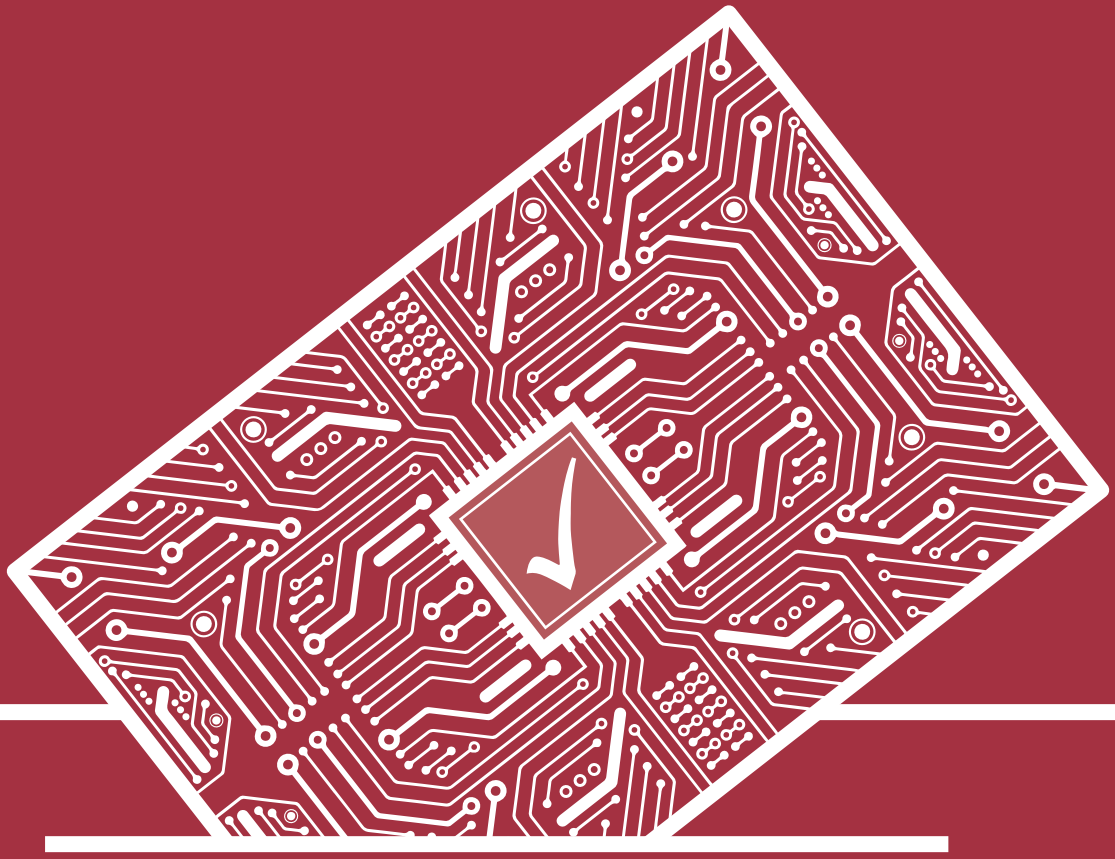
1/2|24

ispa Internet Service Providers Austria

News

wählerisch

Digitalpolitik voranbringen



INHALTS VERZEICHNIS

Impressum: ISPA – Internet Service Providers Austria, 1090 Wien, Währinger Straße 3/18 | ZVR-Zahl: 55 12 23 67 5 | Herausgeber: Stefan Ebenberger | Chefredaktion: Moritz Yvon | Grafik: David Prem | Autor:innen dieser Ausgabe: Stefan Ebenberger, Harald Kapper, Birgit Mühl, Jenana Murtic, Felix Poppeikoff, Moritz Yvon | Blattlinie: Informationsmedium des Vereins Internet Service Providers Austria (ISPA) und dient zur Unterstützung des Ziels der Vereinstätigkeit: »Förderung des Internets in Österreich«. Namentlich gekennzeichnete Beiträge stellen selbstverständlich nicht automatisch die Position der ISPA dar. Die ISPA haftet nicht für Schäden, die aus inkorrekten oder verspäteten Inhalten oder aus Handlungen resultieren, die im Vertrauen auf die Richtigkeit des Inhaltes getätigt wurden. Die in dieser Publikation enthaltenen Informationen stellen keine Rechts- oder Anlageberatung, sondern lediglich eine Information dar.

EDITORIAL

Von
Stefan
Ebenberger

Liebe Leser:innen!

Wir befinden uns mitten in einem globalen Superwahljahr: 3,5 Milliarden Menschen in 70 Ländern werden ihre Parlamente und Staatsoberhäupter wählen. Während mit Indien die größte Demokratie der Welt zu den Urnen schritt, sich in Europa nach den Wahlen zum Europaparlament die Mehrheit verschoben hat, werden die Wahlen in den USA global unter besonderer Beobachtung stehen – und nicht zu vergessen wird Österreich im Herbst ein neuer Nationalrat gewählt. Die ISPA wird die Nationalratswahl aufmerksam begleiten und wir werden uns im Vorfeld sowie während der anschließenden Regierungsbildung aktiv für die Interessen unserer Mitglieder einbringen.
Im Zuge dessen hat die ISPA mit den Mitgliedern ein gemeinsames Forderungspapier für die EU- und Nationalratswahl erstellt, um klarzustellen: „Was braucht das Internet in Österreich und der EU". Dabei haben wir konkrete Lösungsvorschläge erarbeitet, denn Digitalisierung und Telekommunikation sind die Zukunftsthemen, die immer mehr zur Grundlage unserer Volkswirtschaft werden. Dieses Forderungspapier soll unser Beitrag für die anstehenden Wahlen und Regierungsbildungen sein. Von einheitlich gedacht und abgestimmten Maßnahmen und klaren Zuständigkeiten, zum Ergreifen von Chancen und Innovationen sowie der nötigen Infrastruktur samt Fachkräften, über einen fairen Wettbewerb ebenso wie gesellschaftliche Verantwortung und umfassenden Grundrechteschutz.
Die jüngsten Entscheidungen der europäischen Gerichte aber stimmen uns zwiespältig. Das Urteil des EGMR unterstreicht einmal mehr die Bedeutung von Ende-zu-Ende-Verschlüsselung - die auch die ISPA stets betont. Die Entscheidung des EuGH zur Vorratsdatenspeicherung ist hingegen eine deutliche Abkehr von seiner bisher restriktiven Praxis und muss angesichts der riesigen Datenmengen und potentiellen Rückschlüsse von intimsten Details äußerst kritisch gesehen werden – bei allem Verständnis für die Strafverfolgungsbehörden. Es gilt einmal mehr den Grundrechtsschutz deutlich herauszustreichen. Gleichzeitig beschäftigt die nationale Umsetzung der NIS-2-Verordnung aktuell tausende Unternehmen. Das Zeitfenster für eine fristgerechte Umsetzung am 16. Oktober wird unaufhaltbar kleiner und noch immer mangelt es an einem nationalen Gesetz sowie den dazugehörigen Verordnungen zur Umsetzung, und obwohl man den beteiligten Akteur:innen ernsthaftes und qualitatives Bemühen zugutehalten kann: Die Unternehmen müssen schon heute aktiv werden und benötigen dazu endlich Klarheit! Wir versuchen einen Überblick zum Stand und den Risikomanagementmaßnahmen zu geben.
Aber auch Jugendliche benötigen Unterstützung, wächst doch der Druck auf sie durch Schönheitsideale im Internet stetig an, wie die neueste Studie zeigt, die wir im Rahmen des Safer Internet Days als Safer Internet-Initiative Österreich präsentieren durften, und wozu wir mit einer neuen Broschüre dazu Hilfe anbieten. Gleichzeitig erreicht die Meldungszahl zu sexuellen Missbrauchsdarstellungen Minderjähriger und nationalsozialistischer Wiederbetätigung im Internet einen neuen Höchststand, wie die Stopline berichtete – erfreulicherweise aber wurden keine illegalen Inhalte auf österreichischen Seiten gemeldet. Dies zeigt einmal mehr, wie wichtig eine enge Zusammenarbeit von Strafverfolgungsbehörden und Providern ist und unser Grundsatz „Löschen statt sperren" Österreich zu einem unattraktiven Hostingstandort gemacht hat.

Ich freue mich, Ihnen, unseren Leser:innen, mit dieser Ausgabe eine große Themenvielfalt mitzugeben. Besonders aber freuen wir uns auf den regen Austausch mit den Mitgliedern in den Arbeitsgruppen der ISPA, den Stakeholder:innen im engen Diskurs und allen Freund:innen bei den kommenden Veranstaltungen –den Internet Summit Austria 2024 am 12. September bitte gleich vormerken!

Bis dahin wünsche ich Ihnen eine spannende Lektüre!

Ihr

Stefan Ebenberger
ISPA-Generalsekretär

P.S.: Bitte melden Sie sich zum neuen ISPA-Newsletter an!

Photo Ingrid Krammer

ZUKUNFT INTERNET

DIE ISPA HAT IHR POSITIONSPAPIER FÜR DIE DIGITALPOLITIK NACH DER WAHL PRÄSENTIERT.

Nach langer Arbeit in den Arbeitsgruppen der ISPA war es so weit: Das Positionspapier mit den wichtigsten Punkten für eine erfolgreiche Digitalpolitik war abgeschlossen und konnte der Öffentlichkeit präsentiert werden. Denn vom Fachkräftemangel bis zum Infrastruktur-Ausbau, von Künstlicher Intelligenz bis zur diskutierten Messenger-Überwachung: Die digitale Welt berührt heute alle Bereiche unseres Lebens und damit auch die der Politik. Deshalb hat die ISPA vor der Wahl die anstehenden Herausforderungen analysiert und eigene Lösungsvorschläge erarbeitet.

Das Papier umfasst detaillierte Maßnahmen, die eine moderne und zukunftsorientierte Digitalpolitik sicherstellen sollen. Schwerpunkte sind dabei die Förderung von Wettbewerb und Infrastrukturausbau, das richtige Maß und Ziel bei der Regulierung von Content und Services, Schutz und Sicherheit für alle Nutzer:innen des Internets sowie eine langfristig gedachte IKT-Politik, von der weiteren Digitalisierung der Verwaltung bis hin zur umfassenden Förderung digitaler Kompetenzen. Mit diesen Vorschlägen will die ISPA sicherstellen, dass die kommende Regierung fundierte und praxisnahe Ansätze verfolgt, um Österreich als digitalen Vorreiter zu positionieren.

Dabei hat die IKT-Branche durchaus Grund zu Optimismus, denn heute muss niemand in der Politik mehr überzeugt werde, Digitalisierungspolitik ernstzunehmen. Es gab in der vergangenen Legislaturperiode einige Fortschritte, etwa die Förderung des Breitbandausbaus oder die Schaffung der KI-Servicestelle. Allerdings wird die Diskussion manchmal noch etwas unernst geführt, wie ISPA-Generalsekretär Stefan Ebenberger kritisierte: Gerade in Vorwahlzeiten würden immer wieder Scheinlösungen vorgeschlagen, die weder technisch noch gesellschaftlich sinnvoll seien. Aber dafür seien Digitalisierung und Telekommunikation viel zu wichtig, denn sie werden als absolute Zukunftsthemen immer mehr zur Grundlage unserer Volkswirtschaft.

Er führte aus, dass es dabei drei zentrale Prinzipien für eine erfolgreiche Digitalisierungspolitik braucht: Erstens müsse sie einheitlich gedacht und koordiniert werden, mit aufeinander abgestimmten Maßnahmen und klaren Zuständigkeiten in einem eigenen Ministerium. Zweitens sollten immer die Chancen im Mittelpunkt stehen und primär die Grundlagen dafür geschaffen werden, dass diese genutzt werden können. Das reiche von der Investition in Infrastruktur über einen Fachkräfte-Turbo bis hin zu technischen Innovationen und angemessener Regulierung neuer Geschäftsfelder. Und drittens darf Digitalisierungspolitik nicht Einzelziele priorisieren, sondern muss immer die Breite aller legitimen Interessen beachten und diese in Balance halten, sei das der faire Wettbewerb aller Marktteilnehmer oder die Güterabwägung zwischen Sicherheit sowie Grund- und Freiheitsrechten, die online genauso wie offline gelten müssen.

Und dabei geht es nicht nur um die Interessen der Branche selbst. Denn das Internet und die Digitalisierung verändern unser aller Leben in einem nie dagewesenen Tempo, erklärte ISPA-Präsident Harald Kapper. Hier gehe es direkt um die Zukunft und daher immer auch um die Frage, wie wir als Gesellschaft zusammenleben. Das Internet ist nicht nur ein Ort des Austausches und der Diskussion, der als solcher geschützt werden muss, sondern schafft auch enormen Wohlstand und wird noch mehr als bisher die Grundlage der Wirtschaft der Zukunft sein.

Kapper wandte sich dabei direkt an die Politik: Möglichkeiten schaffen, das müsse das Leitbild der Politik sein. Damit unsere Wirtschaft auch in Zukunft wachsen kann und Österreich als zentraler europäischer Wirtschaftsstandort nicht ins Hintertreffen gerate, brauche es klare, positive Rahmenbedingungen. Er sieht hier die ISPA in der Rolle des Wissens-Hubs: Das Positionspapier solle den Verantwortlichen der kommenden Legislaturperiode Klarheit auf Basis der Expertise aus der Praxis der ISPA-Mitglieder in einem sehr technischen Thema zu bieten. ■

Sie wollen mehr wissen?
Hier geht‘s zum Download!

TOP-10-FORDERUNGEN DER INTERNETWIRTSCHAFT ÖSTERREICHS

01 **Fairer Wettbewerb** am Breitbandmarkt, keine Ausnutzung marktbeherrschender Positionen

02 ein Ministerium für Telekom- und Digitalagenden mit **klaren Zuständigkeiten**

03 **angemessene Normierung** von Gesetzesvorhaben - konkret, fundiert für das Notwendige

04 **Prüfung von Gesetzesinitiativen** auf Machbarkeit und Einhaltung der Grundrechtestandards

05 **Infrastrukturförderung** wo notwendig, jedenfalls mit Zugang für Dritte zum gebauten Netz

06 bestehende **Sicherheitsstandards** für neue Rechtsakte beachten

07 Kleinunternehmen **nicht überregulieren** und bei notwendigen Maßnahmen unterstützen

08 **uneingeschränkte Wahrung der Grundrechte** inklusive sicherer Verschlüsselungsstandards

09 **positive Rahmenbedingungen** für KI: Gefahrenminimierung und Innovation fördern

10 **200.000 zusätzliche IKT-Spezialist:innen** für Österreichs Digitale Dekade bis 2030

GROSSE ISPA-WAHLBEFRAGUNG

DIE PARTEIEN UND DIE DIGITALISIERUNGSPOLITIK

Bei der bevorstehenden Nationalratswahl wird auch eines der zentralen Themen unserer Zeit verhandelt: die Digitalpolitik. In einer Ära, in der das Internet und die digitale Transformation alle Bereiche des Lebens durchdringen, wird die Gestaltung der digitalen Gegenwart und Zukunft zu einer der drängendsten Aufgaben der politischen Akteure. Die ISPA hat daher die im Nationalrat vertretenen Parteien zu einigen der wichtigsten Fragen der Branche befragt, um unseren Leser:innen einen besseren Einblick in deren Pläne und Prioritäten zu geben.

Der Ausbau der digitalen Infrastruktur ist dabei natürlich ein wesentliches Thema. Ein flächendeckender Zugang zu schnellem Internet ist nicht nur essenziell für die Wettbewerbsfähigkeit Österreichs, sondern auch für die Sicherstellung gleichberechtigter Teilhabe aller Bürger:innen an der digitalen Welt. Ein weiterer zentraler Aspekt ist der faire Wettbewerb und die Regulierung im digitalen Raum. Die Frage, wie ein Gleichgewicht zwischen großen und kleineren Unternehmen geschaffen werden kann, ist von großer Bedeutung. Hier geht es um Themen wie Marktregulierung und die Förderung von Innovationen.

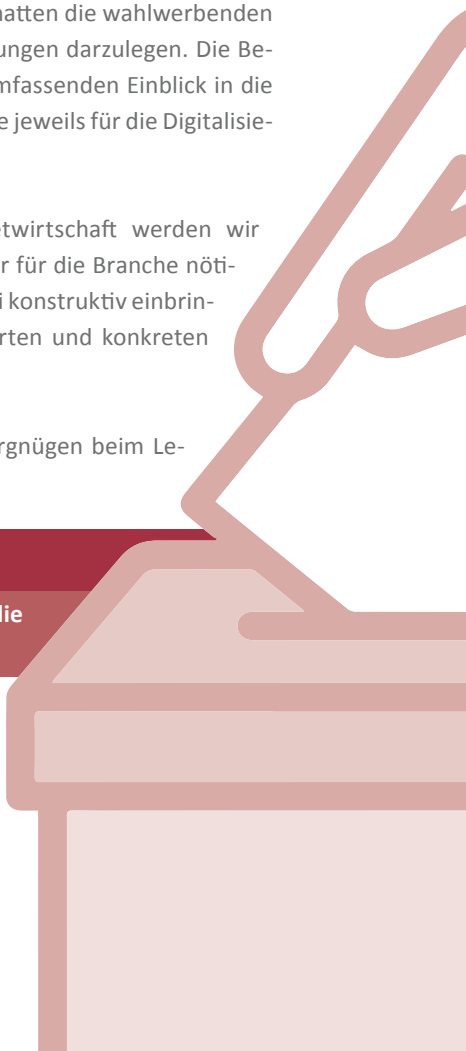
Ebenso wichtig ist für die IKT-Branche die Ausbildung von Fachkräften. Österreich braucht allein 200.000 weitere bis 2030, um die Ziele der digitalen Dekade der EU-Kommission erfüllen zu können.

Aber nicht nur wirtschaftliche Fragen sind für die ISPA immer ein zentrales Anliegen gewesen, sondern auch der Schutz der Grundrechte im Internet, insbesondere vor Überwachung, wie sie derzeit für Messengerdienste diskutiert wird. Und auch die Verteidigung liberaler Demokratien gegen Desinformation im digitalen Raum stellt eine besondere Herausforderung dar. Denn die Verbreitung von falschen Informationen und Fake News kann das Vertrauen in demokratische Prozesse untergraben und die gesellschaftliche Stabilität gefährden.

Zu diesen und vielen weiteren Fragen hatten die wahlwerbenden Parteien die Möglichkeit, ihre Vorstellungen darzulegen. Die Befragung der ISPA bietet somit einen umfassenden Einblick in die Digitalpolitik und zeigt, welche Wege sie jeweils für die Digitalisierung in Österreich einschlagen wollen.

Als Interessenvertretung der Internetwirtschaft werden wir auch nach der Wahl die Umsetzung der für die Branche nötigen Maßnahmen einmahnen, uns dabei konstruktiv einbringen und die Parteien an ihren Antworten und konkreten Taten messen.

Nun wünschen wir Ihnen aber viel Vergnügen beim Lesen!



FRAGE 1:

Was sind Ihre 3 Top-Prioritäten für die Digitalisierung in Österreich?

Die Volkspartei

- Steigerung der digitalen Kompetenzen über die gesamte Bevölkerung

- Österreich als Innovationstreiber in der Digitalisierung weiter stärken (Österreich als KI-Hotspot, eGovernment made in Austria als Benchmark in Europa und International und Unternehmen bei der Digitalen Transformation unterstützen)
- Flächendeckende Gigabit-Verfügbarkeit für die Chancengleichheit zwischen Stadt und Land

SPÖ

- Digitaler Humanismus: Der Mensch steht im Mittelpunkt. Technologie ist für die Menschen da und nicht umgekehrt.
- Die Demokratie stärken durch strengere Regulierung von Plattformen und Social Media.
- Künstliche Intelligenz für die Gesellschaft nutzbar machen und die demokratische Kontrolle künstlicher Intelligenz sicherstellen.

Außerdem ist der SPÖ die Stärkung Digitaler Souveränität wichtig, um die Eigenständigkeit und Unabhängigkeit Europas zu sichern, sowie die Stärkung von Digital- und Medienkompetenz als Rüstzeug für das Digitalzeitalter.

Dazu haben wir auch in den 24 Ideen des „Herz und Hirn"-Plans die Forderungen der SPÖ formuliert: www.mit-herz-und-hirn.at

FPÖ

Die Digitalisierung ist ein zentraler Treiber für die wirtschaftliche Entwicklung und Wettbewerbsfähigkeit Österreichs.
Unsere drei Top-Prioritäten für die Digitalisierung sind:

- Bildung, Ausbildung und Weiterbildung
- Unterstützung der KMUs und Gemeinden
- Inklusive Digitalisierung und auch analoge Weg ermöglichen

DIE GRÜNEN

Wir brauchen ein flächendeckendes, schnelles und zuverlässiges Internet. Daher müssen wir den Breitband-Ausbaut fortsetzen bis ganz Österreich versorgt ist. Um für die Entwicklungen der Zukunft gut gerüstet zu sein, müssen wir die Digitalisierung, freie Software und Künstliche Intelligenz deutlich stärker fördern. Außerdem braucht es mehr heimisches Risikokapital von Investoren u.a. für die Grundlagenforschung und für Start-Ups im Bereich Digitalisierung und KI. Ein Schwerpunkt auf Open Source macht uns unabhängig von ausländischen BigTech-Konzernen. Besonders wichtig ist uns Grünen der Schutz von Grundrechten. Daher bekämpfen wir jegliche Massen-Überwachungspläne und treten für eine freie Gesellschaft, Datenschutz, Konsument:innenschutz und die Bekämpfung von Hass-Algorithmen ein.

