

Open Data im Sicherheitskonflikt

Das Spannungsverhältnis zwischen Digitalen Zwillingen, Open Data und neuen Sicherheitsanforderungen – der Rechtsrahmen

Behördliche Daten im Laufe der Zeit... der Schutz des Datenschutzes



Behördliche Daten im Laufe der Zeit... Kamelle!



Behördliche Daten im Laufe der Zeit... Nachdenklichkeit



Ausgangslage und Konfliktverständnis

Digitale Zwillinge

Digitale Zwillinge sind hochpräzise, digitale Abbilder der realen Welt, wie Infrastruktur, Gebäude und Prozesse. Sie ermöglichen Simulationen, Planung und Echtzeit-Entscheidungen. Der wirtschaftliche Wert dieser Systeme ist enorm, da sie Effizienzgewinne und Innovationen für die öffentliche Verwaltung, Wirtschaft und Forschung ermöglichen.

Hochpräzise Repräsentation
der realen Welt (in Echtzeit)

Ermöglichung dynamischer
Simulation und Analyse

Steigerung der Effizienz
und Innovation

Anwendung in Verwaltung,
Wirtschaft und Forschung

Spannungsfeld zwischen Detailtiefe und Sicherheitsrisiken

- Je höher die Detailtiefe (z.B. Zugangspunkte, unterirdische Versorgungsleitungen, Betriebsabläufe, Notfallpläne, KRITIS-Standorte), desto größer wird die Gefahr von Missbrauch durch:



Cyberangriffe



Spionage



Terrorismus



Sabotage

- Besonders im Kontext des Ukraine-Konflikts hat das Bundesverteidigungsministerium kritisch auf die hohe Offenheit von Geodaten (KRITIS, militärische Liegenschaften) hingewiesen.

Interessenkonflikte

- Öffentliche Verwaltung und Betreiber kritischer Infrastrukturen wollen Schutz
- Wirtschaft und Wissenschaft fordern offenen, vollständigen und aktuellen Zugang zu Daten
- Politik verfolgt Transparenz-, Innovations- und Standortziele, bekennt sich aber zugleich zu Schutz und Resilienz

Gesetzlicher und
gesellschaftlicher Druck für
maximale Transparenz



Notwendigkeit, Systeme und
insbesondere kritische
Informationen zu schützen

Open Data Verpflichtungen (Beispiele)

§ 12a Offene Daten des Bundes, Verordnungsermächtigung (E-Government-Gesetz - EGovG)

- (1) Die Behörden des Bundes mit Ausnahme der Selbstverwaltungskörperschaften stellen unbearbeitete maschinenlesbare Daten, die sie zur Erfüllung ihrer öffentlich-rechtlichen Aufgaben erhoben haben oder durch Dritte in ihrem Auftrag haben erheben lassen, zum Datenabruf über öffentlich zugängliche Netze bereit. Ein Anspruch auf Bereitstellung dieser Daten wird hierdurch nicht begründet. Satz 1 gilt nicht für natürliche Personen und juristische Personen des Privatrechts, denen hoheitliche Aufgaben zur selbständigen Wahrnehmung übertragen wurden.
- (2) Absatz 1 gilt für Daten, die
 1. der Behörde elektronisch gespeichert und in Sammlungen strukturiert vorliegen, insbesondere in Tabellen oder Listen,
 2. ausschließlich Tatsachen enthalten, die außerhalb der Behörde liegende Verhältnisse betreffen,
 3. nicht das Ergebnis einer Bearbeitung anderer Daten durch eine Behörde des Bundes sind,
 4. nach der Erhebung keine Bearbeitung erfahren haben, ausgenommen eine Bearbeitung,
 - a) die der Fehlerbereinigung dient oder
 - b) die aus rechtlichen oder aus tatsächlichen Gründen erfolgt ist und ohne die eine Veröffentlichung der Daten nicht möglich wäre, und
 5. bei Personenbezug derart umgewandelt wurden, dass
 - a) sie sich nicht mehr auf eine identifizierte oder identifizierbare natürliche Person beziehen oder
 - b) die betroffene Person nicht oder nicht mehr identifiziert werden kann.



