VOICE - Bundesverband der IT-Anwender e.V.

FAIRE MARKTBEDINGUNGEN
BÜROKRATIEABBAU
DIGITALE SOUVERÄNITÄT

VOICE
Bundesverband der
IT-Anwender e.V.

Positionen zur Bundestagswahl
'21

12 Forderungen zur Bundestagswahl

VOICE e.V.
Marktbedingungen für IT- und Digital-Anwenderunternehmen verbessern

VOICE-Positionen zur Bundestagswahl: Marktbedingungen für IT- und Digital-Anwenderunternehmen verbessern

VOICE – Bundesverband der IT-Anwender e.V. hat gemeinsam mit seinen 400 Mitgliedern und ihren 2600 Unternehmen 12 Positionen formuliert, die die wichtigsten Anforderungen der Anwenderunternehmen an die Politik adressieren. Dabei geht es einerseits um verbesserte Marktbedingungen also mehr Produktvielfalt und Wettbewerb unter den Anbietern, weniger Lasten und Risiken sowie mehr Rechte für die Anwenderseite. Das gilt zum Beispiel für mehr Herstellerverantwortung für die Qualität ihrer Produkte, mehr Mitsprache bei Standards oder einfachere Softwareverträge.

Zum anderen verlangt VOICE Nachbesserungen für das AÜG, die DSGVO und das IT-Sicherheitsgesetz, um die Gesetze handhabbarer und aufwandsärmer zu gestalten und so den Interessen der vielen Tausend Anwenderunternehmen in Deutschland besser gerecht zu werden.

Kurzübersicht der VOICE-Forderungen:

Verbesserte Marktbedingungen, stärkere digitale Souveränität

1 Offene Standards für mehr Wettbewerb

Mit der Durchsetzung offener Standards den Wettbewerb stärken.
- Nutzung offener Standards insbesondere für Softwareschnittstellen und Datenaustauschformate erzwingen
- Pflege und Weiterentwicklung der offenen Standards durch paritätisch von Anwendern und Anbietern besetzte Gremien

2 Mehr Innovation für mehr digitale Souveränität

Gezielte Förderung digitaler Innovationen und Know-how-Aufbau für alle Wertschöpfungselemente der Digitalisierung.
- Einsatz europäischer IT-Komponenten gezielt fördern
- Förderung des Produkt-Reifeprozesses durch konstruktives Feedback von Anwendern
- Praxisorientierte Innovationspartnerschaften initiieren

3 GAIA-X muss europäisch bleiben

Digitale Souveränität: Bei GAIA-X in der Startphase ausschließlich Anbieter aus Europa einbeziehen.
- Vorzugsweise mittelständische europäische Anbieter in Führungsrollen bringen
- Schnelle Umsetzung durch Fokus auf Kernfunktionalitäten

4 Anbieter haften für ihre Produkte

Produkthaftung für Softwareprodukte auch im B2B-Geschäft.
- Anbieter haften für direkte und indirekte Schäden durch Produktmängel
- Qualitätsmängel bei IT-Security-Produkten als besonders schwerwiegend bewerten

5 Produktsicherheit wird Pflicht für Anbieter

IT-Security: Software und Cloudservices müssen sicher gestaltet sein.

- Strafbewehrte Verpflichtung von Software- und Internetanbietern zu hoher Produktqualität (Stand der Technik)
- Fehlerbeseitigung muss schnell erfolgen
- Aufwand für Anwenderseite minimal halten

6 Einfachere Softwareverträge

Regulierung der Software-Nutzungsverträge und Lizenzvereinbarungen.

- Verträge vereinfachen
- Einseitige Änderungsmöglichkeiten einschränken
- Unrechtmäßige Nutzung technisch ausschließen, um Audits überflüssig zu machen

7 Hilfen für Start-ups

Hands-on-Förderung verbessern.

- Ausbildung unternehmerischer Fähigkeiten gezielt unterstützen
- Coaching junger Unternehmen fördern
- Entrepreneurship-Lehrgänge flächendeckend in Hochschulen anbieten

8 Datenverkehr im Internet konsequent schützen

Sicherheit im Internet erhöhen, „Autokennzeichen und Leitplanken für das Web".

- Breite deutsche/europäische Initiative der Politik für mehr Sicherheit im Datenverkehr
- Aktiv gestaltende Rolle der Regierung bei der Weiterentwicklung des Internets zu einer sicheren Basisinfrastruktur der Wirtschaft
- Nachweisplichten für Kommunikationsteilnehmer (Server, Router und Netzknoten)
- Nachweispflichten für Domain-Halter (Vorbild: Handelsrecht)

9 Flexible Arbeitsformen erlauben

Arbeitnehmerüberlassungsgesetz (AÜG): Höchstüberlassungsdauer für Leiharbeitnehmer in der IT-Branche abschaffen.

- Leiharbeitnehmer mehr als 18 Monate für einen Kunden
- Rechtliche Voraussetzungen für weitere flexible Arbeitsformen schaffen

10 DSGVO Schutz vor Datenmissbrauch

DSGVO Schutz vor Datenmissbrauch wirksamer gestalten und Digitalisierung erleichtern.

- Datenverarbeitung bei konsequenter Einhaltung von Sicherheitsmaßnahmen erlauben und fördern
- Analysen als dedizierte Dienstleistung für den Datenlieferanten erleichtern
- De-Anonymisierung konsequent verbieten

Weniger Bürokratie, präzisere Regeln

11 IT-Sicherheitsgesetz 2.0 praxistauglich machen

Unterstützung statt Sanktionierung

- Anwenderunternehmen in Ausführungspraxis einbeziehen
- Meldepflichten handhabbar machen
- Klare und langfristig geltende Definition der betroffenen Unternehmen festlegen

12 BetrVG: Mitbestimmungsprozess bei IT-Systemen vereinfachen

- Präzisierung des § 87 Betriebsverfassungsgesetz, um Rechtsunsicherheit beim Einsatz von IT-Systemen zu beseitigen.
- Mitbestimmung auf Funktionen mit Gestaltungsspielraum beschränken.
- Festlegen, welche Systemfunktionen und Auswertungsmethoden erlaubt sind.
- Vorwegnahme von Updates erlauben.

Die 12 VOICE-Forderungen im Detail

Verbesserte Marktbedingungen, stärkere digitale Souveränität

1

IT-Märkte: Mit offenen Standards den Wettbewerb stärken.

VOICE fordert die Förderung offener Standards für flexible Software-Schnittstellen und Datenaustauschformate zwischen den Plattformen großer Softwareanbieter und anderer Softwarelösungen im Interesse der Anwender.

Eine der wesentlichen Ursachen für das derzeitige Marktversagen im Bereich der großen Plattformanbieter liegt in der Verwendung von proprietären, ausschließlich von einzelnen Herstellern kontrollierten Software-Schnittstellen (Application Programming Interfaces=APIs), an die auf der Nutzerseite hohe Investitionen vor allem in die Systemkonfiguration, ergänzende Teilfunktionen und die Prozessgestaltung gebunden sind.

Sogenannte Offene Standards für Software-Schnittstellen werden von Nutzern und Herstellern gemeinsam kontrolliert und sind ohne Vorbedingungen auch durch neue Marktteilnehmer nutzbar. Aufgrund ihrer hohen Langzeitstabilität und der angestrebten Aufwärts- bzw. Abwärtskompatibilität senken sie die Eintrittsrisiken für neue Wettbewerber und verringern die Abhängigkeit der Kunden von einzelnen Anbietern. Offene Standards stellen deshalb einen der wesentlichen Garanten für funktionierende Märkte dar.[1]

Um die für die Erarbeitung und Pflege offener Standards benötigten Gremien aufzubauen bzw. zu stärken, fordert VOICE ein Eingreifen der Bundesregierung bzw. des Gesetzgebers, mindestens in der Initialphase. Nur so kann bei den herrschenden Marktbedingungen der überbordende Einfluss einzelner Anbieter kompensiert werden.

Des Weiteren muss die öffentliche Hand als Vorreiter die Verwendung offener Standards fördern, indem diese in Ausschreibungen zur Bedingung gemacht werden.[2] Ein flächendeckender und konsequenter Einsatz ermöglicht kontinuierliche, intensive Rückmeldungen an die Standardisierungsgremien, um die fortwährende Optimierung zu ermöglichen.

