Ethische Leitplanken bei der Entwicklung Darmstadts zur Digitalstadt

Präambel:

Die digitalen Technologien sollen zum Nutzen der Menschen in allen Bereichen städtischen Lebens, entsprechend den Bedürfnissen der Bürgerschaft und der von den Projekten Betroffenen, entwickelt und eingesetzt werden. Um dies zu sichern und möglichen Gefährdungen der Stadtgesellschaft insgesamt und der einzelnen Bürger durch die Digitalisierung zu begegnen, soll dem Einsatz und der Ausgestaltung digitaler Technologien durch die folgenden ethischen Leitplanken ein orientierender und begrenzender Rahmen gesetzt werden.

Die Arbeitsgruppe Ethik des von der Stadtverordnetenversammlung berufenen Ethik- und Technologiebeirats hat diese Leitplanken erarbeitet. Sie gelten für das Handeln der Digitalstadt Darmstadt GmbH, der weiteren städtischen Beteiligungen, sowie der städtischen Verwaltung. Der Ethik- und Technologiebeirat unterstützt hierbei die Digitalstadt Darmstadt insbesondere in der Verantwortung als Modellstadt.

1. **Gemeinwohlverpflichtung**

   Der Digitalisierungsprozess muss dem Gemeinwohl verpflichtet sein. Ziel der digitalen Umgestaltung muss stets eine soziale und/oder ökologische Verbesserung der kommunalen Daseinsvorsorge und anderer städtischer Leistungen sein. Dies soll so wirtschaftlich und effizient wie möglich erfolgen.

2. **Demokratische Kontrolle**

   Die Zielsetzung, Entwicklung, Durchführung und Nutzung von Digitalisierungsprojekten muss gemäß der geltenden/bestehenden Regelungen der parlamentarisch kontrollierten Selbstverwaltung unterliegen. Dies gilt auch für Gesellschaften mit Beteiligungen der Stadt. Es dürfen keine neuen Machtstrukturen entstehen, die sich demokratischer Kontrolle entziehen und eine Gefahr für die Grundrechte, die Sicherheit und Privatsphäre der Einzelnen darstellen.

3. **Verantwortung und Transparenz**

   Die Verantwortung demokratisch gewählter Gremien für Entscheidungen der Stadt muss erhalten bleiben. Automatisierte Verfahren dürfen diese nicht ersetzen Die Kriterien automatisierter Verwaltungsentscheidungen sind offenzulegen. Bei Kommunikationen der Stadt mit Bürgerinnen und Bürgern ist von vornherein klarzustellen, wenn eine Maschine eingesetzt wird.

4. **Diskriminierungs- und barrierefreier Zugang zu Dienstleistungen**

   Die Zugänglichkeit und Nutzbarkeit von analogen Dienstleistungen oder entsprechender analoger Hilfsangebote müssen erhalten bleiben, um die gesellschaftliche Teilhabe aller Gruppen der Stadtbevölkerung zu ermöglichen.

5. Souveränität von Stadt und Bürgerschaft

Die öffentliche Hand und die Bürgerschaft müssen digitale Infrastrukturen, Plattformen und grundlegende Dienste souverän entwickeln, betreiben und nutzen können. Abhängigkeiten von Produkten und Firmen sind zu vermeiden.

6. Datenschutz

Darmstadt will Vorreiter im Datenschutz sein. Bei der Erhebung, Verarbeitung und Veröffentlichung von Daten ist von Anfang an der Datenschutz zu berücksichtigen. Personenbezogene Daten dürfen so wenig wie möglich erfasst und weitergegeben werden. Personenbezogene Daten dürfen nicht verkauft werden. Geben die Stadt oder städtische Gesellschaften Daten an Dritte weiter, ist deren verantwortungsvoller Umgang mit den Daten durch entsprechende Nutzungsvereinbarungen zu regeln.

7. Veröffentlichung von Daten

Nicht-personenbezogene Daten, die für die Öffentlichkeit von demokratisch beschlossenem und legitimiertem Interesse sind, müssen ihr in nutzerfreundlicher Form zugänglich gemacht und zur Verfügung gestellt werden.

8. Technikfolgenabschätzung und Nachhaltigkeit

Bei allen Digitalisierungsprojekten sind von Anfang an die Folgen für die ökologische Nachhaltigkeit, für die Gewährleistung von Information und Kommunikation, für die Mobilität und die Gesundheit, für den sozialen Ausgleich sowie für die Gestaltung der Arbeit zu untersuchen und zu bewerten. Alle Digitalisierungsprojekte sollen heutigen und künftigen Generationen gleichermaßen Entwicklungschancen bieten.

9. Gewährleistung der Infrastruktursicherheit

Bei allen Digitalstadtprojekten ist die Verletzlichkeit der Systeme zur Daseinsvorsorge zu beachten und ihre Funktionssicherheit zu gewährleisten (Cybersicherheit).