NEOS

Unsere Prioritäten für die Digitalisierung in Österreich sind der Ausbau der digitalen Infrastruktur, die Förderung digitaler Kompetenzen und eine Verwaltung, die Digitalisierung für weniger Bürokratie nutzt. Erstens ist ein flächendeckender Glasfaserausbau unerlässlich, um keine Regionen im Land abzuhängen. Zweitens müssen digitale Kompetenzen in Schulen und Weiterbildungseinrichtungen gezielt gefördert werden, um die Bevölkerung auf die Herausforderungen der digitalen Zukunft vorzubereiten. Drittens ist es entscheidend, dass Digitalisierung für Entbürokratisierung genutzt wird, indem wir das bestehende Datenchaos ordnen und das Potenzial für Künstliche Intelligenz nutzen. Dabei sollte besonders auf Cybersicherheit und umfassende Bewusstseinsbildung geachtet werden.

FRAGE 2:

Welche Maßnahmen wollen Sie zu einer Förderung des festen und mobilen Breitbandausbaus ergreifen? Wie sehen Sie das Verhältnis von privatem und geförderten Ausbau?

Die Volkspartei

Gigabitfähiges Breitband ist aktuell für 70 Prozent der Haushalte verfügbar. Zudem besteht bei 95 Prozent der Haushalte eine Outdoor-Verfügbarkeit von 5G-Mobilfunk. Im Zuge der Initiative Breitband Austria 2020 stellt der Bund seit Mitte 2015 österreichweit eine Milliarde Euro an Förderungsmitteln – die sogenannte Breitbandmilliarde – für den Ausbau der Breitbandinfrastruktur zur Verfügung. Mit rund 1,4 Milliarden Euro – der zweiten Breitbandmilliarde – hat die Bundesregierung das bis dato größte

Förderungsbudget für den Breitbandausbau zur Verfügung gestellt. Insgesamt profitieren von den Breitbandinitiativen über 567.000 Haushalte – mehr als 14 Prozent aller Haushalte Österreichs. Der geförderte Breitbandausbau findet damit in 1.600 der rund 2.100 österreichischen Gemeinden statt.

In der im August 2019 veröffentlichten Breitbandstrategie 2030 werden die Rahmenbedingungen für den österreichischen Weg in die Gigabit-Gesellschaft formuliert, auf deren Grundlage die zur Zielerreichung notwendigen privaten und öffentlichen Investitionen ermöglicht und koordiniert werden sollen. In einem seit über 25 Jahren liberalisierten Markt ist klar, dass die Investitionen in erster Linie durch den öffentlichen Sektor erfolgen müssen. Vor diesem Hintergrund bekennt sich die Bundesregierung zur integrierten Planung von fixem und mobilem Ausbau der Kommunikationsinfrastruktur hin zu gigabitfähigen Netzen unter Einsatz von öffentlichen Mitteln in den von Marktversagen betroffenen Gebieten.

SPÖ

Außerhalb der gewinnbringenden städtischen Regionen (Ballungszentren) wird es weiterhin notwendig sein, den Ausbau der Infrastruktur mit staatlichen Mitteln zu fördern. Diesbezüglich müssen die Fördersummen den Ausbauzielen angepasst werden.

FPÖ

Eine zukunftsfähige digitale Infrastruktur ist essenziell für die Wettbewerbsfähigkeit und Innovationskraft der österreichischen Wirtschaft. Dabei spielen sowohl der feste als auch der mobile Breitbandausbau eine entscheidende Rolle. Wir setzen auf private Investitionen als Haupttreiber des Breitbandausbaus. Der Wettbewerb unter privaten Anbietern fördert Innovation und Effizienz. Durch attraktive Rahmenbedingungen und regulatorische Sicherheit schaffen wir Anreize für Unternehmen, in den Breitbandausbau zu investieren. Kooperationen zwischen privaten Unternehmen und öffentlichen Stellen können zusätzlich Synergien schaffen und den Ausbau beschleunigen. Anstatt flächendeckende Subventionen für den Breitbandausbau bereitzustellen, konzentrieren wir öffentliche Fördermittel auf spezifische Bereiche wie Bildung, Ausbildung und Weiterbildung sowie die Unterstützung von KMUs und Gemeinden. Dies stärkt die digitale Kompetenz und die Wettbewerbsfähigkeit unserer Wirtschaft. Öffentliche Mittel sollen gezielt dort eingesetzt werden, wo der private Ausbau aufgrund wirtschaftlicher Unrentabilität stockt, insbesondere in ländlichen und abgelegenen Regionen.

DIE GRÜNEN

Breitbandnetze sind das Rückgrat für eine erfolgreiche Digitalisierung. Unter Grüner Regierungsbeteiligung wurde hier bereits in den vergangenen Jahren eine massive Förder-Initiative gestartet. Eines ist klar: Diese Förderung ist fortzusetzen, und zwar bis es in Österreich keinen Fleck mehr ohne Breitband-Internet gibt – auch im ländlichen Bereich. Dabei brauchen wir – regional angepasst – einen guten Mix aus mobilem und stationärem Breitbandnetz. Wir befürworten einen marktorientierten Netzausbau. Öffentliche Mittel sollen nur dort eingesetzt werden, wo sie unbedingt erforderlich sind – also insbesondere in Bereichen, in denen kaum Chancen bestehen, von privaten Investitionen abgedeckt zu werden.

NEOS

Es braucht beides. Zur Förderung des Breitbandausbaus setzen wir auf eine Kombination aus gezielten staatlichen Fördermaßnahmen und der Mobilisierung privater Investitionen. Öffentliche Förderungen sollten vor allem dort ansetzen, wo der Markt allein nicht aktiv werden kann, um auch ländliche und strukturschwache Regionen zu erschließen.

Der Fokus sollte unbedingt auf dem Glasfaserausbau liegen, da Österreich im EU-Vergleich eine sehr niedrige Take-up Rate hat. Hier sieht man auch leider, dass die bisherigen Förderungen nicht optimal ausgestaltet waren. Es nutzt wenig, wenn die Glasfaseranschlüsse nur bis zur Grundstücksgrenze gehen. Deshalb sollten alte Fördermodelle überdacht und optimiert werden.

FRAGE 3:

Welche Rolle soll die Regulierung spielen und wie soll der Wettbewerb zwischen kleinen und großen Unternehmen am Breitbandmarkt gestaltet werden?

Die Volkspartei

Der rechtliche Rahmen für die Regulierung im Bereich der Telekommunikation hat sich über Jahrzehnte hinweg entwickelt. Dieser Rahmen gibt der Regulierungsbehörde klare Vorgaben mit dem Ziel durch Förderung des Wettbewerbs im Bereich der elektronischen Kommunikation die Versorgung der Bevölkerung und der Wirtschaft mit zuverlässigen, preiswerten, hochwertigen und innovativen Kommunikationsdienstleistungen zu gewährleisten. Um dieses Ziel zu erreichen analysiert die Regulierungsbehörde die verschiedenen Märkte im Hinblick auf deren wettbewerbliche Entwicklungen und hat die Möglichkeit bei Vorliegen von Marktversagen die ihr rechtlich zukommenden Instrumente zur Beseitigung der Probleme zu nutzen.

SPÖ

Die Regulierung soll den Zugang aller Teilnehmer*innen auf Breitbandinfrastrukturen gewährleisten, diesbezüglich sind dort Maßnahmen zu treffen, wo zu hohe Nutzungsgebühren dies verhindern. Speziell im geförderten Bereich haben entsprechende Auflagen den Zugang zu gewährleisten.

FPÖ

Die Regulierung im Breitbandmarkt sollte auf das notwendige Mindestmaß beschränkt sein, um Innovation und Wettbewerb zu fördern. Dabei sind folgende ua. folgende Aspekte entscheidend:
Die Regulierung sollte möglichst zentralisiert und von einer einzigen, spezialisierten Stelle übernommen werden. Dies schafft klare Verantwortlichkeiten und vereinfacht die Prozesse für alle Beteiligten. Der Fokus sollte auf Beratung und Unterstützung der Unternehmen liegen, um Compliance zu gewährleisten und gleichzeitig Innovationshemmnisse zu vermeiden.

DIE GRÜNEN

Regulierung ist dann nötig, wenn ein offensichtliches Marktversagen beim Breitband-Ausbau vorliegt. Regulierung ist weiter dann notwendig, wenn es darum geht, den Wettbewerb abzusichern. Wir halten es für wichtig, kleine lokale Anbieter neben den wenigen großen Playern zu erhalten. Keinesfalls sollte es zu einer Re-Monopolisierung kommen. Wesentlich ist Rechts- und Planungssicherheit für alle Marktteilnehmer - große wie kleine.

NEOS

Regulierung spielt eine entscheidende Rolle, um fairen und nachhaltigen Wettbewerb zwischen kleinen und großen Unternehmen sicherzustellen. Spätestens die notwendige Umsetzung der neuen Gigabit-Infrastrukturverordnung bietet eine Gelegenheit für die nächste Bundesregierung, den Wettbewerb im Breitbandmarkt genau zu untersuchen. Regulierungen müssen so gestaltet sein, dass echter Wettbewerb auf Serviceebene gewährleistet wird. Daher ist ein Regulator notwendig, der über die notwendigen Instrumente verfügt und entsprechende Maßnahmen auch durchsetzen kann. NEOS setzen sich dafür ein, dass der Zugang und Ausbau der Telekommunikations-Infrastruktur optimiert wird. Ziel ist es, einen fairen, produktiven und nachhaltigen Wettbewerb in Österreichs Telekommunikationsmarkt zu schaffen.

FRAGE 4:

Bei Online-Inhalten, die das Urheberrecht verletzen, können schon jetzt Netzsperren verhängt werden. Dabei gibt es aber immer die Gefahr, auch legale Inhalte zu blockieren. Bei der Sperre von Fake-Shops im Sinne des Konsumentenschutzes gibt es deshalb eine behördliche Vorab-Prüfung der Sperre. Fänden Sie die auch bei anderen illegalen Inhalten sinnvoll?

Die Volkspartei

Im Bereich des Telekommunikationsrechts hat bei allfälligen Netzsperren die Regulierungsbehörde zu prüfen, ob damit nicht gegen das Prinzip der Netzneutralität, resultierend aus unionsrechtlichen Vorgaben, verstoßen wird. Die Vorab-Prüfung der Sperre klingt grundsätzlich gut, ist aber immer auch vor dem technisch komplexen Hintergrund zu sehen. Dabei ist beispielsweise die

Löschung von Einträgen der betroffenen Seite aus den DNS-Servern anders zu bewerten als die direkte Sperre einer IP Adresse oder eine URL Sperre. Abgesehen von der Gefahr des Blockierens legaler Inhalte ist insgesamt auch das vielfältige Umgehungspotential zu beachten. Wichtig ist dabei, dass es für die Unternehmen, die die Sperre umsetzen müssen, hinreichend klar und rechtssicher ist.

SPÖ

Die Gefahr von Overblocking ist real. Allerdings gibt es aktuell keine Möglichkeit, Plattformen als private Unternehmen dazu zu verpflichten, dass bestimmte (legale) Inhalte (Texte, Bilder, Videos etc.) aufscheinen. Im Unterschied zu Fake-Shops scheint eine behördliche Vorab-Prüfung bei Sperre oder Löschen zumindest von einzelnen geschützten Inhalten, die darüber hinaus auch oftmals automatisch erfolgen, aufgrund der großen Menge schwierig. Grundsätzlich wäre es jedoch begrüßenswert, die Entscheidung, ob etwas im Internet aufscheint oder nicht, nicht allein den Plattformen oder Providern zu überlassen.

FPÖ

Eine Vorab-Zensur lehne wir ab. Urheberrechtsverletzungen sind bereits gesetzlich ausreichend geregelt.

DIE GRÜNEN

Generell stehen wir Netzsperren sehr zurückhaltend gegenüber und halten eine gerichtliche/behördliche Anordnung für notwendig. Aus unserer Sicht kann es nicht Sache von Unternehmen sein, hier gerichtlichen Entscheidungen vorzugreifen. Problematisch an Netzsperren ist deren Auswirkung auf das Grundrecht auf freie Meinungsäußerung und die Tatsache, dass sie oft auch legale Inhalte mitbetreffen. Schließlich kann die Sperre einer IP-Adresse auch in der Regel nicht zu einer nachhaltigen Beseitigung eines rechtswidrigen Angebots führen. Netzsperren können daher immer nur eine „measure of last resort“ sein z.B. in Hochrisiko-Fällen, etwa bei Darstellungen von Kindesmissbrauch.

NEOS

Eine behördliche Vorab-Prüfung könnte helfen, ungerechtfertigte Netzsperren zu vermeiden, darf aber nicht in zu großer Bürokratie ausarten. Dennoch sollten Netzsperren generell kritisch betrachtet werden, da sie die Freiheit der Bürger:innen einschränken können. Auf der anderen Seite braucht es natürlich effektive Prozesse, damit Urheber:innen sich gegen die missbräuchliche Verwendung ihrer Inhalte wehren können. Es braucht also einen guten Ausgleich zwischen effektiven Maßnahmen, um bei eindeutigen Verletzungen schnell reagieren zu können, und überbordenden Netzsperren.

FRAGE 5:

Wie können österreichische IT-Unternehmen zu Weltmarktführern werden? Welche Maßnahmen planen Sie, damit wir in Europa hier nicht den Anschluss an die USA und China verlieren?

Die Volkspartei

Durch den AI Act, der sowohl den Schutz der Grundrechte als auch die Förderung von Innovationen berücksichtigt, kann ein Umfeld geschaffen werden, das verantwortungsvolle Fortschritte in der KI fördert und gleichzeitig die Werte einer demokratischen Gesellschaft aufrechterhält. Es ist entscheidend, dass sich Europa aktiv an der Gestaltung der globalen KI-Landschaft bzw. generell innerhalb der Digitalisierungslandschaft beteiligt und auch Standards festlegt – und das in allen Bereichen. Mit klaren, von uns entwickelten Regeln und deren wirkungsvollen Durchsetzung haben wir den Hebel unseres gemeinsamen Marktes in der Hand. Sowohl China als auch die USA können den europäischen Gemeinschaftsmarkt nicht ignorieren.

SPÖ

Der zentrale Schlüssel für innovative IT-Unternehmen sind gut ausgebildete Fachkräfte. Digitale Kompetenzen müssen sehr früh, strukturiert erworben werden. Schon in der Volksschule muss das beginnen und in einen gezielten Ausbau der MINT-Absolvent*innen münden. Oft werden innovative und erfolgreiche Start-ups im IKT-Bereich von größerem internationale IT-Giganten aufgekauft. Das lässt sich nur vermeiden, wenn es uns gelingt maßgeschneiderte Finanzierungsmöglichkeiten in der Wachstums Phase anzubieten. Da hat Österreich noch Aufholbedarf.

FPÖ

Um österreichische IT-Unternehmen zu Weltmarktführern zu machen, sind gezielte Maßnahmen in den Bereichen Bildung, Innovation und internationale Zusammenarbeit erforderlich.

DIE GRÜNEN

Wir müssen weg vom nationalstaatlichen Denken, hin zu einem europäischen Denken. Dafür müssen wir uns auf europäischer Ebene gut vernetzen, um Synergien und Stärken nutzen zu können. Durch die Förderung europäischer und österreichischer Unternehmen, durch kartellrechtliche Maßnahmen aber auch durch ein klares Bekenntnis zu quelloffener Software (Open Source), zu offenen Schnittstellen und einer Vergemeinschaftung von digitalen Ressourcen (Open Data) können wir außereuropäischen BigTech Konzernen entgegen treten. Unser Ziel muss eine digitale Souveränität in Europa sein. Dabei ist auch wesentlich, wettbewerbsverzerrende Aktivitäten von Konzernen mit erheblicher Marktmacht gezielt und offensiv zu bekämpfen. Nur in einem fairen Wettbewerbsumfeld können österreichische Unternehmen reüssieren.

NEOS

Wir müssen sowohl auf europäischer als auch nationaler Ebene unsere Hausaufgaben machen und unsere Wettbewerbsfähigkeit stärken. Auf europäischer Ebene muss sich die künftige Bundesregierung für eine Vertiefung des Binnenmarkts und die Kapitalmarktunion einsetzen, um mehr Kapital für Innovationen zu mobilisieren und günstige Energie sicherzustellen. National bedarf es einer deutlichen Senkung der hohen Abgabenlast auf Arbeit und erleichterter qualifizierter Zuwanderung. Zudem plädieren NEOS seit Jahren für eine Zukunftsquote von 25% des Budgets, um die Investitionen in Forschung und Entwicklung zu erhöhen.

Trotz hoher Forschungsquoten stagniert Österreich in den Rankings. Eine Erhöhung der Grundlagenforschung ist überfällig, um die Innovationskraft zu stärken und IT-Unternehmen den notwendigen Schub zu geben.

FRAGE 6:

Österreichs IKT-Wirtschaft leidet unter einem Mangel von Fachkräften, vom Breitbandausbau bis hin zur Cybersicherheit. Welche Maßnahmen wollen Sie für die Ausbildung von IKT-Fachkräften in Österreich, aber auch für deren Gewinnung im Ausland setzen?

Die Volkspartei

Wir sind uns des Fachkräftemangels in der österreichischen IKT-Wirtschaft bewusst und setzt auf eine Kombination aus inländischer Ausbildung und internationaler Anwerbung. Wir fördern die IKTBildung bereits in den Schulen und erweitern die Studiengänge an Universitäten und Fachhochschulen. Für Quereinsteiger bieten wir verstärkte Weiterbildungsmöglichkeiten. Zudem verbessern wir die Arbeitsbedingungen und investieren in Forschung und Innovation, um Österreich als attraktiven Arbeits- und Lebensstandort zu positionieren. Durch internationale Rekrutierungskampagnen und die Vereinfachung der Einwanderungsprozesse möchten wir qualifizierte Fachkräfte aus dem Ausland anziehen und integrieren. So wollen wir sicherstellen, dass die IKT-Wirtschaft in Österreich nachhaltig gestärkt wird.

SPÖ

Wir müssen dieses Problem schon sehr früh – nämlich in der schulischen Ausbildung – lösen. Künftige Fachkräfte fallen nicht vom Himmel. Sie sind ein Ergebnis von Bildungs- und Arbeitsmarktpolitik. Österreich hat mit der dualen Ausbildung gute Erfahrungen gemacht. Die Lehre hat dazu beigetragen, dass wir in einzelnen Branchen Spitzenfachkräfte haben, die am Weltmarkt sehr gefragt sind. Wir müssen diese Erfahrungen – wenn auch nicht 1:1 – auch für den IKT-Bereich nutzen. Eine Aufwertung des MINT-Bereichs bis hin zu mehr Abschlüssen wird nötig sein. Österreich ist ein Land mit hoher Standortqualität und bei vielen Fachkräfte aus dem Ausland sehr beliebt.

Es wird aber wichtig sein, Cluster zu schaffen, um Menschen aus dem Ausland langfristige Perspektiven zu bieten.

FPÖ

Förderung der MINT-Fähigkeiten (Mathematik, Informatik, Naturwissenschaften und Technik) bereits in der Schule. Es gilt, die „Angst“ vor Mathematik zu nehmen und Lehrer so auszubilden, dass sie über entsprechendes Fachwissen verfügen und die Schüler begeistern können. Mehr Engagement der Wirtschaft und tertiärer Bildungseinrichtungen in der schulischen Ausbildung fördern, einschließlich sinnvoller „IT-Unterricht“ und praxisorientierter Projekte

Die Grünen

Wir Grüne haben während unserer Regierungsbeteiligung bereits erste wichtige Impulse gesetzt, insbesondere mit dem neuen Schulfach digitale Grundbildung. Neben dem Ausbau fachspezifischer Ausbildungen, insbesondere auch den Lehrlingsausbildungen im IT-Bereich, sind IKT-Themen verstärkt in allen Schulformen einzubinden. Dazu ist auch eine entsprechende Fortbildung aller Lehrpersonen und natürlich eine moderne IT-Ausstattung an Schulen erforderlich. Es ist absehbar, dass wir den Fachkräfte-Bedarf nicht allein durch österreichischen Nachwuchs abdecken werden können. Wir müssen somit auch IKT-Fachkräfte aus dem Ausland gewinnen. Deshalb braucht es auch eine vernünftige Migrationspolitik. Denn Populismus, Hass und Ausgrenzung werden uns im Wettbewerb um diese Fachkräfte weiter zurückwerfen.

NEOS

Zur Ausbildung von IKT-Fachkräften in Österreich setzen wir auf den Erwerb digitaler Kompetenzen in alle Bildungsstufen, von der Grundschule bis zur Universität. Weiterbildungen und Umschulungsprogramme sollen gezielt gefördert werden, um den Fachkräftemangel zu bekämpfen. Für die Gewinnung internationaler Talente müssen Einwanderungsverfahren vereinfacht und beschleunigt werden.

Eine deutliche Senkung der rekordhohen Steuern auf Arbeit und attraktive Arbeitsbedingungen sind ebenfalls nötig. Leider wurde die neue Mitarbeiterbeteiligung schlecht umgesetzt, da sie jetzt bereits schlechter ist als in anderen europäischen Staaten. Es braucht ein wettbewerbsfähiges, attraktives Angebot für internationale Spitzenkräfte.

FRAGE 7:

Wie sollten westliche Demokratien den gegen sie gerichteten Desinformationskampagnen begegnen, insbesondere vor Wahlen?

Die Volkspartei

Der Schlüssel für einen aufgeklärten Umgang mit neuen Technologien, Sozialen Medien und Informationsplattformen liegt in der Verfügbarkeit entsprechender digitaler Kompetenzen in der Bevölkerung, wenn es beispielsweise um das Erkennen von Falschinformationen im Netz geht. Hier setzt die Digitale Kompetenzoffensive, kurz DKO an, mit dem Ziel, den Menschen zu vermitteln, dass die Digitalisierung keine Zauberei ist, sondern letztendlich auf Mathematik basiert und dazu dient, ihnen das Leben zu erleichtern. Als „Sofortmaßnahme“ wurde im Rahmen der DKO das Workshop-Programm „Digital Überall“ gestartet. Insgesamt werden österreichweit 4.500 Workshops angeboten, bei denen niederschwellig digitale Basis-Skills u.a. in den Bereichen Digitalisierung, Sicherheit und Fake News vermittelt werden.

