

STÄDTE- UND GEMEINDEBUND SACHSEN-ANHALT



SGSA, Sternstr. 3, 39104 Magdeburg

Deutscher Städtetag
Hausvogteiplatz 1
10117 Berlin

Per E-Mail: melissa.schmidt@staedtetag.de

Städte- und Gemeindebund
Sachsen-Anhalt (SGSA)
- Landesgeschäftsstelle -
Sternstraße 3, 39104 Magdeburg

Telefon: 0391 5924-300
Telefax: 0391 5924-444

E-Mail: post@sgsa.info
Internet: www.kommunales-sachsen-anhalt.de

Sparkasse MagdeBurg
IBAN: DE56 8105 3272 0036 0029 00
BIC/SWIFT: NOLADE21MDG

Auskunft erteilt: Frau Schulz
Durchwahl: 0391 5924-390

Ihr Zeichen, Ihre Nachricht vom

Unser Zeichen
38–10–00/Sch

Datum
19.08.2026

Smart Cities: Beiträge der digitalen Transformation zur Urbanen Resilienz Entwurf eines Positionspapiers des Deutschen Städtetages

Sehr geehrter Herr Dr. Lindner,

wir bedanken uns für die Möglichkeit, zu dem Entwurf eines Positionspapiers des Deutschen Städtetages – Smart Cities: Beiträge der digitalen Transformation zur Urbanen Resilienz – Stellung nehmen zu dürfen.

Ausdrücklich wird begrüßt, dass urbane Resilienz nicht auf Katastrophenschutz verengt, sondern als Querschnittsaufgabe der integrierten Stadtentwicklung verstanden wird. Zutreffend sind insbesondere die Forderungen nach dauerhafter Finanzierung, interoperablen Standards, digitaler Souveränität, sicheren Rückfallebenen und einer Übertragung der Ergebnisse aus den Modellprojekten Smart Cities in die Breite.

Aus den Erfahrungen unserer Verbandsmitglieder mit Smart-City-Prozessen sowie mit missionsorientierten und sektorübergreifenden Ansätzen im Umfeld von ProjectTogether wird jedoch Ergänzungsbedarf gesehen. Der Entwurf beschreibt viele geeignete Technologien, bleibt aber bei der Frage, wie Kommunen, Zivilgesellschaft, Wirtschaft und Wissenschaft dauerhaft gemeinsam handlungsfähig werden, also die praktische Umsetzung, noch zu allgemein. Gerade diese Kooperations- und Umsetzungsfähigkeit ist ein Kern urbaner Resilienz.

Der Entwurf bildet die wesentlichen Gefährdungslagen und Handlungsfelder weitgehend realistisch ab. Positiv hervorzuheben sind der integrierte Resilienzbegriff, die Verbindung von Alltagsnutzen und Krisennutzen sowie die klare Warnung vor neuen digitalen Abhängigkeiten. Die vorgeschlagenen Technologien sollten jedoch konsequenter als Mittel zum Zweck und nicht als Ausgangspunkt kommunaler Resilienzpoltik behandelt werden.

1. Resilienz als Fähigkeit zum gemeinsamen Handeln

Resilienz entsteht nicht allein durch Sensorik, Datenplattformen oder digitale Zwillinge. Sie beruht ebenso auf belastbaren Beziehungen, geklärten Rollen, gemeinsam eingeübten Entscheidungswegen und Vertrauen. Verwaltung, kommunale Unternehmen, Hilfsorganisationen, Zivilgesellschaft, lokale Wirtschaft, Wissenschaft und Betreiber versorgungsrelevanter Infrastrukturen sollten bereits vor einer Krise verbindlich zusammenarbeiten. Dafür braucht es lokale Resilienzallianzen oder vergleichbare Kooperationsstrukturen mit klaren Mandaten, Ansprechpartnern, Ressourcen und Übungszyklen.

