Handlungsfeld Datenschutz

CUT | T1 | August 2024

Partnerstädte:

Hamburg

Stadt Leipzig

Landeshauptstadt München

Gefördert durch:

Bundesministerium für Wohnen, Stadtentwicklung und Bauwesen

KFW

Versionierung

Version	Erläuterung	Datum der Änderung
V1.0	Erste Version des Handlungsfelds Datenschutz	31.08.2024

Disclaimer

Dieses Dokument bietet einen Überblick über das Thema Datenschutz im Kontext der kommunalen Datengovernance in den drei beteiligten Städten. Die präsentierte Information basiert auf der Perspektive und Erfahrung in der Verwaltung der Geodateninfrastruktur und der Urbanen Datenplattform.

1. **Zweck und Perspektive:** Dieses Dokument bietet einen Überblick über den Datenschutz, insbesondere über relevante Thematiken in Bezug auf die UDP/GDI/UDZ. Es zielt darauf ab, Erfahrungen und Erkenntnisse der drei CUT-Städte darzustellen.
2. **Begrenzte Abdeckung:** Bitte beachten Sie, dass sich dieses Dokument auf den Datenschutz im Kontext UDZ und UDP/GDI begrenzt. Die bereitgestellten Informationen decken nicht alle Aspekte des Datenschutzes ab, sondern geben Hinweise darauf, welche Themen bei eigenen Projekten beachtet werden müssen.
3. **Keine professionelle Beratung:** Die bereitgestellte Information dient nur zu Informationszwecken. Dieses Dokument ersetzt keine professionelle Beratung durch eine/n Datenschutzbeauftragte/n. Für umfassende Einblicke oder Empfehlungen zu neuen Technologien wird empfohlen, qualifizierte Fachleute zu konsultieren.
4. **Änderungen und Aktualisierungen:** Bitte beachten Sie, dass sich der Inhalt dieses Dokuments ändern kann. Dies ist auf die Weiterentwicklung der gültigen Rechtsprechung zurückzuführen.

Durch die Nutzung dieses Dokuments erkennen Sie diesen Haftungsausschluss an.

Inhalt

Vorwort

Die Handlungsempfehlung zum Datenschutz besteht aus zwei Dokumenten, die Ihnen helfen sollen, datenschutzrechtliche Fragen im Kontext von Verarbeitungsprozessen in Urbanen Digitalen Zwillingen (UDZ), Urbanen Datenplattformen (UDP) und Geodateninfrastrukturen (GDI) zu beantworten.

Teil 1 ist das vorliegende Word-Dokument, das zentrale Begriffe zum Datenschutz erläutert und aufzeigt, wie sich die Bearbeitung des Themas Datenschutz auf die Rollenverteilung im Kontext der Urbanen Digitalen Zwillinge auswirkt.

Teil 2 umfasst die Tabelle „Anforderungen_DSGVO.xlsx", die die zentralen Anforderungen der DSGVO auflistet und mit konkreten Fragen bei der Umsetzung hilft.

Anforderungen der DSGVO	Artikel DSGVO	Gewährleistungsziele	Beschreibung/Fragen	Detaillierte Fragestellungen
Transparenz für Betroffene	Art. 5 Abs. 1 lit a Art. 12 Abs. 1 und 3 bis Art. 15 Art. 34	Transparenz	Welche Maßnahmen wurden getroffen, um der betroffenen Person alle Informationen transparent zu übermitteln?	- Werden die Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache an die betroffene Person übermittelt? - Welche Maßnahmen wurden getroffen, um die Betroffenen unverzüglich und auf jeden Fall innerhalb eines Monats über den Stand der Bearbeitung und der ergriffenen Maßnahmen bezüglich ihres Antrags zu informieren? - Welche Maßnahmen wurden getroffen, um der Benachrichtigungspflicht gegenüber Betroffenen bei einer Datenpanne, nachzukommen?
Zweckbindung	Art. 5 Abs. 1 lit. b	Nichtverkettung	Zu welchem Zweck werden die Daten verarbeitet?	- Welche Bedingung/Erlaubnistatbestand aus Art. 6 DSGVO ist gegeben? - Ist eine darauffolgende Verarbeitung für weitere Zwecke mit dem ursprünglichen Zweck kompatibel? - Müssen Betroffene über eine Weiterverarbeitung über den ursprünglichen Zweck hinaus informiert werden? - Können diese von ihrem unter Umständen bestehenden Widerspruchsrecht Gebrauch machen?
Datenminimierung	Art. 5 Abs. 1 lit. c	Datenminimierung	Sind die erhobenen personenbezogene Daten dem Zweck angemessen, dem Zweck erheblich oder auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt?	- *Angemessen* sind Daten, die einen konkreten inhaltlichen Bezug zum Verarbeitungszweck aufweisen. - *Erheblich* sind Daten, deren Verarbeitung einen Beitrag zur Zweckerreichung leisten. - *Auf das notwendige Maß beschränkt* sind nur die Daten, die zur Erreichung des Zwecks erforderlich sind, ohne deren Verarbeitung der Verarbeitungszweck also nicht erreicht werden kann. - Die Verarbeitung personenbezogener Daten ist demnach nur dann erforderlich, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann. Der Eingriff in das Grundrecht auf Datenschutz ist nur zulässig, soweit er auf das geringstmögliche Maß begrenzt ist. - Wird der Grundsatz der Datenminimierung fortlaufend überprüft? - Wie wird eine frühestmögliche Löschung nicht weiter benötigter und damit nicht mehr erforderlicher personenbezogener Daten sichergestellt?