Open Data Verpflichtungen (Beispiele)



§ 12a Offene Daten des Bundes, Verordnungsermächtigung (E-Government-Gesetz - EGovG)

- (3) Abweichend von Absatz 1 Satz 1 müssen die Daten nicht bereitgestellt werden, wenn
1. An Daten
 - a) kein oder nur ein eingeschränktes Zugangsrecht insbesondere gemäß den §§ 3, 4 und 6 des Informationsfreiheitsgesetzes besteht oder
 - b) ein Zugangsrecht erst nach der Beteiligung Dritter bestünde,
 2. die Daten ohne Auftrag der Behörde von Dritten erstellt und ihr ohne rechtliche Verpflichtung übermittelt werden,
 3. es sich um Daten handelt, die zu Forschungszwecken erhoben wurden und bereits über öffentlich zugängliche Netze entgeltfrei bereitgestellt werden; die Möglichkeit der freiwilligen Bereitstellung dazugehöriger Metadaten über das nationale Metadatenportal GovData bleibt davon unberührt, oder
 4. die Daten unter das Bankgeheimnis fallen. [...]

Verpflichtung, zur Erfüllung öffentlich-rechtlicher Aufgaben erhobene Daten, bereitzustellen

Open by Default

Offenheit, soweit keine spezialgesetzlichen oder schutzwürdigen Ausnahmen greifen

Open Data Verpflichtungen (Beispiele)



§ 16a Offen zugängliche Daten - Open Data (E-Government Gesetz NRW)

- (1) Die **Behörden** des Landes **stellen elektronische Daten**, die sie zur Erfüllung ihrer öffentlich-rechtlichen Aufgaben erhoben haben oder durch Dritte in ihrem Auftrag haben erheben lassen, zum Datenabruf über öffentlich zugängliche Netze **zur Verfügung**. Auch Kommunen können diese Daten zur Verfügung stellen.
- (2) Absatz 1 gilt für Daten, die
 1. der Behörde elektronisch gespeichert und in Sammlungen strukturiert vorliegen, insbesondere in Tabellen- oder Listenform oder Datenbanken, und
 2. ausschließlich Tatsachen enthalten, die außerhalb der Behörde liegende Verhältnisse betreffen.
- (3) Abweichend von Absatz 1 **müssen die Daten nicht bereitgestellt werden, wenn**
 1. zu den Daten kein oder nur ein eingeschränktes Zugangsrecht insbesondere gemäß der §§ 6 bis 9 des Informationsfreiheitsgesetzes Nordrhein-Westfalen vom 27. November 2001 (GV. NRW. S. 806) in der jeweils geltenden Fassung besteht,
 2. ein Zugangsrecht erst nach der Beteiligung Dritter bestünde,
 3. Urheberrechte oder verwandte Schutzrechte Dritter entgegenstehen oder
 4. die Daten bereits von Dritten als offene Daten im Sinne des § 16a zur Verfügung gestellt werden. [...]

Verpflichtung, zur Erfüllung öffentlich-rechtlicher Aufgaben erhobene Daten, bereitzustellen

Open by Default

Offenheit, soweit keine spezialgesetzlichen oder schutzwürdigen Ausnahmen greifen

Open Data Verpflichtungen

- Geodaten, die für Digitale Zwillinge benötigt werden, werden meist von Behörden im Rahmen ihrer gesetzlichen Aufgaben erhoben (z.B. Digitaler Zwilling NRW).
- Diese Geodaten fallen systematisch in den Anwendungsbereich der Open Data-Pflichten – sie unterliegen also grundsätzlich der Veröffentlichungspflicht, sofern keine spezialgesetzlichen oder sonstigen schutzwürdigen Ausnahmen greifen.
- Der Bund selbst ist dabei häufig kein originärer Erzeuger entsprechender Geodaten, sondern auf die Datenerhebung der Länder und Kommunen angewiesen. Daher hat der Bund ein besonderes Interesse an möglichst freier Datenverfügbarkeit.
- Gleichzeitig unterliegen sensible Geodaten im Verantwortungsbereich des Bundes (z. B. Verteidigungsministerium, Sicherheitseinrichtungen) regelmäßig spezialgesetzlichen Ausnahmen und werden aus Sicherheitsgründen nicht veröffentlicht.