SPÖ

In Österreich wurde bereits bei der EU-Wahl im BKA eine Stabsstelle eingerichtet, die eventuelle Desinformation im Zusammenhang mit der bevorstehenden Wahl gezielt bekämpfen und richtigstellen soll. Sollte dies auf Dauer etabliert werden, wäre eine gewisse Unabhängigkeit dieser Einrichtung zu wünschen, auch Expert*innen sollten beigegeben werden. Über mögliche weitere Desinformationen durch gefakte Umfragen würde ein Verbot der Veröffentlichung von Umfragen in einem gewissen Zeitraum vor der Wahl nützlich sein, dass dies natürlich über die neuen Medien umgangen werden kann, müsste bereits im rechtlichen Design berücksichtigt werden. Ganz generell sollten sich sowohl die Politik aber auch die Medien auch darüber klar werden, wie sie auch außerhalb von Wahlzeiten die Bürger*innen vor Desinformationen schützt. Desinformationen hören nicht auf, wenn eine Wahl geschlagen ist.

FPÖ

Nicht durch Zensur! Desinformationskampagnen sind kein neues Phänomen, sondern existieren schon seit jeher. Wichtig ist es, anstatt ständig die Digitalisierung zu verteufeln, ihre Chancen zu nutzen. Dank der Digitalisierung gibt es keine Meinungsmonopole mehr.

Die Grünen

Wir Grüne stehen für ein breites Bündel an Maßnahmen, um gegen demokratiefeindliche Meinungsmanipulation und Fake-Informationen vorzugehen: Die EU-Kommission muss die Möglichkeiten, die der Digital Services Act ihr gegenüber Plattformen wie TikTok, Meta, Youtube, X, etc. einräumt, ausschöpfen und manipulative Algorithmen bekämpfen. Die europäischen Regulierungen, auch der AI Act, müssen voll genutzt, evaluiert und falls nötig nachgeschärft werden.

Gleichzeitig müssen wir Medien, die ihrer Verantwortung zur journalistischen Sorgfalt nachkommen, mit einer gezielten, nachvollziehbaren Förderung stärken. Wichtige Schritte haben wir hier bereits gesetzt. Mit einer breit angelegten Bildungs-Offensive müssen wir unsere Bevölkerung gegen Beeinflussung durch Fake-Informationen „immunisieren“.

NEOS

Demokratien müssen wehrhaft sein und bleiben - besonders gegen gezielte Desinformationskampagnen und Wahlbeeinflussung. Die EU hat hier nun deutlich schärfere Instrumente in die Hand bekommen. Ein wichtiger nationaler Schritt ist eine eigene Abteilung gegen Desinformation, wie es sie auch in Schweden gibt. Diese ist staatlich und wurde speziell gegründet, um Fake-News-Aktionen entgegenzutreten. In dieser Stelle sollen sich unabhängige Expert:innen des Themas Desinformation annehmen. Dazu gehört u. a.: gezielte Strategien entwickeln, Akteur:innen, NGOs und politische Entscheidungsträger:innen miteinander zu vernetzen, Medienkompetenzvermittlung zu koordinieren. Wichtig ist dabei, dass diese Abteilung mit einer gesicherten Finanzierung unabhängig arbeiten kann.

FRAGE 8:

Wie stehen Sie zur diskutierten Überwachung von Messengerdiensten und wo sehen Sie die Balance mit dem Schutz der Grundrechte, den sowohl die Judikatur des VfGH als auch das europäische Recht verlangen?

Die Volkspartei

Bereits jetzt darf die Polizei nach richterlicher Anordnung Telefone und SMS überwachen. Schwerkriminelle nutzen selbstverständlich auch das Internet und Messengerdienste. Die österreichische Polizei und der Verfassungsschutz darf derzeit weder Metadaten (wer mit wem wann wie lange Kontakt hatte) noch Inhaltsdaten auswerten.

Österreich ist das einzige Land in Mitteleuropa, in dem die Polizei diese Befugnisse nicht hat. Zur Verhinderung schwerer Straftaten sind diese erweiterten Befugnisse – nach richterlicher Genehmigung – aber für moderne Polizeiarbeit unabdingbar. Es geht nicht um Massenüberwachung, sondern darum, terroristische Attacken zu verhindern und schwere Straftaten im Bereich der organisierten Kriminalität leichter aufklären zu können.

SPÖ

Die SPÖ ist gegen die anlasslose Überwachung von Messengerdiensten und sieht hier das Grundrecht auf Achtung des Privat- und Familienlebens gefährdet. Dazu gibt es auch einen von der SPÖ mitinitiierten Beschluss im EU-Unterausschuss des Nationalrates, der für die Bundesregierung bindend ist: EU-Unterausschuss äußert Grundrechtsbedenken zu Kommissionsvorschlag (PK1226/03.11.2022) | Parlament Österreich

FPÖ

Die FPÖ ist gegen flächendeckende Überwachung von Messengerdiensten.

Die Grünen

Wir Grünen lehnen eine anlasslose Überwachung von Messengerdiensten ab. Sowohl der VfGH als auch der EGMR haben hier ganz klar Stellung bezogen: So eine Massen-Überwachung ist weder mit den Grundrechten vereinbar, noch in einer freien, demokratischen Gesellschaft erforderlich. Unser zentrales Anliegen ist es, die vielfältigen Bestrebungen zur Massenüberwachung zu verhindern – egal ob Bundestrojaner, Chat-Kontrolle oder Echtzeit-Videoüberwachung im öffentlichen Raum. Gerade im KI Act wird Mitgliedstaaten ein Spielraum bei der Umsetzung von sogenannter „biometrischer Echtzeit-Fernidentifizierung“ (also öffentliche Massen-Video-Überwachung) eingeräumt. Wir Grüne treten klar für ein Verbot so einer Massenüberwachung ein.

NEOS

Für uns NEOS hat der Schutz der Persönlichkeitsrechte oberste Priorität und wir setzen uns entschieden gegen überbordende Überwachungsmaßnahmen ein. Solche Maßnahmen stellen einen massiven Eingriff in die Privatsphäre der Bürger:innen dar und sind mit den Grundsätzen einer liberalen Demokratie unvereinbar. In Bezug auf die Überwachung von Messenger-Diensten sind sich Expert:innen einig, dass es technisch nicht möglich ist, diese Dienste zu überwachen, ohne auf das gesamte System zuzugreifen. Hier muss auch auf das Urteil des Verfassungsgerichtshofs gegen den „Bundestrojaner“ aus dem Jahr 2019 verwiesen werden, in dem dieser für verfassungswidrig erklärt wurde. Überwachungsmaßnahmen müssen stets auf einem spezifischen, begründeten und individuellen Verdacht basieren und dürfen keinesfalls dazu eingesetzt werden, die gesamte individuelle Kommunikation der Bürgerinnen und Bürger zu überwachen. Es darf auch niemals im Sinne des Rechtsstaates sein, dass Sicherheitslücken bewusst offengelassen werden, da diese vorwiegend von Kriminellen ausgenutzt werden können.

FRAGE 9:

Welche Rolle soll das Internet in Österreich haben und wie wollen Sie die digitale Wirtschaft fördern?

Die Volkspartei

Laut einer aktuellen Statistik Austria Studie („IKT-Einsatz in Haushalten 2022“) verfügen neun von zehn Haushalten in Österreich über einen Internetzugang. Aus diesem Grund kann auf eine stark

verbreitete Nutzung des Internets in der österreichischen Bevölkerung geschlossen werden, die eine Basis für die Nutzung von weiteren Informations- und Kommunikationstechnologien darstellt. Die Förderung der digitalen Wirtschaft ist essentiell für das Weiterkommen des Wirtschaftsstandortes Österreich. Wirtschaft ohne Digitalisierung funktioniert nicht mehr. Ein Standort ohne leistungsstarke digitale Infrastruktur kann sich nicht erfolgreich entwickeln. Ziele sind die Verbesserung bestehender Rahmenbedingungen, um digitale Innovation und Technologietransfer zu ermöglichen.

SPÖ

Generell will die SPÖ die Abhängigkeit von Online-Monopolisten im Sinne Digitaler Souveränität reduzieren und eine eigenständige und ganzheitliche Regulierung des digitalen Raums sowie eine Strategie für ein unabhängiges und digital souveränes Europa schaffen. Wir fördern daher österreichische und europäische Software-Entwickler*innen und setzen Initiativen für eine unabhängige digitale Infrastruktur. Wir investieren in Forschung und Entwicklung und setzen auf die Verwendung von Open Source und Open Access Produkten. Außerdem setzen wir auf die duale Ausbildung und darauf, Fachkräfte offensiv auszubilden und in Österreich zu halten – siehe Beantwortung der 6. Frage.

FPÖ

Die Wirtschaft, einschließlich aller Arbeitnehmer, benötigt eine gezielte steuerliche und bürokratische Entlastung. Es ist essenziell, dass Unternehmen und ihre Beschäftigten nicht gegeneinander ausgespielt werden, sondern gemeinsam profitieren – sei es in der „digitalen Wirtschaft“ oder der „analogen Wirtschaft“.

DIE GRÜNEN

Die Digitalisierung verändert das tägliche Leben von Menschen laufend und grundlegend. Wir sind mitten in einer gesellschaftlichen Revolution. Hier gilt es, Chancen für den Wirtschaftsstandort Österreich zu ergreifen, zu fördern und Rahmenbedingungen zu schaffen. Wir müssen die Bevölkerung mitnehmen und mit Bildungsoffensiven für die laufenden Umbrüche stärken. Wesentlich ist, unsere demokratischen Grundwerte zu wahren. Bei Social Media wurde relativ naiv von einer Demokratisierung der Kommunikation und von Selbstregulierung ausgegangen. Das war ein Irrtum. Wichtig ist, diesen Fehler bei künstlicher Intelligenz nicht zu wiederholen. Mit dem AI Act haben wir klare Rahmenbedingungen – auch für die Förderung der Wirtschaft, etwa durch Reallabore und eine Begünstigung von Open Source.

NEOS

Eine leistungsfähige Internetinfrastruktur ist essenziell für Österreichs Zukunft. NEOS setzen sich für einen flächendeckenden Glasfaserausbau ein, damit alle Bürger:innen und Unternehmen Zugang zu schnellem und zuverlässigem Internet haben. Gerade durch die Zunahme von KI-Anwendungen wird ein leistungsfähiges Internet benötigt. Unser Ziel ist es, Österreich zu einem führenden Standort für digitale Innovationen und eine wettbewerbsfähige digitale Wirtschaft zu machen. Der Staat muss klug investieren (Zukunftsquote) und die Rahmenbedingungen so gestalten, dass innovative Unternehmen entstehen und bleiben können. Die nächste Regierung muss mit ambitionierten Reformen den Rückstand aufholen und Österreich zu den innovativsten Standorten weltweit machen, auch wenn sich die nationale Umsetzung in Österreich verzögern sollte. ■

ISPA-FORUM 2024

GAMECHANGER FÜR DIE GLASFASER?

Am 16. Mai war es wieder soweit: Die ISPA lud zu ihrer Fachtagung, dem ISPA-Forum, und machte diesmal den Gigabit Infrastructure Act (GIA) zum Thema. Denn seit er in Brüssel beschlossen wurde, wird in ganz Europa über sein Potenzial gesprochen. Dabei wird besonders eine engagierte Umsetzung in den Mitgliedsstaaten entscheidend sein, sagte ISPA-Generalsekretär Stefan Ebenberger. „Vor allem die Schaffung einer zentralen Anlaufstelle im Sinne eines One-Stop-Shops, über den sämtliche Genehmigungen digital eingeholt werden können, wäre eine massive Erleichterung für die Branche und würde den Ausbau deutlich beschleunigen. Ebenso sollte man die Möglichkeit des GIA nutzen, das Prinzip der stillschweigenden Genehmigung von Anträgen für den Netzausbau festzuschreiben."

Allerdings arbeitete die Fachtagung auch heraus, dass der GIA alleine noch nicht die sogenannte „silver bullet" ist, mit der alle Probleme gelöst werden. Wolfgang Feiel von der Regulierungsbehörde RTR GmbH warnte in seiner Keynote vor überzogenen Hoffnungen. Er skizzierte die Genese des GIA und erklärte, dass er gerade aufgrund der zum Teil sehr unterschiedlichen Voraussetzungen in den EU-Mitgliedsstaaten sehr weit gefasst ist und vor allem auf bestehenden Rechtsrahmen aufbaut. Seine Zusammenfassung war: „Es handelt sich beim GIA eher um eine Evolution als eine Revolution."

In der folgenden Diskussion mit Klaus Parrer aus dem Finanzministerium sowie Florian Parnigoni von spusu ging es dann um die Herausforderungen und Chancen für die Verwaltung in Österreich. Es zeigte sich, dass die Umsetzung der EU-Verordnung die Gelegenheit bietet, viele Vereinfachungen umzusetzen, aber dabei die Harmonisierung von Vorschriften und Verfahren zwischen Bundes- und Länderebenen herausfordernd bleibt.

Stefan Ebenberger sprach in seiner Eröffnung darüber, dass die nationale Umsetzung entscheidend sein wird.

Im zweiten Teil der Veranstaltung ging es um unterschiedliche Erfahrungen mit dem Breitbandausbau in Europa. Dazu war Sven Knapp vom deutschen Bundesverband Breitbandkommunikation BREKO aus Berlin angereist und sprach in seiner Keynote darüber, dass Open Access die Basis für einen schnellen Glasfaserausbau, eine hohe Netzauslastung und attraktive Endkundenprodukte ist.

Mit seiner Open-Access-Definition hat BREKO in Deutschland klare Kriterien gesetzt, die die Interessen der Glasfaser ausbauenden

Sven Knapp von berichtete von den BREKO-Standards in Deutschland.

Unternehmen und der Vorleistungsnachfrager gleichermaßen berücksichtigen. Und er sagte: „Wer jetzt noch ernsthaft behauptet, Open-Access-Geschäftsmodelle im Glasfaserausbau scheiterten an fehlenden technischen Schnittstellen, der will entweder als Anbieter seine Netze nicht öffnen, oder sich als Nachfrager nicht auf anderen Netzen einkaufen."

Die Diskussion danach drehte sich dann um die Praxis des Ausbaus. Philipp Machač von tirolnet sprach darüber, dass dieser im ländlichen Raum dann gut funktioniert, wenn alle Stakeholder eng zusammenarbeiten.

Für Wolfgang Feiel ist der GIA mehr Evolution als Revolution.

Der Bürgermeister Stefan Schröter berichtete vom Pilotprojekt der Gemeinde Ziersdorf und wie schwierig es zum Teil ist, die kritischen Schwellen für die Nachfrage zu erreichen.

Fjodor Gütermann vom Breitbandbüro ergänzte diese Perspektiven um weitere Erfahrungen aus ganz Österreich und eine Einschätzung der weiteren Entwicklung. Abschließend fasste die 1. Vizepräsidentin der ISPA, Natalie Ségur-Cabanac, die Diskussion

Natalie Ségur-Cabanac schlussfolgerte, dass der Schlüssel für den Glasfaserausbau in verstärkter Zusammenarbeit aller Akteure liege.

V. l. n. r.: Wolfgang Feiel, Stefan Schröter, Sven Knapp, Klaus Parrer, Philipp Machač, Natalie Ségur-Cabanac, Fjodor Gütermann, Florian Parnigoni und Stefan Ebenberger

mit der Schlussfolgerung zusammen, dass der GIA allein noch nicht das Allheilmittel ist: „Starker Wettbewerb bildet den Rahmen für Innovation und Transformation. Nicht nur die großen Player sind dabei wichtige Spielteilnehmer, sondern insbesondere auch kleine, lokale Anbieter gewährleisten hier ein faires Spiel – sie sind die ‚local heroes' des Glasfaserausbaus." Für die Zukunft sieht sie vor allem konstruktive Zusammenarbeit als wichtiges Element, denn die Komplexität des Ausbaus fordere alle Akteure, von Gemeinden bis hin zu den Anbietern, weshalb ein verstärktes Miteinander hilfreich sein kann. ■

GIGABIT INFRASTRUCTURE ACT BESCHLOSSEN

Am 11.5.2024 ist der Gigabit Infrastructure Acts (GIA) nach Beschluss durch das Europäische Parlament und den Rat der Europäischen in Kraft getreten. Der GIA stellt eine Neufassung der Kostensenkungs-Richtlinie (KSRL) von 2014 dar und bezweckt die Förderung des Ausbaus von Very High Capacity Networks (VHCN), worunter etwa Festnetze mit Glasfaser bis zum Zugangspunkt, Funknetze mit Glasfaseranbindung bis zur Basisstation oder ähnlich leistungsfähige Netze verstanden werden. Hierfür sieht der GIA einerseits Rechte von Kommunikationsnetzbetreibern vor, für den Ausbau dieser Netze die physische Infrastruktur (z.B. Leerrohre, Masten, Verteilerkästen etc.) anderer Netzbetreiber mitbenutzen zu können. Zudem soll die Erlangung von für den Ausbau erforderlichen Genehmigungen vereinfacht und beschleunigt werden. Weiters beschäftigt sich der GIA mit Vorgaben für die gebäudeinterne Infrastruktur. Zuletzt wurde als sachfremde Regelung auch eine Abschaffung der Gebühren für Anrufe und SMS in andere Mitgliedstaaten (Intra-EU-Kommunikation) aufgenommen.

Anders als die KSRL soll der GIA als Verordnung unmittelbar in allen EU-Mitgliedstaaten anwendbar sein und muss daher nicht in österreichisches Recht umgesetzt werden. Es wurden aber im Rahmen der Trilog-Verhandlungen zahlreiche Bestimmungen so abgeändert, dass diese nur gelten, falls sich die Mitgliedstaaten jeweils freiwillig dazu entschließen, diese auch im nationalen Recht umzusetzen. Von anderen Bestimmungen können die Mitgliedstaaten wiederum im nationalen Recht abweichen. Die Verordnung sieht eine Mindestharmonisierung vor, weshalb strengere oder ausführlichere Maßnahmen durch die Mitgliedstaaten in der Regel zulässig sind.

Im Folgenden sollen auszugsweise einige Inhalte des GIA dargestellt werden:

MITBENUTZUNGSRECHTE

Ein großer Teil der Kosten, die mit der Errichtung von VHCN verbunden sind, entstehen durch die notwendigen Baumaßnahmen (insbesondere Grabungsarbeiten). Aus diesem Grund sah bereits die KSRL vor, dass Netzbetreiber hierfür gegen Abgeltung die physische Infrastruktur anderer Netzbetreiber (wozu beispielsweise auch Energieversorger zählen) nutzen können, wenn dies für den Ausbau erforderlich ist. Somit müssen beispielsweise keine erneuten Grabungsarbeiten für Glasfaserleitungen durchgeführt werden, wenn im Boden bereits Leerverrohrungen mit ausreichend Platz vorhanden sind. Der GIA übernimmt diesen Ansatz und baut ihn weiter aus. So sind nun etwa auch „Tower Companies“ sowie öffentliche Stellen (z.B. Gebietskörperschaften oder öffentliche Versorgungsunternehmen) ausdrücklich im Kreis der mitbenutzungspflichtigen Akteure enthalten. Auch der Begriff der physischen Infrastruktur wurde beispielsweise um Gebäude inklusive Dächer und Fassadenteile sowie Straßenmobiliar wie Lichtmasten, Haltestellen oder Straßenschilder erweitert, was insbesondere für die Anbringung von Funkanlagen für drahtlose Netze relevant sein kann. Aktive Netzelemente, Kabel oder unbeschaltete Glasfaser zählen hingegen nicht zur physischen Infrastruktur im Sinne des GIA.

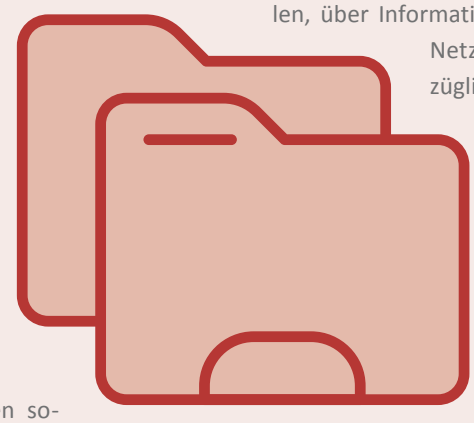
Neu ist zudem, dass auch Eigentümer privater kommerzieller Gebäude in ländlichen bzw. abgelegenen Gebieten unter Umständen gegen Abgeltung eine Mitbenutzung ihres Gebäudes durch Netzbetreiber (z.B. zur Anbringung von Funkanlagen) dulden müssen. Dies kann unter Umständen dazu beitragen, Versorgungslücken zu beheben. Diese Möglichkeit besteht allerdings nur dann, wenn sich die Mitgliedstaaten dafür entscheiden, diese Regelung in nationales Recht umzusetzen. Es bleibt daher abzuwarten, wie sich Österreich diesbezüglich verhalten wird.

Neu ist auch, dass die Mitgliedstaaten vorsehen können, dass Netzbetreiber und öffentliche Stellen die Mitbenutzung ihrer physischen Infrastruktur verweigern können, wenn sie den Nachfra-

gern stattdessen einen aktiven Zugang zu einem VHCN im selben Gebiet anbieten. Diese Ausnahme wurde im Rahmen der Trilogverhandlungen neu aufgenommen, nachdem von einigen Stakeholdern gefordert wurde, insbesondere Investitionen in Leerrohr-Infrastrukturen vor strategischer Überbauung zu schützen.

TRANSPARENZ HINSICHTLICH PHYSISCHER INFRASTRUKTUR

Damit Kommunikationsnetzbetreiber prüfen können, ob und welche physischen Infrastrukturen anderer Netzbetreiber sie nutzen können, müssen sie Zugriff auf die diesbezüglichen Informationen haben. Der GIA sieht nunmehr verpflichtend vor, dass andere Netzbetreiber und öffentliche Stellen entsprechende Mindestinformationen (Verortung, Art und derzeitige Verwendung der Infrastruktur sowie Kontaktangaben) über einen Single Information Point zugänglich machen müssen. Für Gemeinden mit weniger als 3.500 Einwohnern können hierfür auf nationaler Ebene Übergangsfristen von bis zu einem Jahr vorgesehen werden. Da in Österreich bereits jetzt die verpflichtende Einmeldung physischer Infrastrukturen in die bei der RTR-GmbH angesiedelte Zentrale Stelle für Infrastrukturdaten sowie entsprechende Abfragemöglichkeiten durch Kommunikationsnetzbetreiber vorgesehen sind, ist noch nicht gänzlich klar, welche praktischen Auswirkungen der GIA hier haben wird.



