiefern nationale oder auch regionale Alleingänge tatsächlich zielführend sind und es sollte jedenfalls darauf geachtet werden, dass Probleme auf internationaler Ebene unter reger Beteiligung möglichst vieler Staaten geregelt werden. Andernfalls sind zusätzliche Datenlokalisierungsvorschriften zu befürchten. Die damit einhergehende Fragmentierung des Internets, die bereits in Ländern wie Russland oder China betrieben wird, gefährdet zweifellos die Offenheit des Internets, wie wir es kennen.

### **Ein bilaterales Abkommen als Zwischenlösung?**

Trotz erster oberflächlicher Bemühungen auf UN-Ebene sowie aktueller Verhandlungen innerhalb des Europarats kann der akute Rechtskonflikt zwischen SCA und DSGVO auf absehbare Sicht jedoch nicht in einem der internationalen Foren gelöst werden. Dennoch sollte jeglicher Lösungsansatz jedenfalls auf

die Ergebnisse und Entwicklungen in diesen Foren Rücksicht nehmen, um Doppelgleisigkeiten zu vermeiden. Die Suche nach einer Lösung für die Auseinandersetzung führt zurück zum derzeit verhandelten transatlantischen Abkommen. Dieses bietet eine optimale Möglichkeit, um auf den bestehenden Rechtskonflikt einzugehen und eine Lösung zu schaffen, welche sowohl EU- als auch US-amerikanisches Recht bzw. deren Interessen gleichermaßen respektiert. In einem solchen Abkommen könnten Fragen geklärt werden, wie etwa ob der Speicherort von Daten in der heutigen Zeit noch ein angemessenes Kriterium zur Bestimmung der Territorialität ist, um damit eine Grundlage für weitere internationale Abkommen zu schaffen.

Viele Fragen sind in diesem Zusammenhang jedoch noch offen, etwa ob die EU überhaupt die Kompetenz zum Abschluss eines solchen Abkommens hat. Der CLOUD Act selbst stellt bereits Anforderungen an ein solches Abkommen bzw. die jeweilige Regierung, welche ein solches Abkommen eingehen möchte. Die Anforderungen sehen unter anderem vor, dass ein Staat, der ein entsprechendes Abkommen eingehen möchte, sämtliche rechtlichen Hindernisse unter seinem nationalen Recht entfernen muss, um Unternehmen zu erlauben, auf Auskunftsanordnungen von US-Behörden zu reagieren. Dies hätte jedoch zur Folge, dass durch ein solches Abkommen nicht nur zusätzliche grenzüberschreitende Anordnungen geschaffen werden würden, sondern auch die aktuelle Rechtslage nach US-Recht, in der ein US-amerikanisches Unternehmen zur Herausgabe von Daten ihrer Tochterunternehmen auf EU-Territorium gezwungen werden kann, nach EU-Recht legalisiert wird. Da dies die Aufhebung der zuvor erläuterten Beschränkungen für die Übermittlung von Daten an Drittländer im Rahmen der DSGVO zur Folge hätte, muss eine Lösung, die ausschließlich auf dem CLOUD Act basiert und keine zusätzlichen Absicherungen beinhaltet, abgelehnt werden.

Aus Sicht der EU folgt aus der bisher ergangenen Rechtsprechung des EuGH vielmehr, dass ein solches Abkommen den Datenschutzstandard der EU nicht schmälern darf und daher ausreichend Schutzmaßnahmen treffen muss. Gerade angesichts der zum Teil durchaus gravierenden Unterschiede in der Auffassung von Privatsphäre und Datenschutz zwischen den USA und Europa ist hier noch ein langer Weg zu beschreiten. Die gravierendsten Spannungspunkte sind dabei zum einen die relativ laschen Voraussetzungen zur Herausgabe von Nicht-Inhaltsdaten unter US-Recht sowie speziell, dass das Recht auf Privatsphäre in den USA grundsätzlich nur US-Staatsbürgern und permanent Aufenthaltsberechtigten zusteht, während es in der EU als Menschenrecht erachtet wird. Ohne eine Angleichung der Rechte ist es fraglich, ob ein solches Abkommen den Anforderungen des EuGH entspräche. ■

## CPC-VO: Zukunftsweisende Umsetzung der Verordnung über die Zusammenarbeit von Konsumentenschutzbehörden in Österreich

**a**ls einer der ersten EU-Mitgliedstaaten hat Österreich in diesem Frühjahr das nationale Umsetzungsgesetz zur Verordnung über die Zusammenarbeit von Konsumentenschutzbehörden präsentiert. Die ISPA hat sich bereits seit Beginn der Verhandlungen auf europäischer Ebene mit diesem Thema auseinandergesetzt und sich nun auch insbesondere in den nationalen Umsetzungsprozess eingebracht. Erfreulicherweise konnte dabei erreicht werden, dass die von der ISPA wiederholt vorgebrachten Bedenken in Bezug auf die Anordnung von Zugangssperren sowie zur Beauskunftung von Kundendaten im Umsetzungsgesetz berücksichtigt wurden.

### -----> Rückblick

Im Dezember 2017 wurde auf EU-Ebene die Verordnung über die Zusammenarbeit zwischen den für die Durchsetzung der Verbraucherschutzgesetze zuständigen nationalen Behörden (CPC-VO) beschlossen. Ziel war es, die grenzüberschreitende Durchsetzung von Verbraucherschutzbestimmungen auf europäischer Ebene zu verbessern, welche gerade durch die zunehmende Entwicklung eines digitalen Binnenmarktes verstärkt als notwendig erachtet wurde. Aus Sicht der Internetwirtschaft enthält die beschlossene Verordnung jedoch auch bedeutsame Erweiterungen der Ermittlungs- und Durchsetzungsbefugnisse von Konsumentenschutzbehörden. Speziell zwei Bereiche haben dabei für Aufruhr in der Branche gesorgt. Zum einen sah die Verordnung die Möglichkeit vor, Konsumentenschutzbehörden die Kompetenz zu übertragen, Anordnungen von Auskunftsbefehlen über Nutzerdaten an Unternehmen – inklusive Access- und Hosting-Provider – zu richten. Daneben sollte den Behörden die Möglichkeit eingeräumt werden, gegenüber Zugangsanbietern die Sperre von Webseiten bzw. gegenüber Hosting-Provider die Entfernung von Inhalten anzuordnen. Beide Kompetenzen waren bislang grundsätzlich Strafverfolgungsbehörden bzw. den Gerichten vorbehalten.

### -----> Erfolgreiche Einbringung im Rahmen der nationalen Umsetzung

Im Rahmen mehrerer Arbeitsgruppen konnte die ISPA schließlich zur Erarbeitung einer nationalen Lösung

beitragen, in der sowohl die Interessen des Konsumentenschutzes berücksichtigt werden, jedoch auch Rechtssicherheit für Betreiber besteht und Grundrechte gewahrt bleiben. Zum einen verbleibt die Befugnis zur Anordnung von Auskunftsbefehlen gegenüber Providern aufgrund der Sensibilität der Kommunikationsdaten weiterhin bei der Staatsanwaltschaft bzw. den Gerichten. Daneben wurde ein Modell zur verfahrensrechtlichen Umsetzung von Netzsperrern geschaffen, welches Rücksicht auf die aktuell unklare Rechtslage für Betreiber nimmt.

