IDE@S Innovative Data Environment @ Styria	**AP03: Technische Infrastruktur, AP05: Dienstleistungen**

Zusammenfassung vom Workshop *Sicheres Datenmanagement für organisationsübergreifenden Datenaustausch* (12.05.2021)

Am 12.05.2021 trafen sich IT-Rechtsexpert*innen, IT-Sicherheitsspezialist*innen und verschiedene Anwender*innen zum IDE@S Workshop *Sicheres Datenmanagement für organisationsübergreifenden Datenaustausch*. Ziel des Workshops war es, mögliche als auch essentielle Faktoren für eine vertrauenswürdige kollaborative Datenumgebung zu erheben, um sich im weiteren Verlauf Gedanken zu Dienstleistungen sowie organisatorischen und technischen Maßnahmen machen zu können. Die Teilnehmenden aus Wissenschaft, Wirtschaft sowie Öffentlichkeit anwesend von *Karl-Franzens Universität Graz (KFU), FH Joanneum, Joanneum Research, MedUni Graz, Biobank, Material Center Leoben, MyPrivacy, ITG Informationstechnik* und *Technische Universität Graz* hatten dabei im Rahmen des Workshops die Gelegenheit sich zum Thema Sicherheit im föderierten Datensystem auszutauschen. Nach einem Impulsvortrag zu Datenmanagement aus rechtlicher Perspektive von Prof. Wendland (KFU, Smart Regulation) wurden unter anderem folgende Fragen in der Diskussionsrunde behandelt:

(1) Wie kann Sicherheit geboten und erklärt werden um Bedenken eines Datenaustausches zu vermeiden?
(2) Welche Balance zwischen Sicherheit und Komfort ist angemessen?
(3) Welche Dienstleistungen sind vorteilhaft oder notwendig für ein föderiertes Datenmanagementsystem?

Unter Beobachtung der Verbreitung von Technologien und steigender Nutzer-*innenzahlen digitaler Plattformen haben diese bereits an internationaler Akzeptanz gewonnen. Für diese neuen Entwicklungen muss dennoch erst Vertrauen in die Technologien geschaffen werden. Zur Ausarbeitung standen zu gewährleistende Sicherheitsziele, die Anforderungen des Datenschutzes aus gesetzlichen Vorgaben, technischen Systemschutz gegen Missbrauch von innen und außen sowie Verfügbarkeit, Integrität und Vertraulichkeit der Informationen und einen reibungslosen Betrieb in einem föderierten Datenökosystem umfassen. Dies kann eine dezentrale Sicherheitslösung mit sich bringen, in der von Einzelnen Verantwortung für Datensicherheit übernommen werden muss.

Während der Diskussion haben sich folgende essentielle Kernpunkte für einen ungehinderten organisationsübergreifenden Datenaustausch herauskristallisiert: Transparenz sowie Automatismen für offengelegte und standardisierte Richtlinien, Schulungen im Datensicherheitsbereich aber auch Datenmanagement bis hin zum neuen Berufsbild von Data Stewards.

Zur Einleitung der Diskussion wurden allgemeine Erfahrungen und Vertrauen zu Datenaustausch abgefragt. Gemäß der anonymen Umfrage konnten 40% der Teilnehmenden Beispiele zu einer stattgefunden Haftung nach einer „falschen" Datenweitergabe nennen. Knapp 70% haben auf eine Veröffentlichung von Daten verzichtet, wobei der mehrheitliche Anteil dieser nicht wollte, dass Ihre Daten ohne eigenen Nutzen verwendet würden. Dennoch sind 40% der Befragten an einem primär offenen Datenaustausch interessiert, frei für jeglichen Zugriff, wobei der restliche Anteil

einen gesicherten oder auch kontrollierten Zugang erwünscht.

Im Laufe der Diskussion hat sich herauskristallisiert, dass vor allem offene, standardisierte Richtlinien zu erstellen sind, um Vertrauen in sicheren Datenaustausch zu generieren. Im Laufe des Workshops galt Transparenz als Schlüsselelement für den Erfolg. Richtlinien müssen klar kommuniziert werden und in diesem Sinne offengelegte Standards gesetzt werden. Zurzeit werden Regelungen als Einzellösungen, anwendbar nur auf einzelne Projekte, geschaffen und beinhalten oftmals eine größere Anzahl an individuellen Vertraulichkeitsvereinbarungen. Generelle Lösungen, sowohl von juristischer als auch technischer Seite, sind noch Zukunftsthema. Ein weiterer Wunsch sind Automatismen, um der stetigen Dynamik in der Datenwirtschaft nachzukommen. Von juristischer Seite wird eine Reduktion der Komplexität der gegebenen Forderungen aus Datenschutzrecht, sowie auch Urheberrecht und Patentrecht, gewünscht. Als möglichen Ansatz würde eine Standardisierung der Fragestellungen dienen, sowie die Entwicklung halbautomatischer Prozesse wie aus dem Bereich der Legal Tech üblich.

Von technischer Seite wurde eine Vielzahl an Softwarelösungen im Laufe unterschiedlicher Themen erwähnt. Diese umfassen vorhandene Tools zur Anonymisierung, Pseudonymisierung, Datenbereinigung, Datenverschmelzung oder auch Entwicklungen zur Datenkontrolle wie digitale Wasserzeichen. Zur Anwendung kommen kommerzielle Cloudlösungen und Software wie ACP anywhere, Opentext Tempo Box, Cyware aber auch offene Lösungsansätze wie Hibernate, oder auch Bloxberg. Wobei gerade im Bereich größerer Datenmengen und Laufzeiten Eigenentwicklungen bzw. Modifikationen zu Einsatz kommen.

Vollständige Sicherheit kann aber aus technischer Seite nicht geboten werden. In Bezug auf Datenaustauschängste wurde dennoch geklärt, dass eine Haftung in der Regel nicht stattfinden kann, wenn nach aktuell gültigen Sicherheitsstandards gearbeitet wird. Dies soll auch ein Ansporn sein, Systeme auf aktuellem Niveau zu halten. Um die gegenwärtigen Entwicklungen überschauen zu können, wird oft auf externe Expertise zurückgegriffen.

Einen anderen essentiellen Faktor stellt die Informationsweitergabe von entwickelten Leitlinien sowie auch vorhanden Anwendungen dar. Die Übersicht an bereits verfügbaren Tools, ist oftmals nicht gegeben und muss an Forscher und weitere Anwender kommuniziert werden. Zusätzlich wird der Faktor Mensch als größtes Sicherheitsrisiko genannt. Mögliche Dienstleistungen umfassen Schulungen, vor allem auf der Seite der Datenschutzbeauftragten, aber neben dem Sicherheitsrahmen auch im Bereich der Datenanalyse und im Datenumgang. Parallel könnte das neue Berufsbild der Data Stewards integraler Bestandteil werden und ein solches Angebot durch übergreifende Projekte auch der Industrie näher gelegt werden.

Zusammengefasst könnte somit ungehinderter Datenaustausch auf Basis von Rechtssicherheit und Ordnungsmäßigkeit erfolgen, indem Standardisierung, am Beispiel von Zertifizierungen, oder auch Data Stewards zu Einsatz kommen.