Offene Standards für Software—Schnittstellen in diesem Sinne müssen folgende Eigenschaften aufweisen:

- Sie ermöglichen eine unwiderrufliche, freie Nutzung ohne Vorbedingungen. Ihre Definition ist folglich eine vorkommerzielle, gemeinnützige Aktivität der interessierten Marktteilnehmer.
- Sie sind vollständig und verständlich dokumentiert und für alle Marktteilnehmer gleichermaßen frei zugänglich.
- Die Weiterentwicklung folgt einem transparenten und öffentlich nachvollziehbaren Entscheidungsprozess, der insbesondere das Feedback der verschiedenen Nutzergruppen einbezieht und der von Fachexperten überprüft werden kann.
- Im Weiterentwicklungs- und Pflegeprozess liegt ein Schwerpunkt auf der Gewährleistung maximaler Kompatibilität neuer Versionen mit den im Markt befindlichen Anwendungen, sodass für alle Marktteilnehmer eine hohe Investitionssicherheit entsteht.
- Softwaremodule, die von den offenen Standards Gebrauch machen, können dabei Open-Source oder proprietär sein, solange sie an allen Schnittstellen den offenen Standards folgen.
- In die Standardisierung ist dabei insbesondere auch die Schnittstelle zwischen dem menschlichen Anwender und den Softwaresystemen mit einzubeziehen.

Zu den bevorzugt zu standardisierenden Schnittstellen gehören insbesondere Dateiformate zur Übertragung von Datenobjekten zwischen Softwaremodulen (.vcf, .ics, .odf, .step etc.).[3] Wo es gelungen ist, solche Formate zu stabilen Standards zu entwickeln, hat dies sehr positiv zur Produktvielfalt und zum Wettbewerb beigetragen.

[1] In einigen Marktsegmenten werden solche offenen Standards bereits sehr erfolgreich eingesetzt (Hardware-Interface in Server-Systemen, USB-Peripheriegeräte etc.). In diesen Segmenten ist der resultierende Wettbewerb hoch und die Qualität folglich erfreulich hoch.

[2] Die britische Regierung hat die Verwendung offener Standards bereits 2018 definiert: https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles

[3] Dateiformate als offene Standards gibt es seit vielen Jahren. Ihre strikte Anwendung in kommerziellen Softwareprodukten wurde aber bisher nicht eingefordert. Öffentliche Auftraggeber müssen dies jetzt erzwingen, da die Umgehung insbesondere durch die Marktführer einer der wichtigsten Gründe für die starke ungewollte Bindung der Bestandskunden an diese Marktführer darstellt. Formate, die bereits in paritätisch besetzten Konsortien weiterentwickelt werden (.vcf = RFC 6350 und .ics = RFC 5545) leisten bereits einen sehr guten Beitrag zur Kompatibilität zwischen Softwaremodulen verschiedener Hersteller und tragen somit sehr viel zu einem funktionierenden Wettbewerb bei.

2

Digitale Souveränität: gezielte Förderung digitaler Innovationen und Know-how-Aufbau für alle Wertschöpfungselemente der Digitalisierung.

VOICE fordert die gezielte Förderung des Einsatzes europäischer IT-Komponenten zur Erhöhung der Unabhängigkeit und zur Belebung und Diversifizierung des Wettbewerbs in den Schlüsseltechnologien der Digitalisierung.

Digitale Infrastrukturen benötigen eine große Anzahl missionskritischer Schlüsseltechnologien, von denen derzeit nur ein kleiner Teil durch europäische Anbieter auf Augenhöhe mit ihren asiatischen und US-amerikanischen Wettbewerbern erbracht werden kann. Dies führt –zusätzlich zu den ohnehin vorhandenen negativen Effekten der Oligopole- zu außenpolitischen Abhängigkeiten und somit zu zusätzlichen Risiken für die Anwenderunternehmen. Zudem schränkt die Abhängigkeit die diplomatische Handlungsfähigkeit der EU gegenüber den anderen Wirtschaftsmächten massiv ein.

Die in den vergangenen Jahren verfolgte Förderpolitik mit Fokus auf Forschung und Innovationen reicht dabei nicht aus. Trotz exzellenter Spitzenforschung und eines hohen Innovationsgrades ist die Etablierung von Anbietern mit nennenswertem Marktanteil bislang nur in Ausnahmefällen gelungen. Was fehlt ist ein flächendeckender praktischer Einsatz der neuen IT-Produkten als bewusste Unterstützung des Reifeprozesses. Dabei kommt den Anwenderunternehmen auch die Aufgabe einer konstruktiven Rückmeldung für Optimierungen zu.

3

Digitale Souveränität: Bei GAIA-X in der Startphase ausschließlich Anbieter aus Europa einbeziehen.

VOICE fordert, das Projekt für eine eigenständige europäische Daten-Infrastruktur, GAIA-X, in den kommenden ersten Jahren vorzugsweise für mittelständische europäische Anbieter und Anwender zu öffnen.

Das Projekt GAIA-X hat zum Ziel, den Wettbewerb im Markt der Cloud-Plattformanbieter auch für mittelständische europäische Anbieter zu öffnen. Ziel ist es dabei, die bestehende Dominanz einzelner großer Plattformen mittels eines auf offenen Standards basierenden Software-Stacks (dem sog. Sovereign Cloud Stack) zu neutralisieren. Es ist klar, dass dies nicht im Geschäftsinteresse der hierdurch beschränkten Großanbieter sein kann. Bei einer Teilnahme dieser Anbieter, muss ferner von einem krassen Ungleichgewicht bzgl. der Ressourcen und des initialen Know-hows ausgegangen werden, was einer gedeihlichen Zusammenarbeit zwangsläufig entgegensteht. Herausforderungen im Aufbau des Standards sind keinesfalls auf der technischen, viel mehr aber auf der organisationspsychologischen Seite zu erwarten. Der Erfolg hängt letztlich von einem ausgeglichenen Kräfteverhältnis unter den Partnern ab.

VOICE fordert deshalb, diese Anbieter nicht an dem Konsortium zu beteiligen, sondern vorzugsweise mittelständische, europäische Anbieter in eine Führungsrolle zu bringen.
Dabei muss der Fokus auf die wenigen tatsächlich benötigten Kernfunktionalitäten gelegt werden, anstatt durch eine zu große Servicepalette Tempo zu verlieren.

Eine Mitarbeit der großen Anbieter ist dann anzustreben, wenn die erarbeiteten Standards im Markt etabliert und deren Einsatz insbesondere auf Seiten der Beschaffer als mandatorisch definiert ist.

4

Weitgehende Produkthaftung für Softwareprodukte auch im B2B-Geschäft.

VOICE fordert die konsequente Durchsetzung einer Haftung der Softwarehersteller für direkte und indirekte Schäden bei Anwenderunternehmen, die durch Qualitätsmängel entstehen.

Softwareprodukte haben für die Geschäftstätigkeit von Unternehmen und die staatlichen Verwaltungsprozesse eine überragende Bedeutung erlangt. Ihre Qualität bestimmt sowohl den Betriebsaufwand als auch die Sicherheitsrisiken. Dabei kann ein in der Entwicklung eingespartes Personenjahr leicht das zehnfache an Aufwand auf Seiten der Betreiber hervorrufen.[4] Anders als in anderen Industrien (Automobilbau, Anlagenbau) gibt es bisher jedoch keinen monetären Anreiz für Softwareanbieter, die Qualität ihrer Produkte auf einem hohen Niveau zu halten.

Die VOICE Mitglieder sehen die zusätzlichen Investitionen in die Entwicklung mit den folglich höheren Lizenzkosten als volkswirtschaftlich sinnvoll und als deshalb geboten an. Der finanzielle Anreiz für Softwarehersteller, in die Qualität ihrer Produkte zu investieren, muss durch entsprechende Vertragsstrafen und Schadensersatzansprüche geschaffen werden. Dabei sind insbesondere Sicherheitslücken in Produkten mit expliziten Sicherheitsaufgaben (Firewalls, Intrusion

4 Die heute als selbstverständlich hingenommenen, komplexen Prozeduren beim Update von Unternehmenssoftware machen in den Anwenderunternehmen den Einsatz hoch spezialisierter Fachkräfte sowie Betriebsunterbrechungen notwendig, obwohl bei entsprechenden Investitionen in die Produktentwicklung sowohl die Anzahl der Updates als auch der jeweils erforderliche Aufwand drastisch gesenkt werden könnte. Dass dies möglich ist, beweisen Produkte von kleinen Marktteilnehmern bzw. die Updateverfahren im Consumerbereich, bei denen Expertenwissen auf Kundenseite per se ausgeschlossen ist.

Detection / Prevention, Virenschutz) als besonders schwerwiegend zu bewerten und entsprechend zu ahnden. Die relevanten Gesetze und insbesondere die Rechtsprechung muss eine vereinfachte Durchsetzung der Ansprüche ermöglichen.