Abbildung 1: Auszug aus der Tabelle „Anforderungen_DSGVO.xlsx"

0 Datenschutz im Kontext Urbaner Datenplattformen/Geodateninfrastrukturen und Urbaner Digitaler Zwillinge

Im Kontext von UDP/GDI und UDZ ist der Datenschutz von hoher Relevanz, da Daten erhoben, veröffentlicht und analysiert werden. Die Einhaltung des Datenschutzes ist grundlegend für den Betrieb dieser Infrastrukturen. Der Datenschutz muss im Zuge der Erhebung, Integration, Bereitstellung und Verarbeitung (inkl. Analysen und Simulationen) von Daten betrachtet werden.

1 Definitionen

Für das Thema Datenschutz ist die klare Begriffsdefinition des verwendeten Vokabulars von großer Bedeutung. Artikel 4 der DSGVO „Begriffsbestimmungen" behandelt 26 Ausdrücke, die in der Datenschutzgrundverordnung (DSGVO) eine hohe Relevanz besitzen. In diesem Kapitel liegt der Fokus auf den drei zentralen Begriffen „Datenschutz", „personenbezogene Daten" und „Verarbeitung personenbezogener Daten".

1.1 Datenschutz

Der Datenschutz enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.[1] Im Zentrum des Datenschutzes steht das Recht auf informationelle Selbstbestimmung. Jede Person hat die Freiheit, selbst zu entscheiden, wem gegenüber und zu welchen Zwecken sie ihre Daten preisgibt. Personenbezogene Daten dürfen daher nur auf Grundlage einer Einwilligung oder eines Gesetzes verarbeitet werden.[2] In Deutschland wird das allgemeine Datenschutzrecht aus der Datenschutzgrundverordnung (DSGVO) gebildet und mit dem Bundesdatenschutzgesetz (BDSG) und den Landesdatenschutzgesetzen ergänzt.[3]

[1] https://dsgvo-gesetz.de/art-1-dsgvo/ (Zugriff: 07.06.2024)

[2] https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Flyer/Datenschutz-ist.pdf?__blob=publicationFile&v=12 (Zugriff: 07.06.2024)

[3] https://www.bfdi.bund.de/DE/Buerger/Inhalte/Allgemein/Datenschutz/GrundlagenDatenschutzrecht.html (Zugriff: 07.06.2024)

Die Ziele der DSGVO werden im Art. 1 DSGVO „Gegenstand und Ziele“ folgendermaßen beschrieben: “Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.”[1]

Das grundlegende Prinzip der Datenschutz-Grundverordnung (DSGVO) sowie des gesamten Datenschutzrechts ist das sogenannte Verbotsprinzip. Demnach ist die Verarbeitung personenbezogener Daten grundsätzlich untersagt und darf nur bei Rechtmäßigkeit gestattet werden. Diese tritt nur dann ein, wenn die Voraussetzungen einer der Erlaubnistatbestände der DSGVO erfüllt sind (s. Art. 6 Abs. 1 DSGVO).[3]

Eine Ausnahme ist die Verarbeitung von personenbezogenen Daten durch öffentliche Stellen (vgl. Art. 6e DSGVO). Diese ist ausschließlich dann gestattet, wenn sie zur Erfüllung der Aufgaben der Stelle obligatorisch ist. Bei Unternehmen hingegen besteht zum Teil eine Verpflichtung, bestimmte Daten zu verarbeiten. Für sie sind insbesondere die Erlaubnistatbestände der Einwilligung und des überwiegenden berechtigten Interesses relevant.[3]

1.2 Personenbezogene Daten

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.[4] „Verschiedene Teilinformationen, die gemeinsam zur Identifizierung einer bestimmten Person führen können, stellen ebenfalls personenbezogene Daten dar.“[5] Zu personenbezogenen Daten zählen beispielsweise der Name und die Kontaktdaten natürlicher Personen.