### Rechtssicherheit für Provider

Die ISPA macht bereits seit Jahren auf die missliche Rechtslage für Zugangsanbieter in Bezug auf Netzsperrern aufmerksam. Nicht nur werden die Unternehmen – die lediglich eine Dienstleistung in Form eines Internetzugangs erbringen – seit jeher in einen Streit zwischen Webseiten-Betreibern und Rechteinhabern hineingezogen und sind am Ende diejenigen, welche den finanziellen und personellen Aufwand zu bewerkstelligen haben. Zusätzlich wurde mit einer EU-Verordnung aus dem Jahr 2016<sup>1</sup> (TSM-VO) eine Rechtslage geschaffen, in der es den Anbietern grundsätzlich verboten ist, Webseiten zu verlangsamen oder zu sperren, wenn hierfür kein Rechtfertigungsgrund – insbesondere eine entsprechende Entscheidung eines Gerichts oder eine eindeutige Rechtsgrundlage – existiert. Die Access-Anbieter sehen sich dazu verpflichtet, diesen Anforderungen bestmöglich Folge zu leisten und darüber hinaus auch im Interesse ihrer Kundinnen und Kunden hinsichtlich des freien Informationszugangs nur tatsächlich rechtswidrige Inhalte zu sperren. Aufgrund des massiven Drucks einiger Interessensgruppen, welche Zugangssperren auch ohne Vorliegen einer gerichtlichen oder behördlichen Entscheidung fordern, befinden sich die österreichischen Zugangsanbieter jedoch bereits seit beinahe 10 Jahren in langwierigen Gerichtsverfahren, für welche sie noch dazu die Kosten zu tragen haben.

Gemäß dem Gesetzesentwurf zur nationalen Umsetzung der Verordnung wurde nunmehr die Telekom-Control-Kommission, die auch die Einhaltung der TSM-VO überwacht, als zuständige Behörde zur Anordnung von Zugangssperren vorgesehen. Hierdurch soll erreicht werden, dass entsprechende Anordnungen jedenfalls in Konformität mit geltendem EU-Recht erfolgen. Es wäre äußerst positiv, wenn dieses Modell nun auch in anderen Rechtsmaterien übernommen werden würde, um auch dort die notwendige Rechtssicherheit für Provider zu schaffen. ■

<sup>1</sup> Verordnung (EU) 2015/2120 des Europäischen Parlaments und des Rates vom 25. November 2015 über Maßnahmen zum Zugang zum offenen Internet und zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten sowie der Verordnung (EU) Nr. 531/2012 über das Roaming in öffentlichen Mobilfunknetzen in der Union



## ISPA Academy zur Breitbandförderung sorgt für volles Haus

**Praxisnah, leicht verständlich und kompetent präsentierten das Breitbandbüro aus dem BMVIT und die Forschungsförderungsgesellschaft FFG verschiedene Wege zur Förderung. Eine aufbauende Folgeveranstaltung ist bereits in Planung.**

**a**nfang Juni konnten wir uns über eine ausgezeichnet besuchte ISPA Academy in den Räumlichkeiten des ISPA Büros freuen, zu der wir auch zahlreiche Mitglieder aus den Bundesländern begrüßen durften. Die Veranstaltung fand in Kooperation mit dem Breitbandbüro im Bundesministerium für Verkehr, Innovation und Technologie (BMVIT) und der Forschungsförderungsgesellschaft (FFG) statt. Äußerst kompetent und dank vieler konkreter Beispiele auch leicht verständlich wurden den Teilnehmerinnen und Teilnehmern die vier Förderprogramme ›Breitband Austria 2020‹ präsentiert: Leerrohrförderung, Backhaul, Access und Connect.

Die ISPA Academy bot viel Raum für Fragen und Diskussion und nicht zuletzt deswegen sowohl für Unerfahrene im Umgang mit diesem Thema als auch

für Routiniers, die bereits Förderanträge gestellt haben, einen Mehrwert und praktischen Nutzen. Das sehr gute Feedback im Anschluss an die Veranstaltung führte zu dem Entschluss, einen aufbauenden Folgetermin für den Herbst ins Auge zu fassen.

### Varianten der Breitbandförderung

Das Programm ›Breitband Austria 2020‹ hat den Ausbau von Breitbandnetzen in ganz Österreich zum Ziel. Angestrebt wird dabei eine möglichst flächendeckende Versorgung mit ultraschnellem Breitband und einer Verbindungsgeschwindigkeit von 100 Mbit/s.

Das Förderprogramm Access hat die räumliche Ausdehnung von leistungsstarken Zugangsnetzen im Fokus und zielt auf verbesserte Abdeckung. Im Programm Backhaul werden die Verstärkung der Zubringernetze und die Anbindung von Insellösungen an die Kernnetze unterstützt. Die Leerrohrförderung erleichtert die Mitverlegung von Leerverrohrungen für Kommunikationsnetze bei laufenden kommunalen Tiefbauarbeiten. Derzeit läuft ein Aufruf zum Leerverrohrungsprogramm, die Einreichstichtage sind der 13.08. und der 30.10.2019. Das Förderprogramm Connect beschleunigt den hochwertigen und nachhaltigen Glasfaserausbau einzelner Standorte mit Multiplikatorwirkung für den zukünftigen flächendeckenden Ausbau. Für Connect gibt es eine offene Ausschreibung ohne Stichtage.

Insgesamt stellt das BMVIT bis zum Jahr 2020 eine Milliarde Euro zur Verfügung, um das Breitbandnetz in Österreich auszubauen. Für potenzielle Förderungswerber bietet das Breitbandbüro eine umfassende Erstberatung an. Die Beratungstätigkeit umfasst dabei im Bedarfsfall eine Machbarkeits- sowie eine Grobkostenanalyse als Hilfestellung für eine Entscheidungsfindung, besonders bei der Frage nach der passenden Förderungsform. Die Abwicklung der Förderanträge erfolgt durch die FFG. ■



**»Der Online-Zoo« jetzt auch auf Portugiesisch**  
Mit der neuen portugiesischen Übersetzung ist das beliebte ISPA Kinderbuch bereits in zehn Sprachen verfügbar.

**d**ie jüngste Generation der Digital Natives wächst mit Handy, Internet & Co auf und entwickelt auch rasch einen instinktiven Umgang damit. Doch ohne entsprechende Medienbildung sowie kindgerechte Unterstützung beim Erwerb der ersten digitalen Kompetenzen sind die kleinen Userinnen und User sehr oft überfordert. Das ISPA Kinderbuch »Der Online-Zoo« ist diesbezüglich weltweit eines der wenigen Angebote für die Zielgruppe der 4- bis 9-Jährigen, weshalb die Übersetzung in möglichst viele Sprachen sehr wichtig ist.

Mit Unterstützung von Google und DGPI (Direção-Geral da Política de Justiça, dem portugiesischen Justizministerium) konnten wir das Kinderbuch nun auch ins Portugiesische übersetzen. Auch Dank der in Kooperation mit UNODC (United Nations Office on Drugs and Crime) entstandenen Übersetzungen ist der »Der Online-Zoo« mittlerweile auf Deutsch, Englisch, Arabisch, Französisch, Russisch, Spanisch, Farsi, Tschechisch, Chinesisch und Portugiesisch verfügbar. Das Kinderbuch kann in all diesen Sprachen auf [www.ispa.at/onlinezoo](http://www.ispa.at/onlinezoo) gratis heruntergeladen werden. ■

