# Datenschutz bei politischen Informationssystemen

Politische Informationssysteme (auch als Gremieninformationssysteme oder Ratsinformationssysteme bezeichnet) dienen dem Informationsinteresse der Bürgerinnen und Bürger und einem transparenten politischen Willensbildungsprozess. Zugleich muss das Recht auf informationelle Selbstbestimmung der betroffenen Personen geschützt werden. Die nachfolgenden Hinweise sollen bei der Umsetzung der wesentlichen Aspekte des Datenschutzes unterstützen.

Politische Informationssysteme sind IT-basierte Informations- und Dokumentenmanagementsysteme und unterstützen die Gremienarbeit in den Kommunen. Sie dienen insbesondere als Informationsmedium für Mandatsträger und weitere interessierte Personen, die sich über Sitzungen, Niederschriften und Mandatsträger bzw. Gremien bei dem Verantwortlichen informieren möchten. Verantwortlicher ist im Sinne von 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“. In der Regel gibt es in politischen Informationssystemen neben einem öffentlichen Bereich mit eingeschränkten Zugriffsmöglichkeiten (etwa Sitzungstermine, Niederschriften der öffentlichen Tagesordnungspunkte sowie Angaben zu den Mandatsträgern) einen geschlossenen Bereich. Dort sind weitere Unterlagen (etwa Niederschriften der nicht öffentlichen Tagesordnungspunkte) hinterlegt, auf welche lediglich registrierte Nutzer (zugehörige Mandatsträger) Zugriff erhalten. Die Unterlagen enthalten in der Regel personenbezogene Daten, so dass die Anforderungen des Datenschutzes zu berücksichtigen sind.

## I. Rechtsgrundlage

Die Verarbeitung personenbezogener Daten mittels eines politischen Informationssystems ist grundsätzlich gemäß Art. 6 Abs. 1 UAbs. 1 Buchstabe e, Abs. 2 und 3 DS-GVO in Verbindung mit dem Öffentlichkeitsprinzip gemäß § 52 HGO zulässig. Insofern ist die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt. Der Austausch von Informationen ist für den politischen Willensbildungsprozess essentiell. Der Grundsatz der Erforderlichkeit bedingt jedoch, dass personenbezogene Daten nur in dem Umfang verarbeitet (insbesondere offengelegt) werden, in welchem sie für die Aufgabenwahrnehmung tatsächlich notwendig sind (siehe dazu II.).

Der Öffentlichkeitsgrundsatz ist überdies in weiteren Vorschriften der HGO normiert (siehe insbesondere die Regelung über öffentliche Bekanntmachungen nach § 7 HGO, zu der öffentlichen Bekanntmachung von Satzungen gemäß § 5 Abs. 3 HGO und zu der Niederschrift der Gemeindevertretung nach § 61 HGO).

Das Demokratie- und Öffentlichkeitsprinzip ist auch verfassungsrechtlich gemäß Art. 20 Abs. 1 und Abs. 2 GG sowie Art. 65 Verf HE verankert. Dieses gilt nach Art. 28 Abs. 1 GG auch in den Kommunen.

Das Öffentlichkeitsprinzip des § 52 HGO gilt neben der Gemeindevertretung auch für die Ausschüsse der Gemeindevertretung gemäß § 62 HGO (§ 62 Abs. 5 in Verbindung mit § 52 HGO, etwa Finanzausschuss, Sozialausschuss und Umweltausschuss), die Ortsbeiräte gemäß § 81 ff. HGO (§ 82 Abs. 6 in Verbindung mit § 52 HGO) sowie für die Ausländerbeiräte gemäß § 84 ff. HGO (§ 87 Abs. 3 in Verbindung mit § 52 HGO). Daher gelten die hier aufgeführten Maßgaben zusätzlich zu der Gemeindevertretung auch für diese Gremien.

Diese gelten überdies für die entsprechenden Gremien auf Ebene der Landkreise: für den Kreistag gemäß § 32 HKO in Verbindung mit §§ 52, 61 HGO, die Ausschüsse des Kreistages gemäß § 33 HKO sowie die Ausländerbeiräte nach § 4b HKO (siehe auch die Regelung über öffentliche Bekanntmachungen nach § 6 HKO sowie zu der öffentlichen Bekanntmachung von Satzungen gemäß § 5 Abs. 3 HKO).

## II. Weitere datenschutzrechtliche Anforderungen

Die Verarbeitung personenbezogener Daten mittels eines politischen Informationssystems ist in das Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO aufzunehmen (siehe DSK, Kurzpapier Nr. 1 – Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO; sowie Muster-Verzeichnis von Verarbeitungstätigkeiten Verantwortlicher).

Die betroffenen Personen (insbesondere Mandatsträgerinnen und Mandatsträger sowie Beschäftigte der Kommunalverwaltung, aber auch Dritte wie Bürgerinnen und Bürger) sind gemäß Art. 13 DS-GVO über die Datenverarbeitung zu informieren (siehe DSK, Kurzpapier Nr. 10 – Informationspflichten bei Dritt- und Direkterhebung). Dies kann in der Regel mittels einer Datenschutzinformation auf der Webseite erfolgen. Zusätzlich können die Informationen in Papierform (etwa als Aushang im Bürgerbüro) erteilt werden.

