Ratsinformationssysteme und mobile Datenverarbeitung durch kommunale Mandatsträgerinnen und Mandatsträger

Stand 13.03.2018

Ratsinformationssysteme

Ein Ratsinformationssystem ist ein IT-gestütztes Informations- und Dokumentenmanagementsystem, dass die Gremienarbeit in Kommunen unterstützt. Es hilft den politischen Gremien und kommunalen Mandatsträgerinnen und Mandatsträgern bei der Erfüllung ihrer Aufgaben. Gleichzeitig erleichtert es der Verwaltung die Vorbereitung und Unterstützung der Arbeit der Gremien. Typischerweise organisiert ein Ratsinformationssystem einen Workflow für die Informationen, die für die kommunalen Gremien von Belang sind. So bereitet die Verwaltung die Sitzung vor (Aufstellung der Tagesordnung, Versand von Einladungen etc.) und hinterlegt die benötigten Unterlagen und Informationen im System; teilweise tun dies Mandatsträgerinnen, Mandatsträger und Fraktionen auch selbst. Vor, während und nach der Sitzung greifen die kommunalen Mandatsträgerinnen und Mandatsträger auf die Unterlagen zu. Mit Hilfe des Systems wird nach der Sitzung das Protokoll erstellt und verteilt. Die Ergebnisse aus dem öffentlichen Teil der Sitzung können im Internet veröffentlicht werden. Schließlich kann das System dazu genutzt werden, die Umsetzung der Beschlüsse zu überwachen.

Zu den mithilfe eines Ratsinformationssystems verarbeiteten Informationen gehören regelmäßig auch personenbezogene Daten. Dies sind einerseits Daten in Dokumenten mit personenbezogenen Inhalten, andererseits – unabhängig vom Inhalt der Dokumente – Daten über die Nutzenden (Protokolldaten beim Log-In, Abrufe, Webstatistiken). Bei der Datenverarbeitung sind die Vorgaben zu den technisch-organisatorischen Maßnahmen nach den Datenschutzgesetzen zu beachten. Bevor konkrete technisch-organisatorische Hinweise zur Konfiguration von Ratsinformationssystemen gegeben werden können, ist festzustellen, wer in den verschiedenen Konstellationen die Verantwortung für die Verarbeitung personenbezogener Daten trägt.

Die grundsätzlichen Anforderungen an ein Ratsinformationssystem hinsichtlich Benutzerauthentifizierung, rollenbasierter Zugriffsrechte, sicherer Übertragung von Daten und datenschutzkonformem Speichern sowie an Anwendungssoftware für Computer oder mobile Geräte sind dementsprechend hoch und müssen je nach Nutzungsszenario ergänzt werden. Die eingesetzte Software muss dafür ausgelegt sein, den Anforderungen der Datenschutz-Grundverordnung (DSGVO) zu genügen und die Rechte von betroffenen Personen zu schützen.

Wer ist für welche Datenverarbeitung verantwortlich?

„Verantwortlicher“ ist nach Art. 4 Nr. 7 Datenschutz-Grundverordnung (DSGVO) „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“.

Nach Art. 5 Abs. 2 DSGVO ist „der Verantwortliche“ für die Einhaltung der Grundsätze der Datenverarbeitung verantwortlich und muss ihre Einhaltung nachweisen können („Rechenschaftspflicht“). Nach Art. 24 Abs. 1 DSGVO setzt der Verantwortliche „unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrschein-

lichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt“.

Das eigentliche Ratsinformationssystem wird von der Kommune betrieben. Daher ist die Kommune insoweit zunächst Verantwortliche im Sinne der DSGVO. Allerdings kommt es in verschiedenen Szenarien zu einem mehr oder weniger klar definierten Übergang der Verantwortung für die Verarbeitung der im System zur Verfügung gestellten personenbezogenen Daten an die kommunalen Mandatsträgerinnen und Mandatsträger.