<b>A.K.I.S. GmbH</b> ACS	<b>APOLLO.AI GmbH</b> S	<b>Bundesrechenzentrum GmbH</b> ACS	<b>ComneX - Computer und Netzwerk GmbH</b> S	<b>datenwerk innovationsagentur GmbH</b> CS
Meiselstraße 46/4 1150 Wien Tel.: +43 1 50374 51 E-Mail: akis@akis.at Web: www.akis.at	Poschacherstraße 23/1 4020 Linz E-Mail: office@updatemi.com Web: www.apollo.ai	Hinter Zollamtsstraße 4 1030 Wien Tel.: +43 1 71123 0 E-Mail: office@brz.gv.at Web: www.brz.gv.at	Gastgebegasse 27, 1230 Wien Tel.: +43 1 8691981 0 E-Mail: office@comnex.net Web: www.comnex.net	Neubaugasse 68/2/1/20L 1070 Wien Tel.: +43 1 5856071 E-Mail: office@datenwerk.at Web: www.datenwerk.at
<b>abaton EDV-Dienstleistungs GmbH</b> CS	<b>ARApus GmbH - Geschäftsbereich Digital</b> ACS	<b>CC I Communications (CCC.at)</b> AS	<b>Compass-Gruppe GmbH</b> CS	<b>DI Johannes Schulz</b> S
Hans-Resel-Gasse 17 8020 Graz Tel.: +43 5 0240 0 E-Mail: office@abaton.at Web: www.abaton.at	Mariahilfer Straße 123, 1062 Wien Tel.: +43 1 2531001 500 E-Mail: michael.lichtenegger@araplus.at Web: www.araplus.at	Kaiserbrunnstraße 34 3021 Pressbaum Tel.: +43 1 50164 0 E-Mail: office@ccc.at Web: www.ccc.at	Matznergasse 17, 1141 Wien Tel.: +43 1 98116 0 E-Mail: office@compass.at Web: www.compass.at	Scheibenbergstraße 19 1180 Wien Tel.: +43 1 3085544 E-Mail: office@mailplus.co.at Web: www.mailplus.co.at
<b>ACOnet - Vienna University Computer Center</b> A	<b>artegic AG</b> AS	<b>China Telecom (Deutschland) GmbH</b> AS	<b>comteam it-solutions</b>	<b>DIALOG telekom GmbH &amp; Co KG</b> ACS
Universitätsstraße 7 1010 Wien Tel.: +43 1 4277 14030 E-Mail: helpdesk@aco.net Web: www.aco.net	Zanderstraße 7, 53177 Bonn Tel.: +49 228 227797 0 E-Mail: info@artegic.de Web: www.artegic.com	Bockenheimer Landstraße 77 60325 Frankfurt am Main Tel.: +49 69 24003 2929 E-Mail: marketing.germany@chinatelecomglobal.com Web: www.cteurope.net	Mitterfeldstraße 1 3300 Amstetten Tel.: +43 7472 20580 E-Mail: office@it.comteam.at Web: www.comteam.at	Goethestraße 93 4020 Linz Tel.: +43 732 662774 0 E-Mail: rpassecker@dialog-telekom.at Web: www.dialog-telekom.at
<b>adRom Media Marketing GmbH</b> CS	<b>ARZ Allgemeines Rechenzentrum Gesellschaft m.b.H.</b> ACS	<b>Christoph Schmoigl I edvUNION</b> S	<b>connecting : media it &amp; audio - consulting GmbH</b> S	<b>DIC-Online Wolf &amp; Co. KG</b> ACS
Lustenauerstraße 66 6850 Dornbirn Tel.: +43 5522 74813 0 E-Mail: office@adrom.net Web: www.adrom.net	Grasberggasse 13, 1030 Wien Tel.: +43 50 4009 5704 E-Mail: security@arz.at Web: www.arz.at	Landskrongasse 5/1/1/1 1010 Wien Tel.: +43 1 7108502 E-Mail: cs@edvu.at Web: www.edv-union.at	Steinheilgasse 5-7 1210 Wien Tel.: +43 1 2580477 E-Mail: office@conmed.net Web: www.conmed.net	Innrain 117 1. Stock 6020 Innsbruck Tel.: +43 512 341033 0 E-Mail: office@dic.at Web: www.dic.at
<b>AGNITAS AG</b> S	<b>ASCUS Telecom GmbH</b> AS	<b>CIDCOM Werbegagentur GmbH</b> CS	<b>conova communications GmbH</b> ACS	<b>domainname.at - webagentur.at Internet Service GmbH</b> ACS
Werner-Eckert-Straße 6 81829 München Tel.: +49 89 552908 0 E-Mail: info@agnitas.de Web: www.agnitas.de	Adi-Dassler-Gasse 6 9073 Klagenfurt-Viktring Tel.: +43 463 2080 0 E-Mail: office@ascus.at Web: www.ascus.at	Wiedner Hauptstraße 78 1040 Wien Tel.: +43 1 4064814 0 E-Mail: office@cidcom.at Web: www.cidcom.at	Karolingerstraße 36A 5020 Salzburg Tel.: +43 662 2200 0 E-Mail: s.kaltenbrunner@conova.com Web: www.conova.com	Beethovenngasse 4-6, 2500 Baden Tel.: +43 2252 259892 E-Mail: office@webagentur.at Web: www.domainname.at
<b>Algo GmbH</b> CS	<b>atms Telefon- und Marketing Services GmbH</b> S	<b>Cisco Systems Austria GmbH</b> S	<b>CoreTEC IT Security Solutions GmbH</b> S	<b>easyname GmbH</b> CS
Hauptstraße 385 5531 Eben im Pongau Tel.: +43 6458 20242 E-Mail: weitgasser@algo.at Web: www.algo.at	Leonard-Bernstein-Straße 10/17 1220 Wien Tel.: +43 800 2404010 E-Mail: service@atms.at Web: www.atms.at	Handelskai 94-96, 1200 Wien Tel.: +43 1 24030 6024 E-Mail: hgreiner@cisco.com Web: www.cisco.at	Ernst Melchior Gasse 24/DG 1020 Wien Tel.: +43 1 5037273 0 E-Mail: m.kirisits@coretec.at Web: www.coretec.at	Fernkornngasse 10/3/501 1100 Wien Tel.: +43 1 3360006 E-Mail: office@easyname.com Web: www.easyname.com/de
<b>alladin-IT GmbH</b> S	<b>AVM GmbH for International Communication Technology</b> S	<b>Citycom Telekommunikation GmbH</b> AS	<b>COSYS DATA GmbH</b> S	<b>echonet communication GmbH</b> CS
Hebragasse 2/1/6 1090 Wien Tel.: +43 1 8905739 E-Mail: office@alladin.at Web: alladin.at	Alt-Moabit 95, 10559 Berlin Tel.: +49 30 39976 232 E-Mail: ict-info@avm.de Web: www.avm.de	Gadollaplatz 1, 8010 Graz Tel.: +43 316 887 0 E-Mail: bernd.stockinger@holding-graz.at Web: www.citycom.co.at	Stifterstraße 19 4360 Grein Tel.: +43 1 2299600 E-Mail: office@cosys.cc Web: www.cosys.cc	Rosenbursenstraße 2/24 1010 Wien Tel.: +43 1 5122695 E-Mail: office@echonet.at Web: www.echonet.at
<b>ANEXIA Internetdienstleistungs GmbH</b> S	<b>barga.com technische Dienstleistungs GmbH</b> S	<b>CloudNow GmbH</b> AS	<b>Crayon Austria GmbH</b> S	<b>EDV-Dienstleistungen Rappaport GmbH &amp; Co. KG</b> S
Feldkirchnerstraße 140 9020 Klagenfurt am Wörthersee Tel.: +43 463 208501 E-Mail: info@anexia.at Web: www.anexia.at	Leusbundweg 49a 6800 Feldkirch Tel.: +43 676 4355010 E-Mail: reg@barga.com Web: www.barga.com	Kaiser Josef Platz 52, 4600 Wels Tel.: +43 50 152 501 E-Mail: sales@cloudnow.at Web: www.cloudnow.at	Liebermannstraße F04 Tür 201 2345 Brunn am Gebirge Tel.: +43 720 303025 0 E-Mail: office.at@crayon.com Web: www.crayon.com/at	Geblergasse 95/8 1170 Wien Tel.: +43 1 9068020 10 E-Mail: dominik.rappaport@rappaport.at Web: www.rappaport.at
<b>Antares-NetlogiX Netzwerkberatung GmbH</b> AS	<b>BK-DAT Electronics e.U.</b> AS	<b>Colt Technology Services GmbH</b> ACS	<b>CSO.Net Internet Services GmbH</b> ACS	<b>EDV-Himmelbauer</b> A
Feldstraße 13 3300 Amstetten Tel.: +43 7472 65480 E-Mail: office@netlogix.at Web: www.netlogix.at	Hiefelauer Straße 18 8790 Eisenerz Tel.: +43 3848 60048 E-Mail: info@bkdat.net Web: www.bkdat.net	Kärntner Ring 10-12 1010 Wien Tel.: +49 69 56606 6591 E-Mail: christian.weber@colt.net Web: www.colt.net	Franzosengraben 10 1030 Wien Tel.: +43 1 206 30 0 E-Mail: office@cso.net Web: www.cso.net	Kremserstraße 8, 2070 Retz Tel.: +43 2942 20670 E-Mail: jhimmelbauer@edv-himmelbauer.at Web: www.edv-himmelbauer.at
<b>APA-IT Informations Technologie GmbH</b> ACS	<b>Bluespeed e.U.</b> AS	<b>comm-IT EDV Dienstleistungsgmbh</b> ACS	<b>Cu4IT BV</b> A	<b>emerion WebHosting GmbH</b> S
Laimgrubengasse 10 1060 Wien Tel.: +43 1 36060 6060 E-Mail: it-vertrieb@apa.at Web: www.apa-it.at	Kurzschwarza 15, 3944 Schrems Tel.: +43 681 10648707 E-Mail: office@bluespeed.eu Web: bluespeed.eu	Adamsgasse 1/20, 1030 Wien Tel.: +43 1 205210 E-Mail: karl.pusch@comm-it.at Web: www.comm-it.at	PO BOX 9332 1800 GH Alkmaar Tel.: +31 72 5024150 E-Mail: info@Cu4IT.com Web: www.cu4it.com	Hofmühlgasse 3-5 1060 Wien Tel.: +43 1 2988800 E-Mail: office@emerion.com Web: www.emerion.com
	<b>Brennercom Tirol GmbH</b> AS		<b>CUBIT IT Solutions GmbH</b> ACS	<b>Empirion Telekommunikations Services GmbH</b> ACS
	Eduard-Bodem-Gasse 8 6020 Innsbruck Tel.: +43 512 279279 E-Mail: info@brennercom-tirol.at Web: www.brennercom.tirol		Zieglergasse 67/3/1 Hoftrakt 1070 Wien Tel.: +43 1 7189880 0 E-Mail: paul.witta@cubit.at Web: www.cubit.at	Horneckgasse 8, 1170 Wien Tel.: +43 1 4805000 E-Mail: office@empirion.at Web: www.empirion.at
			<b>CYAN Networks Software GmbH</b> AS	<b>Energie AG Oberösterreich Telekom GmbH</b> AS
			Krotenthallergasse 8 1080 Wien Tel.: +43 1 33933 0 E-Mail: klaus.thurnhofer@cyanetworks.com Web: www.cyan-networks.com	Böhmervaldstraße 3 4021 Linz Tel.: +43 5 9000 2575 E-Mail: telekom@energieag.at Web: www.energieag.at