Wenn personenbezogene Daten anonymisiert, verschlüsselt oder pseudonymisiert wurden, bleibt ihre Einordnung als solche bestehen, wenn sie dennoch zur erneuten Identifizierung einer Person genutzt werden können. Sie fallen folglich weiterhin in den Geltungsbereich der Datenschutz-Grundverordnung.[5]

Dagegen gelten personenbezogene Daten, die auf eine Weise anonymisiert wurden, dass die betroffene Person nicht mehr identifiziert werden kann, nicht mehr als personenbezogene Daten. Für eine wirksame Anonymisierung müssen die vorgenommenen Maßnahmen jedoch unumkehrbar sein.[5]

Zudem definiert die DSGVO besondere Kategorien personenbezogener Daten (vgl. Art. 9 DSGVO), wenn sie besonders sensibel und schutzbedürftig sind, da die Verarbeitung dieser

[4] https://dsgvo-gesetz.de/art-4-dsgvo/ (Zugriff: 07.06.2024)

[5] https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_de (Zugriff: 07.06.2024)

Daten erhebliche Risiken für die betroffenen Personen mit sich bringen kann. Unter die Kategorie der besonders schutzwürdigen Daten fallen jene, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie auch genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

„Die Datenschutz-Grundverordnung schützt personenbezogene Daten unabhängig von der zur Datenverarbeitung verwendeten Technik – sie ist technologieneutral und gilt für die automatisierte wie die manuelle Verarbeitung, sofern die Daten nach vorherbestimmten Kriterien (z. B. alphabetische Reihenfolge) geordnet sind. Es ist ebenfalls nicht entscheidend, wie die Daten gespeichert werden – in einem IT-System, mittels Videoüberwachung oder auf Papier. In all diesen Fällen fallen die personenbezogenen Daten unter die in der Datenschutz-Grundverordnung dargelegten Datenschutzklauseln."[5]

Beispiele für personenbezogene Daten in der UDP sind:

- Name und Vorname
- Privatanschrift
- Gebäudescharfe Daten (bspw. Kinder pro Haus, Energieverbrauch)
- Standortdaten (bspw. Fahrradrouten)
- Fotos (Luftbilder, Straßenbefahrungen, …)

1.3 Verarbeitung personenbezogener Daten

Die Verarbeitung personenbezogener Daten beschreibt Vorgänge im Zusammenhang mit personenbezogenen Daten, welche mit oder ohne Hilfe von automatisierten Verfahren durchgeführt werden. Diese Vorgänge beinhalten das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.[6] Beispiele für die Verarbeitung personenbezogener Daten sind die Nutzung einer Datenbank mit personenbezogenen Daten, der Versand von Werbeemails oder die Veröffentlichung eines Fotos von einer Person auf einer Webseite. Die Verarbeitung personenbezogener Daten unterliegt gesetzlichen Regelungen, die Unternehmen, Vereine und Behörden beachten müssen.

[6] https://dsgvo-gesetz.de/art-4-dsgvo/ (Zugriff: 13.06.2024)

2 Das Standard-Datenschutzmodell

Die Verarbeitung personenbezogener Daten geschieht unter Beachtung der rechtlichen Anforderungen aus der DSGVO. Um sicherzugehen, dass alle Anforderungen eingehalten werden können, wurde das Standard-Datenschutzmodell (SDM) etabliert. Es handelt sich um ein Vorgehensmodell nach den Grundsätzen in Artikel 5 DSGVO, das Maßnahmen zu sieben definierten Gewährleistungszielen vorschreibt.[7] Die Systematisierung im Standard-Datenschutzmodell ist notwendig, da sämtliche datenschutzrechtliche Anforderungen über die gesamte DSGVO verstreut und nicht einheitlich konkretisiert sind. Auch das IT-Grundschutzprofil für die Basis-Absicherung von Kommunalverwaltungen[8] verweist im Kapitel Datenschutz auf die Anforderung "CON.2.A1" im IT-Grundschutzkompendium[9], nach der das SDM umgesetzt werden muss.

2.1 Datenschutzrechtliche Anforderungen

Datenschutzrechtliche Anforderungen sind grundsätzlich bei jeder Verarbeitung personenbezogener Daten von der verantwortlichen Stelle umzusetzen. Die Anforderungen entstehen aus den folgenden Gründen:

- Grundsätze der Datenverarbeitung
- Rechte von Betroffenen
- Technische Umsetzung
- Ordnungsgemäßer Umgang bei Datenschutzverletzung
- Rechtmäßigkeit der Verarbeitung stützt sich auf die Einwilligung Betroffener
- Aufsichtsbehördliche Anforderungen

Alle 25 datenschutzrechtlichen Anforderungen, wie beispielsweise Vertraulichkeit oder die Löschbarkeit von Daten sind in der beigefügten Arbeitshilfe (Tabelle) aufgeführt.

[7] https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Technik/SDM.html (Zugriff: 13.06.2024)

[8] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Basis_Absicherung_Kommunalverwaltung.pdf?__blob=publicationFile&v=12 (Zugriff: 13.06.2024)

[9] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4 (Zugriff: 13.06.2024)

2.2 Gewährleistungsziele

Im SDM werden aus den o. g. datenschutzrechtlichen Anforderungen sieben Gewährleistungsziele abgeleitet. Gemeinsam mit den zugeordneten datenschutzrechtlichen Anforderungen bilden sie einen strukturierten Leitfaden. Erforderliche technische und organisatorische Maßnahmen können sich damit an diesen Zielen orientieren, um allen Anforderungen auch in der Praxis gerecht zu werden. Die sieben Gewährleistungsziele sind Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz und Intervenierbarkeit.[10] Die Zuordnung der Gewährleistungsziele zu den einzelnen datenschutzrechtlichen Anforderungen finden Sie in der beigefügten Arbeitshilfe (Tabelle). Die Erläuterung der Gewährleitungsziele steht Ihnen dort, sowie im Anhang des vorliegenden Dokuments zur Verfügung.

