A3

AI Act for Austria - Studie zu Umsetzung des AI Acts in kritischen Infrastrukturen Österreichs

Programm / Ausschreibung	KIRAS, F&E-Dienstleistungen, CS F&EDienstleistungen (FED CS_2022)	**Status**	abgeschlossen
Projektstart	01.09.2023	**Projektende**	28.02.2025
Zeitraum	2023 - 2025	**Projektlaufzeit**	18 Monate
Keywords	AI Act; Data Act;		

Projektbeschreibung

Das Hauptziel des Projekt besteht in der Analyse der neu entstehenden EU-weiten Regularien in Bezug auf die Nutzung von AI, speziell im Hochrisikobereich, bzw. im Anwendungsgebiet kritischer Infrastrukturen. Daraus werden Handlungsleitfäden für das BMI und Betreiber kritischer Infrastrukturen entwickelt, aber auch Empfehlungen für Rückmeldungen des BMI an die EC, sowie für den Umgang mit wesentlichen, den Tätigkeitsbereich des BMI betreffenden, Neuerungen. Dabei ist es wesentlich, dass die Analyse nicht rein auf die drei Regularien „AI-Act“, „Data Act“ und „Data Governance Act“ abstellt, sondern auch das weitere Umfeld an Regularien, Normen und Best-Practices einbezieht. Zusätzlich reicht aufgrund der rasanten Entwicklungsgeschwindigkeit in diesem Bereich eine reine Betrachtung der aktuellen Lage nicht aus, es müssen daher wahrscheinliche künftige Entwicklungen extrapoliert und analysiert werden.

Abstract

The main objective of the project is to analyze the emerging EU-wide regulations regarding the use of AI, especially in the high-risk area or in the area of application of critical infrastructures. From this, action guidelines for the BMI and operators of critical infrastructures will be developed, but also recommendations for feedback from the BMI to the EC, as well as for dealing with significant innovations affecting the BMI's field of activity. It is essential that the analysis does not focus purely on the three regulations "AI Act", "Data Act" and "Data Governance Act", but also includes the wider environment of regulations, standards and best practices. In addition, due to the rapid pace of development in this area, it is not sufficient to simply look at the current situation; probable future developments must therefore be extrapolated and analyzed.

Endberichtkurzfassung

Die rasante Entwicklung und zunehmende Integration von Künstlicher Intelligenz (KI) in verschiedenste gesellschaftliche, wirtschaftliche und politische Bereiche stellen Organisationen, Behörden und Unternehmen vor tiefgreifende Herausforderungen. Einerseits bietet die Implementierung von KI-Technologien enorme Chancen, Effizienzsteigerungen, verbesserte Entscheidungsfindung sowie erhöhte Sicherheit in zahlreichen Anwendungsfeldern. Andererseits gehen mit dem Einsatz von KI jedoch auch erhebliche Risiken einher, die insbesondere in kritischen Infrastrukturen und Hochrisiko-Anwendungen sorgfältig identifiziert, bewertet und behandelt werden müssen.

Das Hauptziel des Projekts bestand in der Analyse der neu entstehenden EU-weiten Regularien in Bezug auf die Nutzung von AI, speziell im Hochrisikobereich, bzw. im Anwendungsgebiet kritischer Infrastrukturen. Daraus wurden Handlungsleitfäden für das BM.I und Betreiber kritischer Infrastrukturen entwickelt. Zusätzlich zu diesen Analysen, wurden im Rahmen einer explorativen Szenarienanalyse analysiert, wie sich das Umfeld künftig entwickeln kann und welche Auswirkungen dies auf die Arbeit der LEAs besitzen wird. Dazu wurde eine prominente Methodik für die Bedürfnisse der ESA in einem sehr rasch wachsenden und sich disruptiv verändernden Forschungsfeld umgebaut. Zusätzlich wurde die Methodik dergestalt verändert, dass sie keinerlei proprietäre Software mehr für ihren Einsatz benötigt, sowie rasch genug durchgeführt werden kann, dass sie auch öfter realistisch eingesetzt werden kann.

Basierend auf den Analysen wurden nicht nur die Use-Cases des Bedarfsträgers bearbeitet, sondern auch neue Werkzeuge entwickelt, die sowohl dem Bedarfsträger als auch Firmen zur Verfügung gestellt werden können: Data-Science-Trajectories erlauben die strukturierte Entwicklung von neuen AI-Anwendung, bzw. deren Wartung und gezielte Änderung. Der Make-or-Buy-Guide hilft Beschaffenden in der Entscheidung, im Lichte der zusätzlichen Rechte und Pflichten, die durch den AI-Act erwachsen, eine Kauf- oder Entwicklungsentscheidung zu treffen. Last, but not least, war auch das Thema des Risikomanagements in AI-Systemen ein wichtiger Aspekt der Analysen dieses Projekts. Durch die Durchführung von Expert*innen-Interviews konnte sichergestellt werden, dass die Erkenntnisse nicht auf rein akademischen Arbeiten basieren, die zum Zeitpunkt der Erfassung in einem sich sehr schnell entwickelnden technologischen Umfeld schon veraltet sein könnten, sondern wichtige Expert*innen auf ihren Gebieten direkt und konkret nach wichtigen Einflussfaktoren, aber auch von ihnen antizipierten neuen Gefahren, sowie Anwendungen, speziell im Umfeld von LEAs, befragt werden konnten.

Die Kombination von juristischem und technischem Fachwissen sowie eine interdisziplinäre Herangehensweise ermöglichten eine fundierte Analyse und praxisorientierte Lösungen.

Projektkoordinator

- Hochschule für Angewandte Wissenschaften St. Pölten GmbH

Projektpartner

- Wiener Zentrum für Rechtsinformatik/Vienna Centre for Computers and Law, kurz: WZRI/VCCL
- Bundesministerium für Inneres