

# Presse

---

Graz, 21. Juli 2021

## 360° Zertifizierung für eine vertrauenswürdige Künstliche Intelligenz (KI)

- **Neue strategische Partnerschaft österreichischer Expertinnen und Experten für vertrauenswürdige und sichere KI-Anwendungen**
- **Die Steiermark als globaler Vorreiter bei Prüfung und Zertifizierung von Künstlicher Intelligenz**
- **Die Initiative ist offen für die Beteiligung weiterer Partner aus Forschung und Industrie**

In der Steiermark entsteht eine neue Initiative, um effiziente und unabhängige Prüfverfahren und Prüftechnologien für KI-Systeme zu entwickeln. Daran beteiligt sind das **Know-Center**, als ein führendes europäisches Forschungszentrum für Data-driven Business und Künstliche Intelligenz, der **SGS-Konzern** als weltweit führender Anbieter für Prüfung, Testen, Verifizieren und Zertifizierungen, und das **IAIK der Technischen Universität Graz**, eines der führenden Forschungsteams für Cybersicherheit. Ethische und rechtliche Aspekte werden über das **Business Analytics and Data Science Center der Universität Graz** eingebracht und **Österreichs Zentrum für sichere Informationstechnologie (A-SIT)** begleitet die Aktivitäten als neutraler Beobachter.

### Vertrauen als Voraussetzung von KI-Anwendungen

Künstliche Intelligenz bietet enormes Potential für neue Geschäftsideen und wirtschaftliches Wachstum. Sie ist eine Schlüsseltechnologie, um die Zukunftsfähigkeit von Wirtschaft und Gesellschaft angesichts globaler Herausforderungen, von Pandemieentwicklungen bis hin zu Klimawandel, zu sichern. Ähnlich wie bei der Datenschutzgrundverordnung (DSGVO) plant die Europäische Kommission eine Verordnung einzuführen, um KI-Systeme künftig zu regulieren. Dabei ist eine umfassende Konformitätsbewertung durch Anbieter vorgesehen, die eine KI-Zertifizierung unumgänglich machen wird.

„Das Potential von KI wird in Europa erst dann ausgeschöpft werden, wenn ein vertrauenswürdiger Umgang mit Daten sowie Fairness und Verlässlichkeit der Algorithmen und deren Sicherheit gewährleistet ist. Über eine 360° Perspektive wollen wir dafür sorgen, dass KI-Anwendungen technisch konform, zuverlässig und unvoreingenommen funktionieren. Im Fokus stehen alle Bereiche, die für eine hohe Qualität und Vertrauenswürdigkeit von KI essentiell sind: Daten, Algorithmen, Cybersicherheit, Prozesse, Ethik und Recht“, erklärt **Stefanie Lindstaedt, CEO des Know-Centers**, das Vorhaben.

**Wirtschafts- und Forschungslandesrätin Barbara Eibinger-Miedl** begrüßt die Initiative: „Künstliche Intelligenz ist ein zentrales Thema der Digitalisierung. Neben großen Chancen gibt es aber auch Herausforderungen. So müssen etwa vertrauenswürdige Systeme und ein hoher Datenschutz sichergestellt werden, um Hemmschwellen beim Einsatz Künstlicher Intelligenz abzubauen. Dass der Weltkonzern SGS dabei auf steirisches Know-how zurückgreift, unterstreicht die hervorragende Arbeit der beteiligten heimischen Akteure. Durch zahlreiche Forschungsprojekte und Digitalisierungsinitiativen ist es uns in der Steiermark gelungen, umfassende Kompetenzen in diesem Bereich aufzubauen und eine globale Vorreiterrolle einzunehmen.“

### **Unabhängige Prüfung und Zertifizierung von KI-Lösungen**

Aktuell gehört KI zu den am schnellsten wachsenden Themenfeldern. Die meisten KI-Systeme sind datengetrieben, das heißt sie erlernen aus großen Mengen von Daten gewünschte Verhaltensweisen. Diese hochmoderne Technologie ermöglicht außergewöhnliche Innovationen, kann jedoch bei nicht adäquater Verwendung ungewollte und sehr negative Auswirkungen haben. Beispiele sind Vorurteile im Rahmen von Personalprozessen oder unsichere Empfehlungen einer KI im Gesundheitswesen.

