Interuniversitäre Forschungsplattform
Zukunft – Technik – Gesellschaft (Z-T-G)

Policy Brief:
Privacy Enhancing Technologies

Entwickelt auf Grundlage der Ergebnisse des Forschungsprojekts Privacy Enhancing AI: Teilen ohne Weitergeben (Z-T-G 004)

Projekt:	Z-T-G 004 (AI Privacy)
Datum:	25. August 2025
Ansprechpersonen:	Roman Lukas Prunč, roman.prunc@tugraz.at Christian Dayé, christian.daye@tugraz.at
Mitwirkende:	Forscher:innenteam des Z-T-G (in alphabetischer Reihenfolge): Christian Dayé[1], Lea Demelius[2], Andreas Trügler[2, 3], Roman Lukas Prunč[1], Bernhard Wieser[1] [1] Technische Universität Graz, STS Unit [2] Know Center GmbH, Graz [3] Universität Graz, Sermilik Research Station

Zusammenfassung

Die nachfolgenden Empfehlungen gründen auf den Ergebnissen des Forschungsprojekts Privacy Enhancing AI: Teilen ohne Weitergeben (Z-T-G 04), in dem die Potentiale von Privacy Enhancing Technologies (PETs) für politische Entscheidungsprozesse erörtert wurden.

Aufbauend auf Expert:innenbefragungen und der Erhebung einer Bürger:innensicht wurden sechs Empfehlungen entwickelt. Diese sollen Personen aus dem Bereich der öffentlichen Verwaltung bei der Implementierung von Systemen unterstützen, bei denen sensible Daten verarbeitet und durch den Einsatz von PETs geschützt werden. Insbesondere bieten sie eine Hilfestellung, wie Vertrauen in solche Systeme hergestellt und erhalten und somit ein gesellschaftlicher Rückhalt dafür geschaffen werden kann.

Sechs Empfehlungen

Empfehlung 1: Sensibilisierung für Themen des Datenschutzes

Datenschutz ist ein grundlegendes Mittel zur Wahrung des Rechts auf Privatheit. Insbesondere aufgrund der Digitalisierung gibt es ein starkes öffentliches Bewusstsein für das Thema. Daher ist es essenziell, dass bei der Umsetzung jedes Systems die notwendigen Schutzmaßnahmen eingehalten werden und dass dem Thema große Aufmerksamkeit geschenkt wird, insbesondere, aber nicht nur, wenn die verarbeitenden Daten sensible persönliche Informationen enthalten.

In diesem Sinne sollte stets die Frage gestellt werden, ob das System tatsächlich keinerlei Rückschlüsse zulässt, ob dieser Schutz Bestand hat und ob weitere Verbesserungen möglich sind.

Empfehlung 2: Datenschutz als Komponente der Systementwicklung

Es gilt, Datenschutz und Datenminimierung bereits bei der Entwicklung des Systems zu berücksichtigen.

Ein sinnvoll konzipiertes System sollte von Grund auf von der Frage angeleitet werden, wie es bestmöglich datenschutzfreundlich umgesetzt werden kann. Kryptografische Methoden sind ein Teil dieser Abwägungen, doch sollten diese grundlegend in die Implementierung integriert sein und keinesfalls lediglich auf ein fertiges System aufgesetzt werden. Zudem

sollte auch hinterfragt werden, ob der Einsatz von Verschlüsselungstechnologien tatsächlich notwendig ist, oder ob ein Schutz auch auf andere Art erreicht werden kann.

Ein wesentlicher Punkt ist dabei auch die Frage, welche Daten und welche Auswertungen tatsächlich für die Funktionalität benötigt werden. Diese sollten stets auf ein quantitatives und identifizierendes Minimum beschränkt werden. Zudem sollte nach Möglichkeit davon abgesehen werden, neue (kombinierte) Datensätze zu erstellen. Durch solche Maßnahmen wird ein zusätzlicher Schutz auch vor zukünftiger missbräuchlicher Verwendung geschaffen.

