Handreichung: Datenschutz in Kommunen

Die Datenschutzgrundverordnung (DS-GVO), das Hessische Datenschutz- und Informationsfreiheitsgesetz (HDSIG) und weitere Spezialregelungen stellen umfangreiche datenschutzrechtliche Anforderungen auf. Die nachfolgenden Hinweise sollen eine erste Hilfestellung und Orientierung insbesondere für kleinere Kommunen bieten.

I. Verantwortlichkeit und Auftragsverarbeitung

Verantwortlicher ist gemäß Art. 4 Nr. 7 DS-GVO „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“. Verantwortlich für die Verarbeitung personenbezogener Daten ist in der Regel die Kommune bzw. die einzelne kommunale Stelle (etwa Dezernat, Fachbereich oder Fachamt).

Sofern zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zu der Verarbeitung festlegen, sind sie nach Art. 4 Nr. 7, Art. 26 DS-GVO gemeinsam Verantwortliche. Dies können etwa zwei (oder mehr) Kommunen, aber auch Kommunen und andere Stellen (etwa private Unternehmen) sein. Diese müssen eine entsprechende Vereinbarung abschließen. Eine besondere Schwierigkeit stellt sich bei der Nutzung von sozialen Medien.

Auftragsverarbeiter ist gemäß Art. 4 Nr. 8, Art. 28 DS-GVO „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet“. Sofern eine Kommune externe Dienstleistungen (etwa Hosting der Webseite, Einscannen und Archivierung von Dokumenten) in Anspruch nimmt, um personenbezogene Daten im Auftrag durch andere Dienstleister verarbeiten zu lassen, ist mit diesen grundsätzlich ein Auftragsverarbeitungsvertrag entsprechend Art. 28 Abs. 3 DS-GVO abzuschließen (ein Muster ist hier abrufbar). Eine besondere Schwierigkeit stellt sich bei der Nutzung von Microsoft 365.

Die Abgrenzung zwischen Verantwortlichkeit, gemeinsamer Verantwortlichkeit und Auftragsverarbeitung ist in der Praxis häufig schwierig und muss für jeden Verarbeitungsvorgang gesondert geprüft werden.

II. Verarbeitung personenbezogener Daten

Personenbezogene Daten sind gemäß Art. 4 Nr. 1 DS-GVO „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“. Dies sind etwa Name, Vorname, Kontaktdaten (Anschrift, E-Mail-Adresse etc.), Größe, Steuer-ID, Kfz-Kennzeichen, Meinungen oder Einkommensverhältnisse. Die Verarbeitung meint nach Art. 4 Nr. 2 DS-GVO jeden Umgang mit personenbezogenen Daten. Erfasst sind z. B. die Erhebung, die Speicherung, die Verwendung in dem jeweiligen (Fach-)Verfahren, die Übermittlung und die Löschung.

Die Grundsätze für die Verarbeitung personenbezogener Daten sind in Art. 5 DS-GVO benannt: Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung sowie Integrität und Vertraulichkeit. Die Kommune ist für deren Einhaltung verantwortlich und muss die Einhaltung nachweisen können („Rechenschaftspflicht“).

Nach dem Grundsatz der Rechtmäßigkeit der Verarbeitung gemäß Art. 5 Abs. 1 Buchst. a, Art. 6 DS-GVO verlangt jede Datenverarbeitung eine Rechtsgrundlage. Diese kann für öffentliche Stellen insbesondere die Erfüllung einer rechtlichen Verpflichtung gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. c, Abs. 2 und Abs. 3 DS-GVO sowie die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe nach Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 2 und Abs. 3 DS-GVO sein. Rechtsgrundlagen für die Verarbeitungen im Sinne des Art. 6 Abs. 2 und Abs. 3 DS-GVO finden sich oftmals in dem jeweiligen Fachrecht (etwa Melderecht, Personalausweisrecht oder Ausländerrecht). Möglicherweise kann auch ein Tatbestand des § 22 HDSIG einschlägig sein. Auf die Generalklausel des § 3 Abs. 1 HDSIG sollte aufgrund der hohen Abstraktheit und Unbestimmtheit sowie fraglichen Europarechtskonformität nur ausnahmsweise bei Datenverarbeitungen mit sehr geringer Eingriffsintensität zurückgegriffen werden. Auf ein „berechtigtes Interesse“ im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO können sich Kommunen ausweislich des Unterabsatzes 2 grundsätzlich nicht berufen. Die jeweilige Rechtsgrundlage ist entsprechend zu dokumentieren (z. B. Art. 6 Abs. 1 UAbs. 1 Buchst. c, Abs. 2 und Abs. 3 DS-GVO in Verbindung mit – jeweils entsprechend anzupassen – der Rechtsgrundlage aus dem Fachrecht).