Zu jedem Gewährleistungsziel werden außerdem technische und organisatorische Maßnahmen zugeordnet, die als einzelne Maßnahmen-Bausteine unter https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/ von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder veröffentlicht werden. Es steht somit eine Handreichung zur Verfügung, mit der abstrakte gesetzliche Forderungen in einen Handlungskatalog übersetzt werden und mit dessen Hilfe der Soll-Zustand mit dem Ist-Zustand verglichen werden kann.

2.3 Anforderungsliste DSGVO

Zur Umsetzung der Anforderungen aus der DSGVO in Projekten soll die mitveröffentlichte Tabelle „Anforderungen_DSGVO." dienen. Die Inhalte aus der Tabelle im Anhang stammen aus dem Dokument „Das Standard-Datenschutzmodell", herausgegeben vom AK Technik der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder[10] und fassen die in Teil D aufgeführten Maßnahmen zur praktischen Umsetzung zusammen. Bei Verständnisproblemen empfehlen wir selbst im Original-Dokument, das unter https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/ veröffentlicht ist, nachzulesen.

Das Tabellenblatt Fragenkatalog enthält konkrete Fragestellungen zu den einzelnen Anforderungen aus der DSGVO, die aufzeigen sollen, welche Themen zur Umsetzung der Anforderungen und zur Einhaltung der Gewährleistungsziele beantwortet und folglich eingehalten werden müssen. Zur besseren Orientierung sind jeweils die Artikel aus der DSGVO mitaufgelistet, die die entsprechende Anforderung beinhalten. Das Tabellenblatt "Gewährleistungsziele" enthält zudem die Erläuterung zu den sieben Gewährleistungszielen, die durch die Umsetzung von Maßnahmen sichergestellt werden sollen.

[10] https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V3.pdf (Zugriff: 13.06.2024)

Ziel der Tabelle soll nicht sein, dass Sie alle Fragen beantworten können, sondern dass Sie Hinweise auf Themen bekommen, die Sie beachten müssen. Zudem ersetzt die Tabelle keine Beratung eines Datenschutzbeauftragten, sie soll viel mehr auf Themen hinweisen, die mit einem solchen besprochen werden müssen. Die Fragen, die hier formuliert sind, sind nicht als allumfassend anzusehen, sie bilden lediglich eine Auswahl an Fragestellungen zu den einzelnen Anforderungen ab.

Im Rahmen unseres Projekts haben wir die Anforderungen der DSGVO mithilfe der Tabelle auf einen Anwendungsfall angewandt. Aus dieser Bearbeitung wurde die Komplexität der Anforderungen und somit der Tabelle sichtbar, die Fragestellungen sind oft nicht ohne weitere Recherche beantwortbar. Daher ist es erforderlich, dass weitere Expertisen, beispielsweise die des Datenschutzbeauftragten, in die Bearbeitung der Anforderungen der DSGVO im Kontext eines Anwendungsfalls einbezogen werden.

3 Rollen im Datenschutz

Rollen und Zuständigkeiten bilden eine wichtige Grundlage im vertraulichen Umgang mit Daten. Von daher werden die Ergebnisse aus dem Handlungsfeld "Rollen" auf den Datenschutz angewendet und spezifiziert. Im Folgenden wird zwischen zentralen und dezentralen Rollen und damit zwischen zentraler und dezentraler Gewährleistung des Datenschutzes unterschieden. Es werden die Rollen mit dem größten Bezug zum Datenschutz beschrieben bzw. Querverweise auf weitere Rollen gesetzt.