Spezialgesetze und Konkurrenzregelungen

- Geodatenzugangsgesetz (GeoZG) (jeweils auf Bundes- und Landesebene)
- Umweltinformationsgesetz (UIG) (Anwendungsvorrang bei Umweltbezug)
 - Enthalten speziellere Bestimmungen zur Bereitstellung, Nutzung und zum Schutz von Geodaten
 - Können Einschränkungen des offenen Datenzugangs bei Gefahr für Sicherheit, Verteidigung, etc. hervorrufen
- Datennutzungsgesetz (DNG) (Bundesebene)
 - Zur Umsetzung EU-Open Data Richtlinie
 - Begründet selbst keine Veröffentlichungspflichten, sondern regelt, wie Daten bereitgestellt werden, wenn ein Zugang(sanspruch) besteht oder Daten freiwillig bereitgestellt werden
- Entwurf für KRITIS-Dachgesetz zur Umsetzung der EU-CER-Richtlinie
 - Gesetz verlangt eine nachvollziehbare, risiko- und sachbezogene Bewertung jeder Datenbereitstellung für KRITIS-relevante Anlagen
 - Erhöhter Druck, detaillierte Daten zurückzuhalten
 - Kreis der (offen) bereitstellbaren Daten wird im Zweifel enger

Open Data Schranken (Beispiele)



§ 12 Schutz öffentlicher und sonstiger Belange (Geodatenzugangsgesetz - GeoZG)

- (1) Der **Zugang** der Öffentlichkeit zu Geodaten und Geodatendiensten über Suchdienste im Sinne des § 6 Absatz 1 Nummer 1 **kann beschränkt werden, wenn er nachteilige Auswirkungen auf die internationalen Beziehungen, bedeutsame Schutzgüter der öffentlichen Sicherheit oder die Verteidigung** haben kann.
- (2) Für den Zugang der Öffentlichkeit zu Geodaten und Geodatendiensten über die Dienste nach § 6 Absatz 1 Nummer 2 bis 5 gelten die Zugangsbeschränkungen nach § 8 Absatz 1 sowie § 9 des Umweltinformationsgesetzes vom 22. Dezember 2004 (BGBl. I S. 3704) entsprechend.
- (3) Gegenüber geodatenhaltenden Stellen mit Ausnahme derjenigen Stellen im Sinne von § 2 Absatz 1 Nummer 2 des Umweltinformationsgesetzes vom 22. Dezember 2004 sowie gegenüber entsprechenden Stellen der Länder, der Kommunen und anderer Mitgliedstaaten der Europäischen Gemeinschaft sowie gegenüber Organen und Einrichtungen der Europäischen Gemeinschaft sowie auf der Grundlage von Gegenseitigkeit und Gleichwertigkeit auch gegenüber Einrichtungen, die durch internationale Übereinkünfte geschaffen wurden, soweit die Europäische Gemeinschaft und ihre Mitgliedstaaten zu deren Vertragsparteien gehören, können der Zugang zu Geodaten und Geodatendiensten sowie der Austausch und die Nutzung von Geodaten beschränkt werden, wenn hierdurch
 1. die Durchführung eines laufenden Gerichtsverfahrens,
 2. der Anspruch einer Person auf ein faires Verfahren,
 3. die Durchführung strafrechtlicher, ordnungswidrigkeitenrechtlicher oder disziplinarrechtlicher Ermittlungen,
 4. **bedeutsame Schutzgüter der öffentlichen Sicherheit,**
 5. **die Verteidigung oder**
 6. die internationalen Beziehungen gefährdet werden können. [...]