5

IT-Security: Software-Anbieter und Internetprovider müssen den Stand der Technik bzgl. minimaler Häufigkeit, Schnelligkeit und Handhabbarkeit von Sicherheitslücken erfüllen.

VOICE fordert die strafbewehrte Verpflichtung der Softwareanbieter und der Internetprovider zu angemessenen Maßnahmen zur Vermeidung von Fehlfunktionen bzw. zur zügigen, aufwands- und störungsfreien Beseitigung im Fehlerfall.

Die derzeitigen gesetzlichen Vorgaben zur Cybersicherheit beziehen sich nahezu ausschließlich auf die Verantwortlichkeiten der Anwenderunternehmen. Sie unterliegen Sorgfalts- und Meldepflichten (IT-Sicherheitsgesetz), tragen Verantwortung dafür, dass die von ihnen eingesetzte Technologie auf dem Stand der Technik befindet (z.B. Solvency 2) und selbstverständlich dafür, dass nachträgliche Fehlerbeseitigungen und die Schließung von Sicherheitslücken (Patches) zeitnah in die laufende IT-Umgebung eingespielt werden. Gleiches gilt im Bereich des Datenschutzes und der Internetsicherheit.

Um das bestehende Ungleichgewicht zu beseitigen, fordert VOICE die Verpflichtung der Software- und Serviceanbieter sowie der Internetprovider zu konkreten Maßnahmen zur Vermeidung bzw. zur zügigen Beseitigung von Sicherheitslücken. Der Gesetzgeber muss sie dazu verpflichten:

- den Stand der Technik bei der Produkt- und Servicequalität zu gewährleisten.
- bei auftretenden Sicherheitsmängeln diese binnen einer festgelegten zeitlichen Frist zu beheben und für das Ausbringen der entstehenden Patches einfache und betriebssichere Verfahren zur Verfügung zu stellen.
- die bekannten und erprobten Schutzmechanismen (z.B. DNSSEC) verpflichtend einzusetzen.

6

Regulierung der Software-Nutzungsverträge und Lizenzvereinbarungen.

VOICE fordert die Vereinfachung der Lizenzverträge sowie die Einschränkung von einseitigen Änderungsmöglichkeiten bzw. erweiterte Bindungs- und Ankündigungsfristen. Außerdem fordert VOICE von den Anbietern die unrechtmäßige Nutzung von lizenzierter Software sicher auszuschließen.

Die Lizensierung von Software und das Management von Software-Nutzungsverträgen nimmt im IT-Betrieb in Unternehmen und Verwaltung inzwischen einen signifikanten Anteil der Ressourcen in Anspruch. Dies ist auf zahlreiche einseitige Änderungen der Bedingungen und auf Vertragsklauseln mit zweifelhafter Rechtsgültigkeit zurückzuführen, die in den Anwenderunternehmen zu Unsicherheit und Managementaufwand führen.[5]

Aus Sicht der Anwenderunternehmen sind große Teile dieser Aufwände verzichtbar, wenn die zulässigen Vertragskonstruktionen gesetzlich detailliert geregelt würden. Dass dies bislang nicht durch den Wettbewerbsdruck selbst geschieht, ist auf das oben erläuterte Marktversagen zurückzuführen. Um dennoch einen rechtssicheren und vor allem aufwandsarmen IT-Betrieb zu ermöglichen, muss der Gesetzgeber entsprechende Vorgaben zu erlaubten Vertragsmodellen machen. Dabei sind insbesondere Vertragsänderungen zur Einschränkung der Nutzung und Veräußerung zu regeln bzw. die entsprechenden Klauseln explizit für rechtens/ nicht rechtens zu erklären sowie die erlaubten Änderungen im prinzipiellen Lizenzmodell (CPU-basiert, Concurrent User, Named User etc.) auf ein faires Maß zu beschränken.

Der Aufwand für das Lizenzmanagement lässt sich vor allem dadurch verringern, dass die Software selbst auf technischem Wege einen Missbrauch ausschließt (z.B. durch Lizenzschlüssel bzw. Token). Sofern eine Software nicht durch unzulässige Manipulation (sog. Crack) verändert wird, darf eine missbräuchliche Nutzung nicht möglich sein.

Zur Vereinfachung des Softwaremanagements muss die Vorinstallation der vollständigen Software (z.B. auf Arbeitsplatzrechnern) erlaubt sein, ohne dass dies im gleichen Zuge Lizenzkosten nach sich zieht. Erst die Installation des Lizenzschlüssels führt zur Inanspruchnahme der Softwarefunktion und somit zur Zahlungspflicht.

Sowohl auf Seiten der Anwenderunternehmen als auch bei den Herstellern von Softwareprodukten ist ein kontinuierlicher Cash-Flow wirtschaftlich vorteilhaft. Lizenzmodelle mit zeit- oder intensitätsbasierter Subskription („pay as you go") sind deshalb gegenüber Kaufoptionen zu bevorzugen. Sie schließen außerdem Konflikte über die Veräußerung von Kauflizenzen von vornherein aus. Entsprechend sind solche Abonnement-Verträge in den gesetzlichen Regelungen zu begünstigen.

[5] CISPE, ein europäischer Verband von Cloud-Anbietern (unter den Mitliedern ist unter anderem aws) hat gemeinsam mit dem französischen Anwenderverband und VOICE-Partnerverband CIGREF 10 Regeln für faire Software-Lizenzen für Cloud-Nutzer veröffentlicht. https://www.fairsoftware.cloud/principles/

7

Start-ups: Hands-on-Förderung verbessern.

VOICE fordert, digitale Start-ups intensiver und direkter zu fördern. Um gezielt Innovationen in Technologie und bei digitalen Geschäftsmodellen zu fördern, muss die deutsche und europäische Administration Mechanismen zur Förderung digitaler Start-ups entwickeln, die über steuerliche Anreize und bürokratische Vereinfachungen für Investoren und Gründer hinausgehen.

Insgesamt stagniert die Zahl der Start-Ups in Deutschland. Im Jahr 2020 waren es laut Förderbank KfW rund 70000 – nicht mehr als im Jahr 2018. Und das trotz der Tatsache, dass die Bundesregierung in den vergangenen Jahren das Gründen entbürokratisiert hat und verschiedene finanzielle Anreize für Investoren entwickelt hat (zum Beispiel Abschreibungsmöglichkeiten).

Zwar spielt Zugang zu Finanzierungskapital eine wichtige Rolle für Start-ups, aber die Gründe, warum Start-ups zu 80 bis 90 Prozent scheitern, liegen Experten zufolge eher an unternehmerischen Aspekten: fehlende fachliche und soziale Kompetenz des Gründerteams, fehlender Kundennutzen des Produkts oder des Service; ein zu kleines oder zu wenig belastbares Netzwerk; eine zu geringe Skalierbarkeit, um starkes Wachstum zu unterstützen.

Genau in diesen Aspekten sollten die Gründer stärker unterstützt werden. Mit Beratung und Coaching zum Beispiel durch erfahrene Praktiker (VOICE bietet das Start-ups mit CIOs an), flächendeckenden Enterpreneurship-Lehrgängen an den Hochschulen besonders in Ingenieur- und Informatikstudiengängen, sowie begleitenden Ausbildungsmöglichkeiten in Sachen praktischem Management und Führung. Außerdem sollte der Bund Startups in der Gründungsphase mit leicht finanzierbaren Marktstudien unter die Arme greifen.

8

Sicherheit im Internet erhöhen, „Autokennzeichen und Leitplanken für das Web".

VOICE fordert eine breit angelegte Initiative der deutschen / europäischen Politik zur Verbesserung der Sicherheit im Datenverkehr. Die Regierung muss eine starke, gestaltende Rolle in der Weiterentwicklung des Internets übernehmen.

Das Internet als bestimmendes Infrastrukturelement der modernen Wirtschaft ist in immer stärkerem Maße von organisierter Kriminalität belastet. Mit steigendem Wertschöpfungsanteil des Datenverkehrs werden die Bedrohungen zum missionskritischen Faktor für die zunehmend digitalen Geschäftsmodelle. Viele Funktionalitäten und Kommunikationskanäle mit an sich hohem Komfort für den Kunden können inzwischen aufgrund der steigenden Gefahr nicht mehr genutzt werden.[6]

Bisherige Ansätze mit Schutz der Geschäftsprozesse stellen fast ausschließlich auf Härtung der zentralen Server und der Endgeräte bzw. auf eine verbesserte Ausbildung der Anwender (Awareness-Schulung) ab. Unternehmen sind darauf angewiesen, aufwendige eigene Überwachungseinrichtungen vorzuhalten, um kriminellen Datenverkehr zu detektieren und sich dagegen zu schützen.