# members

## August 2019

<b>Energie Steiermark AG</b> <b>A</b> Leonhardgürtel 10 8010 Graz Tel.: +43 316 9000 0 E-Mail: info@e-steiermark.com Web: www.e-steiermark.com	<b>Freewave GmbH</b> <b>A</b> Premlechnergasse 12/A7 1120 Wien Tel.: +43 1 8040134 E-Mail: office@freewave.at Web: www.freewave.at	<b>HUAWEI TECHNOLOGIES AUSTRIA GMBH</b> <b>CS</b> Wagramer Str. 19, IZD Tower 1220 Wien Tel.: +43 1 21180 871 E-Mail: atenterprise@huawei.com Web: e.huawei.com/at/	<b>internic Datenkommunikations GmbH</b> <b>S</b> Puchsbauplatz 2/7-8 1100 Wien Tel.: +43 1 3249685 E-Mail: info@internic.at Web: www.internic.at	<b>kabelplus GmbH</b> <b>AS</b> Südtstadtzentrum 4 2344 Maria Enzersdorf Tel.: +43 5 0514 0 E-Mail: ispa@kabelsignal.at Web: www.kabelplus.at
<b>EPB EDV-Partner OG</b> <b>CS</b> Hauptstraße 17 7051 Grobhöflein Tel.: +43 699 12370970 E-Mail: office@epb.at Web: www.epb.at	<b>FunkFeuer Wien - Verein zur Förderung freier Netze</b> <b>AS</b> Gonzagagasse 11/25, 1010 Wien E-Mail: admin@funkfeuer.at Web: www.funkfeuer.at	<b>Huemer Data Center Ges.m.b.H.</b> <b>ACS</b> Leonard-Bernstein-Straße 10 1220 Wien Tel.: +43 664 4118000 E-Mail: walter.huemer@huemer-it.com Web: www.huemer-dc.com	<b>InterXion Österreich GmbH</b> <b>S</b> Louis-Häfliger-Gasse 10 1210 Wien Tel.: +43 1 2903636 0 E-Mail: vienna.info@interxion.com Web: www.interxion.com	<b>KAPPER NETWORK-COMMUNICATIONS GmbH - kapper.net</b> <b>ACS</b> Alserbachstrasse 11/6 1090 Wien Tel.: +43 1 3195500 0 E-Mail: info@kapper.net Web: www.kapper.net
<b>Episerver GmbH</b> <b>S</b> Wallstrasse 16 10179 Berlin Tel.: +49 30 768078 0 E-Mail: infodach@episerver.com Web: www.episerver.de	<b>Futureweb OG</b> <b>CS</b> Innsbrucker Straße 4 6380 St. Johann in Tirol Tel.: +43 5352 65335 0 E-Mail: info@futureweb.at Web: www.futureweb.at	<b>Hutchison Drei Austria GmbH</b> <b>ACS</b> Brünner Straße 52, 1210 Wien Tel.: +43 5 0660 0 E-Mail: serviceteam@drei.at Web: www.drei.at	<b>IP Austria Communication GmbH</b> <b>AS</b> Wienerbergstrasse 11/ B16 1100 Wien Tel.: +43 50 662 0 E-Mail: office@ipaustria.com Web: www.ipaustria.at	<b>Kaufmann Ges.m.b.H</b> <b>A</b> Goldenkronsgasse 9 3500 Krems an der Donau Tel.: +43 2732 85625 E-Mail: office@ktv-krems.at Web: www.ktv-krems.at
<b>eww iTandTEL (Geschäftsbereich der eww Gruppe)</b> <b>ACS</b> Knorrstraße 10 4600 Wels Tel.: +43 7242 9396 7100 E-Mail: office@itandtel.at Web: www.itandtel.at	<b>Gamsjaeger Kabel-TV &amp; ISP Betriebs GmbH</b> <b>AS</b> Unterauer Straße 7, 3370 Ybbs Knorrstraße 10 4600 Wels Tel.: +43 7242 9396 7100 E-Mail: office@wibs.at Web: www.wibs.at	<b>HXS GmbH</b> <b>AS</b> Millergasse 3, 1060 Wien Tel.: +43 1 3441344 E-Mail: office@hxs.at Web: www.hxs.at	<b>IPAX OG</b> <b>AS</b> Barawitzkagasse 10/2/2/11 1190 Wien Tel.: +43 1 3670030 E-Mail: office@ipax.at Web: www.ipax.at	<b>kitznet - Stadtwerke Kitzbühel</b> <b>ACS</b> Jochberger Straße 36 6370 Kitzbühel Tel.: +43 5356 65651 E-Mail: internet@kitz.net Web: www.kitz.net
<b>Facebook Germany GmbH</b> <b>AC</b> »Sony Center« Kemperplatz 1 10785 Berlin Tel.: +49 30 300145553 E-Mail: politik@fb.com Web: www.facebook.com/PublicPolicyOfficeBerlin	<b>GANZRUND Informatik GmbH</b> <b>CS</b> Kurandplatz 1 9020 Klagenfurt a.W. Tel.: +43 5 1709 E-Mail: info@ganzrund.com Web: ganzrund.com	<b>iForce IT GmbH</b> <b>ACS</b> Bandgasse 27/1, 1070 Wien Tel.: +43 1 9076344 300 E-Mail: office@iforce.at Web: www.iforce.at	<b>ipcom GmbH</b> <b>S</b> Karlsplatz 1 1010 Wien Tel.: +43 664 1445686 E-Mail: office@ipcom.at Web: www.ipcom.at	<b>KraftCom e.U.</b> <b>ACS</b> Göstling 108 3345 Göstling / Ybbs Tel.: +43 7484 257012 E-Mail: office@kraftcom.at Web: www.kraftcom.at
<b>Faxonline GmbH</b> <b>S</b> Mariahilferstraße 136 1150 Wien Tel.: +43 800 802102 E-Mail: info@faxonline.at Web: www.faxonline.at	<b>Gemeindewerke Telfs GmbH</b> <b>ACS</b> Bahnhofstraße 40, 6410 Telfs Tel.: +43 5262 62330 E-Mail: office@gwtelfs.at Web: www.gwtelfs.at	<b>ifunk.at</b> <b>AS</b> Gaisberg 5 4175 Herzogsdorf Tel.: +43 720 345488 E-Mail: office@ifunk.at Web: www.ifunk.at	<b>iPlace Internet &amp; Network Services GmbH</b> <b>ACS</b> Ringstraße 5, 1. Stock 6830 Rankweil Tel.: +43 5552 20500 E-Mail: office@iplace.at Web: www.iplace.at	<b>Kreativwirtschaft Austria</b> <b>S</b> Wiedner Hauptstraße 63 1045 Wien Tel.: +43 5 90900 0 E-Mail: gertraud.leimueller@wko.at Web: www.kreativwirtschaft.at