„Ein Eckpfeiler des Vertrauens in KI ist die Einhaltung von Standards und Vorschriften, die durch Konformitätsbewertungen nachgewiesen werden, die akkreditierte Stellen wie SGS durchführen. In unserer Partnerschaft werden wir neue multidisziplinäre Tools und Techniken entwickeln, um diese Bewertungen zu ermöglichen, die Bereiche wie etwa Cybersicherheit oder Ethik umfassen. Das wird Kunden auf der ganzen Welt einen Mehrwert bieten“, erklärt Siddi Wouters, Senior Vice President Digital & Innovation bei SGS.

### **Cyberkriminalität als eine der größten Herausforderungen**

Trotz des enormen technologischen Potentials sind mit dem Einsatz von KI-Anwendungen auch Unsicherheiten und Risiken verbunden. Es gibt eine Vielzahl an Möglichkeiten, KI-Systeme anzugreifen. Eine große Herausforderung bei der Bewertung von KI-Systemen ist daher die Cyberkriminalität. Beispielsweise könnte ein autonomes Fahrzeug fatale Entscheidungen treffen, wenn Daten, die das im Fahrzeug eingesetzte KI-System verarbeitet, manipuliert werden.

„Herkömmliche statische Prüfungen reichen hier nicht aus. Es braucht die Erforschung grundlegend neuer sicherheitstechnischer Konzepte, um einen kontinuierlichen Nachweis der Robustheit von AI-Systemen gegen Cyberattacken zu erhalten und die Privatsphäre zu schützen. Diese Expertise bringt die TU Graz in die strategische Partnerschaft ein. Die Initiative ist für uns zugleich die logische Vertiefung bereits erfolgreich bestehender Kooperationen im Bereich Informatik, Software Engineering und Cybersicherheit mit SGS, dem Know-Center und der Uni Graz. Davon profitieren auch universitäre Forschung und Lehre, in die die neuen und aktuellen Inhalte einfließen“, **erläutert Harald Kainz, Rektor der Technischen Universität Graz.**

## Akzeptanz von KI-Anwendungen erhöhen

Auch wenn der Einsatz von KI in den letzten Jahren über alle Branchen hinweg zugenommen hat, sind Unternehmen im Hinblick auf Datenschutz und rechtliche Vorgaben nach wie vor oft verunsichert. Die geplante EU-Regulierung könnte hier für zusätzliche Überforderung sorgen und die Wertschöpfung von KI verringern oder gar verhindern. Fehlende Rechtssicherheit durch nicht vorhandene Auditcertifikate sind eine der größten Barrieren, die den breiten Einsatz von KI in der Wirtschaft verhindern und damit Unternehmenspotentiale verringern.

„Auditingansätze für KI sind für einen breiten Einsatz von KI in der Wirtschaft essenziell. Das ist nicht nur eine rechtliche Anforderung, sondern wirkt auch vertrauensstiftend und kann die gesellschaftliche Akzeptanz positiv beeinflussen. Unsere Studien im Bereich Recruiting zeigen beispielsweise, dass Menschen, die sich diskriminiert fühlen, die Bewertung ihrer Qualifikationen lieber durch eine KI als durch einen Menschen durchführen lassen würden. Das ist insbesondere der Fall, wenn es sich um eine zertifizierte KI-Anwendung mit Erklärungskomponente handelt“, sagt **Stefan Thalmann, Leiter Business Analytics and Data Science Center** an der Uni Graz.

Auch **Herbert Leitold, Generalsekretär A-SIT** betont: „Durch die Bündelung unterschiedlicher Expertisen können die komplexen Herausforderungen einer KI-Zertifizierung gut gemeistert werden. Österreich ist damit auf dem richtigen Weg, um Anbietern und Nutzern von KI-Anwendungen bessere Orientierung und Gewissheit über die Güte der Applikationen zu geben.“

## Kooperation mit weiteren Partnern

Die **Energie Steiermark AG, Leftshift One, NXP** und **Redwave** beteiligen sich mit Use Cases an dem Vorhaben. Die Initiative ist offen für weitere Partner aus Industrie und Wissenschaft, die gemeinsam an KI-Prüfverfahren arbeiten wollen. Durch das umfassende internationale Partnernetzwerk des Know-Centers ist zudem gewährleistet, dass die Forschung stets am neuesten Stand ist und Prüfwerkzeuge und -verfahren kontinuierlich weiterentwickelt werden.