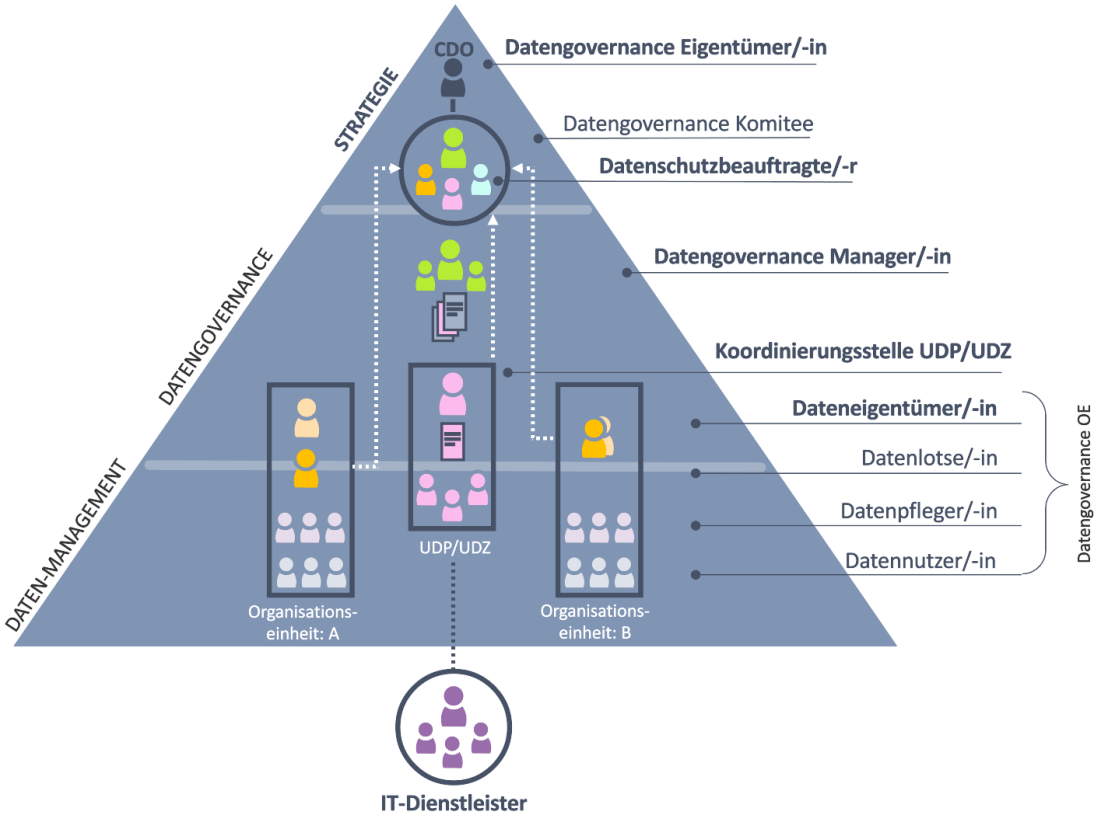

Abbildung 2: Erweitertes Modell aus dem Handlungsfeld "Rollen" (Link) nach Fraunhofer IAO (2023)[11]

3.1 Datengovernance Eigentümer/-in

Die zentrale Rolle **Datengovernance Eigentümer/-in** kann auf strategischer Ebene der Verwaltungsspitze – auch in Personalunion mit der weiter gefassten Rolle Chief Data Officer

[11] Sautter, Johannes; Riess, Stefan; Kopperger, Dietmar; Litauer, Rebecca; Stanisic-Petrovic, Mirjana; Loch, Lisa-Aline; Graf, Eva; Schelling, Caren; Dobrokhotova, Ekaterina; Anniés, Jeannette; Marquardt, Dr. Justus H.,: Data Governance: Zwölf Bausteine einer Organisationsfunktion für Datenexzellenz. Unveröffentlichtes Manuskript, KPMG, Fraunhofer IAO, 2023

(CDO, vgl. Kapitel Rollen) – die Gesamtverantwortung für den Datenschutz der Kommune übernehmen oder diese übertragen.

3.2 Datenschutzbeauftragte/-r

Die zentrale Rolle des/der **Datenschutzbeauftragte/-r** ist die einer Ansprechpartnerin bzw. eines Ansprechpartners für das Thema Datenschutz mit Wirkung in allen drei Ebenen der Datengovernance (siehe Abbildung 2). Die Rolle kann u. a. folgende Aufgaben übernehmen:

- Unterrichtung und Beratung der Verwaltungsspitze, der Dateneigentümer, Organisationseinheiten und Bediensteten hinsichtlich ihrer Pflichten nach den Datenschutzvorschriften
- Überwachung der Einhaltung der Datenschutzvorschriften sowie der Strategien für den Schutz personenbezogener Daten
- Beratung der Dateneigentümer/-innen zur Durchführung und Methodik einer Datenschutz-Folgenabschätzung und die Überwachung ihrer Durchführung
- Zusammenarbeit mit der/dem Datenschutzbeauftragten der jeweiligen Länder und dem/der Bundesdatenschutzbeauftragten
- Beratung von betroffenen Personen zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte in Zusammenhang stehenden Fragen

Die/der Datenschutzbeauftragte ist im Datengovernance Komitee vertreten. Nach IT-Grundschutz-Profil für die Basis-Absicherung von Kommunen[12] muss die Behördenleitung einen Datenschutzbeauftragten oder eine Datenschutzbeauftragte benennen.

3.3 Datengovernance Manager/-in

Die (zentrale) Rolle **Datengovernance Manager/-in** bindet die/den Datenschutzbeauftragte/-n im Rahmen des Stakeholdermanagements und der Organisation des zentralen Datengovernance Komitees mit in Entscheidungsprozesse zur stadtweiten Datengovernance ein.