Bisher wurden aber noch keinerlei Maßnahmen ergriffen, um den Datenverkehr insgesamt sicherer zu gestalten. Im Gegenteil: Viele in den letzten Jahren eingeführte Funktionalitäten (Umlaute und Sonderzeichen in URLs, dynamische IP-Adress- und DNS-Namensverwaltung) haben die Gesamtsicherheit dramatisch verschlechtert.[7] Große Marktteilnehmer behelfen sich mit Spezialdienstleistern, die kriminelle Aktivitäten von Akteuren automatisiert verfolgen.

VOICE fordert die Bundesregierung auf, zusammen mit den Europäischen Partnern in der Festlegung und Normung der Protokolle im Datenverkehr eine aktive Rolle zu übernehmen und –analog zum Straßenverkehr und zum Handelsrecht- die Nachweisplichten für Kommunikationsteilnehmer (Server und Router[8]) und die Nachvollziehbarkeit der Kommunikationswege endlich zu verbessern. Zudem ist den Anwendern durch eindeutige Kennzeichnung der tatsächlichen Herkunft von Nachrichten und Dateien in Bedienoberflächen eine Beurteilung der Sicherheitslage zu erleichtern. Der Einsatz der bereits vorhandenen Sicherheitsmechanismen[9] für den Datenverkehr im WAN bzw. zwischen geografischen Zonen ist durch entsprechende Regelungen als verpflichtend festzulegen.

VOICE fordert die Bundesregierung auf, über entsprechende internationale Normungsverfahren folgende Sicherheitsmaßnahmen anzugehen:

- Einschränkung des (ohnehin ausreichend großen) Namensraumes, sodass Betrug mittels ähnlich klingender URL-Bezeichner leichter erkannt werden kann,

[6] Banken und Paketdienste können zum Beispiel mit ihren Kunden nur noch begrenzt interagieren, da (berechtigtes und unberechtigtes) Misstrauen dies torpediert.

[7] So können Angreifer mit wechselnden Serverbezeichnungen Datenflüsse leicht umlenken und durch Verwendung zum Beispiel diakritischer Zusatzzeichen (Accents etc.) täuschend ähnliche aber betrügerische URLs schaffen.

[8] Die Identitäten der betreffenden Personen sind hiervon unberührt.

[9] Wie DNSSec,STARTTLS, zertifikatbasierte Serverkommunikation etc.

- Einschränkung des Wechsels von DNS-Eintragungen zwischen IP-Adressräumen[10] (analog der Namensänderung oder des Sitzes eines Unternehmens im Handelsregister) und insbesondere die Aufnahme der Wechselhäufigkeit als Merkmal der betreffenden Domäne, sodass diese als Sicherheitsmerkmal genutzt werden kann,
- Verpflichtung der Anbieter zur eindeutigen Sichtbarmachung der Herkunft einer Nachricht in der Benutzeroberfläche, um Betrug leichter erkennbar zu machen,
- Verpflichtung der Registrare (z.B. denic für die .de-Domäne), Domänenanmeldungen im Vorhinein auf Seriosität zu prüfen (analog des Handelsregisters bzw. Post-Ident-Verfahren) und Betrugsgefahren durch Anwendung von Ähnlichkeitsmaßen bereits bei der Anmeldung einzudämmen,
- Feste Kopplung der Kennungen von Internetknoten an ihre geografische Lage, um die betrügerische Umleitung von Datenverkehr (BGP-Hijacking) auszuschließen,
- Anreicherung der Kommunikationsprotokolle mit zertifikatsbasierten Informationen zum Übertragungsweg von Datenflüssen.

Hierzu ist in einem neu zu schaffenden Bundesministerium für Digitalisierung ein dedizierter Bereich einzurichten, der die deutschen Aktivitäten in allen Normungsgremien für IT-Technologie (W3C, CEN/CLC/ETSI, ISO/IEC etc.) bündelt und koordiniert. Hierzu muss das Ministerium mit industrieunabhängigen, spezialisierten Technologieexperten bzw. mit dem Zugang zu solchen Ressourcen aus der deutschen Wissenschaft ausgestattet werden.

Weniger Bürokratie, präzisere Regeln

9

Arbeitnehmerüberlassungsgesetz (AÜG): Höchstüberlassungsdauer für Leiharbeitnehmer in der IT-Branche abschaffen.

VOICE fordert die Überarbeitung des AÜG dahingehend, dass Leiharbeitnehmer in der IT-Branche oberhalb eines festgelegten Mindeststundensatzes nicht unter die Höchstüberlassungsgrenze des Arbeitnehmerüberlassungsgesetz (AÜG) fallen.

Experten[11] gehen davon aus, dass das 2017 in Kraft getretene Arbeitnehmerüberlassungsgesetz 2023 novelliert werden muss.

Im heute geltenden AÜG ist die zeitliche Grenze für die Überlassungsdauer auf 18 Monate festgelegt. Viele erfolgskritische externe Personalressourcen in IT-Projekten müssen aber für einen erheblich längeren Zeitraum verfügbar bleiben, um unnötige Einarbeitungsprozesse und die komplizierte Auswahl immer neuer Spezialkräfte zu vermeiden. Die Höchstgrenze gefährdet die seit langem etablierte und sehr erfolgreiche Co-Innovation in der IT- und Digitalszene. Zum Teil arbeiten freie IT-Berater und freiberufliche Entwickler (gemeinsam mit festangestellten Kolleginnen und Kollegen ihrer Auftraggeber) über Jahre hinweg an einem großen IT-Projekt oder an einer Reihe kleinerer Projekte. Viele IT-Freiberufler arbeiten zudem für Personaldienstleister, die sie dann „verleihen". Die durch das Gesetz beabsichtigte Schutzwirkung für eigentlich abhängig Beschäftigte wird in diesem Bereich nicht benötigt, da eine Festanstellung regelmäßig unattraktiver ist, als die selbständige Beschäftigung.

Denn anders als Zeitarbeitskräfte in der Industrie-, Lebensmittel- und Dienstleistungsbranche verdienen freie ITler weit überdurchschnittlich. Durch die hohe Entwicklungsgeschwindigkeit und den hohen Innovationsdruck leidet der IT-Markt bereits seit Jahren unter einem starken Fachkräftemangel. Dieser wird sich durch die Digitalisierung von Wirtschaft und Gesellschaft weiter erhöhen, mit der Folge, dass die Nachfrage nach IT-Freiberuflern und IT-Beratern in den nächsten Jahren weiter ansteigen wird und diese daher weitgehend die Bedingungen für ihr Engagement selbst bestimmen können.

Die Mehrzahl der IT-Freiberufler hat den Status des „Freien" zudem bewusst gewählt. So können sie in der Regel, die Projekte auswählen, die ihnen die besten Bedingungen bieten. Außerdem gehen Freiberufler davon aus, ihre investierte Arbeitszeit besser kontrollieren zu können als festangestellte Kollegen.

IT-Freiberufler und -Berater gehören also keineswegs zu den Beschäftigten des Niedriglohnsektors, die der Gesetzgeber zu Recht schützen will.

VOICE fordert deshalb, die Höchstüberlassungsdauer des AÜG auf überdurchschnittlich bezahlte Freiberufler nicht mehr anzuwenden.
Ferner müssen die arbeitsrechtlichen Voraussetzungen geschaffen werden, damit agile Teams aus IT-Anwendern, IT-Dienstleistern und Beratern flexibel auch über längere Zeiträume zusammenarbeiten können, ohne rechtliche Risiken in Kauf nehmen zu müssen.

[10] Redundanzbedingte Wechselmöglichkeiten können vorher festgelegt und bekannt gegeben werden, willkürliche Sprünge im Sekundentakt müssen aber als Verlust an Seriosität ausgewiesen werden.

[11] https://www.arbeitsblog.de/themen/artikel/aueg-welche-aenderungen-stehen-2023-bevor/

10

Datenschutz: Illegale Nutzung wirksam verhindern, Datenverarbeitung erleichtern.

VOICE fordert, Datenschutzregelungen stärker gegen unerwünschte und missbräuchliche Analysen (z.B. Financial Scoring, Health Scoring, Persönlichkeitsprofile) auszurichten, anstatt weiterhin die Erfassung von Daten so stark einzuschränken.