Open Data Schranken (Beispiele)



§ 9 Schutz sonstiger Belange (Umweltinformationsgesetz - UIG)

(1) Soweit

1. durch das Bekanntgeben der Informationen **personenbezogene Daten** offenbart und dadurch Interessen der Betroffenen erheblich beeinträchtigt würden,
2. Rechte am geistigen Eigentum, insbesondere **Urheberrechte**, durch das Zugänglichmachen von Umweltinformationen verletzt würden oder
3. durch das Bekanntgeben **Betriebs- oder Geschäftsgeheimnisse** zugänglich gemacht würden oder die Informationen dem Steuergeheimnis oder dem Statistikgeheimnis unterliegen,

ist der Antrag abzulehnen, es sei denn, die Betroffenen haben zugestimmt oder das öffentliche Interesse an der Bekanntgabe überwiegt. Der Zugang zu Umweltinformationen über Emissionen kann nicht unter Berufung auf die in den Nummern 1 und 3 genannten Gründe abgelehnt werden. Vor der Entscheidung über die Offenbarung der durch Satz 1 Nummer 1 bis 3 geschützten Informationen sind die Betroffenen anzuhören. Die informationspflichtige Stelle hat in der Regel von einer Betroffenheit im Sinne des Satzes 1 Nummer 3 auszugehen, soweit übermittelte Informationen als Betriebs- und Geschäftsgeheimnisse gekennzeichnet sind. Soweit die informationspflichtige Stelle dies verlangt, haben mögliche Betroffene im Einzelnen darzulegen, dass ein Betriebs- oder Geschäftsgeheimnis vorliegt.

- (2) Umweltinformationen, die private Dritte einer informationspflichtigen Stelle übermittelt haben, ohne rechtlich dazu verpflichtet zu sein oder rechtlich verpflichtet werden zu können, und deren Offenbarung nachteilige Auswirkungen auf die Interessen der Dritten hätte, dürfen ohne deren Einwilligung anderen nicht zugänglich gemacht werden, es sei denn, das öffentliche Interesse an der Bekanntgabe überwiegt. Der Zugang zu Umweltinformationen über Emissionen kann nicht unter Berufung auf die in Satz 1 genannten Gründe abgelehnt werden.

Recht auf Informationszugang und Ausnahme

- Veröffentlichungspflicht gilt nur, “soweit geltendes Recht dem nicht entgegensteht”
- Zentrale gesetzliche Ausschlussgründe:
 - Schutz öffentlicher Sicherheit (insbesondere Verteidigung, KRITIS) (wichtig)
 - Schutz von Betriebs- und Geschäftsgeheimnissen, Datenschutz, Urheberrechte
 - Behördlicher Entscheidungsbildungsprozess/laufende Verfahren
 - Sonderfall: Eingestufte Daten dürfen nicht veröffentlicht werden

Unterschiede im Schutzrahmen

- Ermessensspielraum im GeoZG (Gefahr des „Overblocking“) \leftrightarrow Ablehnungszwang im UIG
- DNG sieht selbst keine Einschränkung der Veröffentlichung vor, sondern regelt nur Formfragen
- Verbindliche Vorgaben für sog. “hochwertige Daten” (HVD-DVO)

Entwicklungstendenzen



Ruf nach Daten- bzw. Digitalsouveränität wächst → Verwaltung soll souverän entscheiden, welche Daten mit wem, in welchem Umfang, unter welchen Bedingungen geteilt werden



EU-weit einheitlichere Vorgaben durch DNG/HVD-DVO für hochwertige Daten (Verpflichtung zur umfassenden, standardisierten Bereitstellung über APIs, freie Lizenzen)



Stärkere Risiko- und Resilienz-Pflichten durch das neue KRITIS-Dachgesetz und Umsetzung der EU-CER-Richtlinie (All-Risk-Ansatz; Registrierung, Kontaktstellen, Melde- und Schutzpflichten)