Sonderregelungen bestehen bei der Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 DS-GVO (etwa Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen hervorgehen, und Gesundheitsdaten). Deren Verarbeitung ist grundsätzlich untersagt, sofern nicht auch ein Ausnahmetatbestand im Sinne des Art. 9 Abs. 2 DS-GVO (siehe auch § 20 HDSIG) einschlägig ist. Bei der Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses sind die Maßgaben des § 23 HDSIG (bei der Personaldatenverarbeitung diejenigen der §§ 86 ff. des Hessischen Beamtengesetzes) zu berücksichtigen. Wenn personenbezogene Daten an Drittländer übermittelt werden, sind zudem die Vorschriften der Art. 44 ff. DS-GVO einzuhalten.

III. Datenschutzbeauftragte gemäß Art. 37 ff. DS-GVO, §§ 5 ff. HDSIG

Kommunen müssen gemäß Art. 37 Abs. 1 Buchst. a DS-GVO, § 5 Abs. 1 HDSIG einen Datenschutzbeauftragten und dessen Vertreter benennen (siehe dazu mein Arbeitspapier „Behördliche und betriebliche Datenschutzbeauftragte“). Möglich ist nach Art. 37 Abs. 6 DS-GVO, § 5 Abs. 4 HDSIG auch die Benennung eines externen Datenschutzbeauftragten auf der Grundlage eines Dienstleistungsvertrages. Insbesondere kleinere Kommunen können gemäß Art. 37 Abs. 3 DS-GVO, § 5 Abs. 2 HDSIG einen gemeinsamen Datenschutzbeauftragten benennen. Der Datenschutzbeauftragte muss nach Art. 37 Abs. 5 DS-GVO, § 5 Abs. 3 HDSIG über hinreichende Qualifikationen verfügen und gemäß Art. 38 Abs. 2 DS-GVO, § 6 Abs. 2 HDSIG mit entsprechenden (insbesondere zeitlichen und materiellen) Ressourcen ausgestattet werden. Die Kontaktdaten des Datenschutzbeauftragten sind gemäß Art. 37 Abs. 7 DS-GVO, § 5 Abs. 5 HDSIG zu veröffentlichen (Webseite etc.) und meiner Behörde (etwa mittels des Formulars auf meiner Webseite) mitzuteilen.

IV. Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO

Kommunen müssen gemäß Art. 30 Abs. 5 DS-GVO regelmäßig ein Verzeichnis von Verarbeitungstätigkeiten führen (ein Muster ist hier abrufbar). Dabei sind die Verarbeitungstätigkeiten der einzelnen Ämter, Verwaltungsstellen, Eigenbetriebe etc. zu dokumentieren. Das Verzeichnis dient als wesentliche Grundlage für eine strukturierte Datenschutzdokumentation und als Nachweis, dass die datenschutzrechtlichen Vorgaben eingehalten werden („Rechenschaftspflicht“ gemäß Art. 5 Abs. 2 DS-GVO). Die Anforderungen an die ordnungsgemäße Erstellung

und kontinuierliche Pflege des Verzeichnisses sollten nicht unterschätzt werden. Dieses kann von meiner Behörde nach Art. 30 Abs. 4 DS-GVO angefordert werden.