Die kommunalen Mandatsträgerinnen und Mandatsträger sind, anders als Mitarbeiterinnen und Mitarbeiter der kommunalen Verwaltung, nicht als Bestandteil der Verwaltung anzusehen. Den kommunalen Mandatsträgerinnen und Mandatsträgern sind Aufgaben und Kompetenzen zur eigenverantwortlichen Wahrnehmung zugewiesen (VGH Mannheim, KommJur 2017, 457). Sie unterliegen einer eigenständigen Verschwiegenheitspflicht (§ 21 Abs. 2 Gemeindeordnung [GO], für Kreistagsabgeordnete i. V. m. § 27 Abs. 3 Kreisordnung [KrO]).

Den Mandatsträgerinnen und Mandatsträgern werden für die Zwecke der Ausübung ihres Mandats personenbezogene Daten von der Verwaltung zur Verfügung gestellt. Haben die kommunalen Mandatsträgerinnen und Mandatsträger die personenbezogenen Daten danach vollständig in ihrer Verfügungsgewalt, so können sie von diesem Zeitpunkt an die Zwecke und Mittel der Verarbeitung bestimmen und sind demnach Verantwortliche im Sinne der DSGVO.

Dies ist z. B. der Fall, wenn die Mandatsträgerinnen und Mandatsträger die personenbezogenen Daten in Papierform erhalten und z. B. in ihren häuslichen Bereich einbringen. Nichts anderes gilt, wenn der Zugang zu den Daten über ein Web-Frontend des Ratsinformationssystems ermöglicht wird und die Mandatsträgerinnen und Mandatsträger die Daten auf ihre privaten Computer herunterladen und dort speichern. Auch die weitere Bearbeitung von Daten, z.B. bei der Erstellung von Änderungsanträgen, gehört dazu.

In diesen Konstellationen haben die Mandatsträgerinnen und Mandatsträger selbst die datenschutzrechtlichen Vorschriften einzuhalten. Dazu gehört die Gewährung der Rechte der Betroffenen (Art. 12 ff.) und die Umsetzung der technisch-organisatorischen Maßnahmen (Art. 24 ff.). Die Verwaltung der Kommune hat ab diesem Zeitpunkt nicht mehr die Möglichkeit, auf die Datenverarbeitung Einfluss zu nehmen und verliert insoweit für die bei den Mandatsträgerinnen und Mandatsträgern befindlichen Daten die Eigenschaft als Verantwortliche.

Konstellationen bei der Nutzung mobiler Endgeräte

Häufig stellen Ratsinformationssysteme die Möglichkeit zur Verfügung, dass Mandatsträgerinnen und Mandatsträger mittels mobiler Endgeräte (zumeist „Tablets“) auf die Informationen zugreifen. Dazu wird eine „App“ auf dem Endgerät installiert, die in der Regel über eine verschlüsselte Verbindung (https-Kanal) auf den Server des Ratsinformationssystems zugreift. Die App kann es ermöglichen, die Unterlagen nur zu betrachten oder diese auch lokal abzuspeichern.

Im Hinblick auf den Eigentumsstatus der mobilen Endgeräte gibt es im Wesentlichen drei Szenarien:

1. Von der Kommunalverwaltung bereitgestelltes Endgerät, private Nutzung verboten und technisch unmöglich gemacht;
2. Von der Kommunalverwaltung bereitgestelltes Endgerät, private Nutzung erlaubt;
3. Privates Endgerät wird für die Gremienarbeit zugelassen - „Bring Your Own Device“ (BYOD).

Im Hinblick auf die eigenständige Rechtsstellung der kommunalen Mandatsträgerinnen und Mandatsträger ist keine dieser Konstellationen per se unzulässig. Allerdings ergeben sich daraus unterschiedliche Konsequenzen im Hinblick auf die Verantwortlichkeit im Sinne des Datenschutzrechts für die mobilen Endgeräte (unabhängig von der Verantwortung der Kommune für das von ihr betriebene zentrale Ratsinformationssystem).