Weitere Informationen zur Initiative: <https://sichere-ki.at/>

## Ansprechpartner für Journalisten:

Know-Center  
Wilma Mert  
Tel.: +43 664/888 92 170  
E-Mail: [wmert@know-center.at](mailto:wmert@know-center.at)

Folgen Sie uns auf Twitter: [https://twitter.com/Know\\_Center](https://twitter.com/Know_Center)

**Über das Know-Center**

Das Know-Center ist eines der führenden europäischen Forschungszentren für Data-driven Business und AI. Seit 2001 werden namhafte Unternehmen dabei unterstützt, Daten als Erfolgsfaktor für ihr Unternehmen zu nutzen. Als fixer Bestandteil der europäischen Forschungslandschaft wickelt das Zentrum sehr erfolgreich zahlreiche Projekte und Auftragsforschung auf EU- und nationaler Ebene ab. Das im Rahmen von COMET geförderte K1-Kompetenzzentrum ist die führende Ausbildungsstätte für Data-Scientists in Österreich und bietet ebenfalls eine Bandbreite an AI-Trainings und Beratung für Firmen an. Mehrheitsgesellschafterin des Know-Centers ist die TU Graz, eine wesentliche Trägerin der heimischen AI-Forschung, deren Institute zahlreiche Projekte gemeinsam mit dem Know-Center abwickeln. 2020 wurde das Know-Center als einziges Österreichisches Zentrum mit dem iSpace Gold Award der Big Data Value Association ausgezeichnet, das in der gesamten EU nur neun Mal vergeben wurde. <https://www.know-center.at>

**Über SGS**

Die SGS-Gruppe ist das weltweit führende Unternehmen in den Bereichen Prüfen, Testen, Verifizieren und Zertifizieren. Es gilt als weltweiter Maßstab für Qualität und Integrität. Mit mehr als 93.000 Mitarbeiterinnen und Mitarbeitern betreibt SGS ein Netzwerk von weltweit mehr als 2.600 Niederlassungen und Laboratorien. Die SGS-Gruppe hat ihren Hauptsitz in Genf in der Schweiz. <https://www.sgs.com>

**Über die TU Graz**

An der TU Graz steht Cybersicherheit seit vielen Jahren im Fokus der Forschung. Mit dem Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologien (IAIK) beherbergt die Universität eine der weltweit führenden Forschungseinrichtungen auf diesem Gebiet. Die IAIK-Forschenden beschäftigen sich mit Kryptologie & Privatsphäre Technologien, mit Fragen der Systemsicherheit sowie mit formalen Methoden, und sie entwickeln Werkzeuge, die mobile Geräte sicherer machen und die Sicherheit von elektronischen Signaturen und elektronischen Geräten gewährleisten. Teams des IAIK sind laufend an der Entdeckung von Prozessorschwachstellen beteiligt, oftmals federführend, wie bei den bekannten „Meltdown“ und „Spectre“-Attacken. Im Bereich der Kryptografie nehmen sie äußerst erfolgreich an großen weltweiten Wettbewerben und Verschlüsselungsverfahren teil und setzen dabei neue Kryptografie-Standards, so geschehen etwa beim CAESAR-Chiffre, der AES-Verschlüsselung oder der Post-Quantum Kryptographie. Die Expertise spiegelt sich auch in der wissenschaftlichen Arbeit wider – bisher wurden vom Institut mehr als 1000 Publikationen veröffentlicht. <https://www.tugraz.at>

**Über das Business Analytics and Data Science Center**

Das BANDAS (Business Analytics and Data Science)-Center beschäftigt sich mit datenbasierten Technologien, die bei sehr großen, heterogenen und volatilen Datenmengen (Big Data) zur Anwendung kommen. Der Fokus des Centers gliedert sich in die zwei Schwerpunkte Business Analytics und Data Science. <https://business-analytics.uni-graz.at/de/>

**Über A-SIT**

Das Zentrum für sichere Informationstechnologie - Austria A-SIT ist der Berater und Unterstützer des öffentlichen Sektors zur Informationssicherheit. Kernkompetenzen sind elektronische Signatur und Identität, E-Government, Zahlungssysteme, Kryptographie und aus deren Aktualität und zunehmender Bedeutung mobile Technologien und Cloud Computing. Darüber hinaus wird die Kompetenz über internationale Projekte und Einbeziehung der Wissenschaft gestärkt. A-SIT ist benannte Zertifizierungsstelle sowie akkreditierte Konformitätsbewertungsstelle nach der EU eIDAS Verordnung. <https://www.a-sit.at/>