V. Informationspflichten gemäß Art. 13 und 14 DS-GVO

Die betroffenen Personen sind entsprechend Art. 13 DS-GVO (Direkterhebung) bzw. Art. 14 DS-GVO (Dritterhebung) zu informieren. Die inhaltlichen Anforderungen ergeben sich aus den Absätzen 1 und 2 des jeweiligen Artikels. Die Informationen sind gemäß Art. 12 DS-GVO transparent, verständlich und leicht zugänglich zu erteilen. Sie können etwa auf kommunalen Schreiben, Aushängen vor Ort sowie auf der Webseite abgebildet werden. Dies kann auch in abgestufter Form geschehen: Zunächst genügen verkürzte Informationen, sofern an anderer Stelle (Webseite, Informationsblatt o. Ä.) alle notwendigen Informationen des Art. 13 bzw. Art. 14 DS-GVO bereitgehalten werden und darauf (etwa mittels Links oder QR-Codes) hingewiesen wird. Die Informationen sind seitens der Kommune lediglich zu erteilen. Eine „Zustimmung“, „Einwilligung“ o. Ä. durch die betroffenen Personen ist dagegen nicht einzuholen.

VI. Rechte der betroffenen Personen gemäß Art. 15 ff. DS-GVO

Betroffene Personen haben nach Art. 15 ff. DS-GVO mehrere Rechte. Neben dem Auskunftsrecht nach Art. 15 DS-GVO als zentralem Betroffenenrecht (siehe dazu meine Handreichung „Auskunftsrecht gemäß Art. 15 DS-GVO gegenüber Kommunen“) stehen ihnen insbesondere folgende Rechte zu:

- Recht auf Berichtigung (Art. 16 DS-GVO),
- Recht auf Löschung (Art. 17 DS-GVO),
- Recht auf Einschränkung der Verarbeitung (Art. 18 DS-GVO),
- Widerspruchsrecht (Art. 21 DS-GVO)

Sofern eine betroffene Person von ihrem Auskunftsrecht nach Art. 15 DS-GVO Gebrauch macht, ist die Datenauskunft grundsätzlich vollständig zu erteilen (siehe die einzelnen Punkte der Absätze 1 und 2). Sofern eine große Menge von Informationen über die betroffene Person verarbeitet wird, kann zunächst eine allgemein gehaltene Auskunft erteilt werden. Sodann kann die betroffene Person ihr Auskunftsrecht entsprechend des Erwägungsgrunds 63 S. 7 DS-GVO konkretisieren. Auch die Herausgabe von Kopien einzelner Dokumente, Unterlagen etc. (etwa Schreiben, E-Mails oder Aktenvermerke) kann nach Art. 15 Abs. 3 DS-GVO geschuldet sein. Das Recht auf Erhalt einer Kopie darf aber gemäß Art. 15 Abs. 4 DS-GVO die Rechte und Freiheiten anderer Personen nicht beeinträchtigen. Kopien sind daher ggf. entsprechend zu schwärzen.

Der Antrag ist grundsätzlich auf dem Kommunikationskanal zu erfüllen, auf dem er gestellt worden ist (siehe zu der elektronischen Antragstellung Art. 15 Abs. 3 DS-GVO). Dies gilt jedoch nur, sofern die Identität des Antragsstellers bzw. dessen (alleinige) Verfügungsgewalt über erhaltene Nachrichten sichergestellt ist. Eine Auskunft per E-Mail ist etwa nicht zu erteilen, wenn nicht verifiziert ist, dass die E-Mail-Adresse zu dem Antragsteller gehört. Der Antrag ist gemäß Art. 12 Abs. 3 DS-GVO grundsätzlich spätestens innerhalb eines Monats nach Eingang des Antrages zu erfüllen.

Bei „begründeten Zweifeln“ an der Identität des Antragstellers können nach Art. 12 Abs. 6 DS-GVO zusätzliche Informationen angefordert werden. Es kann etwa die Kopie des Personalausweises (versehen mit dem Hinweis auf die Möglichkeit von Schwärzungen nicht erforderlicher Angaben) verlangt werden. Eine voraussetzungslose Anforderung weiterer Informationen ist jedoch nicht zulässig.

Das Recht auf und die Pflicht zu der Löschung nach Art. 17 DS-GVO besteht nicht voraussetzungslos, sondern unterliegt den Einschränkungen des Absatzes 3. Eine Datenlöschung muss etwa nicht erfolgen, soweit die Verarbeitung zu der Erfüllung einer rechtlichen Verpflichtung oder zu der Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist.