Technische Anforderungen (Maschinenlesbarkeit, offene Formate, APIs, Metadaten, Massen-Download) werden verbindlicher – besonders für “hochwertige Daten” und Geodaten

Entwicklungstendenzen

Faktische Hürden und Störungen

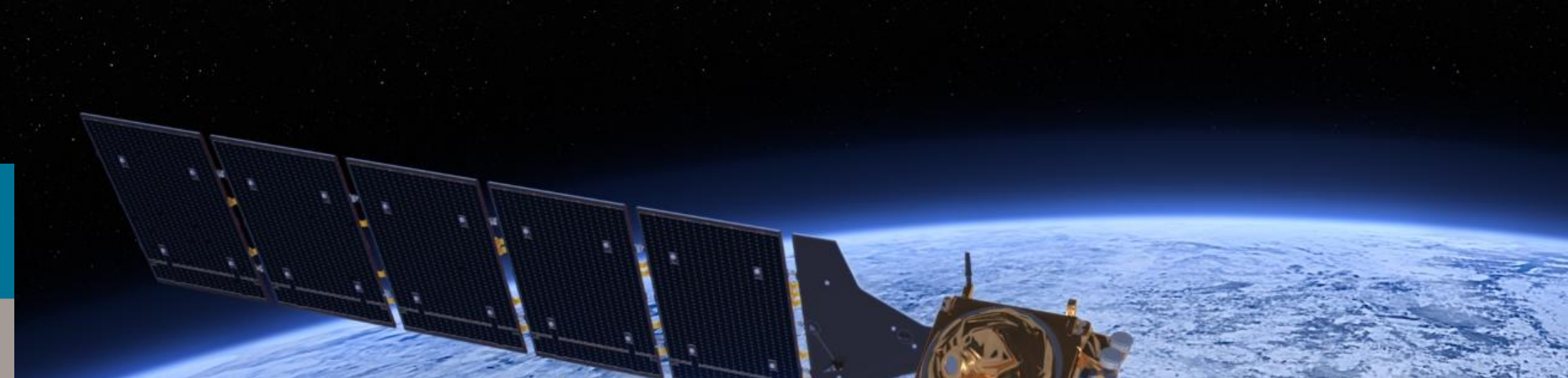
- Lückenhafte Datenklassifizierung (keine durchgängige Kennzeichnung/bestehende Unsicherheiten, welche Daten offen, beschränkt/gesichert bereitgestellt werden dürfen)
- Potenziell unzureichende IT-Infrastruktur
- Unklarheit bzgl. Prozesse und Verantwortlichkeiten
- Risiko des „Overblocking“ durch Behörden zum Schutz vor Risiken/Haftung

Rechtliche Hürden und Störungen

- Unterschiedliche Auslegungsmaßstäbe
- Kein bundeseinheitlicher Maßstab zur Gefährdungseinschätzung – IFG, GeoZG, DNG, KRITIS-Gesetze und EU-Recht setzen teils unterschiedliche Schwellen und Ermessensspielräume für Beschränkungen beim Zugang
- Allgemeine Leitlinien zur Veröffentlichung von offenen Daten fehlen

Folgen für Wirtschaft

- Unterteilung der Geodatenbranche in “öffentliche Daten” und “kritische/gesicherte Daten”
- Investitionsunsicherheiten
- Notwendigkeit eines verbesserten Datenmanagements (Datenanalyse, Datenklassifizierung, Schutzbedürftigkeit, Sensibilisierung für Schutz- und Veröffentlichungspflichten)



Kontakt

BHO Legal

Hohenstaufenring 29-37
50674 Köln

Tel.: + 49 (0) 221 270 956 0
Fax: + 49 (0) 221 270 956 222

cologne@bho-legal.com

Gerhard Deiters

Rechtsanwalt | Partner

Tel.: + 49 (0) 221 270 956 160
Mobil: + 49 (0) 162 283 1869

gerhard.deiters@bho-legal.com