<b>Feistritzwerke-STEWEAG GmbH</b> <b>A</b> Gartengasse 36, 8200 Gleisdorf Tel.: +43 3112 2653 0 E-Mail: erich.rybar@feistritzwerke.at Web: www.feistritzwerke.at	<b>GiGaNet.at, Bernhard Kröll</b> <b>AS</b> Rauchenwald 651 6290 Mayrhofen Tel.: +43 5285 630 850 E-Mail: office@giganet.at Web: www.giganet.at	<b>IKARUS Security Software GmbH</b> <b>S</b> Blechturmstraße 11 1050 Wien Tel.: +43 1 58995 E-Mail: pichlmayr.j@ikarus.at Web: www.ikarus.at	<b>ITEG IT-Engineers GmbH</b> <b>S</b> Conradstraße 5 6020 Innsbruck E-Mail: office@iteg.at Web: www.iteg.at	<b>KT-NET Communications GmbH</b> <b>ACS</b> Ramingdorf 51, 4441 Behamberg Tel.: +43 7252 77852 10 E-Mail: office@kt-net.at Web: www.kt-net.at
<b>Feistritzwerke-STEWEAG GmbH</b> <b>A</b> Gartengasse 36, 8200 Gleisdorf Tel.: +43 3112 2653 0 E-Mail: erich.rybar@feistritzwerke.at Web: www.feistritzwerke.at	<b>Google Austria GmbH</b> Graben 19, 1010 Wien Tel.: +43 1 23060 6001 E-Mail: press@google.com Web: www.google.at	<b>Infotech EDV-Systeme GmbH</b> <b>AS</b> Schaerdinger Straße 35 4910 Ried im Innkreis Tel.: +43 7752 81711 0 E-Mail: office@infotech.at Web: www.infotech.at	<b>IT-Technology Gesellschaft für industrielle Elektronik und Informationstechnologie mbH</b> <b>S</b> Grillgasse 18 1110 Wien Tel.: +43 1 229922 0 E-Mail: office@it-technology.at Web: www.it-technology.at	<b>Kumi Systems e.U.</b> <b>ACS</b> Sternäckerweg 51a/2 8041 Graz Tel.: +43 800 093004 E-Mail: office@kumi.systems Web: kumi.systems
<b>FH des BFI Wien</b> Maria Jacobigasse 1/3 1030 Wien Tel.: +43 1 72012860 940 E-Mail: info@fh-vie.ac.at Web: www.fh-vie.ac.at	<b>GRZ IT Center GmbH</b> <b>S</b> Goethestraße 80, 4020 Linz Tel.: +43 732 6929 1507 E-Mail: bachleitner@grz.at Web: www.grz.at	<b>Innosoft GmbH</b> <b>A</b> Speckbacherstraße 12 6380 St. Johann Tel.: +43 5352 207207 E-Mail: d.hirschbichler@innosoft.at Web: www.innosoft.at	<b>IT-Technology Gesellschaft für industrielle Elektronik und Informationstechnologie mbH</b> <b>S</b> Grillgasse 18 1110 Wien Tel.: +43 1 229922 0 E-Mail: office@it-technology.at Web: www.it-technology.at	<b>LED.net GmbH</b> <b>ACS</b> Lederergasse 6 5204 Straßwalchen Tel.: +43 6215 20888 E-Mail: office@domainttechnik.at Web: www.domainttechnik.at
<b>FH Technikum Wien</b> <b>C</b> Höchstädtplatz 6 1200 Wien Tel.: +43 1 3334077 E-Mail: info@technikum-wien.at Web: www.technikum-wien.at	<b>GExperts GmbH</b> <b>S</b> Gutenberggasse 1/13 1070 Wien Tel.: +43 1 2362933 E-Mail: info@g-experts.net Web: www.g-experts.net	<b>Innsbrucker Kommunalbetriebe AG</b> <b>AS</b> Langer Weg 29 6020 Innsbruck Tel.: +43 512 502 6410 E-Mail: kundenservice@ikb.at Web: www.internet.ikb.at	<b>IT-Technology Gesellschaft für industrielle Elektronik und Informationstechnologie mbH</b> <b>S</b> Grillgasse 18 1110 Wien Tel.: +43 1 229922 0 E-Mail: office@it-technology.at Web: www.it-technology.at	<b>Leitstelle Tirol</b> <b>ACS</b> Hunoldstraße 17 a 6020 Innsbruck Tel.: +43 512 3313 E-Mail: it@leitstelle.tirol Web: www.leitstelle.tirol
<b>Flughafen Wien AG</b> <b>AS</b> Objekt 660 1300 Wien-Flughafen Tel.: +43 1 7007 0 E-Mail: m.dohnal@viennaairport.com Web: www.viennaairport.com	<b>HEROLD Business Data GmbH</b> <b>CS</b> Guntramsdorfer Straße 105 2340 Mödling Tel.: +43 2236 401 651 E-Mail: frank.bieser@herold.at Web: www.herold.at	<b>Institut für empirische Sozialforschung (IFES) GmbH</b> <b>C</b> Teinfaltstraße 8 1010 Wien Tel.: +43 1 54670 E-Mail: wasserbacher@ifes.at Web: www.ifes.at	<b>IT-Technology Gesellschaft für industrielle Elektronik und Informationstechnologie mbH</b> <b>S</b> Grillgasse 18 1110 Wien Tel.: +43 1 229922 0 E-Mail: office@it-technology.at Web: www.it-technology.at	<b>LexisNexis Verlag ARD Orac GmbH &amp; Co KG</b> <b>CS</b> Marxergasse 25 1030 Wien Tel.: +43 1 53452 1010 E-Mail: verlag@lexisnexis.at Web: www.lexisnexis.at
<b>fonira Telekom GmbH</b> <b>AS</b> Prager Straße 6 1210 Wien Tel.: +43 1 23400 E-Mail: service@mediainvent.com Web: www.mediainvent.com	<b>hotze.com GmbH</b> <b>AS</b> Eduard-Bodem-Gasse 6 6020 Innsbruck Tel.: +43 512 353640 E-Mail: office@hotze.com Web: www.hotze.com	<b>Internet Viennaweb Service GmbH</b> <b>S</b> Perfektastraße 19/2 1230 Wien Tel.: +43 1 9564606 E-Mail: office@viennaweb.at Web: www.viennaweb.at	<b>Jumper GmbH</b> <b>ACS</b> Siegfriedgasse 23 Tor1 1210 Wien Tel.: +43 1 9051155 E-Mail: office@jumper.at Web: www.jumper.at	<b>Licht- und Kraftvertrieb der Gemeinde Hollenstein/Ybbs</b> <b>AS</b> Walcherbauer 2 3343 Hollenstein an der Ybbs Tel.: +43 7445 218 16 E-Mail: lkv@hollenstein.at Web: www.oganet.at
<b>Foundation for Applied Privacy - Verein zur Förderung der digitalen Privatsphäre</b> <b>S</b> Floragasse 7/5 1040 Wien Tel.: +43 681 10895330 E-Mail: contact@appliedprivacy.net Web: www.appliedprivacy.net			<b>KABEL TV AMSTETTEN GMBH</b> <b>AS</b> Kruppstraße 3 3300 Amstetten Tel.: +43 7472 66667 0 E-Mail: office@ktvam.at Web: www.ktvam.at	



OH, HEY, YOU ORGANIZED  
OUR PHOTO ARCHIVE!