VII. Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO

Kommunen haben gemäß Art. 32 DS-GVO geeignete technische und organisatorische Maßnahmen zu der Gewährleistung eines dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenen Schutzniveaus zu ergreifen. Dazu muss zunächst das Risiko für die Rechte und Freiheiten der von der Verarbeitung ihrer Daten betroffenen Personen ermittelt werden. Darauf aufbauend müssen unter Berücksichtigung der übrigen Aspekte des Art. 32 Abs. 1 DS-GVO geeignete technische und organisatorische Maßnahmen konzipiert und umgesetzt werden. Diese Maßnahmen sind regelmäßig sowie anlassbezogen zu überprüfen und bei Bedarf anzupassen. Als Grundlage sind in jedem Fall Basismaßnahmen zu ergreifen. Dazu zählen insbesondere zeitnah mit Sicherheits-Updates aktuell gehaltene Betriebssysteme und Anwendungen, eine einheitliche durchgehend umgesetzte Passwortrichtlinie, regelmäßige Backups, aktuelle Anti-Virus-Software und ein durchgehendes Benutzer-Rollen-Konzept. Dokumente in Papierform sind unbedingt (mittels Papierschredders oder Aktenvernichters) ordnungsgemäß zu vernichten. Besondere Schwierigkeiten – nicht nur hinsichtlich der Sicherheit der Verarbeitung – stellen sich bei der Nutzung von Videokonferenzsystemen. Im Rahmen von IT-Projekten sollten datenschutzrechtliche Anforderungen von Beginn an, umfassend und durchgängig berücksichtigt und umgesetzt werden.

VIII. Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO

Sofern eine Datenverarbeitung voraussichtlich ein hohes Risiko für betroffene Personen zur Folge hat, ist vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge durchzuführen. Eine solche ist insbesondere in den Fällen des Art. 35 Abs. 3 DS-GVO (etwa umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DS-GVO oder systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche) sowie der Liste der Verarbeitungsvorgänge nach Absatz 4 erforderlich.

IX. Datenschutzverletzungen gemäß Art. 33 und 34 DS-GVO

Im Falle einer Verletzung des Schutzes personenbezogener Daten bestehen die Meldungs- und Benachrichtigungspflichten gemäß Art. 33 und 34 DS-GVO. Häufige Praxisfälle sind etwa der Diebstahl oder Verlust von Smartphone, Laptop o. Ä., der Fehlversand von Unterlagen sowie Hacking- oder Phishing-Vorfälle.

Eine Meldung an die Aufsichtsbehörde nach Art. 33 DS-GVO muss in der Regel erfolgen (etwa mittels des Formulars auf meiner Webseite). Eine Bagatellgrenze besteht nicht. Eine Meldung ist nur dann nicht erforderlich, wenn kein Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Ein Risiko im Sinne der DS-GVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann. Das Risiko hat zwei Dimensionen: die Schwere des voraussichtlichen Schadens sowie die Wahrscheinlichkeit, dass das Ereignis und die Folgeschäden eintreten. Die Einschätzung ist zum Zeitpunkt der Entscheidung über die Meldung vorzunehmen und muss im weiteren Verlauf bei Bedarf angepasst werden. Bei der Meldung gegenüber meiner Behörde sollte der Sachstand zu dem Vorfall derart ausführlich

beschrieben werden, dass der Vorfall und dessen Kontext möglichst vollständig nachvollziehbar ist.

Der Prozess und die Zuständigkeit für die Meldung sind innerhalb der Kommune festzulegen. Die 72-Stunden-Frist ab Bekanntwerden der Verletzung muss eingehalten werden. Dabei sieht Art. 33 Abs. 4 DS-GVO auch die Abgabe einer Meldung mit unvollständigen Informationen vor. Fehlende Informationen können ohne unangemessene Verzögerungen nachgereicht werden.

Nach Art. 33 Abs. 5 DS-GVO sind Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen zu dokumentieren. Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen des Art. 33 DS-GVO ermöglichen. Eine Benachrichtigung der betroffenen Personen gemäß Art. 34 DS-GVO muss dagegen nur bei einem „hohen Risiko“ erfolgen. Ein solches ist etwa bei einer hohen Anzahl betroffener Personen oder der Verarbeitung besonderer Kategorien personenbezogener Daten wie etwa Gesundheitsdaten anzunehmen.

Stand: 11.2.2026