KOORDINIERUNG VON BAUARBEITEN

Wie auch bislang in der KSRL vorgesehen, haben Netzbereitsteller das Recht, mit anderen Netzbereitstellern (und nunmehr auch öffentlichen Stellen) Vereinbarungen über die Koordinierung von Bauarbeiten („Mitverlegung“) zum Zweck des Ausbaus von VHCN auszuhandeln. Dies verfolgt insbesondere den Zweck, dass bei Grabungsarbeiten (etwa zur Energieversorgung) auch gleich die für VHCN erforderlichen Infrastrukturelemente (z.B. Lichtwellenleiter) mitverlegt werden können.
Bei öffentlich geförderten Bauvorhaben besteht dabei grundsätzlich auch die Pflicht, zumutbaren schriftlichen Anfragen zur Mitverlegung unter transparenten und nicht-diskriminierenden Bedingungen stattzugeben, wobei es Ausnahmen für den Schutz von Ausbauvorhaben vor strategischer Überbauung durch Konkurrenten gibt.

Das österreichische TKG 2021 geht jedoch – wie auch dessen Vorgängergesetz TKG 2003 – bei der Koordinierung von Bauarbeiten bereits über die Vorgaben der KSRL hinaus. So müssen in Österreich auch solche Netzbereitsteller, die nicht öffentlich geförderte Bauarbeiten durchführen, auf Anfrage ein entsprechendes Angebot zur Koordinierung abgeben und können dem nur eingeschränkt widersprechen. Zudem gilt die Möglichkeit der Koordinierung von Bauarbeiten in Österreich auch vice versa, d.h. auch andere Netzbereitsteller (z.B. Energieversorger) können ihrerseits bei Betreibern öffentlicher Kommunikationsnetze um eine Koordinierung nachfragen, wenn letztere z.B. Grabungsarbeiten durchführen. Aufgrund der Mindestharmonisierung ist die österreichische Regelung vermutlich auch weiterhin zulässig.

TRANSPARENZ ZU GEPLANTEN BAUMASSNAHMEN

Um die Koordinierung von Bauarbeiten in Anspruch nehmen zu können, müssen Netzbetreiber, die Infrastruktur mitverlegen wollen, über Informationen zu den geplanten Bauarbeiten anderer Netzbereitsteller verfügen. Die KSRL hatte diesbezüglich vorgesehen, dass Betreiber von Kommunikationsnetzen bei anderen Netzbetreibern dementsprechende Informationen zu laufenden oder geplanten Bauarbeiten erfragen können. Der GIA sieht nunmehr vor, dass diese Mindestinformationen (unter anderem Ort, Art und Zeitraum der Bauarbeiten) in elektronischem Format über einen von den Mitgliedstaaten einzurichtenden Single Information Point eingemeldet werden müssen und abgefragt werden können. Da im österreichischen TKG 2021 bereits jetzt die Einmeldung von Mindestinformationen zu geplanten Bauarbeiten bzw. deren Abfragemöglichkeit bei der Zentralen Stelle für Infrastrukturdaten (ZIB) bei der RTR-GmbH verpflichtend vorgesehen ist, können die praktischen Änderungen des GIA noch nicht gänzlich abgeschätzt werden.

VERFAHREN FÜR GENEHMIGUNGEN

Ein wesentliches Ziel des GIA ist es, die Verfahren zur Erlangung von für den Ausbau von VHCN erforderlichen (z.B. bau- oder straßenverkehrsrechtlichen) Genehmigungen zu erleichtern. Hierfür hatte der Gesetzesvorschlag der Kommission noch vorgesehen, dass die Mitgliedstaaten ihre diesbezüglichen Regelungen national vereinheitlichen müssen. Dies stieß insbesondere in föderal organisierten Mitgliedstaaten auf Widerspruch, weshalb die Regelung im Trilog dahingehend abgeschwächt wurde, dass sich die Mitgliedstaaten nur mehr „nach Kräften“ um die Vereinheitlichung der Regelungen bemühen müssen.

Neu ist zudem, dass Anträge auf elektronischem Weg über einen

Single Point of Contact („One Stop Shop“) eingebracht werden können. Die zuständigen Behörden müssen anschließend binnen 4 Monaten (in begründeten Ausnahmefällen ist eine Verlängerung auf 8 Monate möglich) über den Antrag entscheiden. Haben die zuständigen Behörden nicht binnen dieser Frist über den Antrag entschieden, kommt es zur stillschweigenden Genehmigung des Antrags. Die stillschweigende Genehmigung gilt jedoch nicht, wenn Wegerechte beantragt werden, also etwa das Recht zum Führen einer Leitung über ein Grundstück.

Allerdings wurde in den Trilog-Verhandlungen eine Zusatzbestimmung aufgenommen, nach der die Mitgliedstaaten insgesamt vom Prinzip der stillschweigenden Genehmigung abweichen können, sofern der Antragsteller Schadenersatz für die Verzögerung verlangen oder das Genehmigungsverfahren an ein Gericht oder eine Aufsichtsbehörde verweisen kann. Es ist derzeit noch unklar, ob die in Österreich zur Verfügung stehenden Behelfe der Amtshaftungsklage und des Fristsetzungsantrags diese Kriterien erfüllen. Falls ja, müsste Österreich aber nach Ansicht der ISPA wohl dennoch eine ausdrückliche Opt-Out-Regelung in das nationale Begleitgesetz aufnehmen.

GEBÄUDEINTERNE INFRASTRUKTUR

Bereits die KSRL sah vor, dass in neu errichteten bzw. umfangreich renovierten Gebäuden hochgeschwindigkeitsfähige gebäudeinterne physische Infrastruktur bzw. bei Mehrfamilienhäusern auch ein Zugangspunkt, der für Kommunikationsnetzbetreiber den Anschluss ihrer Netze an die gebäudeinterne Infrastruktur ermöglicht, vorhanden sein muss. Dies wurde in den Bauordnungen der österreichischen Bundesländer umgesetzt.

Der GIA geht insofern darüber hinaus, als nunmehr auch gebäudeinterne Glasfaserverkabelung bis zum Netzabschlusspunkt gefordert wird. Hierfür müssen die Mitgliedstaaten die notwendigen technischen Spezifikationen erlassen. Die Mitgliedstaaten können zudem bestimmte Kategorien von Gebäuden festlegen, die von den Vorgaben ausgenommen sind.

ABSCHAFFUNG DER GEBÜHREN FÜR INTRA-EU-KOMMUNIKATION

Aufgrund einer Forderung des EU-Parlaments wurde im Trilog auch eine Abschaffung der Gebühren für Intra-EU-Kommunikation, d.h. Anrufe und SMS aus dem Heimatstaat eines Verbrauchers in einen anderen Mitgliedstaat, beschlossen. Nach derzeit geltender Rechtslage sind diese bis 14. Mai 2024 mit € 0,19 pro Minute für Anrufe und mit € 0,06 pro SMS gedeckelt. Im Rahmen des GIA wurde diese Deckelung nun einerseits bis zum 30. Juni 2032 verlängert. Anderseits wurde beschlossen, dass es ab 1. Januar 2029 keine Preisdifferenzierung zwischen Inlandskommunikation und Intra-EU-Kommunikation mehr geben darf, wobei dies einen bis zum 30.6.2028 zu erlassenden Durchführungsrechtsakt der EU-Kommission voraussetzt, in dem etwa Maßnahmen gegen Fraud oder zu Fair Use geregelt werden. Die Kommission ist zudem verpflichtet, bis zum 30.6.2027 eine Überprüfung der rechtlichen Regelungen zur Intra-EU-Kommunikation durchzuführen und gegebenenfalls einen Gesetzesvorschlag zu deren Abänderung einzubringen.

AUSBLICK

Der Gigabit Infrastructure Act ist am 11.5.2024 in Kraft getreten und wird größtenteils ab 12.11.2025 anzuwenden sein, wobei einzelne Bestimmungen längere Übergangsfristen haben. Nach Ansicht der ISPA sollte bereits jetzt in intensiver Diskussion mit den beteiligten Stakeholdern mit dem Entwurf des österreichischen Begleitgesetz begonnen werden. Dabei sollte genau geklärt werden, welche der fakultativen Bestimmungen des GIA sinnvollerweise in Österreich umgesetzt werden sollten, um dessen Potenziale voll auszuschöpfen. Die ISPA wird den Implementierungsprozess auch weiterhin verfolgen und ihre Mitglieder über neue Entwicklungen informieren. ■

ISPA ACADEMYS

Im Rahmen unserer Weiterbildungsreihe „ISPA-Academy“ werden regelmäßig aktuelle Themen und Entwicklungen der IKT-Branche vorgestellt. Expert:innen aus den eigenen Reihen oder externe Vortragende geben ihre Expertise und ihr Know-how an die Teilnehmer:innen weiter. Im ersten Halbjahr 2024 fanden zwei ISPA-Academy-Webinare statt.

KI – CHANCEN, POTENZIALE UND ANWENDUNGEN FÜR IKT-UNTERNEHMEN

Am 21. März 2024 veranstalteten wir ein Webinar zum Thema „KI – Chancen, Potenziale und Anwendungen für IKT-Unternehmen“. Unser Vortragender Andreas Lederer, Gründer von ADVANTAGE AI, einer Agentur für digitale Transformation, bot einen Überblick über die aktuellen Möglichkeiten von generativer künstlicher Intelligenz. Anhand von praktischen Beispielen und Vorführungen zeigte er, wie verschiedene Tools funktionieren und wofür sie eingesetzt werden können. Dabei ging er sowohl auf die Vorteile als auch die Limitationen der aktuellen Werkzeuge ein.
Besonders eindrucksvoll demonstrierte er eine generative künstliche Intelligenz, die Übersetzungen von Videos erstellen kann. Dabei wurde nicht nur das Gesprochene mit einer virtuellen Stimme wiedergegeben, die der Originalstimme sehr nahekam, sondern auch die Lippenbewegungen an die Übersetzung angepasst. Um KI-Tools möglichst sinnvoll im Arbeitsumfeld einzusetzen, rät Lederer sich folgende Fragen zu stellen:

- Was kostet viel Zeit/Geld?
- Was ist lästig?
- Was funktioniert nicht?

Delegierbare Tätigkeiten könnten evtl. von KI-Werkzeugen übernommen werden. Am häufigsten werden generative KI-Tools heute schon zur Erstellung von Texten verwendet. Die Landschaft an KI-Anwendung entwickelt sich rasant weiter, es lohnt sich also die Neuigkeiten im Blick zu haben. Lederer glaubt, dass Funktionen, die das größte wirtschaftliche Potential bringen, noch kommen werden. Im abschließenden Erfahrungsaustausch diskutierten die Teilnehmer:innen des Webinars, ob es dezidierte KI-Regelungen in jedem Unternehmen braucht. Es wurde von unterschiedlichen Zugängen berichtet, einig waren sie sich allerdings bei der Bewusstseinsbildung. Da z. B. datenschutzrechtliche Aspekte beim Einsatz von KI-Tools eine Rolle spielen, sollte auf jeden Fall Bewusstsein bei allen geschaffen werden.

VON SPF BIS BIMI: E-MAIL-AUTHENTIFIZIERUNG DURCH DNS-EINTRÄGE

Am 28. Mai 2024 stellte ISPA-Vorstand Peter Miller, Gründer und Gesellschafter der HXS GmbH, Möglichkeiten zur E-Mail-Authentifizierung durch DNS-Einträge näher vor. Miller erklärte, dass die korrekte Einrichtung der entsprechenden DNS-Records immer wichtiger werde, da Anbieter wie Google und Yahoo ihre Einstellungen auf den E-Mail-Empfangsservern immer strenger gestalten. Eine große Umstellung gab es Anfang des Jahres, wodurch die Zustellbarkeit von nicht authentifizierbaren E-Mails erschwert wurde. Eine große Fehlerquelle sieht er z. B. beim Wechsel von Domain oder E-Mail-Server, da hier oft vergessen wird, die entsprechenden Einträge aufeinander abzustimmen und zu aktualisieren. Im Webinar stellte er die Möglichkeiten SPF, DKIM, DMARC und BIMI näher vor. ■

SPF (Sender Policy Framework) hilft dabei, E-Mail-Spoofing zu verhindern, indem es den Empfangsservern ermöglicht, zu überprüfen, ob eingehende E-Mails tatsächlich von den im DNS der Domain autorisierten Servern gesendet wurden.

DKIM (DomainKeys Identified Mail) hilft dabei, die Integrität und Authentizität von E-Mails sicherzustellen, indem es den Inhalt der E-Mail mit einer digitalen Signatur versieht, die vom sendenden Server erstellt wird.

DMARC (Domain-based Message Authentication, Reporting & Conformance erweitert SPF und DKIM, um E-Mail-Absender zu authentifizieren und Phishing und E-Mail-Spoofing zu verhindern. Es gibt Domaininhabern auch Berichte über gefälschte E-Mails, die ihre Domain verwenden.

BIMI (Brand Indicators for Message Identification) ermöglicht es Markeninhabern ihr Logo in unterstützten E-Mail-Clients anzuzeigen, um das Vertrauen der Empfänger zu erhöhen und die Markenidentität zu stärken.

CYBERSECURITY-RICHTLINIE NIS-2

BIS ZU 5.000 UNTERNEHMEN BETROFFEN

Die NIS-1-Richtinie legte einen rechtlichen Rahmen über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz -und Informationssystemen in der EU fest. Die NIS-1-Richtlinie wird durch die NIS-2-Richtlinie ersetzt.

Während der Anwendungsbereich der NIS-1-Richtlinie in Österreich etwa 100 - 200 Unternehmen umfasst hat, betrifft die Nachfolgerrichtlinie NIS-2 Schätzungen zufolge bis zu 5.000 Unternehmen.

Für die Mitgliedsstaaten werden insbesondere die Pflicht nationale Cybersicherheitsstrategien zu verabschieden und die Pflicht eine zuständige nationale Behörde; Behörden für das Cyberkrisenmanagement; zentrale Anlaufstellen für Cybersicherheit und Computer-Notfallteams zu benennen oder einzurichten, normiert.

Für betroffene Einrichtungen normiert die NIS-2-Richtlinie Cybersicherheitsrisikomanagement-Maßnahmen sowie Berichtspflichten.

BIS WANN MÜSSEN BETROFFENE UNTERNEHMEN „CYBERSICHER“ SEIN?

Die NIS-2-Richtlinie ist am 16. Jänner 2023 in Kraft getreten und ist von den Mitgliedstaaten bis zum 17. Oktober 2024 umzusetzen.

WER IST VON DER NIS-2 BETROFFEN?

In den Anwendungsbereich fallen alle öffentlichen und privaten Einrichtungen die in Anhang I oder II genannt sind und über 50 Beschäftigte und mehr als 10 Mio. Euro Jahresumsatz oder mehr als 10 Mio. Euro Jahresbilanzsumme haben.

Anhang I enthält Sektoren mit hoher Kritikalität, beispielsweise die Sektoren Energie, Verkehr, Bankwesen, Trinkwasser und Abwasser. Anhang II enthält kritische Sektoren wie beispielsweise Post- und Kurierdienste, Abfallbewirtschaftung, Produktion/ Herstellung und Handel von chemischen Stoffen oder Lebensmitteln.

NICHT DIE KLEINEN – ODER DOCH?

Grundsätzlich fallen kleine Unternehmen nicht unter die NIS-2-Richtlinie. „Essenzielle“ Einrichtungen und die meisten Einrichtungen der Digitalen Infrastruktur stellen eine Ausnahme von der Grundregel dar. Beispielsweise fallen Vertrauensdiensteanbieter, Anbieter öffentlicher elektronischer Kommunikationsnetze und Anbieter öffentlich zugänglicher Kommunikationsdienste TLD-Namenregister und DNS-Diensteanbieter -ausgenommen Betreiber von Root-Namenservern - auch als kleine (!) Unternehmen unter NIS-2.

WELCHE PFLICHTEN TREFFEN DIE NIS-2-UNTERWORFENEN?

In der NIS-2-Richtlinie werden Risikomanagementmaßnahmen und Berichtspflichten normiert. Weiters wird die Verpflichtung zur Überwachung der Regeln der NIS-2-Richtlinie durch die Leitungsorgane (Geschäftsführer der GmbH, Vorstände der Aktiengesellschaft) und deren Haftung statuiert.

RISIKOMANAGEMENTMASSNAHMEN

Folgende Riskomanagementmaßnahmen werden in der Richtlinie festgelegt und ist die nähere Gestaltung der Pflichten durch nationale Durchführungsverordnungen derzeit in Arbeit:

- Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;
- Bewältigung von Sicherheitsvorfällen;
- Aufrechterhaltung des Betriebs, wie Backup-Management und

Wiederherstellung nach einem Notfall, und Krisenmanagement;

- Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;
- grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;
- Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

VERPFLICHTENDES DREISTUFIGES MELDEVERFAHREN

Folgende Berichtspflichten werden in der Richtlinie festgelegt:

- Bei erheblichen Cybersicherheitsvorfällen gibt es ein dreistufiges Meldeverfahren an das zuständige Cybersecurity Incident Response Team (CSIRT): Die Unternehmen müssen sich an folgende Berichtspflichten halten.
- Unverzüglich, innerhalb von 24 Stunden haben Unternehmen eine Frühwarnung, in der gegebenenfalls angegeben wird, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte, zu übermitteln
- Unverzüglich, jedenfalls innerhalb von 72 Stunden, haben Unternehmen eine Meldung in der die in der Frühwarnung genannten Informationen aktualisiert werden und eine erste Bewertung des erheblichen Sicherheitsvorfalls (inkl. Schweregrad, Auswirkungen, ggf. Kompromittierungsindikatoren) stattfindet, zu übermitteln.
- Weiters ist ein Zwischenbericht auf Ersuchen eines CSIRT zu übermitteln.
- Schließlich hat das Unternehmen spätestens einen Monat nach der Frühwarnung einen Abschlussbericht, der eine ausführliche Beschreibung des Sicherheitsvorfalls (inkl. Schweregrad, Auswirkungen; Art der Bedrohung bzw. Ursache; Abhilfemaßnahmen; ggf. grenzüberschreitenden Auswirkungen) enthält, zu übermitteln.

WELCHE SCHRITTE SIND ZU UNTERNEHMEN?

Da die NIS-2-Richtlinie bis zum 17. Oktober 2024 von den Mitgliedstaaten (durch ein NIS-Gesetz und weitere Durchführungsverordnungen) umgesetzt werden muss, ist bereits jetzt die Prüfung des Anwendungsbereiches, Ressourcenplanung sowie die Beschäftigung mit den künftigen Risikomanagementmaßnahmen, bereits jetzt anzuraten. ■

EUGH VORRATSDATEN-SPEICHERUNG

Anfang Mai hat der Europäische Gerichtshof (EuGH) das Urteil in der Rechtssache C-470/21 (La Quadrature du Net u.a.) veröffentlicht, in dem er sich mit der Zulässigkeit der Vorratsdatenspeicherung von IP-Adressen durch Internetzugangsdiensteanbieter und dem Zugriff darauf durch Behörden auseinandersetzt.

Ausgangspunkt des Verfahrens waren mehrere französische Rechtsakte. Ein Gesetz verpflichtet Anbieter von Internetzugangsdiensten dazu, Verkehrsdaten wie anderem die Quell-IP-Adressen der Verbindungen ihrer Nutzer ein Jahr lang zu speichern. Ein weiteres Gesetz sieht vor, dass Vereinigungen von Urheberrechte-Inhabern IP-Adressen ermitteln und sammeln, die in Peer-to-Peer-Netzen Dateien (z.B. Videos oder Musik) austauschen und damit mutmaßlich Urheberrechtsverstöße begehen. Diese Vereinigungen stellen die IP-Adressen anschließend der Hohen Behörde für die Verbreitung von Werken und den Schutz von Rechten im Internet (HADOPI) zur Verfügung, welche über die Anbieter von Internetzugangsdiensten die Identität der entsprechenden Nutzer ermittelt und nach zwei Verwarnungen eine Anzeige an die zuständige Staatsanwaltschaft erhebt („Three Strikes Law"). Mehrere zivilgesellschaftliche Vereinigungen zum Schutz der Rechte und Freiheiten im Internet haben dagegen ein Rechtsmittel an den französischen Conseil d'État erhoben, welcher den EuGH im Rahmen eines Vorabentscheidungsverfahren um Klärung der Vereinbarkeit dieser Gesetze mit dem Unionsrecht (insbesondere der Grundrechtecharta und der E-Privacy-Richtlinie) ersucht hat.

In seinem Urteil stellte der EuGH fest, dass es das Unionsrecht den Mitgliedstaaten nicht verbietet, Anbieter von Internetzugangsdiensten zu einer allgemeinen und unterschiedslosen Vorratsspeicherung von IP-Adressen zu verpflichten. Die Mitgliedstaaten müssen allerdings gewährleisten, dass der Zugriff auf diese Daten keine genauen Schlüsse auf das Privatleben der Inhaber:innen der IP-Adressen ermöglicht. Dafür können laut EuGH bestimmte Speichermodalitäten der Anbieter sorgen, die eine wirksame strikte Trennung der IP-Adressen und der übrigen Kategorien personenbezogener Daten (Identitätsdaten und sonstige Verkehrs- und Standortdaten) sicherstellen. Im Stadium der Speicherung muss jede kombinierte Nutzung der verschiedenen Datenkategorien verhindert werden. Auch das Verfahren, mit dem diese getrennt gespeicherten Daten kombiniert werden, darf die Wirksamkeit dieser strikten Trennung nicht in Frage stellen. Die Zuverlässigkeit der Trennung muss zudem regelmäßig durch eine andere Behörde als diejenige, welche Zugang zu den Daten begehrt, kontrolliert werden. Auch die Dauer der Speicherung muss auf das absolut Notwendige begrenzt sein.