Vorgeschlagene Ergänzung: „Urbane Resilienz ist nicht nur eine Eigenschaft technischer Systeme, sondern die Fähigkeit lokaler Akteure, unter Unsicherheit gemeinsam zu entscheiden und zu handeln. Bund und Länder sollten Kommunen beim Aufbau dauerhaft finanzierter, sektorübergreifender Resilienzallianzen unterstützen.“

2. Zivilgesellschaft und soziale Infrastruktur verbindlich einbeziehen

Der Abschnitt zur sozialen Resilienz ist richtig angelegt, behandelt Bürgerinnen und Bürger aber überwiegend als Adressaten von Warnung, Information und Qualifizierung. Sie sollten zusätzlich als Mitgestaltende, Wissensgeber und Träger lokaler Unterstützungsstrukturen verstanden werden. Nachbarschaftsinitiativen, Vereine, Wohlfahrtsverbände, Migrant*innenorganisationen, Religionsgemeinschaften, Freiwilligenagenturen und soziale Orte sind im Alltag Vertrauensanker und können in Krisen entscheidende Reichweite schaffen. Diese Leistungen benötigen verlässliche Schnittstellen zur Verwaltung sowie Finanzierung, Qualifizierung und Absicherung.

Digitale Beteiligung darf analoge Zugänge nicht ersetzen. Barrierefreiheit, Mehrsprachigkeit, Datenschutz, digitale Grundkompetenzen und die gezielte Einbindung vulnerabler oder digital wenig erreichbarer Gruppen sollten als verbindliche Qualitätskriterien benannt werden.

3. Vom Pilotprojekt zur verlässlichen kommunalen Infrastruktur

Der Entwurf fordert zu Recht Transfer und Nachnutzung. Wissensplattformen und Open-Source-Veröffentlichungen allein reichen jedoch nicht. Eine Lösung ist erst übertragbar, wenn Dokumentation, Wartung, Support, IT-Sicherheit, Datenschutz, Beschaffung, Schulung, Datenmigration, Finanzierung des laufenden Betriebs und ein Ausstieg aus Anbieterabhängigkeiten geklärt sind. Förderfähig sein sollten deshalb nicht nur Entwicklung und Einführung, sondern auch Konsolidierung, Produktpflege, gemeinschaftliche Betreiberstrukturen und die Anpassung an unterschiedliche kommunale Ausgangslagen.

4. Wirkung, Lernfähigkeit und Rechenschaft

Benchmarking und Indikatoren werden angesprochen, sollten aber konkreter gefasst werden. Nicht die Zahl installierter Sensoren oder veröffentlichter Datensätze ist entscheidend, sondern die nachgewiesene Wirkung: verkürzte Warn- und Reaktionszeiten, bessere Erreichbarkeit, geringere Ausfallzeiten, erreichte vulnerable Gruppen, schnellere Wiederherstellung und ein messbarer Alltagsnutzen. Resilienzchecks und Stresstests sollten regelmäßig, sektorübergreifend und unter Beteiligung externer Akteure durchgeführt werden. Nach Ereignissen und Übungen braucht es verbindliche Auswertungen, öffentlich nachvollziehbare Lernschleifen und aktualisierte Maßnahmenpläne. Auch nicht erfolgreiche Pilotvorhaben sollten dokumentiert werden, damit andere Kommunen daraus lernen können.

5. Digitale Sicherheit, KI und analoge Rückfallebenen präzisieren

Der Entwurf benennt digitale Verwundbarkeiten, verwendet KI- und ML-Anwendungen aber an mehreren Stellen fast selbstverständlich als Lösung. Im Krisenmanagement müssen Eignung, Datenqualität, Verzerrungsrisiken, Nachvollziehbarkeit, menschliche Letztentscheidung

und Ausfallverhalten vorab geprüft und regelmäßig getestet werden. Für sicherheitsrelevante Anwendungen sind manuelle Übersteuerung, Offline-Fähigkeit, dokumentierte Wiederanlaufziele, Notstrom, Datenminimierung, Lieferketten- und Dienstleisterrisiken sowie erprobte Exit- und Wiederherstellungsverfahren erforderlich.