Die Datenschutzgrundverordnung ist geprägt vom Prinzip der Datensparsamkeit. Dieser in Deutschland Ende der 80iger Jahr postulierte Grundsatz resultiert vor allem aus der Absicht, einem möglichen Missbrauch durch staatliche Stellen den Riegel vorzuschieben. Damals hatten Unternehmen den Wert von Daten noch nicht entdeckt. Das ist heute diametral anders. Daten sind für Unternehmen neben Kapital, Arbeit und Rohstoffen zu einem vierten Produktionsfaktor geworden und zunehmend sind sie in der einen oder anderen Form personenbeziehbar.

Ziel muss es also sein, die Verarbeitung und Nutzung dieses Produktionsfaktors auch für europäische Unternehmen zu ermöglichen und dabei die informationelle Selbstbestimmung der Bürger zu wahren und gleichzeitig Rechtssicherheit für die verarbeitenden Unternehmen herzustellen. Ansätze hierzu sind:

- Erlaubnis zu Auswertungen, wenn die Rückverfolgung der Ursprungsdaten sicher ausgeschlossen werden kann
- Kontrolle der Auswertung statt generelle Vermeidung der Verarbeitung
- Generelles Verbot von De-Anonymisierung

VOICE fordert die schrittweise Anpassung der DSGVO.

11

IT-Sicherheitsgesetz 2.0: Unterstützung statt Sanktionierung.

VOICE fordert für die Umsetzung und Anwendung des IT-Sicherheitsgesetzes 2.0 einen Fokus auf Dialog und Unterstützung anstelle Kontrolle und Sanktionierung.

Das vom Bundestag und Bundesrat verabschiedete IT-Sicherheitsgesetz 2.0 (ITSiG 2.0) erweitert den Kreis der Unternehmen, die der sogenannten kritischen Infrastruktur (KRITIS) angehören, und verschärft zugleich die gestellten Anforderungen. Zudem skizziert es eine neue Gruppe von „Unternehmen im besonderen öffentlichen Interesse", die nunmehr einer Meldepflicht und Pflicht zur Selbsterklärung unterliegen. Neben Rüstungsunternehmen, Betrieben nach Störfallverordnung der oberen Klasse und „Unternehmen erheblicher volkswirtschaftlicher Bedeutung" werden nun auch deren Zulieferer mit „Alleinstellungsmerkmalen von wesentlicher Bedeutung" hierzu gezählt.

Die unscharfe Abgrenzung macht undifferenziert ganze Unternehmen zum Gegenstand des Gesetzes, obwohl das Risiko in einzelnen Unternehmensbereichen / Betrieben typischerweise unterschiedlich verteilt ist. Hierdurch wird den Unternehmen die Möglichkeit genommen, die Mittel zur Sicherstellung der IT-Sicherheit risikobasiert einzusetzen. Insbesondere die auferlegte Meldepflicht führt zu erheblichen Investitionen in darauf spezialisierte Systeme und rund um die Uhr verfügbares Fachpersonal zur Auswertung, die der Gesetzgeber bei der Abschätzung des Erfüllungsaufwandes der Wirtschaft augenscheinlich nicht berücksichtigt hat. Erschwerend kommt hinzu, dass Meldungen nicht nur nach einer faktischen Störung zu erfolgen haben, sondern auch sobald es zu einer solchen kommen kann. Diese Auflage geht weit über die Forderung der zugrundeliegenden NIS-Richtlinie hinaus und trägt weder zum allgemeinen Lagebild noch zur Störungsbehebung bei. Dabei wird das angedrohte Strafmaß bei Nicht-Meldung absehbar zu unnötigem Aufwand auf Seiten der Unternehmen und Behörden führen.

VOICE begrüßt die Zielsetzung der Bundesregierung, die Robustheit gegen Cyber-Angriffe für den Wirtschaftsstandort Deutschland zu erhöhen.

VOICE fordert, dass die (noch zu erstellenden) Verordnungen zur Umsetzung des IT-Sicherheitsgesetzes 2.0 die „Unternehmen im besonderen öffentlichen Interesse" und deren Zulieferer mit „Alleinstellungsmerkmalen von wesentlicher Bedeutung" zweifelsfrei und langfristig planbar definiert und ihnen den Freiraum gibt, um Mittel zur Sicherstellung der IT-Sicherheit auf Basis des Risikos zielgerichtet einzusetzen. Hierbei dürfen die Forderungen nicht unverhältnismäßig über die Forderungen der geltenden NIS-Richtlinie hinausgehen, um den Wirtschaftsstandort Deutschland nicht zu gefährden. Dabei wäre der Fokus auf Unterstützung anstelle Sanktionierung durch Behörden Grundlage einer vertrauensvollen Zusammenarbeit. Hilfreich wäre hier insbesondere eine zeitnahe und branchenspezifische Versorgung der durch die Behörden gewonnenen Informationen zu Lagebild und Schwachstellen.

12

Betriebsverfassungsgesetz: Mitbestimmungsprozess bei IT-Systemen vereinfachen

VOICE fordert die Präzisierung des § 87 Betriebsverfassungsgesetz, um Rechtsunsicherheit beim Einsatz von IT-Systemen zu beseitigen.

Die Digitalisierung der Geschäftsprozesse in der deutschen Wirtschaft muss zügig und mit möglichst geringem Gesamtaufwand erfolgen. Workflow- und Collaboration-Systeme etablieren sich zunehmend. Sie helfen mit hoher Wertschöpfung, die Betriebe auf dem

Weltmarkt konkurrenzfähig zu halten.
In der Praxis führt eine bislang uneinheitliche Rechtsprechung im Umfeld des Betriebsverfassungsgesetzes zu unnötig hohen Aufwänden im Mitbestimmungsprozess. Denn unterschiedliche Auslegungen des § 87 BetrVG führen dazu, dass jede einzelne IT-Komponente als mitbestimmungspflichtig angesehen werden kann.[12] Mit zunehmender Durchdringung der Prozesse mit IT führt dies zu immer höherem Abstimmungsaufwand mit hohen zeitlichen Risiken. Über kurz oder lang wären alle Geschäftsprozesse vollständig mitbestimmungspflichtig.

Ähnlich anderer Rechtsbereiche (Arbeitssicherheit, Brandschutz etc.) muss deshalb die Mitbestimmung auf Funktionen beschränkt werden, die auch den entsprechenden Gestaltungsspielraum aufweisen. So kann z.B. die Konfiguration von Präsenzanzeigen Gegenstand der Verhandlung sein. Für den Normalbetrieb von IT-Werkzeugen und Anwendungen muss der Umgang und die Administration so geregelt werden, dass Verhandlungen darüber unnötig werden.

VOICE fordert deshalb eine Präzisierung und Detaillierung dahingehend, welche Systemfunktionen und Auswertungsmethoden erlaubt bzw. welche verboten sind. Dies muss keinesfalls mit der Einschränkung von Arbeitnehmerrechten einhergehen. Im Gegenteil: VOICE unterstützt in der modernen Wissensgesellschaft ausdrücklich Führungsmethoden, die auf Kreativität und Eigenverantwortung setzen. Verhaltenskontrolle ist – insbesondere im Kontext zunehmender Remote-Arbeit - generell als veraltete Führungsmethode anzusehen. Dies ist ein Grund mehr, bei dem bestehenden Digitalisierungsdruck auf ausufernde Verhandlungen mit den Mitbestimmungsgremien so weit wie möglich zu verzichten.

[12] Der Passus „Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen." wird dabei in der Rechtsprechung teilweise sehr weitgehend interpretiert. So kann selbst ein einfacher Login-Vorgang bei einer SaaS Anwendung als im Sinne des §87 BetrVG für eine Verhaltenskontrolle nutzbarer Schritt gesehen werden. Siehe Dauerbrenner: Software vs. Mitbestimmung https://www.luther-lawfirm.com/newsroom/newsletter/detail/newsletter-arbeitsrecht-1-ausgabe-2021#acc-3

IMPRESSUM

VOICE
CIO Bundesverband der IT-Anwender e.V.

VOICE – Bundesverband der IT-Anwender e.V.
Invalidenstraße 91, 10115 Berlin Berlin
Tel.: +49 30 2084 964 70
Fax: +49 30 2084 964 79
E-Mail: voice-info@voice-ev.org

USt-IdNr: DE 281638339
VR 31149 B Berlin Charlottenburg

Vertreten durch:

Dr. Bettina Uhlich
Vorsitzende des Präsidiums

Dr. Hans-Joachim Popp
Stellvertretender Vorsitzender des Präsidiums

Thomas Rössler
Stellvertretender Vorsitzender des Präsidiums

Geschäftsführer und verantwortlich für den Inhalt nach § 55 Abs. 2 RStV: Wolfgang Storck

Veröffentlicht:
Berlin, den 15.06.2021

FAIR MARKET CONDITIONS
REDUCING BUREAUCRACY
DIGITAL SOVEREIGNTY

VOICE - Bundesverband der IT-Anwender e.V.