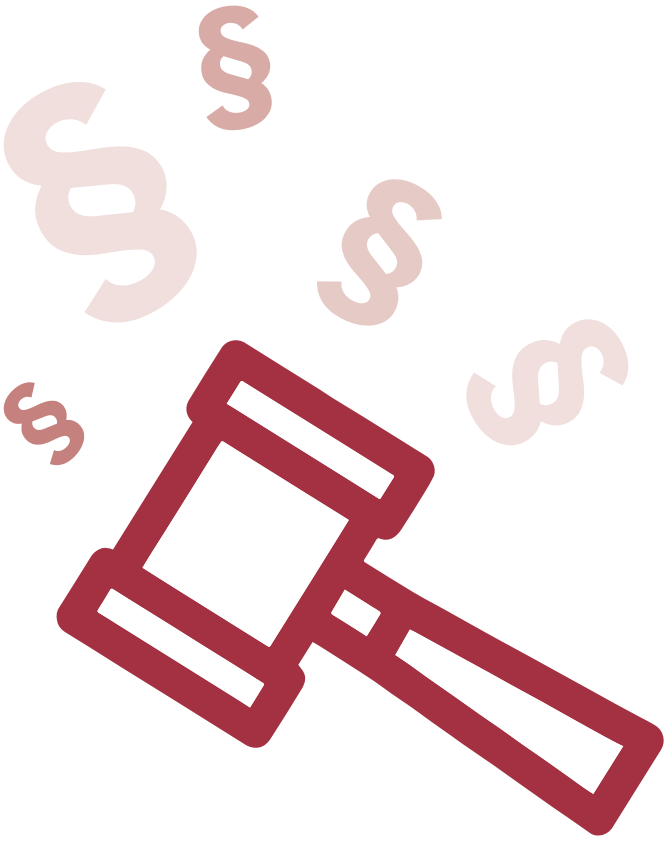
Unter diesen Umständen kann der Zugang zu den auf Vorrat ge-

speicherten Daten durch Behörden zum Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten im Allgemeinen (und darunter auch online begangene Verletzungen von Urheberrechten) erfolgen. Allerdings darf auch der Zugang der Behörde zu diesen Daten ausschließlich der Identifikation der Teilnehmer:innen dienen und abgesehen von atypischen Situationen keine genauen Schlüsse auf deren Privatleben erlauben, wofür geeignete Garantien vorzusehen sind.

Eine vorherige Kontrolle des behördlichen Zugriffs auf die gesammelten Daten durch ein Gericht oder eine unabhängige Verwaltungsstelle ist laut EuGH lediglich dann erforderlich, wenn die Besonderheiten des nationalen Verfahrens es durch die Verknüpfung der im Lauf der verschiedenen Stufen des Verfahrens gesammelten Daten und Informationen ermöglichen können, genaue Schlüsse auf das Privatleben der betreffenden Person zu ziehen. Die Betroffenen müssen aber über wirksame Garantien zum Schutz von Missbrauch und unberechtigtem Zugang zu oder Nutzung der Daten verfügen.

Mit diesem Urteil ändert der EuGH seine bisherige restriktive Rechtsprechung zur Zulässigkeit der Vorratsdatenspeicherung (ua C-623/17 und C-511/18, C-512/18, C-520/18), da die Speicherung von und der Zugang zu den auf Vorrat gespeicherten Daten nicht länger nur zur Bekämpfung schwerer Kriminalität oder der Verhütung schwerer Sicherheitsbedrohungen zulässig ist, sondern eben auch für die Verfolgung von Straftaten im Allgemeinen und damit auch für online begangene Verletzungen von Urheberrechten. Zudem ist für den Zugriff auf die Daten nicht notwendigerweise eine Genehmigung durch ein Gericht oder eine unabhängige Verwaltungsbehörde erforderlich.

Die ISPA sieht diese Änderung der Judikatur äußerst kritisch und vermutet, dass sie vor dem Hintergrund des kontinuierlichen Drucks einiger Mitgliedstaaten erfolgt ist, die starke Befürworter der Vorratsdatenspeicherung sind.



Durch die Vorratsdatenspeicherung werden von jedem Menschen, egal ob an Straftaten beteiligt oder nicht, riesige Mengen an Daten gespeichert, die – gerade aufgrund der mittlerweile ubiquitären Nutzung des Internets in allen Lebensbereichen – detaillierte Rückschlüsse auf deren intimstes Privatleben ermöglichen. Es ist zu befürchten, dass ein derartiger Datenfriedhof in weiterer Folge immer ausuferndere Begehrlichkeiten zum Zugriff auf die gesammelten Daten für immer mehr Zwecke nach sich ziehen würde. Das würde zahlreiche Maßnahmen im Sinne des Datenschutzes der Nutzer:innen konterkarieren und eine Gefahr für diese darstellen. Zudem ist auch die im Urteil vorausgesetzte strikte Trennung der gespeicherten Datenkategorien in der Praxis kaum umsetzbar, da vom Zeitpunkt der Speicherung an die Gefahr von Rückschlüssen auf das intimste Privatleben der betroffenen (und damit allen) Nutzer:innen niemals gänzlich ausgeschlossen werden kann. Auch wenn die Bedürfnisse der Strafverfolgungsbehörden verständlich sind, braucht es nach Ansicht der ISPA primär mehr Ressourcen und Know-how, um die bereits vorhandenen Daten effektiv auswerten zu können. ■

EGMR ENTSCHEIDET

ENTSCHLÜSSELUNG VON ENDE-ZU-ENDE-VERSCHLÜSSELUNG VERLETZT RECHT AUF PRIVATLEBEN NACH ART 8 EMRK

AUSGANGSVERFAHREN

Laut russischem Informationsgesetz ist der Messenger-Dienst Telegram seit Juni 2017 als „Internet-Kommunikationsveranstalter“ (im Folgenden „ICO“) dazu verpflichtet, alle Kommunikationsdaten für ein Jahr und den Inhalt aller Kommunikationen für sechs Monate zu speichern und den Strafverfolgungsbehörden zusammen mit den für die Entschlüsselung erforderlichen Informationen zu übermitteln. Auf dieser Grundlage forderte der FSB dann Telegram auf, technische Informationen offenzulegen, unter anderem eine IP-Adresse, eine TCP/UDP-Portnummer und die Daten zu den Schlüsseln der Ende-zu-Ende-Verschlüsselung der Funktion „geheimer Chat“.

Telegram weigerte sich und argumentierte, dass es technisch unmöglich sei, dies auszuführen, ohne die Verschlüsselung für alle Nutzer:innen zu schwächen. Telegram wurde zu einer Geldstrafe verurteilt und in weiterer Folge in Russland gesperrt. Die Bekämpfung der Urteile durch Telegram war in allen Instanzen erfolglos. Danach bekämpften Telegram-Nutzer:innen die Sperrungsverfügung und argumentierten: Die vom FSB geforderten Informationen über den Schlüssel ermöglichen die Entschlüsselung der Kommunikation aller Nutzer:innen. Diese Klage wurde in Russland in allen Instanzen abgewiesen, danach eine Beschwerde beim EGMR (Europäischen Gerichtshof für Menschenrechte) eingebracht.

Beschwerdeinhalt war, dass dies einen Eingriff in das Recht des Klägers auf Achtung seines Privatlebens und seiner Korrespondenz darstelle. Darüber hinaus war es technisch unmöglich, den Behörden die Verschlüsselungscodes bestimmter Nutzer:innen der Telegram-Messenger-Anwendung zur Verfügung zu stellen.

DER EINGRIFF (IST NICHT GLEICH VERLETZUNG)

Bei der gegenständlichen Entscheidung prüfte der EGMR den Verstoß gegen Art 8 EMRK (Europäische Menschenrechtskonvention) einerseits aufgrund der weitreichenden Speicherverpflichtung der ICOs und andererseits wegen der Verpflichtung zur Entschlüsselung verschlüsselter Nachrichten.

Zur Feststellung eines Verstoßes wird zunächst geprüft, ob ein Eingriff in das geschützte Recht vorliegt. Dazu führt der EGMR aus, nicht nur die bloße Speicherung, sondern auch die Möglichkeit für nationale Behörden später auf diese Daten zugreifen zu können, einen Eingriff in das von Art 8 EMRK geschützte Privatleben bzw. die geschützte Privatsphäre darstellt. Der EGMR führt weiter aus, dass die bloße Existenz der angefochtenen Rechtsvorschriften für sich genommen einen Eingriff in die Ausübung der Rechte des Beschwerdeführers nach Artikel 8 EMRK darstellt. Demnach ist für einen Eingriff in Art 8 EMRK bereits die bloße Möglichkeit ausreichend, dass die Daten der Beschwerdeführerin tatsächlich gespeichert und an die Strafverfolgungsbehörden übermittelt werden.

DAS KERNARGUMENT DES KLÄGERS

Die Entschlüsselung der Verschlüsselungsschlüssel betrifft alle Nutzer:innen unterschiedslos. Eine Beschränkung nur auf bestimmte Nutzer:innen (für Straftaten verdächtige Personen) ist technisch nicht möglich. Da der Eingriff überschießend ist und – hinsichtlich der Nutzer:innen, die nicht von der Überwachungsanordnung betroffen sind – keinen legitimen Zweck erfüllt, verstößt das Informationsgesetz gegen Art 8 EMRK.

RECHTFERTIGUNG?

Ein Eingriff in das von Art 8 EMRK geschützte Recht auf Privatleben kann gerechtfertigt sein, wenn es eine entsprechende Rechtsgrundlage gibt, eines oder mehrere der legitimen Ziele (nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer (vgl Art 8 Abs 2 EMRK) verfolgt, auf und in einer demokratischen Gesellschaft notwendig ist, um ein solches Ziel zu erreichen. Das innerstaatliche Recht muss außerdem angemessene Garantien dafür bieten, dass gespeicherte personenbezogene Daten wirksam vor Missbrauch geschützt werden.

Die angefochtene Regelung verlangt die kontinuierliche

automatische Speicherung und Speicherung der Inhalte aller Internetkommunikationen für die Dauer von sechs Monaten und der zugehörigen Kommunikationsdaten für die Dauer von einem Jahr.

Die Strafverfolgungsbehörden in Russland sind nach innerstaatlichem Recht nicht verpflichtet, dem ICO die gerichtliche Genehmigung vorzulegen, bevor sie Zugang zu den Kommunikationen einer Person erhalten, deshalb sei der wirksame Schutz vor Missbrauch nicht gegeben. Die russischen, geheimen Überwachungsmaßnahmen entsprechen daher nicht den Anforderungen an die „Rechtsqualität", weil sie keine angemessenen und wirksamen Garantien gegen Willkür und das Risiko von Missbrauch vorsehen. Zur Verschlüsselung von Nachrichten erwägt der EGMR, dass diese den Bürger:inenn und Unternehmen dabei hilft, sich gegen den Missbrauch von Informationstechnologien wie Hacking, Identitätsdiebstahl und Diebstahl personenbezogener Daten, Betrug und die unzulässige Offenlegung vertraulicher Informationen zu verteidigen. Der EGMR hält ausdrücklich fest, dass die Vertraulichkeit der Kommunikation ein wesentlicher Bestandteil des in Artikel 8 EMRK verankerten Rechts auf Achtung des Privatlebens und der Korrespondenz ist. Nutzer von Telekommunikations- und Internetdiensten müssen eine Garantie dafür haben, dass ihre Privatsphäre und ihre Meinungsfreiheit gewährleistet sind und respektiert werden.

Die Verpflichtung zur Offenlegung der Verschlüsselungsschlüsseln kann nicht auf bestimmte Personen beschränkt werden und würde alle unterschiedslos betreffen, auch Personen, die keine Gefahr für ein legitimes Regierungsinteresse darstellen. Daher kommt der EGMR zu dem Schluss, dass die Speicherung der gesamten Internetkommunikation aller Nutzer:innen, den direkten Zugriff der Sicherheitsdienste auf die gespeicherten Daten ohne angemessene Schutzmaßnahmen gegen Missbrauch und die Verpflichtung zur Entschlüsselung verschlüsselter Kommunikation vorsehen Ende-zu-Ende-verschlüsselte Kommunikation in einer demokratischen Gesellschaft nicht als notwendig angesehen werden kann. Daher stellte der EGMR einstimmig einen Verstoß gegen Art 8 EMRK fest.

Schadenersatz aufgrund der Grundrechtsverletzung?
Den eingeklagten Schadenersatz für einen immateriellen Schaden (ein Schaden, der kein Vermögensschaden ist, wie bspw. die Verletzung eines Grundrechtes) wies der EGMR mit der Begründung, die Feststellung des Verstoßes von Art 8 EMRK stelle eine ausreichende Entschädigung für den Kläger dar, ab.

PRÄJUDIZIENWIRKUNG - BINDUNG DES VFGH UND EUGH AN DIE RECHTSPRECHUNG DES EGMR?

In Österreich stehen die Grundrechte der EMRK im Verfassungsrang und daher kann jeder, der zu einer Beschwerde vor dem Verfassungsgerichtshof (VfGH) berechtigt ist, die Beschwerde mit der Verletzung eines nach der EMRK garantierten Rechtes durch einen Bescheid, ein Gesetz oder eine Verordnung, begründen. Eine Präjudizienwirkung, also eine Bindung des VfGHs an die Judikatur des EGMR ist aber nicht normiert. Die gegenständliche Entscheidung des EGMR ist nur für den am Verfahren beteiligten Mitgliedsstaat (Russland) bindend. Der VfGH hielt aber bereits in vergangenen Entscheidungen fest, dass bei der Auslegung der EMRK der Rechtsprechung des EGMR „als dem zur Auslegung der EMRK zunächst berufenen Organ besonderes Gewicht einzuräumen" ist.

Wie der VfGH ist der EuGH (Europäischer Gerichtshof) nicht an die Rechtsprechung des EGMR gebunden. Bei der Prüfung von Grundrechtsverletzungen ist es allerdings wahrscheinlich, dass der EuGH sich an der Entscheidung des EGMR orientiert. Sobald eine Entscheidung des EuGH vorliegt, ist diese für den am Verfahren beteiligten Mitgliedsstaat bindend, wobei sich in der Praxis die Übung einer sogenannten „erga-omnes" Wirkung ergeben hat: Die Entscheidung selbst ist nicht für alle Gerichte der Mitgliedsstaaten bindend, jedoch haben sie sich an der Auslegung des EuGH zu orientieren.

Abschließend bleibt daher abzuwarten, wie der VfGH und der EuGH sich zu der End-zu-End-Verschlüsselung positionieren werden, wobei die Entscheidung des EGMR erfahrungsgemäß eine wichtige Auslegungshilfe darstellen wird.

ISPA-POSITION

Die ISPA setzt sich seit jeher für hohe Sicherheitsstandards bei der Online-Kommunikation ein und sieht Ende-zu-Ende-Verschlüsselung als das Fundament moderner und sicherer Kommunikation und damit auch Grundvoraussetzung, damit österreichische und europäische Internetunternehmen ein angemessenes Sicherheits- und Datenschutzniveau für ihre Kund:innen gewährleisten können. Eine bewusste Schädigung der Verschlüsselungsstandards führt direkt zum Nachteil sämtlicher betroffener Nutzer:innen, die dadurch leichter zum Opfer von Cybercrime-Delikten werden können. Zudem betrifft nur ein verschwindend geringer Anteil der Kommunikation über Ende-zu-Ende verschlüsselte Dienste illegale Inhalte. Es widerspricht daher jeglicher Verhältnismäßigkeit, hierfür die Sicherheit sämtlicher Nutzer:innen aufs Spiel zu setzen.

UND EWIG LOCKT DIE SCHLICHTHEIT

EIN KOMMENTAR VON HARALD KAPPER

Wer unter den geneigten Leser:innen schon ein paar Jahre auf Social-Media unterwegs ist oder sich noch an frühere Plattformen - bis hin zurück zum Usenet – erinnert, der kennt den Diskurs, der sich seit jeher um die Verwendung von Pseudonymen oder echten Namen auf Plattformen entsponnen hat.

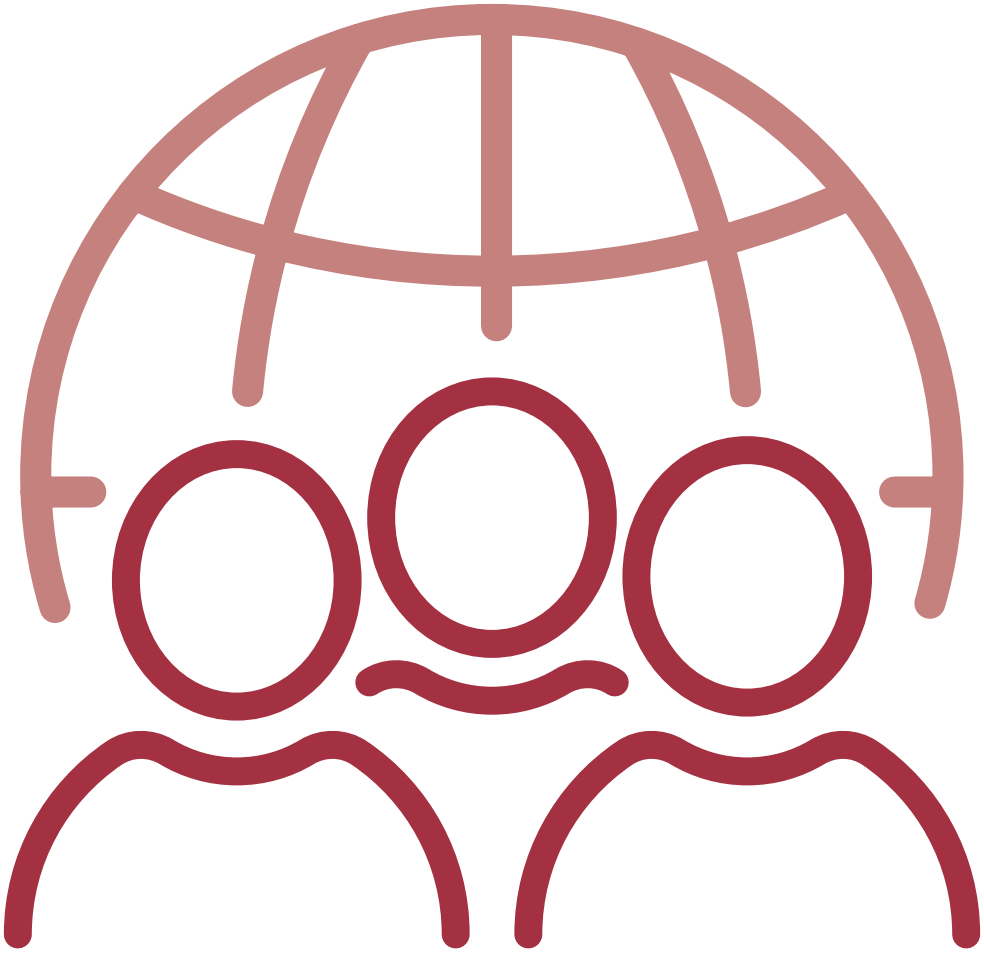
In Österreich rückte dieser vor 10 Jahren in die breitere Öffentlichkeit, als „die Meinungsmutigen“ – eine PR-Initiative – die Werbetrommel für die sogenannte Klarnamen-Pflicht rührte. Die Forschungsfrage, ob die Verwendung des eigenen Namens im Internet zu einer besseren Diskussionskultur führt, kann man rund zehn Jahre später als beantwortet sehen: Mitnichten, die prominenten Verfahren der letzten Jahre zeigen deutlich: Die Sichtbarkeit des eigenen Namens führt bei zahlreichen Menschen nicht zu Zurückhaltung oder gar Höflichkeit.
Damit könnte man die Beweisführung um den vermeintlichen Nutzen von „Klarnamen“ beenden. Allerdings – Österreich 2024 ist Wahlkampfzeit und das ist um Michael Häupl zu bemühen bekanntlich die „Zeit fokussierter Unintelligenz“ und daher bringen ihn einige politische Proponenten wieder auf die Bühne: den Klarnamen als Allheilmittel für einen höflichen und rechtskonformen Umgang im Netz.

Als ISPA haben wir bereits 2014 die Thematik der „Anonymität im Netz“ am „Internet Summit Austria“ umfassend mit Vertretern aus Politik, Medien, Wirtschaft und Zivilgesellschaft diskutiert – und unsere Position geklärt: Wer Klarnamen fordert, fordert effektiv Zensur des Internets, oft aus egoistischen Motiven und verweigert schlicht die Abwägung der Schutz- und Freiheitsrechte von Menschen.

„Aber das Internet darf kein rechtsfreier Raum sein“ – wer im Jahr 2024 noch so einen Satz schreibt oder gar sagt ohne dabei die Schamesröte ins Gesicht getrieben zu bekommen, kann vermutlich auf eine ausgezeichnete Rhetorikschule zurückgreifen oder nähert sich dem Themenkreis ohne jegliche Hintergründe zu kennen.

Besonders der DSA (Digital Services Act der EU) hat hier die unter anderem von der ISPA lange geforderte europäische Lösung für Plattformbetreiber geliefert. Der DSA ermöglicht dabei illegale Inhalte effektiv zu bekämpfen, stärkt die Benutzer:innenrechte mit Hilfe der Beschwerdemechanismen, legt aber auch ganz besonderen Wert auf den Schutz der Grundrechte der Nutzer:innen.

Photo ISPA/APA-Fotoservice/Hörmandiger



Dieser Schutz der Grundrechte ist aber leider allzu oft den selbsternannten „Meinungsmutigen“ kein besonderes Anliegen, es sei denn man sieht sich selbst in diesem Grundrecht. Etwa, dem Grundrecht sich nicht mit vermeintlich anonymen Antworten oder anderen Meinungen zur eigenen Meinung auseinandersetzen zu müssen – oder das Grundrecht Frauen misogyn zu beschimpfen oder andere Menschen mit Ad-hominem-Argumenten anzugreifen. Es gibt im Online-Diskurs leider wirklich selten den Effekt, dass die Kommunikation unter eigenem Namen auch tatsächlich automatisch die Qualität der eigenen Beiträge erhöht.