YEAH, I TRAINED A NEURAL  
NET TO SORT THE UNLABELED  
PHOTOS INTO CATEGORIES.

WHOA! NICE WORK!



**ENGINEERING TIP:**  
WHEN YOU DO A TASK BY HAND,  
YOU CAN TECHNICALLY SAY YOU  
TRAINED A NEURAL NET TO DO IT.

© Randall Munroe - xkcd.com

#### LINZ AG Telekom **AS**

Wiener Straße 151  
4021 Linz  
Tel.: +43 732 3400 7315  
E-Mail: m.past@linzag.at  
Web: www.linzag-telekom.at

#### LinzNet Internet Service **AS**

Hafenstraße 1-3  
4020 Linz  
Tel.: +43 732 2360  
E-Mail: office@linznet.at  
Web: www.linznet.at

#### LIWEST Kabelmedien **AS**

Lindengasse 18  
4040 Linz  
Tel.: +43 732 942424  
E-Mail: g.singer@liwest.at  
Web: www.liwest.at

#### Magenta Telekom **A**

Rennweg 97-99  
1030 Wien  
Tel.: +43 1 79585 0  
E-Mail: ispa@magenta.at  
Web: www.magenta.at

#### MakeNewMedia **ACS**

Wilhelminenstraße 80 - 82  
1160 Wien  
Tel.: +43 1 338333 0  
E-Mail: sales@  
makenewmedia.com  
Web: www.makenewmedia.com

#### Mapp Digital Germany GmbH **S**

Dachauer Straße 63  
80335 München  
Tel.: +49 89 12009 600  
E-Mail: andre.goerner@  
teradata.com  
Web: www.teradata.com

#### Marc Schwaar **S**

Gumpendorferstraße 60/6  
1060 Wien  
Tel.: +43 1 5852666  
E-Mail: schwaar@schwaar.com  
Web: www.schwaar.com

#### Mass Response **AS**

Service GmbH  
Donau-City-Straße 7; DC  
Tower 1, 38th floor  
1220 Wien  
Tel.: +43 1 2702825  
E-Mail: office@  
massresponse.com  
Web: www.massresponse.com

#### MediaCian - Gesellschaft für **CS**

Online Medien G.m.b.H.  
Nestroyplatz 1/1/14a  
1020 Wien  
Tel.: +43 1 4075060 0  
E-Mail: office@mediacian.at  
Web: www.mediacian.at

#### MELON Informationstechno- **C**

logie GmbH  
Weyringergasse 13, 1040 Wien  
Tel.: +43 1 5056610  
E-Mail: office@melon.at  
Web: www.melon.at

#### Microsoft Österreich **CS**

GesmbH.  
Am Euro Platz 3, 1120 Wien  
Tel.: +43 1 61064 0  
E-Mail: austria@microsoft.com  
Web: www.microsoft.com/austria

#### mieX GmbH - Mühlviertler **AS**

Internet Exchange  
Markt 8, 4153 Peilstein  
Tel.: +43 5 9008 008  
E-Mail: office@mieX.at  
Web: www.mieX.at

#### MMC Kommunikationstechno- **ACS**

logie GesmbH  
Mühlgasse 14/E, 2353 Guntramsdorf  
Tel.: +43 2236 3903  
E-Mail: office@mmc.at  
Web: www.mmc.at

#### ms-cns Communication **A**

Network Solutions GmbH  
Scheydgasse 34-36, 1210 Wien  
Tel.: +43 1 2703070  
E-Mail: office@ms-cns.com  
Web: www.ms-cns.com

#### Multikom Austria Telekom **AS**

GmbH  
Jakob-Haringer-Straße 1  
5020 Salzburg  
Tel.: +43 59 333 1000  
E-Mail: office@xlink.at  
Web: www.xlink.at

#### mur.at - Verein zur Förderung **ACS**

von Netzwerkunst  
Leitnergasse 7a, 8010 Graz  
Tel.: +43 316 821451 26  
E-Mail: verein@mur.at  
Web: www.mur.at

#### mWS myWorld Solutions AG **S**

Grazbachgasse 87-93  
8010 Graz  
Tel.: +43 316 70770  
E-Mail: office@myworld.com  
Web: www.myworld-  
solutions.com

#### myNET gmbh **AS**

Bruggfeldstraße 5, 6500 Landeck  
Tel.: +43 676 841810300  
E-Mail: hh@mynet.at  
Web: www.mynet.at

#### NA-NET Communications **AS**

GmbH  
Neudorf bei Staats 276  
2135 Neudorf bei Staats  
Tel.: +43 2572 20233 0  
E-Mail: office@nanet.at  
Web: www.nanet.at

#### nemox.net Informationstechno- **AS**

logie OG  
Eduard-Bodem-Gasse 9  
6020 Innsbruck  
Tel.: +43 5 0234 0  
E-Mail: info@nemox.net  
Web: nemox.net

#### NeoTel Telefonservice **S**

GmbH & Co KG  
Esterhazygasse 18a/15, 1060 Wien  
Tel.: +43 1 4094181 0  
E-Mail: office@neotel.at  
Web: www.neotel.at

#### Nessus GmbH **ACS**

Fernkorngasse 10/3/501  
1100 Wien  
Tel.: +43 1 3360006  
E-Mail: fs@nessus.at  
Web: www.nessus.at

#### Net4You Internet GmbH **ACS**

Tiroler Straße 80, 9500 Villach  
Tel.: +43 4242 5005  
E-Mail: office@net4you.net  
Web: www.net4you.net

#### NETPLANET GmbH **ACS**

Louis-Häfliger-Gasse 10  
1210 Wien  
Tel.: +43 1 3430343  
E-Mail: billing@netplanet.at  
Web: www.netplanet.at

#### netSERVICE gmbh **S**

Bundesstraße 66, 8740 Zellweg  
Tel.: +43 3577 81180 0  
E-Mail: office@netservice.at  
Web: www.netservice.at

#### Netvisual OG **ACS**

Zirkusgasse 36/1, 1020 Wien  
Tel.: +43 1 24299  
E-Mail: office@netvisual.tv  
Web: www.netvisual.tv

#### Network & Internet **CS**

Technologies  
Am Sonnenhang 9  
8700 Leoben  
Tel.: +43 3842 22287  
E-Mail: kundensupport@nit.at  
Web: www.nit.at

#### next layer Telekommunikationsdienstleistungs- und **AS**

BeratungsGmbH  
Mariahilfer Gürtel 37/7  
1150 Wien  
Tel.: +43 5 1764 0  
E-Mail: office@nextlayer.at  
Web: www.nextlayer.at

#### nfon GmbH **S**

Linzer Straße 55  
3100 St. Pölten  
Tel.: +43 2742 75566  
E-Mail: office.at@nfon.net  
Web: www.nfon.at

#### Niederösterreichische **A**

Glasfaserinfrastrukturgesell-  
schaft mbH  
Niederösterreich-Ring 2/B/4  
3100 St. Pölten  
Tel.: +43 2742 9000 19767  
E-Mail: office@noegig.at  
Web: www.noegig.at

#### Nokia Solutions and Networks **AS**

Österreich GmbH  
Leonard-Bernstein-Straße 10  
1220 Wien  
Tel.: +43 05 70020  
E-Mail: office.vienna@nokia.com  
Web: www.nokia.at

#### Ocilion IPTV Technologies **ACS**

GmbH  
Schaerdinger Straße 35  
4910 Ried im Innkreis  
Tel.: +43 7752 2144 0  
E-Mail: office@ocilion.com  
Web: www.ocilion.com