In der **ersten Konstellation** bleibt die Kommune Verantwortlicher im Sinne des Datenschutzrechts. Dies gilt jedenfalls solange, wie die personenbezogenen Daten das mobile Endgerät nicht verlassen. Dieses ist als Teil des von der Kommune administrierten Ratsinformationssystems anzusehen.

In der **zweiten Konstellation** kann es zu einer gemeinsamen Verantwortlichkeit von Verwaltung einerseits und Mandatsträgerinnen und Mandatsträger andererseits im Sinne von Art. 26 DSGVO kommen, da beide Stellen jeweils teilweise die Zwecke der und die Mittel zur Verarbeitung festlegen können. Nach Art. 26 Abs. 1 Satz 2 DSGVO haben dann beide in einer Vereinbarung festzulegen, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht.

In der **dritten Konstellation** ist die kommunale Mandatsträgerin bzw. der Mandatsträger Verantwortlicher im Sinne der DSGVO. Hier gilt nichts anderes als in den oben angesprochenen Konstellationen, in denen die Mandatsträgerin bzw. der Mandatsträger die Daten vollständig in seinem Verfügungsbereich hat. Mit der Nutzung eines privaten Tablets vergleichbar ist auch die Nutzung eines eigenen PCs oder Notebooks.

Gefährdungen bei der Nutzung mobiler Endgeräte

Aus der Nutzung von IT-Systemen können Gefahren für einen unbefugten Zugriff resultieren – sei es durch unbefugte Zugriffe auf die Datenbestände im zentralen Ratsinformationssystem (z. B. durch erratene oder ausgespähte Passwörter) oder unbefugte Zugriffe auf Kopien in den Endgräten der Mandatsträgerinnen und Mandatsträger. Mobile Endgeräte sind dabei besonders gefährdet, da sie leichter verloren oder gestohlen werden können, einige Betriebssysteme verhältnismäßig leicht angreifbar sind und Daten möglicherweise bei Defekt, Aussonderung, Verkauf oder Weitergabe der Geräte versehentlich an Dritte übergeben werden.

Um ein Ratsinformationssystem mit mobilen Endgeräten datenschutzkonform betreiben und nutzen zu können, sind Pflichten und Zuständigkeiten der Verwaltung einerseits und der Mandatsträgerinnen und Mandatsträger andererseits zu klären und schriftlich niederzulegen. Dies betrifft neben der Nutzung auch die Gestaltung (u. a. Art. 25 DSGVO) und die sichere Konfiguration und den Betrieb (Art. 32 DSGVO). Sie hängen, wie oben dargestellt, vom Einsatzszenario ab. Die klarste Regelungen und Trennungen zwischen Mandatstätigkeit einerseits und Privattätigkeit andererseits ergibt sich, wenn die Verwaltung die Geräte beschafft und ausschließlich eine dienstliche Nutzung zugelassen ist (Konstellation 1).

Es bieten sich dazu individuelle Nutzungsvereinbarungen oder eine verpflichtende zentrale Regelung, etwa im Annex zu einer Geschäftsordnung, an. Wesentliche Punkte hierbei sind:

- Endgeräte-Auswahl und -Beschaffung (Wer? Welche Geräte)
- Einrichtung eines Zugangsschutzes (PIN, Passwort einschließlich Längenvorgabe)
- Einrichtung einer Verschlüsselung auf dem Endgerät (ohne Zugriffsmöglichkeit durch die Hersteller des Gerätes)
- Einbindung in eine zentrale Verwaltungsplattform (Mobile Device Management, MDM)
- Installation von Betriebssystem/Firmware-Updates auf den Endgeräten (Wer? Wann?)
- Installation eines Schutzprogramms vor Schadsoftware (herstellerabhängig) (Wer? Wann?)
- Installation von Apps (Zulässigkeit? Durch wen?)
- Nutzung von Druckfunktionen (Zulässigkeit? Wer?)
- Zulässigkeit der E-Mail-Nutzung (E-Mail-Adresse durch Verwaltung bereitgestellt; private E-Mail-Adresse)
- Zulässigkeit der Internetnutzung (im Rahmen der Mandatstätigkeit; privat)
- Verbot eines administrativen Zugangs zum Endgerät („rooten“, „Jail-Breaking“) oder Nutzung nicht unterstützter Betriebssysteme
- Verpflichtende Nutzung einer Ratsinformations-App
- Speicherung von Daten aus dem Ratsinformationssystem in Bereichen, die anderen Gerätebenutzern nicht zugänglich sind (kontrolliert durch die App), optimal verschlüsselt auf austauschbaren Datenträgern
- Verbot der Speicherung von Daten des Ratsinformationssystems außerhalb eines von der App kontrollierten Bereichs
- Benutzersupport für das Ratsinformationssystem und das Endgerät; Ansprechpartner in der Verwaltung
- Meldungen, Meldewege und Maßnahmen bei Sicherheitsvorfällen
- Auskunfts-, Korrektur- und Löschersuchen (Art. 15-18 DSGVO)
- Informationspflichten bei Datenschutzvorfällen (Artikel 33, 34 DSGVO)
- Maßnahmen bei Wartung/Reparatur des Endgerätes (insb. Entfernen externer Datenträger)
- Maßnahmen bei Verlust/Diebstahl des Endgerätes (insb. Löschen)
- Maßnahmen bei Beendigung der Mandatsträgertätigkeit (Löschen, Rückgabe)
- Maßnahmen bei der Entsorgung oder Weitergabe der Geräte
- Maßnahmen bei Verstößen gegen Nutzungsvereinbarungen/Nutzungsbedingungen
- Kontrollmöglichkeiten durch die Verwaltung (inkl. automatisierter Überprüfung durch eine MDM)
- Maßnahmen beim Ausfall des Ratsinformationssystems, einzelner Geräte oder anderer Infrastruktur (z. B. WLAN)

Diese Punkte sind in erster Linie für mobile Endgeräte wie Tablets und Smartphones formuliert, lassen sich aber auch auf andere Endgeräte wie Notebooks und Arbeitsplatz-PCs übertragen. Je nach Einsatzszenario ist zu klären, wer für die Umsetzung der Punkte zuständig ist (Verwaltung oder Mandatsträger) und ob bestimmte Nutzungen (etwa Privatnutzungen oder Nutzungen durch Dritte) zulässig sind oder nicht.

Zur Durchsetzung der Regelungen und zur Unterstützung der Mandatsträger sollten die Geräte in eine technische Verwaltungslösung (Mobile Device Management) eingebunden sein. Unabhängig von der gewählten Konstellation sind die Mandatsträgerinnen und Mandatsträger schriftlich zu informieren, zu schulen und zu sensibilisieren.

Ein Verzicht auf die Durchsetzung technisch-organisatorischer Maßnahmen in den Endgeräten kommt nur infrage, wenn sicher ausgeschlossen ist, dass mit ihnen personenbezogene Daten aus dem Ratsinformationssystem verarbeitet werden. Dies wäre etwa der Fall, wenn Unterlagen mit personenbezogenen Daten nicht elektronisch abrufbar sind und ausschließlich in Papierform an die Mandatsträgerinnen und Mandatsträger übergeben werden. Zu beachten ist, dass es zudem Informationen wie Betriebs- oder Geschäftsgeheimnisse gibt, die zwar nicht dem Datenschutzrecht unterfallen, aber gleichfalls schutzbedürftig sind.

Bei Fragen oder Beratungswünschen können Sie sich gerne an uns wenden:

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
Holstenstraße 98
24103 Kiel
Telefon: +49 (0) 431 988-1200
E-Mail: mail@datenschutzzentrum.de
https://www.datenschutzzentrum.de/