Empfehlung 3: Freiwilligkeit

Im Sinne der demokratischen Qualität eines Systems aber auch der Schaffung von Vertrauen diesem gegenüber ist die Frage maßgebend, inwiefern die Teilnahme beziehungsweise die Bereitstellung der eigenen Daten verpflichtend ist oder auf Freiwilligkeit beruht. Die Möglichkeit, zu entscheiden, was mit persönlichen Informationen geschieht ist wesentlich für eine breite Zustimmung. Dabei reicht es für diese Zwecke eine einfach zugängliche Opt-out Option zu bieten, mittels welcher Bürger:innen ihre Zustimmung verweigern können. Fehlt eine solche Möglichkeit der autonomen Entscheidung, schafft dies Unmut und Misstrauen bezüglich des Zwecks und der Absichten, die hinter dem System stehen und schafft Platz für Vorwürfe der Kontrolle und der Überregulierung.

Empfehlung 4: Transparenz

Des Weiteren ist es wichtig, dass die eingesetzten Methoden nachvollziehbar und transparent kommuniziert werden. Das bedeutet, dass sie prinzipiell offen und die Informationen leicht zugänglich und klar sind. Dies ist umso wichtiger, je sensibler die eingesetzten Daten und der zugehörige Themenbereich sind.

Da Verschlüsselungsmethoden auf komplexen mathematischen Verfahren beruhen, bedarf es zudem eines gewissen Aufklärungs- und Informationsaufwands. Somit braucht es bei der Kommunikation der Maßnahmen nicht nur Personen und Institutionen, die für die Sicherheit der Systeme bürgen, sondern dazu auch Erklärungen, die breit nachvollziehbar sind. In diesem Kontext können auch NGOs eine bedeutende Rolle als Kontrollinstanzen und damit als vertrauensbildende Institutionen sowie auch als komplexitätsreduzierende Kommunikatoren an die Öffentlichkeit spielen.

Empfehlung 5: Gesetzmäßigkeit

Eine wichtige vertrauensbildende Maßnahme bei der Umsetzung datenverarbeitender Systeme ist die Bindung staatlicher Maßnahmen an Gesetze. Einerseits die Notwendigkeit, Verfassungsgesetzen zu entsprechen, was bedeutet, dass gewisse Schutzgarantien stetig

bestehen bleiben und Grundrechte nicht verletzt werden dürfen. Andererseits die Notwendigkeit, auch jede einzelne Maßnahme auf einem entsprechenden Gesetz zu begründen oder dieses zu beschließen. Auch die Gesetzmäßigkeit von Maßnahmen bedarf einer klaren Kommunikation, um Vertrauen zu schaffen und zu erhalten. Es muss deutlich sein, dass alles grundrechtskonform gelöst wurde und keine Ambiguitäten enthalten sind. Sobald hier etwas unklar erscheint oder Anlass für Debatten und Auslegungsfragen bietet, schafft dies Zweifel. Dementsprechend sollte neben der DS-GVO stets auch mitbedacht werden, ob durch die relevante Maßnahme auch in andere Rechte eingegriffen wird und inwiefern ein solcher Eingriff vertretbar ist.

Empfehlung 6: Zweck

Schließlich ist es nicht nur die implementierte Technologie an sich, welche die Perspektive von Bürger:innen formt und somit für den Erfolg eines Systems verantwortlich ist. Auch deren Umsetzung ist nur zweitrangig, wenn auch nicht unwesentlich. Im Vordergrund steht stets der Zweck, zu welchem ein System eingeführt wird. Ist dieser belastet, kann dies selbst das datenschutzfreundlichste System nicht ausgleichen. Vielmehr noch werden die Zweifel, die dem Gesamtthema eigen sind, auch auf die Technologie übertragen. So kann auch Vertrauen in die Methode und in die Institution die Hemmnisse nicht kompensieren, die schlagend werden, wenn der Zweck des Systems abgelehnt wird. Daher ist es unabdingbar, offen zu kommunizieren, wofür das System eingesetzt wird und eine breite gesellschaftliche Mehrheit dahinter zu wissen.

Die Einhaltung aller zuvor genannten vertrauensfördernden Maßnahmen ist für jedes System von Anfang an notwendig. Denn hat sich Misstrauen einmal breitgemacht, ist es nahezu unmöglich dieses wieder loszuwerden