Es gibt aber auch historisch positive Beispiele – noch vor 10 Jahren meinten mitunter prominente Fernsehsprecher:innen die „Klarnamen“ müssten sein, denn sie lösen das Problem. Tatsächlich bekennen nun viele der damaligen Befürworter: Das war eine krasse Fehleinschätzung, viele Beschimpfungen oder auch Drohungen kommen von Absendern mit Namen und oft auch mit Adresse, die Lösung muss also tatsächlich eine andere sein. Die gute Nachricht: Der DSA sieht auch den Zugang zu Daten für Forschungszwecke vor, hier dürfen wir uns künftig bessere Antworten auf die Frage nach dem rüden Umgang auf Plattformen und seinen Ursachen erwarten.

Wenn es um Grundrechte geht, dann ist besonders ein neuerer Entscheid des EGMR zum Thema Ende-zu-Ende-Verschlüsselung ein klarer Fingerzeig, wie diese im Sinne der EMRK in der digitalen Welt zu verstehen sind.

Der Europäische Gerichtshof hat hier klar für den Schutz der Nutzer:innen-Daten entschieden, ähnliches Gewicht wird wohl auch die Freiheit der Meinungsäußerung haben. Leider – für viele Menschen gibt es diese nur, wenn man sich nicht öffentlich mit seinem Namen zeigen muss. Auch die Idee der Pseudonyme ist mit viel Vorsicht zu bewerten: Datenleaks oder auch missbräuchliche Verwendung von Kundendaten sind keine Unmöglichkeit, gefährden aber möglicherweise Nutzer:innen – und dieses Risiko für Menschen scheint mir schlicht zu hoch, um dafür die Wünsche weniger zu befrieden, man möge doch einen „Klarnamen“ zu einer unangenehmen anderen Sichtweise sehen. Die bessere Option wäre klar: sich einem Argument stellen und nicht in Schlichtheit nach dem Privatleben des anderen zu trachten. ■

STOPLINE

KLEINE MELDESTELLE, GROSSE WIRKUNG

NOCH NIE SO VIELE ZUTREFFENDE MELDUNGEN

Von über 33.000 im Jahr 2023 eingegangenen Hinweisen bei Stopline, der Online-Meldestelle gegen sexuelle Missbrauchsdarstellungen Minderjähriger und nationalsozialistische Wiederbetätigung, wurden knapp 11.000 Inhalte als illegal eingestuft.

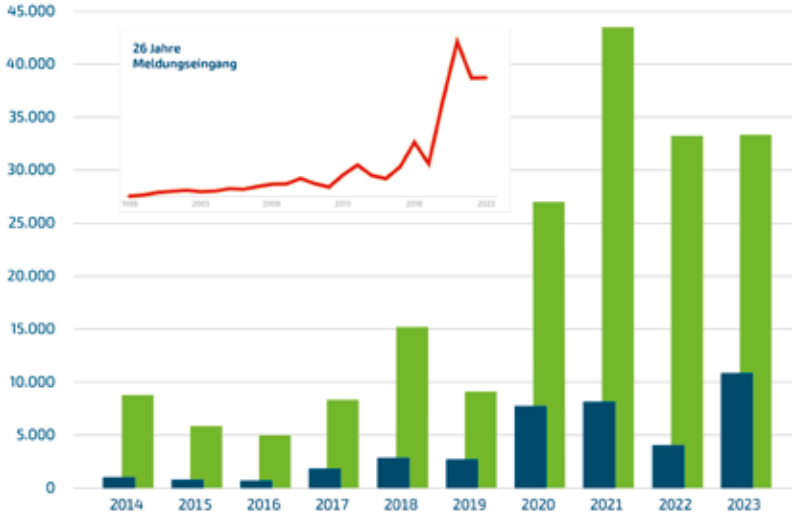
Seit den Corona-Jahren bleiben die Meldungen bei der Stopline konstant hoch. Der aktuelle Stopline Jahresbericht zeigt, dass 2023 insgesamt 33.349 Meldungen zu sexuellen Missbrauchsdarstellungen Minderjähriger und nationalsozialistischer Wiederbetätigung im Internet an Stopline übermittelt wurden. Bei den zutreffenden Meldungen wurde zudem eine neue Höchstmarke erreicht: Von den eingegangenen Meldungen klassifizierten die Mitarbeiter:innen der Stopline 33 % der gemeldeten Inhalte, nämlich 10.850, als tatsächlich gesetzwidrig. Dies entspricht mehr als einer Verdoppelung gegenüber 2022 mit 4.048 illegal eingestuften Meldungen. Bei den zutreffenden Meldungen handelt es sich überwiegend um sexuelle Missbrauchsdarstellungen Minderjähriger (99 %), da hier die Meldebereitschaft der Internet-Nutzer:innen besonders hoch ist.

2023 KEINE HINWEISE ZU ILLEGALEN INHALTEN AUF ÖSTERREICHISCHEN WEBSITES

Österreich ist weltweit seit Jahren zu einem der unattraktivsten Hosting-Standorte für illegale Inhalte geworden. 2023 wurden von Stopline keine Meldungen zu Inhalten auf österreichischen Servern als illegal eingestuft. Stefan Ebenberger, ISPA-Generalsekretär ist überzeugt: „Löschen statt Sperren hat sich als erfolgreiches Modell im Kampf gegen illegale Inhalte bewährt. Es macht sich bezahlt, dass die heimischen Internetanbieter ihre gesellschaftliche Verantwortung wahrnehmen.

Die geteilte Verantwortung zwischen Meldestelle, Providern und Behörden im Kampf gegen illegale Inhalte im Internet ist besonders wirkungsvoll. Denn damit illegale Inhalte im Internet nicht mehr auffindbar sind, ist das rasche Handeln aller Beteiligten erforderlich.“ Die Steigerung der Bekanntheit der österreichischen Meldestelle, die 2023 ihr 25-jähriges Bestehen feierte, ist von großer Bedeutung. Denn nur wenn Internet-Nutzer:innen vermeintlich illegale Inhalte melden, kann Stopline aktiv werden.

Eingegangene vs. zutreffende Meldungen der letzten 10 Jahre (2014-2023)



Grün = Eingegangene / Blau = Zutreffende

Ursprungsländer 2023

STOPLINE IST WESENTLICHER TEIL DES INTERNATIONALEN MELDESTELLEN-NETZWERKS INHOPE

Oberstes Ziel der Stopline ist die schnelle und unbürokratische Entfernung illegaler Inhalte aus dem Internet. Dies ist nicht nur aufgrund der raschen und professionellen Bearbeitung des Stopline Teams möglich. Dank starker Partnerschaften und internationaler Kooperationen kann dieses Ziel Jahr für Jahr erreicht werden.

Da im Jahr 2023 alle, also 100 % der illegalen Inhalte im Ausland gehostet wurden, informierte Stopline in diesen Fällen die Partner-Hotlines im jeweiligen Host-Land. Barbara Schloßbauer, Projektleiterin der Stopline, berichtet stolz: „Obwohl Stopline eine der kleineren Meldestellen im Netzwerk der mittlerweile mehr als 50 weltweiten Partner-Hotlines ist, waren wir eine jener Hotlines, welche die meisten Meldungen zu illegalen Inhalten in die gemeinsame INHOPE Datenbank eingepflegt haben."

Um den Austausch weiter zu fördern, unterstützt Stopline – als Gründungsmitglied von INHOPE – den Ausbau weiterer Partner-Hotlines weltweit.

Barbara Schloßbauer und Stefan Ebenberger präsentierten den Jahresbericht bei der gemeinsamen Pressekonferenz.

ÜBER STOPLINE

Stopline wurde 1998 von der ISPA gegründet und ist eine von den Behörden anerkannte Meldestelle gegen sexuelle Missbrauchsdarstellungen Minderjähriger und nationalsozialistische Wiederbetätigung im Internet. Stopline ist eingebunden in INHOPE, ein weltweites Netzwerk an Meldestellen, das 1999 im Rahmen des Safer Internet Action Plans der Europäischen Kommission gegründet wurde. Finanziell unterstützt wird Stopline von Mitteln des Safer-Internet-Programms der EU und der österreichischen Domain-Registry nic.at.

Photo ISPA/APA-Fotoservice/Hörmandiger

UNREALISTISCHE SCHÖNHEITSIDEALE IM INTERNET

NEUE STUDIENERGEBNISSE BELEGEN DEN DRUCK AUF JUGENDLICHE

In einer zunehmend digitalisierten Welt nehmen soziale Medien und digitale Plattformen einen bedeutenden Raum im Leben der Jugendlichen ein. Durch die dort vorherrschenden scheinbar perfekten Bilder und inszenierten Videos entsteht oft Druck, diesem vermeintlichen Ideal zu entsprechen. Anlässlich des 21. internationalen Safer Internet Day am 6. Februar 2024 präsentierte Saferinternet.at gemeinsam mit Jugendstaatssekretärin Claudia Plakolm Ergebnisse einer neuen Jugendstudie zum Thema „Schönheitsideale im Internet". Jugendliche fühlen sich durch die omnipräsenten idealisierten Körperbilder im digitalen Raum großem Druck ausgesetzt: Über die Hälfte der Befragten würde gerne etwas am eigenen Aussehen ändern, mehr als ein Viertel hat schon einmal über eine Schönheitsoperation nachgedacht. Dabei wird Social Media und insbesondere Influencer:innen ein großer Einfluss auf die Selbstwahrnehmung zugeschrieben. Doch Jugendliche sehen auch Möglichkeiten, sich diesem Druck zu entziehen – zumindest in der Theorie.

DIGITALE BILDERWELTEN VERSTÄRKEN DRUCK AUF JUGENDLICHE

Neu ist der Druck, den solche Idealvorstellungen auf Jugendliche ausüben, nicht: Seit jeher beeinflussen Medien und das persönliche Umfeld besonders stark, wie junge Menschen ihren Körper wahrnehmen. In einer Lebensphase, in der die eigene Identität noch nicht gefestigt ist und Selbstwertgefühle oft nur schwach ausgeprägt sind, können realitätsferne Ansprüche an das Aussehen eine große Belastung darstellen.

GUTES AUSSEHEN FÜR MÄDCHEN UND BURSCHEN WICHTIG

Rund 70 Prozent der befragten Jugendlichen geben an, zumindest „eher zufrieden" mit ihrem Aussehen zu sein. Dennoch gaben mehr als die Hälfte der Befragten an, gerne etwas an ihrem Aussehen ändern zu wollen, wobei Mädchen mit 60 Prozent häufiger diesen Wunsch äußern als Jungen.

Das eigene Aussehen ist allerdings für beide Geschlechter von großer Bedeutung – sowohl offline als auch online. So posten 61 Prozent aller Befragten Fotos bzw. Videos, auf denen sie selbst zu sehen sind, und legen dabei großen Wert auf ihr äußeres Erscheinungsbild. Wichtig ist es ihnen vor allem, schön (68 %), gestylt (64 %) und schlank (54 %) auszusehen. Sich sexy darzustellen, ist für 34 Prozent von Bedeutung, wobei Burschen (40 %) darauf deutlich mehr Wert legen als Mädchen (27 %). Hier zeigt sich, dass der Fokus auf das eigene Aussehen entgegen der weitverbreiteten Annahme längst kein reines Mädchenthema mehr ist. Um möglichst gut auszusehen, nutzen die Jugendlichen Licht, Posen und/oder Handywinkel (54 %) und bearbeiten die Fotos und Videos, zum Beispiel mit Filtern (41 %).

Stefan Ebenberger, Matthias Jax, Claudia Plakolm und Barbara Buchegger führten am Safer Internet Day durch die Studienergebnisse.

EINFLUSS AUF SELBSTWAHRNEHMUNG

Soziale Netzwerke wirken sich auf die Selbstwahrnehmung aus und beeinflussen, ob man sich selbst schön findet oder nicht – dieser Meinung sind zwei Drittel der Jugendlichen (65 %). Insbesondere Mädchen (76 %) und Befragte ab 15 Jahren (78 %) stimmen dieser Aussage zu. Vergleiche mit anderen spielen eine große Rolle – und diesen sind Jugendliche gerade im Internet stark ausgesetzt. Fast drei Viertel (71 %) der Jugendlichen bestätigen, dass die in sozialen Netzwerken konsumierten Bilder dazu führen, dass man sich mit anderen Personen vergleicht. Über ein Viertel (27 %) betont die negativen Folgen und gibt an, sich nach dem Scrollen durch die diversen Social-Media-Feeds schlecht zu fühlen. Vor allem Influencer:innen aus den Bereichen Beauty und Fitness haben einen Einfluss auf Kinder und Jugendliche, meinen

Photo Saferinternet.at/APA-Fotoservice/Juhasz

drei Viertel der Befragten (74 %). Rund die Hälfte (53 %) gibt an, aufgrund entsprechender Bilder schon einmal etwas am eigenen Aussehen geändert zu haben. Ebenso viele Jugendliche haben bereits Produkte gekauft, die von Influencer:innen empfohlen wurden. 28 Prozent haben sogar schon einmal über eine Schönheitsoperation nachgedacht.

BELEIDIGUNGEN BEZÜGLICH DES AUSSEHENS AUCH ONLINE AN DER TAGESORDNUNG

Aber nicht nur der Druck, unrealistischen Schönheitsidealen zu entsprechen, belastet Jugendliche im digitalen Zeitalter. Auch das Risiko von Beleidigungen bezüglich ihres Aussehens im Internet ist allgegenwärtig. 74 Prozent haben eine solche Situation schon einmal beobachtet. Insbesondere Mädchen (84 %) berichten von abwertenden Äußerungen im Internet und in sozialen Netzwerken. Vielleicht spielen auch deshalb Avatare in der digitalen Welt eine zunehmend wichtigere Rolle. Immerhin gibt fast ein Drittel (30 %) an, ein solcher Avatar sollte möglichst gut aussehen.

STRATEGIEN GEGEN DEN SCHÖNHEITSWAHN

Trotz dieser Herausforderungen haben Jugendliche auch Strategien entwickelt, um sich dem Druck, der von diesen unrealistischen Schönheitsidealen ausgeht, zu entziehen. Dazu zählt zum einen die Beschäftigung mit der Selbstwahrnehmung: Als hilfreich wird empfunden, an der Selbstakzeptanz zu arbeiten (67 %), aktiv zu versuchen, sich nicht unter Druck setzen zu lassen (60 %) und zu hinterfragen, warum die konsumierten Inhalte einen selbst stressen oder Druck erzeugen (55 %). Als weitere Strategie nennen die Jugendlichen einen bewussten Umgang mit sozialen Netzwerken. Dazu zählt vor allem, weniger Zeit in sozialen Netzwerken zu verbringen (63 %), Social-Media-Pausen einzulegen (60 %) und gezielt solchen Influencer:innen oder Inhalten zu folgen, die einem gut tun (60 %). Auch gegenseitige Unterstützung wird als relevant empfunden: Sich im Freundeskreis immer wieder Komplimente zum Aussehen zu machen finden 59 Prozent hilfreich, während 38 Prozent dafür plädieren, sich gemeinsam über stressige Inhalte lustig zu machen und darüber zu lachen. Auch wenn sich die Jugendlichen dieser Strategien bewusst sind, können sie diese in der Praxis zum Teil nur schwer umsetzen.

KRITISCHER UMGANG MIT SCHÖNHEITSIDEALEN IST LERNBAR

Um Jugendliche bei einem kritischen Umgang mit Schönheitsidealen im Internet und bei der Entwicklung eines gesunden körperbezogenen Selbstbildes zu unterstützen, sind neben Lehrenden und Onlineplattformen vor allem Eltern gefordert. 57 Prozent der Befragten sind dieser Ansicht. Allerdings verfügen die Eltern oft selbst nicht über ausreichend Medienkompetenz. Sie benötigen nach Meinung der Jugendlichen ebenfalls Unterstützung, damit sie ihre Kinder bei der kompetenten Mediennutzung begleiten können. Den Schulen fällt dabei die Schlüsselrolle zu, auch die Eltern zu erreichen und ihnen Aufklärungsmaterial anzubieten. Gleichzeitig wird die Schule von 47 Prozent auch als wichtiger Ort gesehen, um die Jugendlichen direkt anzusprechen. Möglichkeiten, den Umgang mit Schönheitsidealen im Unterricht zu thematisieren, sehen die Jugendlichen viele. Eine kritische Auseinandersetzung mit dem Thema anzuregen und die Medienkompetenz junger Menschen zu fördern, ist demnach eine entscheidende Aufgabe der Lehrenden. Aber auch die Plattformbetreiber sind gefordert, ein möglichst vielfältiges Angebot für die Nutzer und Nutzerinnen zu schaffen. Die Plattformbetreiber sind sich bewusst, dass unrealistische Schönheitsideale in sozialen Netzwerken die Selbstwahrnehmung von Jugendlichen negativ beeinflussen können. Sie bemühen sich daher laufend, das Nutzungserlebnis für jeden einzelnen positiv zu beeinflussen, zum Beispiel durch die Möglichkeit, persönliche Präferenzen für Inhalte zu treffen. Die Ergebnisse der Studie verdeutlichen die Dringlichkeit, das Bewusstsein für die Auswirkungen von Schönheitsidealen im Internet zu schärfen und gezielte Maßnahmen zu ergreifen, um Jugendliche in ihrer digitalen Lebenswelt zu unterstützen.

SAFERINTERNET.AT UNTERSTÜTZT MIT VIELFÄLTIGEM ANGEBOT

Um Jugendliche bei allen Herausforderungen rund um das körperbezogene Selbstbild zu unterstützen, bietet Saferinternet.at zahlreiche Maßnahmen und Informationsmaterialien an. Im Rahmen von Workshops und Elternabenden, mithilfe einer FAQ-Sammlung zum Thema Selbstdarstellung, diversen Unterrichtsmaterialien und vielem mehr erhalten Interessierte konkrete Hilfestellung und Anregungen zum Thema. Auch die neue ISPA-Broschüre „Schönheitsideale im Internet: Tipps für selbstbewussten Umgang mit Schönheitsidealen in virtuellen Welten“ informiert über das Thema und unterstützt mit Tipps für einen selbstbestimmten Umgang mit körperlichen Idealvorstellungen im Internet und auf sozialen Medien (nähere Informationen zur Broschüren auf S. 34).

ÜBER DIE STUDIE

Die Studie „Schönheitsideale im Internet“ wurde vom Institut für Jugendkulturforschung und Kulturvermittlung im Auftrag des Österreichischen Instituts für angewandte Telekommunikation (ÖIAT) und der ISPA – Internet Service Providers Austria im Rahmen der EU-Initiative Saferinternet.at durchgeführt. Im Befragungszeitraum (Dezember 2023) nahmen 400 Jugendliche im Alter von 11 bis 17 Jahren teil, repräsentativ nach Alter, Geschlecht und Bildungshintergrund. Zusätzlich wurden vier Fokusgruppen-Gespräche mit insgesamt 56 Jugendlichen zwischen 13 und 19 Jahren durchgeführt.

NEUE ISPA-BROSCHÜRE

WIE KÖNNEN WIR MIT UNREALISTISCHEN SCHÖNHEITSIDEALEN IM INTERNET UMGEHEN?

Laut einer aktuellen Studie von Saferinternet.at sehen 65 % der Jugendlichen einen Zusammenhang zwischen Inhalten in Sozialen Netzwerken und dem eigenen Schönheitsempfinden (siehe S. 32-33). Anlässlich des Safer Internet Day am 6. Februar veröffentlichte ISPA eine neue Broschüre mit Tipps im Umgang mit unrealistischen Schönheitsidealen im Internet.

Soziale Netzwerke sind aus der Lebensrealität von Kindern und Jugendlichen nicht mehr wegzudenken. Damit der Umgang mit diesen aber das Selbstbewusstsein stärkt, ist es wichtig, dass sie über die Mechanismen und Herausforderungen im Zusammenhang mit der Selbstwahrnehmung Bescheid wissen.

UNREALISTISCHE DARSTELLUNGEN

Durch den Einsatz von Bildbearbeitungssoftware und automatischen Filtern sind Kinder und Jugendliche in den sozialen Netzwerken mit unrealistischen Körperbildern konfrontiert. Influencer:innen, deren Job es ist, möglichst gut auszusehen, weil sie dadurch Geld verdienen, verzerren mit ihren Inhalten mitunter ebenfalls die Wahrnehmung der Jugendlichen. Ein unreflektierter Umgang mit diesen Inhalten kann dazu führen, dass die eigene Körperwahrnehmung beeinflusst wird. Die neue ISPA-Broschüre klärt über die Phänomene im Zusammenhang mit unrealistischen Schönheitsidealen im Internet auf und gibt praktische Tipps, wie der Druck, der von diesen ausgeht, reduziert werden kann.