Die rechtzeitige und ordnungsgemäße Erfüllung der Betroffenenrechte stellt Verantwortliche bei politischen Informationssystemen vor nicht unerhebliche Herausforderungen. Daher ist vorab ein entsprechender Prozess zu etablieren und regelmäßig zu evaluieren. Insbesondere muss dem Auskunftsrecht betroffener Personen des Art. 15 DS-GVO vollumfänglich entsprochen werden (siehe DSK, Kurzpapier Nr. 6 – Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO).

Überdies haben betroffene Personen gemäß Art. 17 DS-GVO ein Recht auf Löschung (siehe DSK, Kurzpapier Nr. 11 – Recht auf Löschung / „Recht auf Vergessenwerden“). Es besteht zudem die Pflicht des Verantwortlichen, personenbezogene Daten unverzüglich in den dort genannten Fällen zu löschen, sofern kein Ausnahmetatbestand nach Absatz 3 eingreift. Der Verantwortliche hat zudem grundsätzlich dem „Recht auf Vergessenwerden“ gemäß Absatz 2 nachzukommen. Insofern muss er angemessene (auch technische) Maßnahmen ergreifen, „um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat“. Der Verantwortliche hat ein Löschkonzept zu erarbeiten und regelmäßig zu überprüfen.

Um den Anforderungen des Art. 17 DS-GVO in der Praxis gerecht zu werden, sind die in das politische Informationssystem eingestellten Unterlagen vorab hinsichtlich der auf diesen ersichtlichen personenbezogenen Daten zu überprüfen. Angesichts der weltweiten und unbegrenzten Verfügbarkeit von im Internet veröffentlichten Informationen ist ein datensparsamer Umgang dringend zu empfehlen. Dies betrifft insbesondere die personenbezogenen Daten von Bürgerinnen und Bürgern. Sofern diese (ggf. mittelbar) im Sinne des Art. 4 Nr. 1 DS-GVO etwa im Rahmen von Grundstücksgeschäften identifizierbar sind, müssen die personenbezogenen Daten in der Regel vorab (durch Schwärzungen) unkenntlich gemacht werden bzw. müssen die Unterlagen entsprechend angepasst werden (siehe zur Veröffentlichung von Sitzungsprotokollen im Internet, HBDI, 50. Tätigkeitsbericht, S. 97 f.).

Auch sind die weiteren Grundsätze für die Verarbeitung personenbezogener Daten des Art. 5 DS-GVO im Rahmen von politischen Informationssystemen vollumfänglich zu berücksichtigen. Dahingehend ist insbesondere auf die „Zweckbindung“ gemäß Art. 5 Abs. 1 Buchstabe b DS-GVO hinzuweisen. Die „Datenminimierung“ und die „Speicherbegrenzung“ nach Art. 5 Abs. 1 Buchstabe c und e DS-GVO bedingen eine kritische Prüfung, welche Informationen (personenbezogene Daten) in welchem Umfang für welchen Zeitraum zu der Erfüllung des Informationsinteresses erforderlich sind. Der Grundsatz der „Richtigkeit“ des Art. 5 Abs. 1 Buchstabe d DS-GVO fordert, dass die bereitgestellten Informationen (personenbezogene Daten) korrekt sind und ggf. aktualisiert werden. Der Verantwortliche ist ausweislich der „Rechenschaftspflicht“ im Sinne des Art. 5 Abs. 2 DS-GVO für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können.

Besonders relevant sind geeignete technische und organisatorische Maßnahmen zwecks Gewährleistung eines dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenen Schutzniveaus gemäß Art. 5 Abs. 1 Buchstabe f in Verbindung mit Art. 32 DS-GVO (siehe DSK, Kurzpapier Nr. 18 – Risiko für die Rechte und Freiheiten natürlicher Personen). Erforderlich in technischer Hinsicht sind insbesondere ein Zugriffskonzept, eine sichere Webseite (mit Sicherheits-Updates aktuell gehaltene Anwendungen), eine Passwortkomplexität bei dem Zugang zu geschlossenen Bereichen sowie regelmäßige Backups. Organisatorisch sind vor allem Regelungen betreffend die Unkenntlichmachung personenbezogener Angaben zu treffen und es ist auf die Verschwiegenheitspflicht hinzuweisen (siehe auch § 24 HGO).

Es sind ggf. vertragliche Regelungen erforderlich. Sofern externe Dienstleister eingesetzt werden (etwa zu der Bereitstellung der Hard- und Software zu dem Betrieb des politischen Informationssystems), ist mit diesen in der Regel ein Auftragsverarbeitungsvertrag gemäß Art. 28 Abs. 3 DS-GVO abzuschließen (siehe DSK, Kurzpapier Nr. 13 – Auftragsverarbeitung, Art. 28 DS-GVO sowie Formulierungshilfe für einen Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO).

Der behördliche Datenschutzbeauftragte ist gemäß Art. 39 Abs. 1 Buchstabe a und b DS-GVO, § 7 Abs. 1 S. 1 Nr. 1 und Nr. 2 HDSIG kontinuierlich einzubeziehen.

*Stand: 24.07.2024*