3.4 Dateneigentümer/-in

Die (dezentrale) Rolle **Dateneigentümer/-in** ist verantwortlich für die Umsetzung und Einhaltung der jeweils anzuwendenden Datenschutzvorschriften. Ihre Aufgaben umfassen u.a.:

[12] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Basis_Absicherung_Kommunalverwaltung.pdf?__blob=publicationFile&v=12 (Zugriff: 10.07.2024)

- Gewährleistung der recht- und ordnungsgemäßen Datenverarbeitung bei Auftragserteilung und -verarbeitung
- Feststellung des Schutzbedarfs und Durchführung von Datenschutz-Folgenabschätzungen (s. Art. 35 DSGVO)
- Erstellung, Fortschreibung, Umsetzung und Kontrolle von Sicherheitskonzepten in Absprache mit Datenschutzbeauftragten
- Unverzügliche Meldung und Bewältigung von Datenschutzvorfällen
- Information der/des Datenschutzbeauftragten über Schreiben und Besuche der Datenschutzaufsichtsbehörden
- Gewährleistung von Betroffenenrechten und Erfüllung der Informationspflichten
- Erstellung und Führung des Verzeichnisses von Verarbeitungstätigkeiten (s. Art. 30 DSGVO)
- Verpflichtung der beteiligten Personen zur Vertraulichkeit und Einhaltung von Amtsgeheimnissen
- Information der Bediensteten über Datenschutzvorschriften und Informationssicherheitsvorgaben
- Erfüllung der Informationspflichten bei Erhebung und Zweckänderung personenbezogener Daten

Die Durchführung dieser Aufgaben kann auf Bedienstete und/oder Rollen der Organisationseinheit übertragen werden (z. B. Datenlotse/-in, Datenpfleger/-in, Datennutzer/-in).

3.5 IT-Dienstleister

Die (zentrale) Rolle **IT-Dienstleister** ist verantwortlich für den technischen Betrieb der Infrastruktur von UDP/UDZ. Eine Stadt oder Kommune kann einen (stadteigenen/externen) IT-Dienstleister mit dem technischen Betrieb von UDP/UDZ beauftragen. Damit übernimmt der IT-Dienstleister auch Verantwortung zur Einhaltung der DSGVO unter Berücksichtigung der Anforderungen des SDM. Konkrete Maßnahmen, wie Sicherstellung der Autorisierung und Authentifizierung sind gemeinsam mit der/dem Datenschutzbeauftragten und der Koordinierungsstelle UDP/UDZ abzustimmen.

3.6 Koordinierungsstelle UDP/UDZ

Die (zentrale) Rolle **Koordinierungsstelle UDP/UDZ** ist verantwortlich für den fachlichen Betrieb einer Urbanen Datenplattform (UDP) bzw. Urbaner Digitaler Zwillinge (UDZ) und in diesem Zusammenhang auch verantwortlich für die Durchsetzung und Einhaltung der jeweils anzuwendenden Datenschutzvorschriften in Abstimmung mit dem Datenschutzbeauftragten und ggf. mit dem IT-Dienstleister.

Die im Folgenden aufgeführten Beispiele zeigen, dass die zu erfüllenden Datenschutzrechtlichen Anforderungen an UDP/UDZ je nach Anwendungsfall und Kommune differieren können. Es empfiehlt sich in Abstimmung mit den Datenschutzbeauftragten pro Anwendungsfall/Komponente entsprechende Maßnahmen zu erarbeiten und diese z.B. in einem erweiterbaren Sicherheitskonzept (SiKo) zu dokumentieren. Die oben genannte Anforderungsliste kann dabei helfen.

Beispiel 1: UDP als Datendrehscheibe für offene Daten

Eine UDP nimmt Daten von unterschiedlichen Dateneigentümern entgegen und stellt diese über ein Open Data Portal bereit. Die Hauptverantwortung liegt hier im einfachsten Fall bei den Dateneigentümern. Diese dürfen der UDP nur Datensätze zur Verfügung stellen, die nicht datenschutzrelevant sind, und müssen das u.a. durch eine Datenschutzerklärung bestätigen. In diesem Fall ist die UDP selbst Nutzer offener Daten. Die UDP-Koordinierungsstelle bringt diese Regelung über das Datengovernance Komitee in die stadtweite Datengovernance ein.

Beispiel 2: UDP stellt datenschutzrelevante Daten bereit

Eine UDP nimmt datenschutzrelevante Daten (z.B. Eigentümerdaten) aus einer externen Quelle (z.B. Kataster) auf und stellt diese für einen eingeschränkten Nutzerkreis zur Verfügung. In diesem Fall müssen durch die UDP unterschiedliche datenschutzrechtliche Anforderungen erfüllt werden. So muss die UDP-Koordinierungsstelle gewährleisten, dass die Nutzung der datenschutzrelevanten Daten zweckgebunden bleibt und die Zugriffe protokolliert werden, da die Betroffenen das Recht haben, die getätigten Abfragen einzusehen. In diesem Fall nimmt die UDP über die Protokollierung z. B. selbst datenschutzrelevante Daten der kommunalen Mitarbeitenden auf. Diese Protokollierung muss dann entsprechende Löschfristen einhalten. In diesem Fall ist die UDP selbst Nutzer und Eigentümer datenschutzrelevanter Daten.

Beispiel 3: UDZ leitet personenbezogene Entscheidungen her

Ein UDZ nutzt Algorithmen, um personenbezogene Entscheidungen (z.B. sicherer Schulweg pro Schulkind) herbeizuführen. Zum einen sind hier Maßnahmen zu ergreifen, die eine Fehlerfreiheit und Diskriminierungsfreiheit bezogen auf den eingesetzten Algorithmus gewährleisten, und zum anderen sollte bei den Ergebnissen auf Datenminimierung durch Anonymisierung geachtet werden. In diesem Fall ist der UDZ der Nutzer und Eigentümer datenschutzbezogener Daten/Algorithmen. Die UDZ-Koordinierungsstelle stellt neu eingeführte Algorithmen z. B. im Datengovernance Komitee vor und lässt diese durch angebundene Gremien (z. B. “KI-Board”) abnehmen.