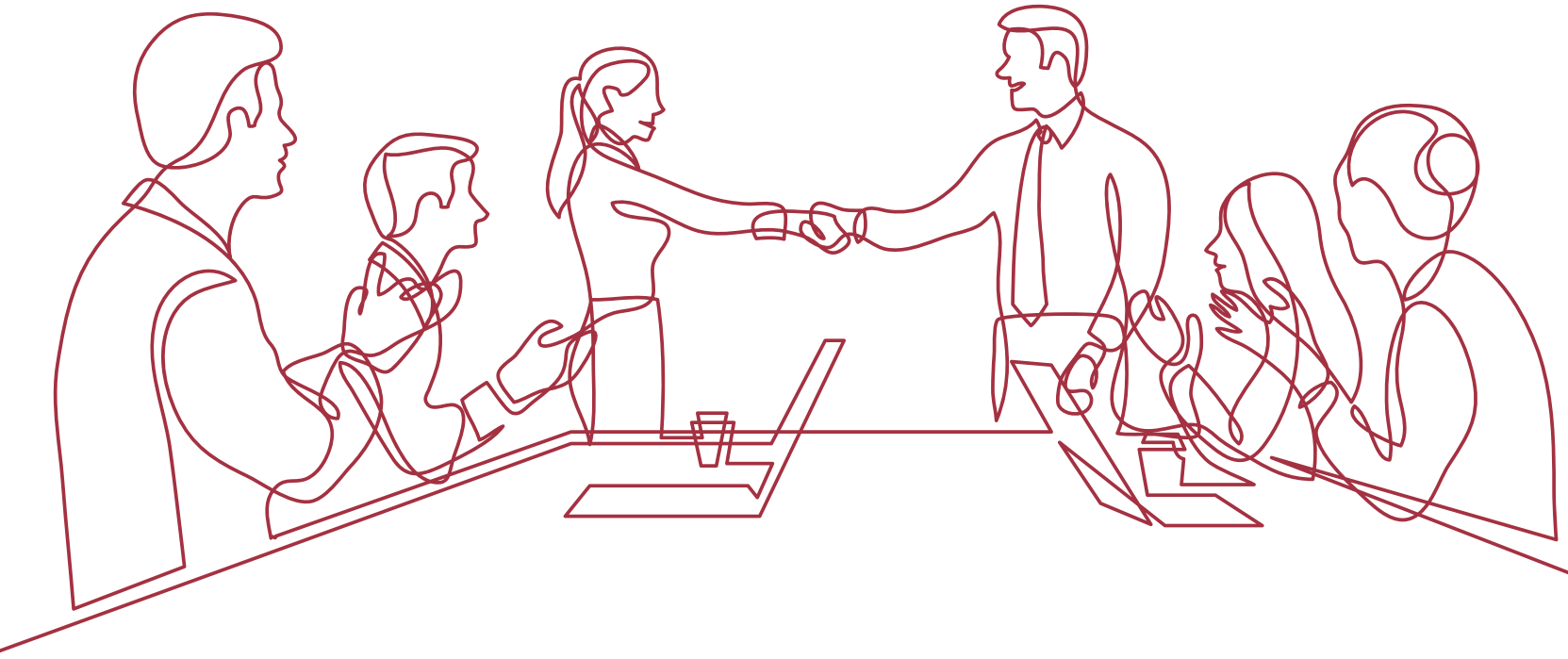
"Unrealistische Schönheitsideale in sozialen Netzwerken können dazu führen, dass Jugendliche eine verzerrte Sicht auf ihren eigenen Körper haben. Die Plattformbetreiben bemühen sich deshalb, die Nutzer:innen mit individuellen Einstellungsmöglichkeiten zu unterstützen. Ein reflektierter und aufmerksamer Umgang mit den Inhalten ist jedoch auch unbedingt notwendig", betont Stefan Ebenberger, ISPA-Generalsekretär.

INDIVIDUELLE EINSTELLUNGEN NUTZEN

Neben der bewussten Auswahl von Accounts und Personen, denen man folgt, können auch die Einstellungen der Apps und des Betriebssystems helfen. Wenn man bemerkt, dass man zu viel Zeit in den sozialen Medien verbringt, kann man z. B. ein Zeitlimit für bestimmte Apps festlegen oder Benachrichtigungen deaktivieren. Darüber hinaus können bestimmte Stichwörter oder Hashtags automatisch aus dem Feed ausgeblendet werden, wenn die Nutzer:innen dies in den Einstellungen festlegen.

BROSCHÜREN KOSTENLOS BESTELLEN

Um digitale Medienkompetenz bei den Nutzer:innen zu fördern, hat ISPA im Rahmen der Initiative Saferinternet.at bereits eine große Anzahl an Informationsmaterialien veröffentlicht. Der neue Folder „Schönheitsideale im Internet" und alle weiteren Broschüren können kostenlos heruntergeladen und ausgewählte in Druckform bestellt werden: **www.ispa.at/broschueren** ■



NEUE ISPA-MITGLIEDER

KOMMUNALBETRIEBE HOPFGARTEN GMBH

Die Kommunalbetriebe Hopfgarten GmbH ist als EVU für die Stromversorgung und den Betrieb des Stromnetzes im Gemeindegebiet von Hopfgarten zuständig, ebenso für die Wasserversorgung und die Abwasserentsorgung. Des Weiteren betreibt die Kommunalbetriebe Hopfgarten GmbH ein öffentliches Kommunikationsnetz. Folgende Technologien kommen zum Einsatz: Glasfaser, Koaxialkabel, 5Ghz Funk, Richtfunk Punkt zu Punkt. Folgende Orte werden versorgt: 6361 Hopfgarten, 6305 Itter, 6364 Brixen im Thale, 6363 Westendorf. In der Abteilung Telekommunikation sind derzeit 5 Mitarbeiter beschäftigt. Im gesamten Unternehmen sind es derzeit 15 Mitarbeiter. Die Marktgemeinde Hopfgarten im Brixental ist zu 100% Eigentümer der Kommunalbetriebe Hopfgarten GmbH.

AUSTRIAN DATA CENTER ASSOCIATION

Der Verein „Austrian Data Center Association“ hat die Aufgabe, die gemeinsamen wirtschaftlichen, technischen, rechtlichen und wissenschaftlichen Interessen der Betreiber, Bauherren und Eigentümer von Rechenzentren zu vertreten. Der Verein strebt an, den Standort Österreich als führenden Standort für die Entwicklung und Präsenz von Rechenzentren zu stärken und eine starke, unabhängige Rechenzentrumsbranche in Österreich zu etablieren.

A.K.I.S. GmbH ACS
Meiselstraße 46/4, 1150 Wien
+43 1 50374 51
akis@akis.at
www.akis.at

abaton EDV-Dienstleistungs GmbH CS
Hans-Resel-Gasse 17, 8020 Graz
+43 5 0240 0
office@abaton.at
www.abaton.at

ACOnet - Vienna University Computer Center A
Universitätsstraße 7, 1010 Wien
+43 1 4277 14030
helpdesk@aco.net
www.aco.net

adRom Media Marketing GmbH CS
Lustenauerstraße 66,
6850 Dornbirn
+43 5522 74813 0
office@adrom.net
www.adrom.net

AGNITAS AG S
Werner-Eckert-Straße 6,
81829 München
+49 89 552908 0
info@agnitas.de
www.agnitas.de

AiNetTelekommunikations-Netzwerk Betriebs GmbH ACS
Burggasse 15, 8750 Judenburg
+43357283146181
office@ainet.st
www.ainet.at

Alpen Glasfaser GmbH A
Handelskai 92, 1200 Wien
+43 1 795850
office@alpenglasfaser.at
www.alpenglasfaser.at

Alphaphone Telekommunikations GmbH AS
Perfektastraße 57/4, 1230 Wien
+43 5 93200
office@alphaphone.at
www.alphaphone.at

Amazon Deutschland Services GmbH CS
Marcel-Breuer-Straße 12,
80807 München
+43 30 303062511
publicpolicy-de@amazon.de
www.amazon.de

ANEXIA Internetdienstleistungs GmbH AS
Feldkirchnerstraße 140,
9020 Klagenfurt am Wörthersee
+43 50 556
info@anexia-it.com
www.anexia.com

Antares-NetlogiX Netzwerkberatung GmbH AS
Feldstraße 13,
3300 Amstetten
+43747265480
office@netlogix.at
www.netlogix.at

APA-IT Informations Technologie GmbH ACS
Laimgrubengasse 10,1060 Wien
+43 1 36060 6060
it-vertrieb@apa.at
www.apa-it.at

APOLLO.AI GmbH S
Poschacherstraße 23/1, 4020 Linz
office@updatemi.com
www.apollo.ai

ARAplus GmbH - Geschäftsbereich Digital ACS
Mariahilfer Straße 123, 1062 Wien
+43 1 2531001 500
michael.lichtenegger@araplus.at
www.araplus.at

Arelion Austria GmbH S
c/o CCFA, Am Heumarkt 10,
1030 Wien
+43 1 205305 17
frank.kirchner@arelion.com
www.arelion.com

artegic AG AS
Zanderstraße 7, 53177 Bonn
+49 228 227797 0
info@artegic.de
www.artegic.com

ATVIRTUAL.NET KG S
Albert Heypeter-Gasse 25,
2301 Gross-Enzersdorf
+43224920277
contact@atvirtual.net
atvirtual.eu

Austrian Data Center Association
Rockhgasse 6/6, 1010 Wien
+43 664 88378955
coffice@austriandatacenter.org
www.austriandatacenter.org

AVM GmbH for International Communication Technology S
Alt-Moabit 95, 10559 Berlin
+49 30 39976 232
ict-info@avm.de
www.avm.de

BBOÖ Breitband Oberösterreich GmbH A
Energiestraße 1, 4020 Linz
office@bbooe.at
www.bboe.at

Ing.ᵐ Claudia Behr C
Stöberplatz 5/3, 1160 Wien
4.369.911.357.969
admin@com-and-com.com
www.com-and-com.com

BK-DAT Electronics e.U. AS
Hieflauer Straße 18,
8790 Eisenerz
+43384860048
info@bkdat.net
www.bkdat.net

Breitbandserviceagentur Tirol GmbH S
Südtiroler Platz 8,
6020 Innsbruck
+43512209309
office@bbsa.tirol
www.bbsa.tirol

Brennercom Tirol GmbH AS
Eduard-Bodem-Gasse 8,
6020 Innsbruck
+43512279279
info@brennercom-tirol.at
www.brennercom.tirol

Bundesrechenzentrum GmbH CS
Hintere Zollamtsstraße 4,
1030 Wien
+43 1 71123 0
office@brz.gv.at
www.brz.gv.at

CC I Communications (CCC.at) AS
Kaiserbrunnstraße 34,
3021 Pressbaum
+43 1 50164 0
office@ccc.at
www.ccc.at

CCD Cogent Communications Deutschland Gmbh Austria Branch AS
Atricom Geb.B, St.6, Lyoner Str 15, 60528 Frankfurt
+49-69-299 896 1026
alexander.valenta@t-mobile.com
www.cogentco.com

China Telecom (Deutschland) GmbH AS
Bockenheimer Landstraße 77,
60325 Frankfurt am Main
+49 69 24003 2929
marketing.germany@chinatele-comglobal.com
www.cteurope.net

Christoph Schmoigl I edvUNION S
Landskrongasse 5/1/1/1,
1010 Wien
+43 1 7108502
cs@edvu.at
www.edv-union.at

CIDCOM Werbeagentur GmbH CS
Wiedner Hauptstraße 78,
1040 Wien
+43 1 4064814 0
office@cidcom.at
www.cidcom.at

Cisco Systems Austria GmbH S
MilleniumTower,
Handelskai 94-96, 1200 Wien
+43 1 24030 6024
hgreiner@cisco.com
www.cisco.at S

Citycom Telekommunikation GmbH AS
Gadollaplatz 1, 8010 Graz
+433168876200
bernd.stockinger@citycom-austria.com
www.citycom-austria.com

CloudNow GmbH AS
Kaiser Josef Platz 52, 4600 Wels
+43 50 152 501
sales@cloudnow.at
www.cloudnow.at

Colt Technology Services GmbH AS
Kärnter Ring 10-12, 1010 Wien
+49 69 56606 6591
christian.weber@colt.net
www.colt.net

comm-IT EDV Dienstleistungsgmbh A
Adamsgasse 1/20, 1030 Wien
+43 1 205210
office@comm-it.at
www.comm-it.at

Compass-Gruppe GmbH CS
Schönbrunner Straße 231,
1120 Wien
+43 1 98116 0
office@compass.at
www.compass.at

comteam it-solutions GmbH AS
Mitterfeldstraße 1,
3300 Amstetten
+43747220580
office@it.comteam.at
www.comteam.at

conova communications GmbH ACS
Karolingerstraße 36A,
5020 Salzburg
+43 662 2200 0
s.kaltenbrunner@conova.com
www.conova.com

CoreTEC IT Security Solutions GmbH S
Ernst Melchior Gasse 24/DG,
1020 Wien
+43 1 5037273 0
m.kirisits@coretec.at
www.coretec.at

COSYS DATA GmbH ACS
Jörgmayrstraße 12,
4111 Walding
+43 1 2299600
office@cosys.cc
www.cosys.cc

CUBiT IT Solutions GmbH. ACS
Zieglergasse 67/3/1 Hoftrakt,
1070 Wien
+43 1 7189880 0
paul.witta@cubit.at
www.cubit.at

cyan Security Group GmbH AS
ICON Tower 24, Wiedner Gürtel 13/16.Stock, 1100 Wien
+43 1 3366911 0
office@cyansecurity.com
www.cyansecurity.com

datenwerk innovationsagentur GmbH CS
Margaretenstraße 70/2/10,
1050 Wien
+43 1 5856071
office@datenwerk.at
www.datenwerk.at

DI Johannes Schulz S
Scheibenbergstraße 19,
1180 Wien
+43 1 3085544
spam@mailplus.co.at
www.mailplus.co.at

DIALOG telekom GmbH & Co KG ACS
Goethestraße 93, 4020 Linz
+43 732 662774 0
rpassecker@dialog-telekom.at
www.dialog-telekom.at

DIC-Online Wolf & Co. KG AS
Innrain 117 1. Stock,
6020 Innsbruck
+43 512 341033 0
office@dic.at
www.dic.at

Digital Realty S
Louis-Häfliger-Gasse 10,
1210 Wien
+43 1 2903636 0
vienna.info@digitalrealty.com
www.digitalrealty.com

digitalnova it & web solutions e.U. S
Krottendorfer Strasse 9a/9,
8052 Graz
+43316225670
office@digitalnova.at
www.digitalnova.at

doloops accessible web technologies GmbH S
Bräuhausgasse 6/2/6,
1050 Wien
+43 1 997430100
office@doloops.net
www.doloops.net

easyname GmbH CS
Canettistraße 5/10, 1100 Wien
+43 1 3532222
office@easyname.com
www.easyname.com/de

echonet communication GmbH CS
Rosenbursenstraße 2/24, 1010 Wien
+43 1 5122695
office@echonet.at
www.echonet.at

Elektrizitätswerk Gösting V. Franz GmbH AS
Viktor-Franz-Straße 13-23,
8051 Graz
+43 316 6077 0
office@ewg.at
www.ewg.at

Empirion Telekommunikations Services GmbH AS
Leonard-Bernstein-Straße 10,
1220 Wien
+43 1 4805000
office@empirion.at
www.empirion.at

Energie AG Oberösterreich Telekom GmbH AS
Böhmerwaldstraße 3,
4021 Linz
+43 5 9000 2575
telekom@energieag.at
www.energieag.at

Energie AG Oberösterreich Vertrieb GmbH A
Böhmerwaldstraße 16, 4020 Linz
+43 5 9000
service@energieag.at
www.energieag.at

Energie Steiermark AG ACS
Leonhardgürtel 10, 8010 Graz
+43 316 9000 0
info@e-steiermark.com
www.e-steiermark.com

EPB IT-Services GmbH CS
Hauptstraße 17, 7051 Großhöflein
+4369912370970
office@epb.at
www.epb.at

Episerver GmbH S
Wallstrasse 16, 10179 Berlin
+49 30 768078 0
infodach@episerver.com
www.episerver.de

MEMBERS
JUNI 2024

Erste Digital GmbH ACS
Am Belvedere 1, 1100 Wien
+43510039637
horst.ganster@erstegroup.com
www.erstegroup.com

eww ITandTEL (Geschäftsbereich der eww Gruppe) ACS
Knorrstraße 10, 4600 Wels
+43724293967100
office@itandtel.at
wholesale.itandtel.at

Facebook Germany GmbH AC
„Sony Center" Kemperplatz 1,
10785 Berlin
+49 30 300145553
politik@fb.com
www.facebook.com/PublicPolicyOfficeBerlin

Farmer Diamonds - IT Service Provider GmbH S
Jensengasse 6, 8010 Graz
+43316375028
office@farmer.diamonds
farmer.diamonds

Faxonline GmbH S
Mariahilferstraße 136, 1150 Wien
+43800802102
info@faxonline.at
www.faxonline.at

Feistritzwerke-STEWEAG GmbH A
Gartengasse 36,
8200 Gleisdorf
+43 3112 2653 0
erich.rybar@feistritzwerke.at
www.feistritzwerke.at

FH des BFI Wien
Maria Jacobigasse 1/3,
1030 Wien
+43 1 72012860 940
info@fh-vie.ac.at
www.fh-vie.ac.at

FH Technikum Wien C
Höchstädtplatz 6, 1200 Wien
+43 1 3334077
info@technikum-wien.at
www.technikum-wien.at

FiberEins TK GmbH AC
Gartengasse 14, 1050 Wien
+43 1 2810281
info@fibereins.at
www.fibereins.at

Flughafen Wien AG AS
Objekt 660, 1300 Wien-Flughafen
+43 1 7007 0
m.dohnal@viennaairport.com
www.viennaairport.com

fonira Telekom GmbH AS
Prager Straße 6, 1210 Wien
+43 1 23400
service@mediainvent.com
www.mediainvent.com

Freewave GmbH A
Premlechnergasse 12/A7, 1120 Wien
+43 1 8040134
office@freewave.at
www.freewave.at

FunkFeuer Wien - Verein zur Förderung freier Netze AS
Laudongasse 15-19, c-o
Volkskundemuseum Wien,
1080 Wien
admin@funkfeuer.at
www.funkfeuer.at

Futureweb GmbH CS
Innsbruckerstraße 7,
6380 St. Johann in Tirol
+43 5352 65335 0
info@futureweb.at
www.futureweb.at

Gamsjaeger Kabel-TV & ISP Betriebs GmbH AS
Unterauer Straße 7, 3370 Ybbs
+43741252249
office@wibs.at
www.wibs.at

GANZRUND Informatik GmbH CS
Doblhoffgasse 7, 1010 Wien
+43 5 1709
info@ganzrund.com
ganzrund.com

Gemeindewerke Telfs GmbH ACS
Bahnhofstraße 40, 6410 Telfs
+43526262330
office@gwtelfs.at
www.gwtelfs.at

GiGaNet.at, Bernhard Kröll AS
Rauchenwald 651, 6290 Mayrhofen
+435285630850
office@giganet.at
www.giganet.at

Google Austria GmbH
Graben 19/9, 1010 Wien
+43 1 23060 6001
press@google.com
www.google.at

GXperts GmbH S
Richtergasse 7/5, 1070 Wien
+43 1 2362933
info@g-experts.net
www.g-experts.net

HALLAG Kommunal GmbH AS
Augasse 6, 6060 Hall in Tirol
+43522358552100
m.kofler@citynet.at
www.citynet.at

Heliot GmbH AS
Am Belvedere 10 / QBC2b, 1100 Wien
+43 1 9346081
info@heliot.at
www.heliot.at

helloly GmbH S
Rainerstraße 25, 4020 Linz
+43732350023
office@helloly.com
www.helloly.com

homeway GmbH AS
Liebigstraße 6,
96465 Neustadt bei Coburg
+49 9568 8979 30
info@homeway.de
www.homeway.de

HostCube e.U. S
Ruppersthal 30, 3701 Großweikersdorf
+43720880806
office@hostcube.at
hostcube.at

HostProfis ISP Telekom GmbH AS
Hans-Sittenberger-Straße 13,
9500 Villach
+4359900202
oberdorfer@hostprofis.com
www.hostprofis.com

hosttech GmbH AS
Warwitzstraße 9, 5020 Salzburg
+43720511333
postfach@hosttech.at
www.hosttech.at

hotze.com GmbH AS
Eduard-Bodem-Gasse 6, 6020 Innsbruck
+43512353640
office@hotze.com
www.hotze.com

Huawei Technologies Austria GmbH CS
Wagramer Str. 19, 9. Stock, 1220 Wien
+43 1 211 80871 0
feiyun.chen@huawei.com
e.huawei.com/at/

Huemer Data Center Ges.m.b.H. ACS
Leonard-Bernstein-Straße 10,
1220 Wien
+436644118000
walter.huemer@huemer-it.com
www.huemer-dc.com

Hutchison Drei Austria GmbH ACS
Brünner Straße 52, 1210 Wien
+43 5 0660 0
serviceteam@drei.at
www.drei.at

HXS GmbH AS
Ungargasse 37, 1030 Wien
+43 1 3441344
office@hxs.at
www.hxs.at

IForce IT GmbH ACS
Richtergasse 4 / Lokal, 1070 Wien
+43 1 9076344 300
office@iforce.at
www.iforce.at

ifunk.at AS
Gaisberg 5, 4175 Herzogsdorf
+43720345488
office@ifunk.at
www.ifunk.at

IKARUS Security Software GmbH S
Blechturmgasse 11, 1050 Wien
+43 1 58995
pichlmayr.j@ikarus.at
www.ikarus.at

Incom Technologies Kft. A
Pajkos u. 23 1LH 2/14,
1119 Budapest
+36 1 222
info@incom-technologies.hu
www.smartwifi.hu

Infotech EDV-Systeme GmbH AS
Schaerdinger Straße 35,
4910 Ried im Innkreis
+43 7752 81711 0
office@infotech.at
www.infotech.at

Innosoft GmbH AS
Speckbacherstraße 12,
6380 St. Johann
+435352207207
d.hirschbichler@innosoft.at
www.innosoft.at

Innospiration GmbH S
Kiningergasse 18/1,
1120 Wien
nikolaus.futter@innospiration.at
www.innospiration.at

Innsbrucker Kommunalbetriebe AG AS
Langer Weg 29,
6020 Innsbruck
+435125026410
kundenservice@ikb.at
www.internet.ikb.at

Institut für empirische Sozialforschung (IFES) GmbH C
Teinfaltstraße 8, 1010 Wien
+43 1 54670
wasserbacher@ifes.at
www.ifes.at

internic Datenkommunikations GmbH S
Puchsbaumplatz 2/7-8,
1100 Wien
+43 1 3249685
info@internic.at
www.internic.at

IP Austria Communication GmbH AS
Wienerbergstrasse 11/ B16,
1100 Wien
+43 50 662 0
office@ipaustria.com
www.ipaustria.at