#### OeKB - Oesterreichische **CS**

Kontrollbank AG  
Strauchgasse 3  
1011 Wien  
Tel.: +43 1 53127 2175  
E-Mail: ewald.jenisch@oekb.at  
Web: www.oekb.at

#### ÖIAT - Österreichisches **C**

Institut für angewandte  
Telekommunikation  
Ungargasse 64-66/3/4/404  
1030 Wien  
Tel.: +43 1 5952112 0  
E-Mail: office@oiat.at  
Web: www.oiat.at

#### OmanBros.com Internetdienst- **CS**

leistungen GmbH  
Guglgasse 8/2/85  
1110 Wien  
Tel.: +43 1 9690304 0  
E-Mail: office@omanbros.com  
Web: www.omanbros.com

#### OpenNet GmbH **AC**

Gartengasse 14  
1050 Wien  
Tel.: +43 1 9072429  
E-Mail: office@open-net.at  
Web: www.open-net.at

#### Orange Business **AS**

Austria GmbH  
Laxenburgerstrasse 2 / 1 / 4  
1100 Wien  
Tel.: +43 1 36037 0  
E-Mail: josef.canete@orange.com  
Web: www.orange-  
business.com

#### ORF Online und Teletext **CS**

GmbH & Co KG  
Würzburggasse 30  
1136 Wien  
Tel.: +43 1 50277 0  
E-Mail: online@orf.at  
Web: www.orf.at

#### Ortswärme St. Johann in Tirol **A**

GmbH  
Speckbacherstraße 33  
6380 St. Johann in Tirol  
Tel.: +43 5352 20766  
E-Mail: office@ortswaerme.info  
Web: www.ortswaerme.info

#### Österreichische Post **AC**

Aktiengesellschaft  
Rochusplatz 1, 1030 Wien  
Tel.: +43 57767 0  
E-Mail: kundenservice@post.at  
Web: www.post.at

#### Peter Ostry e.U. **CS**

Wiener Landstraße 9/1  
3452 Michelndorf  
Tel.: +43 1 8777454 0  
E-Mail: email@ostry.com  
Web: www.ostry.com

#### Peter Rauter GmbH **ACS**

Bahnhofstr. 11  
5202 Neumarkt  
Tel.: +43 6216 5721 0  
E-Mail: rauter@rauter-it.at  
Web: www.rauter-it.at

#### pflaeging.net **CS**

In den Jochen 49  
2122 Ulrichskirchen  
E-Mail: office@pflaeging.net  
Web: www.pflaeging.net

#### PGV Computer Handels **AS**

GmbH & CoKG  
Kremser Landstraße 34  
3100 St. Pölten  
Tel.: +43 2742 366301  
E-Mail: online@pgv.at  
Web: www.pgv.at

#### Preisvergleich Internet **CS**

Services AG  
Obere Donaustraße 63/2  
1020 Wien  
Tel.: +43 1 5811609  
E-Mail: markus.nigl@geizhals.at  
Web: www.geizhals.at

#### quintessenz **A**

c/o quartier21 / MQ,  
Museumsplatz 1 (Electric Avenue)  
1070 Wien  
E-Mail: office@quintessenz.org  
Web: www.quintessenz.org

#### Raiffeisen Informatik **ACS**

GmbH  
Lilienbrunnengasse 7 - 9, 1020 Wien  
Tel.: +43 1 99399 0  
E-Mail: info@r-it.at  
Web: www.r-it.at

#### Riepert Informations- **AS**

technologie OG  
Bad Kreuzen 95, 4362 Bad Kreuzen  
Tel.: +43 7266 5901  
E-Mail: g.riepert@riepert.at  
Web: www.riepert.at

#### RIS GmbH **AS**

Im Stadtgut A1  
4407 Steyr-Gleink  
Tel.: +43 7252 86186 0  
E-Mail: info@ris.at  
Web: www.ris.at

#### roNet GmbH **AS**

Ahornweg 9, 4150 Rohrbach  
Tel.: +43 676 9112777  
E-Mail: office@ronet.at  
Web: www.ronet.at

#### RTCnow Streaming Services **CS**

GmbH  
Zirkusgasse 36/1, 1020 Wien  
Tel.: +43 50 955  
E-Mail: ispa@rtcnow.com  
Web: www rtcnow.com

**Russmedia Digital GmbH ACS**  
Gutenbergstraße 1  
6858 Schwarzach  
Tel.: +43 5572 501 727  
E-Mail: webmaster@austria.com  
Web: werbung.vol.at

**Russmedia IT GmbH ACS**  
Gutenbergstraße 1  
6858 Schwarzach  
Tel.: +43 5572 501 735  
E-Mail: webmaster@vol.at  
Web: highspeed.vol.at

**s IT Solutions AT Spardat GmbH ACS**  
Geiselbergstraße 21 - 25  
1110 Wien  
Tel.: +43 5100 39637  
E-Mail: horst.ganster@s-itsolutions.at  
Web: www.s-itsolutions.com

**Salzburg AG für Energie, Verkehr und Telekommunikation ACS**  
Bayerhamerstraße 16  
5020 Salzburg  
Tel.: +43 662 8884 2781  
E-Mail: herbert.stranzinger@salzburg-ag.at  
Web: www.salzburg-ag.at

**SBR-net Consulting AG S**  
Parkring 10/1/10, 1010 Wien  
Tel.: +43 1 5135140 0  
E-Mail: ruhle@sbr-net.com  
Web: www.sbr-net.com

**Schallert.com e.U. S**  
Hauptstraße 35b, 6800 Feldkirch  
Tel.: +43 5522 26500  
E-Mail: office@schallert.com  
Web: www.schallert.com

**SC-Networks / EVALANCHE - eMail Marketing Solution CS**  
Enzianstraße 2, 82319 Starnberg  
Tel.: +49 8151 555 160  
E-Mail: info@sc-networks.com  
Web: www.sc-networks.com

**SIPit Kommunikationsmanagement GmbH ACS**  
Scherzergasse 12/1, 1020 Wien  
Tel.: +43 1 342342  
E-Mail: office@sipit.at  
Web: www.sipit.at

**siplan gmbH, Ing. Alfred Gunsch ACS**  
Einfang 29/3  
6130 Schwaz  
Tel.: +43 512 268000  
E-Mail: office@siplan.at  
Web: www.siplan.at

**sourceheads Information Technology GmbH C**  
Bräuhausgasse 6/2/6  
1050 Wien  
Tel.: +43 1 917 417 0  
E-Mail: info@sourceheads.com  
Web: www.sourceheads.com

**SPÖ Informations-technologiezentrum S**  
Windmühlgasse 26  
1060 Wien  
Tel.: +43 1 53427 283  
E-Mail: office@itz.spoe.at  
Web: www.spoe.at

**Sprint International Austria GmbH ACS**  
Schottenring 16, 1010 Wien  
Tel.: +43 1 53712 4167  
E-Mail: alexander.valenta@sprint.com  
Web: www.sprintworldwide.com

**Stadtwerke Feldkirch AS**  
Leusbündtweg 49  
6800 Feldkirch  
Tel.: +43 5522 9000  
E-Mail: kundencenter@stadtwerke-feldkirch.at  
Web: www.stadtwerke-feldkirch.at

**Stadtwerke Hall in Tirol GmbH AS**  
Augasse 6  
6060 Hall in Tirol  
Tel.: +43 5223 5855 2100  
E-Mail: m.kofler@hall.ag  
Web: www.citynet.at

**Stadtwerke Imst ACS**  
Pfarrgasse 3, 6460 Imst  
Tel.: +43 5412 63324  
E-Mail: stadtwerke@stwmst.at  
Web: www.cni.at

**Stadtwerke Kapfenberg GmbH AS**  
Stadtwerkestraße 6  
8605 Kapfenberg  
Tel.: +43 3862 23516 0  
E-Mail: ispa@hiway.at  
Web: www.hiway.at

**Stadtwerke Klagenfurt Aktiengesellschaft AS**  
St. Veiter Straße 31  
9020 Klagenfurt am Wörthersee  
Tel.: +43 463 521 603  
E-Mail: guenter.glaboniat@stw.at  
Web: www.stw.at