VOICE
Bundesverband der
IT-Anwender e.V.

Positions on the federal elections
'21

12 demands for the federal elections

VOICE e.V.
Market conditions for IT and digital
Improve user companies

VOICE positions on the federal election: Improving market conditions for IT and digital user companies

Together with its 400 members and their 2600 companies, VOICE - Bundesverband der IT-Anwender e.V. (Federal Association of IT Users) has formulated 12 positions that address the most important demands of user companies on politics. On the one hand, this is about improved market conditions, i.e. more product diversity and competition among providers, fewer burdens and risks as well as more rights for the user side. This applies, for example, to more manufacturer responsibility for the quality of their products, more say in standards or simpler software contracts.

On the other hand, VOICE demands improvements to the Temporary Employment Act (AÜG), the GDPR and the IT Security Act in order to make the laws more manageable and less burdensome and thus better serve the interests of the many thousands of user companies in Germany.

Brief overview of VOICE demands:

Improved market conditions, stronger digital sovereignty

1 Open standards for more competition

Strengthen competition by enforcing open standards.
- Enforce the use of open standards, especially for software interfaces and data exchange formats.
- Maintenance and further development of the open standards through committees with equal representation of users and providers

2 More innovation for more digital sovereignty

Targeted promotion of digital innovations and know-how development for all value creation elements of digitalisation.
- Promote the use of European IT components in a targeted manner
- Promoting the product maturity process through constructive feedback from users
- Initiate practice-oriented innovation partnerships

3 GAIA-X must remain European

Digital sovereignty: GAIA-X to include only providers from Europe in the start-up phase.
- Preferably bring medium-sized European suppliers into leading roles
- Fast implementation through focus on core functionalities

4 Suppliers are liable for their products

Product liability for software products also in B2B business.
- Suppliers are liable for direct and indirect damage caused by product defects
- Assess quality defects in security products as particularly serious

5 Product safety becomes mandatory for suppliers

IT security: Software and cloud services must be designed securely.

- Punitive obligation of software and internet providers to high product quality (state of the art)
- Troubleshooting must take place quickly
- Keeping the effort for the user side to a minimum

6 Simpler software contracts

Regulation of software use contracts and licence agreements.

- Simplify contracts
- Limit unilateral possibilities for change
- Technically exclude unlawful use to make audits superfluous

7 Aid for start-ups

Improve hands-on promotion.

- Provide targeted support for the training of entrepreneurial skills
- Promote coaching of young enterprises
- Offer entrepreneurship courses across the board in higher education institutions

8 Consistently protect data traffic on the internet

Increasing security on the Internet, „License plates and guard rails for the web".

- Broad German/European policy initiative for more security in data traffic
- Active role of the government in shaping the further development of the internet into a secure basic infrastructure for the economy.
- Verification obligations for communication participants (servers, routers and network nodes)
- Obligation to provide evidence for domain holders (model: commercial law)

9 Allow flexible forms of work

Temporary Employment Act (AÜG): Abolish maximum temporary employment period for temporary workers in the IT sector.

- Temporary worker more than 18 months for one client
- Create legal conditions for further flexible forms of work

Less bureaucracy, more precise rules

10 GDPR protection against data misuse

GDPR Make protection against data misuse more effective and facilitate digitalisation.

- Allow and encourage data processing with consistent adherence to security measures
- Facilitate analyses as a dedicated service for the data provider
- Consistently prohibit de-anonymisation

11 Making the IT Security Act 2.0 practicable

Support instead of sanctioning

- Involve user companies in implementation practice
- Making reporting obligations manageable
- Establish clear and long-term definition of the companies concerned

12 BetrVG: Simplify the co-determination process for IT systems

- Clarification of § 87 of the Works Constitution Act to eliminate legal uncertainty in the use of IT systems.
- Limit co-determination to functions with scope for design.
- Determine which system functions and evaluation methods are allowed.
- Allow anticipation of updates.

Improved market conditions, stronger digital sovereignty

1

IT markets: Strengthening competition with open standards.

VOICE calls for the promotion of open standards for flexible software interfaces and data exchange formats between the platforms of major software vendors and other software solutions in the interest of users.

One of the main reasons for the current market failure in the area of large platform providers is the use of proprietary software interfaces (Application Programmable Interfaces = APIs) controlled exclusively by individual manufacturers, to which high investments are tied on the user side, especially in system configuration, supplementary sub-functions and process design.

So-called open standards for software interfaces are jointly controlled by users and manufacturers and can also be used by new market participants without preconditions. Due to their high long-term stability and the intended upward or downward compatibility, they lower the entry risks for new competitors and reduce the dependence of customers on individual providers. Open standards therefore represent one of the essential guarantors for functioning markets.[1]

In order to establish or strengthen the bodies needed for the development and maintenance of open standards, VOICE calls for intervention by the federal government or the legislator, at least in the initial phase. This is the only way to compensate for the excessive influence of individual providers under the prevailing market conditions.

Furthermore, the public sector must be a pioneer in promoting the use of open standards by making them a requirement in tenders.[2] A widespread and consistent use enables continuous, intensive feedback to the standardisation bodies in order to enable continuous optimisation.

Open standards for software interfaces in this sense must have the following properties:

- They allow irrevocable, free use without preconditions. Their definition is consequently a pre-commercial, non-profit activity of the interested market participants.
- They are fully and comprehensibly documented and freely accessible to all market participants.
- Further development follows a transparent and publicly comprehensible decision-making process, which in particular incorporates feedback from the various user groups and which can be reviewed by subject matter experts.
- In the further development and maintenance process, one focus is on ensuring maximum compatibility of new versions with the applications on the market, so that a high level of investment security is created for all market participants.
- Software modules that make use of the open standards can be open source or proprietary, as long as they follow the open standards at all interfaces.
- In particular, the interface between the human user and the software systems must also be included in the standardisation.

The preferred interfaces to be standardised include, in particular, file formats for the transfer of data objects between software modules (. vcf, . ics, . odf, . step etc.).[3] Where it has been possible to develop such formats into stable standards, this has contributed very positively to product diversity and competition.

[1] in some market segments, such open standards are already used very successfully (hardware interface in server systems, USB peripherals, etc.). In these segments, the resulting competition is high and the quality consequently gratifyingly high.

[2] The UK government defined the use of open standards back in 2018: https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles.

[3] File formats as open standards have existed for many years. However, their strict application in commercial software products has not been demanded so far. Public sector clients may now have to enforce this, as circumvention, especially by the market leaders, is one of the main reasons for the strong unwanted loyalty of existing clients to these market leaders. Formats that are already being further developed in consortia with equal representation (. vcf = RFC 6350 and . ics = RFC 5545) already make a very good contribution to compatibility between software modules from different manufacturers and thus contribute a great deal to functioning competition.

2

Digital sovereignty: targeted promotion of digital innovations and know-how development for all value creation elements of digitalisation.

VOICE calls for the targeted promotion of the use of European IT components to increase independence and to stimulate and diversify competition in the key technologies of digitalisation.

Digital infrastructures require a large number of mission-critical key technologies, only a small part of which can currently be provided by European suppliers on an equal footing with their Asian and US competitors. In addition to the already existing negative effects of oligopolies, this leads to foreign policy dependencies and thus to additional risks for user companies. Moreover, this dependency massively limits the EU's ability to act diplomatically vis-à-vis the other economic powers.
The funding policy pursued in recent years with a focus on research and innovation is not sufficient. Despite excellent top-level research and a high degree of innovation, the establishment of providers with a noteworthy market share has only succeeded in exceptional cases so far. What is missing is the widespread practical use of new IT products as conscious support for the maturing process. The user companies also have the task of providing constructive feedback for optimisation.

3

Digital sovereignty: GAIA-X to include only providers from Europe in the start-up phase.

VOICE calls for the project for a stand-alone European data infrastructure, GAIA-X, to be preferably opened to medium-sized European providers and users in the coming first years.

The GAIA-X project aims to open up competition in the cloud platform provider market to medium-sized European providers as well. The aim is to neutralise the existing dominance of individual large platforms by means of a software stack based on open standards (the so-called sovereign cloud stack). It is clear that this cannot be in the business interests of the large providers who are limited by this. If these providers participate, it must also be assumed that there will be a gross imbalance in terms of resources and initial know-how, which will inevitably stand in the way of successful cooperation. Challenges in setting up the standard are by no means to be expected on the technical side, but much more on the organisational psychological side. Success ultimately depends on a balance of power among the partners.
VOICE therefore demands that these providers should not be involved in the consortium, but that preferably medium-sized, European providers should be brought into a leading role.
The focus must be on the few core functionalities that are actually needed, instead of losing speed by offering too many services.