Zudem sollte der Begriff „kritische Infrastruktur“ differenziert verwendet werden. Nicht jede Smart-City-Komponente ist rechtlich oder funktional kritische Infrastruktur; Schutzanforderungen sollten anhand der tatsächlichen Kritikalität, der Folgen eines Ausfalls und der Abhängigkeiten festgelegt werden.

6. Kleinere Kommunen, Stadt-Umland-Verflechtungen und regionale Kooperation

Der Entwurf ist stark aus der Perspektive größerer Städte formuliert. Resilienz entsteht jedoch in funktionalen Räumen: Energie, Wasser, Mobilität, Gesundheit, Rettungswesen, Lebensmittelversorgung und digitale Netze überschreiten Gemeindegrenzen. Kleinere und mittlere Kommunen benötigen regionale Daten- und Betriebsmodelle, interkommunale Kompetenzpools, gemeinsame Beschaffung sowie Unterstützung durch Länder und kommunale IT-Dienstleister. Skalierung sollte daher nicht nur als Übernahme einer Software, sondern als Aufbau geteilter Dienste und regionaler Verantwortung verstanden werden.

7. Verteilungsgerechtigkeit und Schutz vor unbeabsichtigten Folgen

Resilienzmaßnahmen können Belastungen und Nutzen ungleich verteilen. Hitzeschutz, Warnsysteme, Mobilitätssteuerung oder datenbasierte Priorisierung müssen deshalb auf Verteilungseffekte geprüft werden. Notwendig sind sozialräumliche Analysen, Datenschutz-Folgenabschätzungen, barrierefreie Alternativen und transparente Kriterien für Priorisierungsentscheidungen. Effizienzgewinne dürfen nicht zulasten derjenigen gehen, die digital schlechter erreichbar sind oder bereits höhere Krisenrisiken tragen.

Die Forderungen können priorisiert zusammengefasst werden:

1. Dauerfinanzierung statt Projektlogik: Vollkosten einschließlich Personal, Betrieb, Wartung, Sicherheit, Schulung, Evaluation und Weiterentwicklung müssen förderfähig sein.
2. Gemeinsame Basisinfrastrukturen und Standards: Bund und Länder sollten verbindliche Mindeststandards, Referenzarchitekturen, Musterverträge und sichere Basisdienste bereitstellen, ohne kommunale Gestaltungsspielräume zu verengen.
3. Finanzierter Transfer: Nachnutzung braucht Transferstellen, technische Unterstützung, rechtssichere Beschaffungswege, Migrationshilfen und gemeinschaftliche Betreiber- und Supportmodelle.
4. Kommunale Kompetenz und Personal: Förderung muss dauerhafte Fach- und Koordinationsstellen, interkommunale Teams und Qualifizierung ermöglichen; reine Sachmittelförderung greift zu kurz.
5. Sektorübergreifende Resilienzallianzen: Kooperation mit Zivilgesellschaft, Wirtschaft, Wissenschaft, Hilfsorganisationen und Infrastrukturbetreibern sollte als förderfähiger Bestandteil kommunaler Resilienzstrategien anerkannt werden.
6. Wirkungsorientierung und Lernsystem: Gemeinsame Kernindikatoren, wiederkehrende Stresstests, Lernberichte und eine systematische Auswertung von Erfolgen wie Fehlschlägen sollten verbindlich vorgesehen werden.

Das Positionspapier setzt einen wichtigen und richtigen Rahmen. Es wird deutlich gewinnen, wenn es Resilienz konsequent als gemeinschaftliche, lernende und dauerhaft finanzierte Handlungsfähigkeit beschreibt. Digitale Technik ist dabei unverzichtbar, aber nicht hinreichend. Erst das Zusammenspiel von sicheren Infrastrukturen, handlungsfähiger Verwaltung,

tragfähigen lokalen Beziehungen, sozialer Teilhabe, klarer Verantwortung und systematischem Transfer macht Smart-City-Ansätze krisenfest und im kommunalen Alltag wirksam.

Mit freundlichen Grüßen
Im Auftrage

A handwritten signature in blue ink, appearing to read 'A. Schulz'.

Schulz