Datenschutz und Beschaffungsrecht
Effizienzgewinn versus Grundrechtsgefährdung bei KI-Projekten der öffentlichen Hand

Wenn die öffentliche Hand Lösungen mit KI-Technik einkauft, muss dem Datenschutz besondere Aufmerksamkeit gelten. Denn die neuen Technologien schaffen nicht nur mehr Effizienz, sie können auch einen Eingriff in die Grundrechte darstellen. Die Problemfelder und Lösungsansätze werden anhand eines Veranschaulichungsbeispiels der SBB erläutert.

«SBB wollen mit Gesichtserkennung Reisende ausspionieren.» So titelte der K-Tipp im Februar 2023. Inwiefern das stimmt und datenschutzrechtlich problematisch ist, darüber lieferten sich Fachpersonen und die SBB in den darauffolgenden Wochen eine medial aufgeladene Schlammschlacht. Fakt ist: Die SBB schrieb anfangs Februar einen Auftrag für ein «KundenFrequenzMessSystem» (KFMS) aus (Projekt-ID 251404, siehe intelliprocure.ch). Ziel des Beschaffungsprojekts war es Daten zu sammeln mittels vom Anbieter betriebenen «smarten» Kameras. Damit sollten Personenbewegungen an Bahnhöfen gemessen sowie Kundensegmente nach Alter, Grösse und mitgeführten Gegenständen wie Koffer oder Kinderwagen unterschieden werden, hiess es in den Ausschreibungsunterlagen. Fakt ist: Die SBB ist nicht allein. Die öffentliche Hand verwendet zunehmend technische Tools, die auf KI-Systemen basieren. Dabei ist Vorsicht geboten (vgl. «Rechtliche Aspekte von KI», S. 60), besonders wenn mit den Systemen Personendaten gespeichert oder anderswie bearbeitet werden.

Höhere Pflichten für öffentliche Unternehmen

Der Datenschutz ist ein Grundrecht. Es schützt die Privatsphäre und damit die persönlichen Daten vor einer missbräuchlichen Bearbeitung. Als personenbezogene Daten gelten solche, die sich auf eine bestimmte oder bestimmbare Person beziehen, beispielsweise Name, Adressen oder Beruf. Will eine Firma oder eine Verwaltungseinheit Personendaten bearbeiten, ist sie an die Datenschutzgesetze gebunden. So darf sie nur so viele Daten wie nötig sammeln (Prinzip der Datensparsamkeit) und muss diese nach ihrer Nutzung löschen. An «besonders schützenswerte» Personendaten werden höhere Anforderungen gestellt. Darunter fallen zum Beispiel die religiöse Zugehörigkeit, sexuelle Orientierung, biometrische Daten oder das «Profiling». Um die beiden letztgenannten Kategorien ging es bei der Ausschreibung der SBB. Das Datenschutzgesetz des Bundes unterscheidet ausserdem zwischen «normalen Firmen» (juristische Personen) und öffentlichen Unternehmen. Für Letztere gelten strengere Regeln, weil sie oft Dienstleistungen mit Monopolcharakter aufweisen, die zum Teil auch zwingend genutzt werden müssen.

Spannungsfeld Effizienzgewinn und Grundrechtsgefährdung

Mit KI-Technologien kann die öffentliche Hand ihre Prozesse effizienter gestalten, Kosten sparen und Innovationspotenziale erschliessen (vgl. «KI im öffentlichen Sektor», S. 56). Doch wenn die KI-Technologien Personen identifizieren, stellt das immer auch einen Eingriff in die Grundrechte der betroffenen Personen dar, der gerechtfertigt sein muss. Bei der Beschaffung von KI-Lösungen mit Personendatenbezug ist es deshalb wichtig, die Brücke zu schlagen zwischen der Gewährleistung des Datenschutzes und der gewinnbringenden Nutzung dieser Technologien. Das gelingt nur, wenn eine gesetzliche Grundlage für die Datenerhebung besteht und wenn der Datenschutz in den Beschaffungsprozess integriert wird. Dazu gehört auch, dass entsprechende Kriterien und Spezifikationen in die Ausschreibung aufgenommen werden. Und was geschah nun mit der Causa SBB? Nach der medialen Aufmerksamkeit um die Ausschreibung des «KundenFrequenzMessSystems» brach die SBB die Ausschreibung ab – in der neuen Ausschreibung «KFMS 2.0» (Projekt-ID 258560) vom Juni 2023 verzichtete sie gänzlich auf die Unterscheidung von Kundensegmenten und wies explizit darauf hin, dass keine Personendaten erfasst werden.

Unsere Empfehlungen

1. Datenschutzgrundsätze bereits bei der Bedarfsanalyse berücksichtigen

Bereits von Anfang an Lösungen ausschliessen, die mehr Personendaten als nötig erheben oder einer gesetzlichen Grundlage entbehren.

2. Datenschutz in Ausschreibungen verankern

Spezifikationen oder Eignungskriterien in Bezug auf den Datenschutz definieren wie zum Beispiel «Privacy by Design», Datenschutzkonzept oder Zertifizierung verlangen.

3. Aktive und transparente Kommunikation

Die Bevölkerung sollte über potenziell umstrittene Ausschreibungen informiert werden. Ausserdem sollte vorgängig ein Stakeholder-Dialog durchgeführt werden um potenzielle Datenschutzrisiken frühzeitig zu erkennen.

Mehr Informationen

Kontaktmöglichkeiten und weitere Informationen zu Datenschutz und Beschaffungsrecht: bfh.ch/ipst/public-procurement

Kontakt

Prof. Dr. Rika Koch
Professur Public Procurement

rika.koch@bfh.ch
T +41 31 848 41 68

Safiya Verbruggen
Koordinatorin Lehre, Weiterbildung und Events

safiya.verbruggen@bfh.ch
T +41 31 848 53 42