The cooperation of the large suppliers should be sought when the developed standards are established in the market and their use is defined as mandatory, especially on the part of the procurers.

4

Extensive product liability for software products also in B2B business.

VOICE demands the consistent enforcement of a liability of software producers for direct and indirect damages to user companies caused by quality deficiencies.

Software products have become of paramount importance for the business activities of companies and the administrative processes of the state. Their quality determines both the operating costs and the security risks. In this context, one person-year saved in development can easily generate ten times the effort on the part of the operators.[4] Unlike in other industries (car manufacturing, plant engineering), however, there has been no monetary incentive for software providers to maintain the quality of their products at a high level.

VOICE members see the additional investment in development with the consequent higher licence costs as economically sensible and therefore necessary. The financial incentive for software producers to invest in the quality of their products must be created through corresponding contractual penalties and claims for damages. In particular, security gaps in products with explicit security tasks (firewalls, intrusion detection/prevention, virus protection) are to be assessed as especially serious and punished accordingly. The relevant laws and especially case law must allow for simplified enforcement of claims.

[4] The complex procedures for updating business software, which are taken for granted today, make it necessary for user companies to employ highly specialised staff and to interrupt operations, although with appropriate investment in product development, both the number of updates and the effort required in each case could be drastically reduced. The fact that this is possible is proven by products from small market participants or the update procedures in the consumer sector, where expert knowledge on the customer side is excluded per se.

5

IT security: Software providers and internet providers must comply with the state of the art in terms of minimum frequency, speed and manageability of security breaches.

VOICE calls for software providers and internet providers to be obliged to take appropriate measures to prevent malfunctions and to eliminate them quickly and without effort or disruption in the event of an error.

The current legal requirements on cyber security almost exclusively relate to the responsibilities of the user companies. They are subject to due diligence and reporting obligations (IT Security Act), bear responsibility for ensuring that the technology they use is state of the art (e.g. Solvency 2) and, of course, for ensuring that subsequent bug fixes and the closure of security gaps (patches) are promptly applied to the running IT environment. The same applies in the area of data protection and internet security.

In order to redress the existing imbalance, VOICE calls for the obligation of software and service providers as well as internet providers to take concrete measures to avoid or quickly eliminate security vulnerabilities. The legislator must oblige them to do so:

- ensure state-of-the-art product and service quality.
- in the event of security deficiencies occurring, to rectify these within a specified time period and to provide simple and operationally reliable procedures for the deployment of the resulting patches.
- use the known and proven protection mechanisms (e.g. DNSSEC) on a mandatory basis.

6

Regulation of software use contracts and licence agreements.

VOICE calls for the simplification of licence agreements as well as the restriction of unilateral modification options and extended commitment and notice periods. VOICE also calls on providers to ensure that the unlawful use of licensed software is excluded.

Software licensing and the management of software usage contracts now take up a significant proportion of resources in corporate and government IT operations. This is due to numerous unilateral changes in terms and conditions and contractual clauses with dubious legal validity, which lead to uncertainty and management effort in user companies[5].

From the point of view of the user companies, large parts of these efforts could be dispensed with if the permissible contract constructions were regulated in detail by law. The fact that this has not yet been done by competitive pressure itself is due to the market failure explained above. In order to nevertheless enable legally secure and, above all, low-effort IT operations, the legislator must make corresponding specifications on permissible contract models. In particular, contract amendments to restrict use and sale must be regulated, or the corresponding clauses must be explicitly declared legal/not legal, and the permitted changes in the basic licensing model (CPU-based, concurrent user, named user, etc.) must be limited to a fair level.

The effort for licence management can be reduced above all by ensuring that the software itself excludes misuse by technical means (e.g. through licence keys or tokens). As long as a software is not changed by unauthorised manipulation (so-called crack), misuse must not be possible.

To simplify software management, pre-installation of the complete software (e.g. on workstations) must be allowed without incurring licence costs in the same process. Only the installation of the licence key leads to the use of the software function and thus to the obligation to pay.

A continuous cash flow is economically advantageous for both the user companies and the manufacturers of software products. Licensing models with time- or intensity-based subscription („pay as you go") are therefore to be preferred over purchase options. They also rule out conflicts over the disposal of purchase licences from the outset. Accordingly, such subscription contracts are to be favoured in the legal regulations.

7

Start-ups: Improve hands-on support.

VOICE calls for more intensive and direct support for digital start-ups. In order to specifically promote innovation in technology and digital business models, the German and European administration must develop mechanisms to support digital start-ups that go beyond tax incentives and bureaucratic simplifications for investors and founders.

Overall, the number of start-ups in Germany is stagnating. According to the development bank KfW, there were around 7,000 in 2020 - no more than in 2018. And this is despite the fact that the federal government has made start-ups less bureaucratic in recent years and developed various financial incentives for investors (for example, depreciation options).

While access to financing plays an important role for

5 CISPE, a European association of cloud providers (among its members is aws), together with the French user association and VOICE partner association CIGREF, has published 10 rules for fair software licences for cloud users. https://www.fairsoftware.cloud/principles/

start-ups, the reasons why start-ups fail in 80 to 90 percent of cases, according to experts, are more likely to be related to entrepreneurial aspects: lack of technical and social competence of the founding team, lack of customer value of the product or service; a network that is too small or not resilient enough; insufficient scalability to support strong growth.

It is precisely in these aspects that the founders should be supported more strongly. With advice and coaching, for example by experienced practitioners (VOICE offers this to start-ups with CIOs), comprehensive entrepreneurship courses at universities, especially in engineering and computer science courses, as well as accompanying training opportunities in practical management and leadership. In addition, start-ups should be supported in the founding phase with easily financed market studies.

8

Increasing security on the Internet, „License plates and guard rails for the web".

VOICE calls for a broad-based German / European policy initiative to improve security in data traffic. The government must take a strong, formative role in the further development of the internet.

The internet, as a defining infrastructure element of the modern economy, is increasingly plagued by organised crime. As the value-added share of data traffic increases, threats are becoming a mission-critical factor for increasingly digital business models. Many functionalities and communication channels that are in themselves highly convenient for the customer can now no longer be used due to the increasing threat.[6]

Previous approaches to protecting business processes focus almost exclusively on hardening the central server and the end devices or on improved user training (awareness training). Companies are dependent on having their own elaborate monitoring equipment in order to detect criminal data traffic and protect themselves against it.

So far, however, no measures have been taken to make data traffic more secure overall. On the contrary, many functionalities introduced in recent years (umlauts and special characters in URLs, dynamic IP address and DNS name management) have dramatically worsened overall security.[7] Large market players make do with special service providers that automatically track criminal activities of actors.

VOICE calls on the German government, together with its European partners, to take an active role in the definition and standardisation of protocols in data traffic and - in analogy to road traffic and commercial law - to finally improve the obligations of proof for communication participants (servers and routers[8]) and the traceability of communication paths. In addition, it must be made easier for users to assess the security situation by clearly marking the actual origin of messages and files in user interfaces. The use of the already existing security mechanisms[9] for data traffic in the WAN or between geographical zones must be made obligatory through corresponding regulations.

VOICE calls on the Federal Government to address the following security measures through appropriate international standardisation processes:

- Restricting the (already sufficiently large) namespace so that fraud can be more easily detected by means of similar-sounding URL identifiers,
- Restricting the switching of DNS records between IP address spaces[10] (analogous to the change of name or registered office of a company in the commercial register) and, in particular, including the switching frequency as a feature of the domain in question so that it can be used as a security feature,
- Obligation of providers to make the origin of a message clearly visible in the user interface in order to make fraud easier to detect,
- Obligation of registrars (e.g. denic for the .de domain) to ¬check domain applications in ¬advance for seriousness (analogous to the commercial register or Post-Ident procedure) and to contain the risk of fraud by applying similarity measures already at the application stage,
- Fixed coupling of the identifiers of internet nodes[11] to their geographical location in order to exclude the fraudulent rerouting of data traffic (BGP hijacking),
- Enrichment of communication protocols with certificate-based information on the transmission path of data flows.

To this end, a dedicated department must be set up in a newly created Federal Ministry for Digitisation to bundle and coordinate German activities in all standardisation bodies for IT technology (W3C, CEN/CLC/ETSI, ISO/IEC, etc.). To this end, the ministry must be equipped with industry-independent, specialised technology experts or with access to such resources from German science.

[6] Banks and parcel services, for example, can only interact with their customers to a limited extent because (justified and unjustified) mistrust torpedoes this.