4 Ausblick

Die Nutzung von Daten ist in den letzten Jahren stark angestiegen und wird dies in einer immer stärker digitalisierten Gesellschaft auch weiterhin tun, was das Thema Datenschutz vor notwendige Entwicklungsbedarfe stellt. Zusätzlich haben die rasante Entwicklung und zunehmende Verbreitung von KI-Systemen tiefgreifende Auswirkungen auf verschiedene Aspekte des Datenschutzes, die sorgfältig abgewogen und adressiert werden müssen (siehe u.a. auch EU AI Act - EU Artificial Intelligence Act). Durch die Verarbeitung großer Datenmengen in Urbanen Datenplattformen und Urbanen Digitalen Zwillingen ist der Ausschluss personenbezogener Daten nicht mehr auf einfache Weise zu garantieren und zu prüfen. Zudem können KI-Technologien durch Big-Data-Verfahren und maschinelles Lernen das Verhalten von Individuen überwachen und analysieren, was zu unerwünschtem Erzeugen personenbezogener Daten führen kann.

Dennoch gibt es durch KI-Technologien und andere Automatisierungen auch große Chancen im Rahmen des Datenschutzes. KI-Systeme können entwickelt werden, um beispielsweise Daten automatisch wirksam zu anonymisieren und sensible Informationen zu schützen. Solche Technologien können helfen, Datenschutzverletzungen zu verhindern und die Sicherheit von Daten zu gewährleisten. Zudem können sie dabei helfen, große Datenmengen effizient zu analysieren und potenzielle Sicherheitslücken zu identifizieren.

Ein weiteres Thema für zukünftige Arbeiten ist die Problematik der Legitimation für die Veröffentlichung von Geodaten. Hier spielt insbesondere die Fragestellung eine Rolle, ob und in welchem Ausmaß Geodaten überhaupt als personenbezogene/personenbeziehbare Daten gewertet werden können oder ob sie als datenschutzrechtlich irrelevante Sachdaten gelten.[13] Je nach aktueller Rechtsprechung kann sich die Beantwortung verändern, da es keine eindeutigen Gesetze dafür gibt. Bisher wurde das Thema Datenschutz und Geodaten in der Rechtsprechung beispielsweise für die Einsicht in das Liegenschaftskataster näher betrachtet, zahlreiche andere Fragestellungen bleiben allerdings noch unbeantwortet.[13] Mit zunehmender Bedeutung von Geodaten müssen diese Thematiken in Zukunft bearbeitet werden, um Fragestellungen möglichst rechtssicher beantworten zu können.

Auch das Thema „Rollen" befindet sich in einer ständigen Weiterentwicklung. Um das Potenzial von offenen Daten und generell das Teilen von Daten vertrauenswürdiger und sicherer für alle Akteure zu gestalten, wurde die Rolle des Datentreuhänders eingeführt.

[13] https://geodaesie.info/images/zfv/146-jahrgang-2021/downloads/zfv_2021_5_Kriesten.pdf (Zugriff: 07.06.2024)

Ein Datentreuhänder ist laut Fraunhofer IESE eine „Vertrauensinstanz, die schützenswerte Daten zwischen Datengebern und Datennutzern unter Wahrung der Interessen beider Seiten digital vermittelt.“ [14] Der Datentreuhänder ist ein sehr offenes Konzept, welches weniger über eine konkrete Definition, als eher über Beispiele und Szenarien beschrieben werden kann. Konkrete Umsetzungen gibt es in den Projektstädten aktuell noch nicht. Auf europäischer Ebene wird das Thema im Rahmen des Projektes Gaia-X[15] behandelt und entsprechende Infrastrukturen aufgebaut. Ziel von Gaia-X ist ein sicheres föderiertes Datenökosystem, das für digitale Souveränität der Dateninhaber, Interoperabilität sowie den Open Source-Gedanken steht und die föderale Idee Europas umsetzt[16]. Die Partnerstadt Hamburg ist hier u.a. in der Domäne ”Geoinformation” aktiv.

[14] https://www.iese.fraunhofer.de/blog/datentreuhaender-definition/ (Zugriff: 10.06.2024)

[15] https://gaia-x-hub.de/ (Zugriff: 10.06.2024)

[16] https://www.bmwk.de/Redaktion/DE/Dossier/gaia-x.html (Zugriff: 10.06.2024)

5 Anhang

5.1 Gewährleistungsziele

Wie in 2.2 beschrieben, werden im Standard-Datenschutzmodell sieben zentrale Gewährleistungsziele aus den datenschutzrechtlichen Anforderungen abgeleitet. Diese sind in folgender Tabelle näher beschrieben. Eine umfassende Ausarbeitung dieser Ziele findet sich im Dokument „Standard-Datenschutzmodell“[17].