**Stadtwerke Kufstein GmbH A**  
Fischergries 2  
6330 Kufstein  
Tel.: +43 5372 69303 23  
E-Mail: schuster@stwk.at  
Web: www.kufnet.at

**Stadtwerke Wörgl Ges.m.b.H. AS**  
Zauberwinklweg 2a  
6300 Wörgl  
Tel.: +43 5332 72566 303  
E-Mail: steinwender@stadtwerke.woergl.at  
Web: www.stadtwerke.woergl.at

**Streams Telecommunications-services GmbH AS**  
Universitätsstraße 10/7  
1090 Wien  
Tel.: +43 1 40159 128  
E-Mail: office@streams.at  
Web: www.streams.at

**StuOnline Internet Service ACS**  
Neuhofweg 8, 9560 Feldkirchen  
Tel.: +43 4276 5121 0  
E-Mail: info@stuonline.at  
Web: www.stuonline.at

**SysUP OG S**  
Herrgottwiesgasse 149/2  
8055 Graz  
Tel.: +43 59222 0  
E-Mail: office@sysup.at  
Web: www.sysup.at

**Telekurier Online Medien GmbH & CoKG C**  
Leopold-Ungar-Platz 1  
1190 Wien  
Tel.: +43 1 52100 0  
E-Mail: service@kurier.at  
Web: kurier.at

**TeleMax Internet Service CS**  
Sandgasse 26  
6923 Lauterach  
Tel.: +43 5574 79489  
E-Mail: office@telemax.at  
Web: www.telemax.at

**Tele-Tec GmbH AS**  
Gerasdorferstrasse 139/1C  
1210 Wien  
Tel.: +43 1 2566604 0  
E-Mail: office@tele-tec.at  
Web: www.tele-tec.at

**TeleTronic Telekommunikations Service GmbH**  
Am Concorde Park 1/C5  
2320 Schwechat  
Tel.: +43 1 2810000  
E-Mail: office@teletronic.at  
Web: teletronic.at

**Telia Carrier Austria GmbH S**  
c/o CCFa, Am Heumarkt 10  
1030 Wien  
Tel.: +43 1 205305 17  
E-Mail: frank.kirchner@telasonera.com  
Web: www.telasonera.com

**TIWAG-Tiroler Wasserkraft AG, Bereich IT A**  
Eduard-Wallnöfer-Platz 2  
6020 Innsbruck  
Tel.: +43 50607 0  
E-Mail: bit-tk-abwicklung@tiwag.at  
Web: www.tiroler-wasserkraft.at

**TMS IT-Dienst S**  
Hinterstadt 2, 4840 Vöcklabruck  
Tel.: +43 720 501078  
E-Mail: office@tms-itdienst.at  
Web: www.tms-itdienst.at

**Tripple Internet Content Services CS**  
Florianigasse 54/2-5  
1080 Wien  
Tel.: +43 1 406 5927 0  
E-Mail: office@trippel.at  
Web: www.trippel.at

**TTG Tourismus Technologie GmbH S**  
Freistädter Straße 119  
4041 Linz  
Tel.: +43 732 7277 333  
E-Mail: karl.mitteregger@ttg.at  
Web: www.ttg.at

**Türk Telekom International AT GmbH S**  
Ortsstraße 24, 2331 Vösendorf  
Tel.: +43 1 6999408 0  
E-Mail: office@turktelekomint.com  
Web: www.turktelekomint.com

**Unwired Networks GmbH ACS**  
Gonzagagasse 11/2/5/25  
1010 Wien  
Tel.: +43 1 9962051  
E-Mail: office@unwired.at  
Web: www.unwired.at

**upstreamNet Communications GmbH AS**  
Lilienbrunnengasse 7-9/3. OG  
1020 Wien  
Tel.: +43 1 2128644 0  
E-Mail: office@upstreamnet.at  
Web: www.upstreamnet.at

**Ventocom GmbH AS**  
Baumgasse 60B  
1030 Wien  
Tel.: +43 1 9320677  
E-Mail: info@ventocom.at  
Web: www.ventocom.at

**VERBUND Services GmbH ACS**  
Am Hof 6A  
1010 Wien  
Tel.: +43 50 313 50901  
E-Mail: office.dt@verbund.com  
Web: www.verbund.com

**Verein servus.at - Kunst & Kultur im Netz CS**  
Kirchengasse 4  
4040 Linz  
Tel.: +43 732 731300  
E-Mail: office@servus.at  
Web: www.servus.at

**Verizon Austria GmbH AS**  
Handelskai 340  
1023 Wien  
Tel.: +43 1 72714 0  
E-Mail: tech-support@verizonbusiness.com  
Web: www.verizonbusiness.com/at/

**VIPweb.at Th. Dorn ACS**  
Kerpengasse 69, 1210 Wien  
Tel.: +43 1 27145 50  
E-Mail: office@vipweb.at  
Web: www.vipweb.at

**virtual-business**  
Hoelzelgasse 8  
1230 Wien  
Tel.: +43 676 7062299  
E-Mail: office@vibu.at  
Web: www.vibu.at

**web-crossing GmbH CS**  
Eduard-Bodem-Gasse 8  
6020 Innsbruck  
Tel.: +43 512 206567  
E-Mail: info@web-crossing.com  
Web: www.web-crossing.com

**WEB-TECH COACHING CS**  
Märzstraße 7, 1150 Wien  
Tel.: +43 1 4925163  
E-Mail: info@web-tech.at  
Web: www.web-tech.at

**Wien Energie GmbH A**  
Thomas-Klestil-Platz 14  
1030 Wien  
Tel.: +43 1 4004 8100  
E-Mail: stefan.koehler@wienerenergie.at  
Web: www.wienenergie.at

**Wiener Zeitung GmbH C**  
Maria-Jacobi-Gasse 1  
1030 Wien  
Tel.: +43 1 20699 290  
E-Mail: wolfgang.riedler@wienerzeitung.at  
Web: www.wienerzeitung.at

**willhaben internet service GmbH & Co KG**  
Landstraßer Hauptstraße  
97-101 / Bürozentrum 1  
1030 Wien  
E-Mail: info@willhaben.at  
Web: www.willhaben.at

**Wingsoft S**  
Lanzendorfer Straße 45  
2481 Achau  
Tel.: +43 664 1029991  
E-Mail: wilhelm.holzgruber@wingsoft.at  
Web: www.wingsoft.at

**WNT Telecommunication GmbH AS**  
Haydngasse 17  
1060 Wien  
Tel.: +43 1 6163090  
E-Mail: office@wnt-telecom.net  
Web: www.wnt.at

**World4You Internet Services GmbH S**  
Hafenstraße 35  
4020 Linz  
Tel.: +43 732 93035  
E-Mail: office@world4you.com  
Web: www.world4you.com

**WVNET Informations und Kommunikations GmbH AS**  
Edelhof 3  
3910 Zwettl  
Tel.: +43 2822 53633 0  
E-Mail: sales@wvnet.at  
Web: www.wvnet.at

**www.funknetz.at MH GmbH AS**  
Hirschstettner Straße 19-21 L1  
1220 Wien  
Tel.: +43 1 2929699 0  
E-Mail: m.urbanek@funknetz.at  
Web: www.funknetz.at

**XINON GmbH AS**  
Fladnitz im Raabtal 150  
8322 Studenzen  
Tel.: +43 3127 20500  
E-Mail: jantscher@xinon.at  
Web: www.xinon.at

**XQueue GmbH S**  
Christian-Pleß-Straße 11-13  
63069 Offenbach am Main  
Tel.: +49 69 83008980  
E-Mail: info@xqueue.com  
Web: www.xqueue.de

## Internet Summit Austria

12. 09. 2019

Schau mal, wer da spricht!  
Sprachliche Zukunftsszenarien mit künstlicher Intelligenz.

[www.ispa.at/isa2019](http://www.ispa.at/isa2019)

Save the date:

05. 12. 2019

ISPA  
Weihnachtsfeier