[7] Attackers can easily divert data flows with changing server names and create deceptively similar but fraudulent URLs by using, for example, diacritical marks (accents, etc.).

[8] The identities of the persons concerned are not affected by this.

[9] Like DNSSec,STARTTLS, certificate-based server communication etc.

[10] Redundancy-related changes can be defined and announced in advance, but arbitrary jumps every second must be reported as a loss of seriousness.

[11] This in no way excludes the redundant use of different data paths (e.g. in the event of an error), but the change of a geographical identifier can only be made as a „notarial act".

Less bureaucracy, more precise rules

9

Temporary Employment Act (AÜG): Abolish maximum temporary employment period for temporary workers in the IT sector.

VOICE calls for the revision of the AÜG to ensure that temporary workers in the IT sector above a fixed minimum hourly rate do not fall under the maximum hiring-out limit of the German Temporary Employment Act (Arbeitnehmerüberlassungsgesetz, AÜG).

Experts[12] assume that the Temporary Employment Act, which came into force in 2017, will have to be amended in 2023. In the AÜG currently in force, the time limit for temporary employment is set at 18 months. However, many success-critical external personnel resources in IT projects must remain available for a considerably longer period of time in order to avoid unnecessary familiarisation processes and the complicated selection of ever new specialised staff. The maximum limit endangers the long-established and very successful co-innovation in the IT and digital scene. In some cases, freelance IT consultants and freelance developers work (together with permanent colleagues of their clients) for years on one large IT project or on a number of smaller projects. Many IT freelancers also work for personnel service providers who then „lend" them out. The protective effect intended by the law for actually dependent employees is not needed in this area, as permanent employment is regularly less attractive than self-employment.

Because unlike temporary workers in the industrial, food and service sectors, freelance IT workers earn well above average. Due to the high speed of development and the high pressure to innovate, the IT market has already been suffering from a severe shortage of skilled workers for years. This will continue to increase due to the digitalisation of the economy and society, with the consequence that the demand for IT freelancers and IT consultants will continue to rise in the coming years and that they can therefore largely determine the conditions of their engagement themselves.

The majority of IT freelancers have also deliberately chosen the status of „freelancer". This way, they can usually choose the projects that offer them the best conditions. Moreover, freelancers assume that they can control their invested working time better than permanent colleagues.

IT freelancers and consultants are therefore by no means part of the low-wage sector that the legislator rightly wants to protect.

VOICE therefore demands that the AÜG's maximum transfer period should no longer be applied to freelancers with above-average salaries.
Furthermore, the conditions under labour law must be created so that agile teams of IT users, IT service providers and consultants can work together flexibly, even over longer periods of time, without having to accept legal risks.

[12] https://www.arbeitsblog.de/themen/artikel/aueg-welche-aenderungen-stehen-2023-bevor/

10

Data protection: Effectively prevent illegal use, facilitate data processing.

VOICE calls for data protection regulations to be more targeted against unwanted and abusive analytics (e.g. financial scoring, health scoring, personality profiling) instead of continuing to restrict data collection so much.

The General Data Protection Regulation is characterised by the principle of data economy. This principle, which was postulated in Germany at the end of the 1980s, resulted primarily from the intention to put a stop to possible misuse by government agencies. At that time, companies had not yet discovered the value of data. This is diametrically different today. Data has become a fourth production factor for companies alongside capital, labour and raw materials, and increasingly it can be related to people in one form or another.

The aim must therefore be to enable the processing and use of this production factor for European companies as well, while preserving the informational self-determination of citizens and at the same time creating legal certainty for the processing companies. Approaches to this are:

- Permission for evaluations if the traceability of the original data can be reliably ruled out
- Control of the evaluation instead of general avoidance of processing
- General ban on de-anonymisation

VOICE calls for the gradual adaptation of the GDPR.

11

IT Security Act 2.0: Support instead of sanctioning.

VOICE calls for a focus on dialogue and support instead of control and sanctioning for the implementation and application of the IT Security Act 2.0.

The IT Security Act 2.0 (ITSiG 2.0) passed by the Bundestag and Bundesrat expands the group of companies belonging to the so-called critical infrastructure (CRITIS) and at the same time tightens the requirements imposed. In addition, it outlines a new group of „com-

panies in the special public interest", which are now subject to a reporting obligation and a duty to self-declare. In addition to defence companies, companies in the upper class according to the Major Accidents Ordinance and „companies of considerable economic importance", their suppliers with „unique selling propositions of essential importance" are now also included.

The fuzzy demarcation makes entire companies the subject of the law in an undifferentiated manner, although the risk is typically distributed differently in individual divisions / companies. This deprives companies of the opportunity to use the means to ensure IT security in a risk-based manner. In particular, the obligation to report leads to considerable investments in specialised systems and qualified personnel for evaluation, which the legislator apparently did not take into account when estimating the compliance costs for the economy. Another complicating factor is that reports not only have to be made after a factual disruption, but also
as soon as such an incident may occur. This requirement goes far beyond the demands of the underlying NIS Directive and contributes neither to the general situation nor to the elimination of disruptions. At the same time, the threatened penalty for non-reporting will foreseeably lead to unnecessary effort on the part of the companies and authorities.

VOICE welcomes the Federal Government's objective to increase the robustness against cyber attacks for Germany as a business location.

VOICE demands that the regulations (still to be drawn up) for the implementation of the IT Security Act 2.0 define the „companies in the special public interest" and their suppliers with „unique selling propositions of essential importance" beyond doubt and in a way that can be planned in the long term, and give them the freedom to use means to ensure IT security in a targeted manner on the basis of risk. In this context, the requirements must not disproportionately exceed the requirements of the current NIS Directive in order not to endanger Germany as a business location. The focus on support instead of sanctions by the authorities would be the basis for a trusting cooperation. In particular, a timely and sector-specific supply of information obtained by the authorities on the situation and vulnerabilities would be helpful.

12

Works Constitution Act: Simplify co-determination process for IT systems

VOICE calls for the specification of § 87 of the Works Constitution Act to eliminate legal uncertainty in the use of IT systems.

The digitalisation of business processes in the German economy must take place quickly and with as little overall effort as possible. Workflow and collaboration systems are becoming increasingly established. With high added value, they help keep businesses competitive on the global market.

In practice, inconsistent case law in the area of the Works Constitution Act has led to unnecessarily high costs in the co-determination process. This is because different interpretations of section 87 of the Works Constitution Act mean that each individual IT component[13] can be regarded as requiring co-determination. With the increasing penetration of processes with IT, this leads to ever greater coordination efforts with high time risks. Sooner or later, all business processes would be fully subject to co-determination.

Similar to other areas of law (occupational safety, fire protection, etc.), co-determination must therefore be limited to functions that also have the corresponding scope for design. For example, the configuration of presence displays can be subject to negotiation. For the normal operation of IT tools and applications, the handling and administration must be regulated in such a way that negotiations on this become unnecessary.

VOICE therefore calls for a more precise and detailed definition of which system functions and evaluation methods are permitted and which are prohibited. This does not have to go hand in hand with the restriction of workers' rights. On the contrary, in the modern knowledge society, VOICE explicitly supports management methods that focus on creativity and personal responsibility. Behavioural control - especially in the context of increasing remote working - is generally regarded as an outdated management method. This is one more reason to refrain as far as possible from excessive negotiations with co-determination bodies in the face of the existing pressure for digitalisation.

[13] The phrase „introduction and use of technical equipment intended to monitor the behaviour or performance of employees" is sometimes interpreted very broadly in case law. For example, even a simple login process for a SaaS application can be seen as a step that can be used to monitor behaviour in the sense of section 87 of the Works Council Constitution Act (BetrVG). See perennial topic: Software vs. co-determination https://www.luther-lawfirm.com/newsroom/newsletter/detail/newsletter-arbeitsrecht-1-ausgabe-2021#acc-3

IMPRESSUM

VOICE
CIO
Bundesverband der
IT-Anwender e.V.

VOICE – Bundesverband der IT-Anwender e.V.
Invalidenstraße 91, 10115 Berlin Berlin
Tel.: +49 30 2084 964 70
Fax: +49 30 2084 964 79
E-Mail: voice-info@voice-ev.org

VAT ID: DE 281638339
VR 31149 B Berlin Charlottenburg

Represented by:

Dr. Bettina Uhlich
Chairwoman of the Presidium

Dr. Hans-Joachim Popp
Vice Chairman of the Presidium

Thomas Rössler
Vice Chairman of the Presidium

Managing Director and responsible for the content according to § 55 Abs. 2 RStV: Wolfgang Storck

Published:
Berlin, 15.06.2021