Gewährleistungsziel	Beschreibung
Datenminimierung	Die Verarbeitung personenbezogener Daten soll auf das dem Zweck angemessene, erhebliche und notwendige Maß beschränkt werden. Datenminimierung bezieht sich nicht ausschließlich auf die Menge der verarbeiteten Daten, sondern auch auf ihre Zugänglichkeit, Speicherfrist und den Umfang ihrer Verarbeitung. Die Datenminimierung hat einen direkten Einfluss auf die anderen Gewährleistungsziele, die bei Einhaltung ebenso in Umfang und Intensität geringgehalten werden können.
Integrität	Integrität beinhaltet eine Vielzahl an Anforderungen. Informationstechnische Prozesse und Systeme müssen kontinuierlich ihre festgelegten Spezifikationen einhalten. Die Daten, die verarbeitet werden sollen, müssen unversehrt, vollständig, richtig und aktuell gehalten werden. Um gegebenenfalls eine Korrektur vornehmen zu können, müssen die genannten Eigenschaften angemessen überwacht werden. Ebenfalls gilt, dass die Anforderungen auch dann eingehalten werden müssen, wenn das System unerwartet hoher Last unterliegt. Werden automatisierte Prozesse auf die Daten angewandt, muss sichergestellt sein, dass diese diskriminierungsfrei sind.
Intervenierbarkeit	Die verantwortliche Stelle ist verpflichtet Maßnahmen umzusetzen, um den Betroffenen ihre zustehenden Rechte jederzeit zu gewähren. Dabei handelt es sich um die Rechte auf Benachrichtigung, Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch und Erwirkung des Eingriffs in automatisierte Einzelentscheidungen. Ist es möglich, Betroffene zu identifizieren, müssen Maßnahmen zur Identifizierung und Authentifizierung ergriffen werden, damit Betroffene ggf. ihre Rechte wahrnehmen können. Verantwortliche müssen jederzeit in die Verarbeitungsprozesse eingreifen können, um behördliche Anordnungen umzusetzen oder bei Datenschutzverletzungen für Abhilfe zu sorgen. Ist eine Einwilligung von Betroffenen nötig für die Verarbeitung, so muss sichergestellt sein, dass

[17] https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V31.pdf (Zugriff: 07.06.2024)

	diese nicht widerrufen wurde. Haben Betroffene selbst Zugriff auf Einstellungen, weil es sich z.B. um eine Verarbeitung in einer Anwendung auf dem Smartphone handelt, so ist die verantwortliche Stelle gezwungen, datenschutzfreundliche Voreinstellungen (sog. Data Protection by Default) zu treffen.
Nichtverkettung	Personengebundene Daten dürfen nur zweckgebunden verarbeitet werden. Dies bedeutet, dass über den definierten Zweck hinaus keine Zusammenführung (Verkettung) von Datenbeständen erfolgen darf. Unter eng definierten Umständen kann eine Weiterverarbeitung gewährt werden, aber nur wenn entsprechende technische und organisatorische Maßnahmen wie bspw. eine Pseudonymisierung durchgeführt wurden, sodass die Nichtverkettung gewährleistet werden kann.
Transparenz	Es muss bei einer Verarbeitungstätigkeit jederzeit ersichtlich sein, welche Daten, wann und für welchen Zweck erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten fließen und wer die rechtliche Verantwortung besitzt. Die Forderung nach Transparenz gilt nicht nur für die verantwortliche Stelle, sondern auch für Betroffene, Systembetreiber und zuständige Kontrollinstanzen. Dies ist u.a. notwendig, falls ein Einwilligungsmanagement zum Tragen kommt. Sollten Mängel im Datenverarbeitungsprozess auftreten, können diese schnell erkannt und ausgebessert werden, wenn die Transparenz gewährleistet wurde.
Verfügbarkeit	Verfügbarkeit bedeutet, dass die Verarbeitung personenbezogener Daten unverzüglich möglich ist, da sichergestellt wurde, dass der Datenzugriff gewährleistet und ordnungsgemäß im Prozess verankert ist. Dies beinhaltet mitunter Zugriffsberechtigungen, aber auch die Auffindbarkeit von Daten durch eine strukturierte Ablage sowie eine angemessene Darstellung. Ebenso wird unter Verfügbarkeit verstanden, dass die Daten verarbeitet werden können, wenn eine hohe Last der Systeme zu erwarten ist, und dass diese nach einem Zwischenfall auch rasch wiederhergestellt werden können.
Vertraulichkeit	Es muss gewährleistet sein, dass die Daten vertraulich behandelt werden, also kein Unbefugter Zugriff auf die Daten erhält. Dabei ist zu beachten, dass es sich bei Unbefugten nicht ausschließlich um Dritte außerhalb der Organisation handeln kann, sondern bspw. auch um technische Dienstleister oder Personen aus anderen Einheiten der Organisation. Auch bei diesem Ziel gilt die Einhaltung unter hoher Last sowie die Erhebung von Maßnahmen bei einer Datenschutzverletzung.