IPAX OG AS
Barawitzkagasse 10/2/2/11,
1190 Wien
+43 1 3670030
office@ipax.at
www.ipax.at

ipcom GmbH S
Karlsplatz 1, 1010 Wien
+436641445686
office@ipcom.at
www.ipcom.at

iPlace Internet & Network Services GmbH ACS
Ringstraße 5, 1. Stock,
6830 Rankweil
+43555220500
office@iplace.at
www.iplace.at

ITEG IT-Engineers GmbH S
Salurner Straße 18,
6020 Innsbruck
+436763674710
office@iteg.at
www.iteg.at

IT-Technology Gesellschaft für industrielle Elektronik und Informations-technologie mbH S
Grillgasse 18, 1110 Wien
+43 1 229922 0
office@it-technology.at
www.it-technology.at, www.talk2u.at

IT-world ITW GmbH AS
Brunner Straße 29/6/2,
1230 Wien
+437202733700
office@it-world.eu
www.it-world.eu

JM-DATA Telekom GmbH AS
Hackl-Straße 1 / Objekt 2,
4050 Traun
+43 50 305080
office@jm-data.at
www.jm-data.at

Jumper GmbH ACS
Industriestraße 1/14,
2100 Korneuburg
+43 2262 236401 0
office@jumper.at
www.jumper.at

KABEL TV AMSTETTEN GMBH AS
Kruppstraße 3, 3300 Amstetten
+43 7472 66667 0
office@ktvam.at
www.ktvam.at

kabelplus GmbH AS
Südstadtzentrum 4,
2344 Maria Enzersdorf
+43 5 0514 0
ispa@kabelsignal.at
www.kabelplus.at

KAPPER NETWORK-COMMUNICATIONS GmbH - kapper.net ACS
Alserbachstrasse 11/6,
1090 Wien
+43 1 3195500 0
info@kapper.net
www.kapper.net

Kaufmann Ges.m.b.H A
Goldenkrongasse 9
3500 Krems an der Donau
+43273285625
office@ktv-krems.at
www.ktv-krems.at

K-Businesscom AG AS
Wienerbergstrasse 53,
1120 Wien
+43 50 811
info@k-business.com
k-business.com

k-digital Medien GmbH & Co KG C
Leopold-Ungar-Platz 1, 1190 Wien
+43 1 52100 0
service@kurier.at
kurier.at

Kelag A
Arnulfplatz 2, 9020 Klagenfurt
+43463525
kundenservice@kelag.at
www.kelag.at

kitznet - Stadtwerke Kitzbühel ACS
Jochberger Straße 36,
6370 Kitzbühel
+43535665651
office@stwk.kitz.net
www.kitz.net

Kommunalbetriebe Hopfgarten GmbH ACS
Kühle Luft 2, 6361 Hopfgartenl
+43 5335 2500
office@kbh.at
www.kbhnet.at

KraftCom Service GmbH ACS
Göstling 108,
3345 Göstling / Ybbs
+437484257012
office@kraftcom.at
www.kraftcom.at

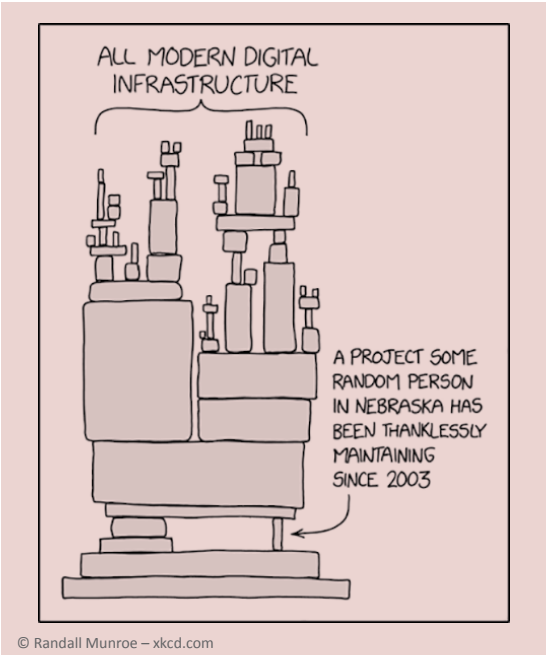
Kreativwirtschaft Austria C
Wiedner Hauptstraße 63,
1045 Wien
+43 5 90900 0
gertraud.leimueller@wko.at
www.kreativwirtschaft.at

KT-NET Communications GmbH ACS
Ramingdorf 51, 4441 Behamberg
+43 7252 77852 10
office@kt-net.at
www.kt-net.at

Kumi Systems e.U. ACS
Gartengasse 22/7/3, 8010 Graz
+43800093004
office@kumi.systems
kumi.systems

Ledl.net GmbH ACS
Lederergasse 6,
5204 Straßwalchen
+43621520888
office@domaintechnik.at
www.domaintechnik.at

Leitstelle Tirol gemeinnützige GmbH ACS
Hunoldstraße 17 a,
6020 Innsbruck
+435123313
it@leitstelle.tirol
www.leitstelle.tirol



Licht- und Kraftvertrieb der Gemeinde Hollenstein/Ybbs AS
Walcherbauer 2,
3343 Hollenstein an der Ybbs
+43 7445 218 16
lkv@hollenstein.at
www.oganet.at

LINZ AG Telekom AS
Wiener Straße 151, 4021 Linz
+4373234007315
m.past@linzag.at
www.linzag-telekom.at

LinzNet Internet Service Provider GmbH AS
Landwiedstrasse 211, 4020 Linz
+437322360
office@linznet.at
www.linznet.at

LIWEST Kabelmedien GmbH. AS
Lindengasse 18, 4040 Linz
+43732942424
guenther.singer@teamliwest.at
www.liwest.at

Magenta Telekom A
Rennweg 97-99, 1030 Wien
+43 1 79585 0
impressum@magenta.at
www.magenta.at

MakeNewMedia Communications GmbH ACS
Sandleitengasse 17, 1160Wien
+43 1 338333 0
sales@makenewmedia.com
www.makenewmedia.com

Mass Response Service GmbH AS
Donau-City-Straße 7;
DC Tower 1, 38th floor, 1220 Wien
+43 1 2702825
office@massresponse.com
www.massresponse.com

MediaClan - Gesellschaft für Online Medien G.m.b.H. CS
Nestroyplatz 1/1/14a,
1020 Wien
+43 1 4075060 0
office@mediaclan.at
www.mediaclan.at

mieX GmbH - Mühlviertler Internet Exchange AS
Markt 8, 4153 Peilstein
+43 5 9008 008
office@miex.at
www.miex.at

MMC Kommunikations-technologie GesmbH ACS
Mühlgasse 14/E,
2353 Guntramsdorf
+4322363903
office@mmc.at
www.mmc.at

ms-cns Communication Network Solutions GmbH A
Scheydgasse 34-36, 1210 Wien
+43 1 2703070
office@ms-cns.com
www.ms-cns.com

Multikom Austria T elekom GmbH AS
Jakob-Haringer-Straße 1,
5020 Salzburg
+43 59 333 1000
office@xlink.at
www.xlink.at

mur.at - Verein zur Förderung von Netzwerkkunst ACS
Leitnergasse 7, 8010 Graz
+43 316 821451 26
verein@mur.at
www.mur.at

myNET gmbh AS
Bruggfeldstraße 5, 6500 Landeck
+43676841810300
hh@mynet.at
www.mynet.at

myWorld International AG S
Grazbachgasse 87-91, 8010 Graz
+4331670770
office@myworld.com
corporate.myworld.com

NA-NET Communications GmbH AS
Laaer Straße 44,
2135 Neudorf im Weinviertel
+43 2572 20233 0
office@nanet.at
www.nanet.at

nemox.net Informations-technologie OG AS
Eduard-Bodem-Gasse 9,
6020 Innsbruck
+43 5 0234 0
info@nemox.net
nemox.net

NeoTel Telefonservice GmbH & Co KG S
Esterhazygasse 18a/15,
1060 Wien
+43 1 4094181 0
office@neotel.at
www.neotel.at

Nessus GmbH ACS
Fernkorngasse 10/3/501,
1100 Wien
+43 1 3360006
fs@nessus.at
www.nessus.at

Net4You Internet GmbH ACS
Tiroler Straße 80,
9500 Villach
+4342425005
office@net4you.net
www.net4you.net

netelligenz S
Felbigergasse 101 Tür 6,
1140 Wien
ke@netelligenz.at
www.netelligenz.at

NETPLANET GmbH ACS
Louis-Häfliger-Gasse 10,
1210 Wien
+43 1 3430343
billing@netplanet.at
www.netplanet.at

Netzware Handels- und IT-Dienstleistungs GmbH AS
Davidgasse 85-89, 1100 Wien
+43 1 3577777
office@netzware.at
www.netzware.at

next layer Telekommunikations-dienstleistungs- und BeratungsGmbH AS
Mariahilfer Gürtel 37/7, 1150 Wien
+43 5 1764 0
office@nextlayer.at
www.nextlayer.at

nfon GmbH S
Linzer Straße 55,
3100 St. Pölten
+43274275566
office.at@nfon.net
www.nfon.at

nöGIG Service GmbH A
Stattersdorfer Hauptstraße 56/2,
3100 St. Pölten
+43274230750767
office@noegig.at
www.noegig.at

Nöhmer GmbH AS
Gahberggasse 19,
4861 Schörfling am Attersee
+4376623131
office@expert-noehmer.at
www.expert-noehmer.at

Nokia Solutions and Networks Österreich GmbH AS
Leonard-Bernstein-Straße 10,
1220 Wien
+43 05 70020
office.vienna@nokia.com
www.nokia.at

Ocilion IPTV Technologies GmbH ACS
Schaerdinger Straße 35,
4910 Ried im Innkreis
+43 7752 2144 0
office@ocilion.com
www.ocilion.com

OeKB - Oesterreichische Kontrollbank AG CS
Strauchgasse 3, 1011 Wien
+43 1 53127 2175
ewald.jenisch@oekb.at
www.oekb.at

öGIG GmbH A
Europaplatz 7, 3100 St. Pölten
436.649.652.372
office@oegig.at

ÖIAT - Österreichisches Institut für angewandte Telekommunikation C
Ungargasse 64-66/3/4/404,
1030 Wien
+43 1 5952112 0
office@oiat.at
www.oiat.at

oja.at GmbH ACS
Adi-Dassler Gasse 6,
9073 Viktring
+43463597597
office@oja.at
www.oja.at

OmanBros.com Internetdienstleistungen GmbH CS
Guglgasse 8/2/85, 1110 Wien
+43 1 9690304 0
office@omanbros.com
www.omanbros.com

onelayer it-solutions e.U. AS
Hirschstettner Straße 19-21
Objekt G,
1220 Wien
+43 1 4120156
office@onelayer.at
onelayer.at

Orange Business Austria GmbH AS
Laxenburgerstrasse 2 / 1 / 4,
1100 Wien
+43 1 36037 0
josef.canete@orange.com
www.orange-business.com

ORF Online und Teletext GmbH & Co KG C
Hugo-Portisch-Gasse 1,
1136 Wien
+43 1 50277 21300
online@orf.at
www.orf.at

Ortswärme St. Johann in Tirol GmbH A
Speckbacherstraße 33
6380 St. Johann in Tirol
+43535220766
office@ortswaerme.info
www.ortswaerme.info

Österreichische Post Aktiengesellschaft AC
Rochusplatz 1, 1030 Wien
+43 57767 0
kundenservice@post.at
www.post.at

Peter Rauter GmbH ACS
Bahnhofstr. 11, 5202 Neumarkt
+43 6216 5721 0
rauter@rauter-it.at
www.rauter-it.at

pflaeging.net CS
In den Jochen 49,
2122 Ulrichskirchen
+4369914107990
office@pflaeging.net
www.pflaeging.net

PPTV GmbH A
Egger-Weg 9,
4582 Spital am Pyhrn
+43756321800
office@pptv.at
www.pptv.at

Preisvergleich Internet Services AG C
Rothschildplatz 3, 1020 Wien
+43 1 5811609
markus.nigl@geizhals.at
www.geizhals.at

quattroSEC GmbH CS
Zipf 65, 4871 Zipf
+43 1 268444
office@quattrosec.com
www.quattrosec.com

quintessenz A
c/o quartier21 / MQ,
Museumsplatz 1 (Electric Avenue),
1070 Wien
office@quintessenz.org
www.quintessenz.org

Raiffeisen Informatik GmbH & Co KG ACS
Lilienbrunngasse 7 - 9,
1020 Wien
+43 1 99399 0
info@r-it.at
www.r-it.at

RAITEC GmbH S
Goethestraße 80, 4020 Linz
+4373269291507
johannes.bachleitner@raitec.at
www.raitec.at

RDI Solutions e.U. AS
Spratzeck 10, 2812 Hollenthon
+4326457481
office@rdi.at
www.rdi.at

Riepert Informations-technologie GmbH AS
Bad Kreuzen 95,
4362 Bad Kreuzen
+4372665901
g.riepert@riepert.at
www.riepert.at

RIS GmbH AS
Im Stadtgut A1, 4407 Steyr-Gleink
+43 7252 86186 0
info@ris.at
www.ris.at

roNet GmbH AS
Ahornweg 9, 4150 Rohrbach
+436769112777
office@ronet.at
www.ronet.at

RTCnow Streaming Services GmbH CS
Renngasse 5/ Top 11,
1010 Wien
+43 50 955
ispa@rtcnow.com
www.rtcnow.com

Russmedia Digital GmbH ACS
Gutenbergstraße 1,
6858 Schwarzach
+435572501727
webmaster@austria.com
werbung.vol.at

Russmedia IT GmbH ACS
Gutenbergstraße 1,
6858 Schwarzach
+435572501735
webmaster@vol.at
highspeed.vol.at

Salzburg AG für Energie, Verkehr und Telekommunikation AS
Bayerhamerstraße 16,
5020 Salzburg
+4366288842776
markus.wiedhoelzl@salzburg-ag.at
www.salzburg-ag.at

SBR-net Consulting AG S
Parkring 10/1/10, 1010 Wien
+43 1 5135140 0
ruhle@sbr-net.com
www.sbr-net.com

servus.at - Kunst & Kultur im Netz CS
Kirchengasse 4, 4040 Linz
+43732731209300
office@servus.at
www.servus.at

simpli services GmbH & Co KG AC
Hugo-Portisch-Gasse 1, 1136 Wien
+43 1 8760760 13503
office@simpliTV.at
www.simpliTV.at

SIPit Kommunikations-management GmbH AS
Scherzergasse 12/1, 1020 Wien
+43 1 342342
office@sipit.at
www.sipit.at

siplan gmbh ACS
Angererweg 3, 6271 Uderns
+43524264519
office@siplan.at
www.siplan.at

sourceheads Information Technology GmbH S
Bräuhausgasse 6/2/6, 1050 Wien
+43 1 917 417 0
info@sourceheads.com
www.sourceheads.com

Speed Connect Netzwerks-errichtungs GmbH A
Karl-Farkas-Gasse 22/7. OG,
1030 Wien
+43 1 9089501109
procurement@speed-connect.at
www.speed-connect.at

SPÖ Informations-technologiezentrum S
Windmühlgasse 26, 1060 Wien
+43 1 53427 283
office@itz.spoe.at
www.spoe.at

Stadtwerke Feldkirch AS
Leusbündtweg 49,
6800 Feldkirch
+4355229000
kundencenter@stadtwerke-feldkirch.at
www.stadtwerke-feldkirch.at

Stadtwerke Imst ACS
Pfarrgasse 3, 6460 Imst
+43541263324
stadtwerke@stwimst.at
www.cni.at

Stadtwerke Kapfenberg GmbH AS
Stadtwerkestraße 6,
8605 Kapfenberg
+43 3862 23516 0
ispa@hiway.at
www.hiway.at

Stadtwerke Klagenfurt Aktiengesellschaft AS
St. Veiter Straße 31,
9020 Klagenfurt am Wörthersee
+43463521603
guenter.glaboniat@stw.at
www.stw.at

Stadtwerke Kufstein GmbH A
Fischergries 2,
6330 Kufstein
+43 5372 69303 23
schuster@stwk.at
www.kufnet.at

Stadtwerke Wörgl Ges.m.b.H. AS
Zauberwinklweg 2a,
6300 Wörgl
+43 50 6300 30
steinwender@stww.at
www.stww.at

STANDARD Verlagsgesellschaft m.b.H. C
Vordere Zollamtsstraße 13,
1030 Wien
+43 1 53170 0
redaktion@derStandard.at
www.derStandard.at

Streams Telecommunications-services GmbH AS
Wasserzeile 27,
3400 Klosterneuburg
+43224331340
office@streams.at
www.streams.at

StuOnline Internet Service AS
Neuhofweg 8, 9560 Feldkirchen
+43 4276 5121 0
info@stuonline.at
www.stuonline.at

Summit Solutions GmbH CS
Egon Schiele-Gasse 54,
3400 Klosterneuburg
+43 1 2532213
office@summitsolutions.at
www.summitsolutions.at

SysUP IT GmbH & Co KG S
Herrgottwiesgasse 149/2,
8055 Graz
+43 59222 0
office@sysup.at
www.sysup.at

Tele-Tec GmbH AS
Gerasdorferstrasse 139/1C,
1210 Wien
+43 1 2566604 0
office@tele-tec.at
www.tele-tec.at

TeleTronic Telekommunikations Service GmbH AS
Am Concorde Park 1/C5,
2320 Schwechat
+43 1 2810000
office@teletronic.at
teletronic.at

telitall.net GmbH
Gewerbepark C2 2821
Lanzenkirchen +43
57 745745 office@telitall.net
www.telitall.net

TikTok C
Stralauer Allee 2, 10245 Berlin
491.766.125.250
melanie.ohnemus@tiktok.com
www.tiktok.com

TMS IT-Dienst S
Hinterstadt 2, 4840 Vöcklabruck
+43720501078
office@tms-itdienst.at
www.tms-itdienst.at

toscom - Philipp Kobel S
Breiteneckergasse 32,
1230 Wien
+43720116606
office@toscom.at
www.toscom.at

Tripple Internet Content Services CS
Florianigasse 54/2-5, 1080 Wien
+43 1 406 5927 0
office@tripple.at
www.tripple.at

TTG Tourismus Technologie GmbH S
Freistädter Straße 119,
4041 Linz
+437327277333
karl.mitteregger@ttg.at
www.ttg.at

Türk Telekom International AT GmbH S
campus 21, Europaring F13,
Ebene 3, 2345 Brunn am Gebirge
+43 1 6999408 0
office@turktelekomint.com
www.turktelekomint.com

ufdroht.net Internet Service GmbH ACS
Beim Gräble 2,
6800 Feldkirch
+43552270154
office@ufdroht.net
www.ufdroht.at

Unwired Networks GmbH ACS
Gonzagagasse 11/2/5/25,
1010 Wien
+43 1 9962051
office@unwired.at
www.unwired.at

upstreamNet Communications GmbH AS
Ruckergasse 30-32, 1120 Wien
+43 1 2128644 0
office@upstreamnet.at
www.upstreamnet.at

Ventocom GmbH AS
Baumgasse 60B, 1030 Wien
+43 1 9320677
info@ventocom.at
www.ventocom.at

VERBUND Services GmbH ACS
Am Hof 6A, 1010 Wien
+43 50 313 50901
office.dt@verbund.com
www.verbund.com

Verizon Austria GmbH AS
Handelskai 340, 1023 Wien
+43 1 72714 0
tech-support@at.verizonbusiness.com
www.verizonbusiness.com/at/

ViPweb.at Th. Dorn ACS
Kerpengasse 69, 1210 Wien
+43 1 27145 50
office@vipweb.at
www.vipweb.at

virtual-business
Hoelzelgasse 8, 1230 Wien
+436767062299
office@vibu.at
www.vibu.at

webagentur.at Internet Services GmbH ACS
Beethovengasse 4-6,
2500 Baden
+432252259892
office@webagentur.at
www.webagentur.at

web-crossing GmbH CS
Eduard-Bodem-Gasse 8,
6020 Innsbruck
+43512206567
info@web-crossing.com
www.web-crossing.com

webLyzard technology gmbh CS
Liechtensteinstraße 41/26,
1090 Wien
+43 1 8909063
info@weblyzard.com
www.weblyzard.com

Wien Energie GmbH A
Thomas-Klestil-Platz 14, 1030 Wien
+43 1 4004 8100
herbert.schmitt@wienenergie.at
www.wienenegie.at

Wiener Zeitung GmbH C
Maria-Jacobi-Gasse 1, 1030 Wien
+43 1 20699 290
wolfgang.riedler@wienerzeitung.at
www.wienerzeitung.at

willhaben internet service GmbH & Co KG
Landstraßer Hauptstraße 97-101 / Bürozentrum 1,
1030 Wien
info@willhaben.at
www.willhaben.at

WNT Telecommunication GmbH AS
Richard-Strauss-Straße 43,
1230 Wien
+43 1 6163090
office@wnt.at
www.wnt.at

World4You Internet Services GmbH S
Hafenstraße 35, 4020 Linz
+4373293035
office@world4you.com
www.world4you.com

WVNET Informations und Kommunikations GmbH AS
Edelhof 3, 3910 Zwettl
+43 2822 57003 0
sales@wvnet.at
www.wvnet.at

www.funknetz.at LE GmbH AS
K01 Business Park, Industriestrasse 1/Büro 11,
2100 Korneuburg
+43 2262 236401 0
office@funknetz.at
www.funknetz.at

XINON GmbH AS
Fladnitz im Raabtal 150,
8322 Studenzen
+43312720500
jantscher@xinon.at
www.xinon.at

XQueue GmbH S
Christian-Pleß-Straße 11-13,
63069 Offenbach am Main
+49 69 83008980
info@xqueue.com
www.xqueue.de

yuutel GmbH S
Leonard-Bernstein-Straße 10/17 - Saturn Tower, 1220 Wien
+438002404010
service@yuutel.at
www.yuutel.at

ispa

A Access C Content S Services

Schon abonniert?
Der neue
ISPA-Newslettter!

Anmelden!

Internet
Summit
Austria

12.09.2024

VORMERKEN:

ISPA-GENERALVERSAMMLUNG
14.11.2024