Handreichung zum Datenschutz für kommunale Mandatsträger

(Stand: April 2022)

Inhaltsverzeichnis

Seite

I. Ratsarbeit und Datenschutz – Fragen und Antworten

Die haupt- und ehrenamtlichen Mandatsträger einer Kommune haben in Ausübung ihrer Tätigkeit Zugang zu sehr vertraulichen Daten, die nicht für die Öffentlichkeit bestimmt sind.

Personenbezogene Daten werden durch das Grundrecht auf informationelle Selbstbestimmung verfassungsrechtlich geschützt (vgl. das sogenannte „Volkszählungsurteil“ des Bundesverfassungsgerichts, BVerfG, Urteil vom 15.12.1983 - 1 BvR 209/83 -, Rn. 1-215). Dieser Schutz gilt sowohl für die personenbezogenen Daten der Einwohner als auch für die Daten der Mandatsträger.

Seit dem 25.05.2018 gilt die EU-Datenschutzgrundverordnung (DS-GVO; ABl. L 119/2016) unmittelbar in allen EU-Mitgliedsstaaten. Ein wesentlicher Grundsatz der DS-GVO ist das sogenannte Verbot mit Erlaubnisvorbehalt. Dies bedeutet, dass die Verarbeitung personenbezogener Daten nur zulässig ist, wenn eine Rechtsvorschrift dies ausdrücklich erlaubt oder die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.

Für die Verarbeitung personenbezogener Daten durch Mitglieder der Vertretung finden neben den allgemeinen Bestimmungen der DS-GVO vor allem das Datenschutz-Grundverordnungs-Ausfüllungsgesetz Sachsen-Anhalt vom 18.02.2020 (DSAG LSA, GVBl. LSA 2020, S. 25 ff.) sowie spezialgesetzliche Regelungen wie zum Beispiel das Kommunalverfassungsgesetz des Landes Sachsen-Anhalt vom 17.06.2014 (KVG LSA, GVBl. LSA 2014, S. 288 ff.)

Der nachfolgende Katalog enthält Antworten auf häufig gestellte Fragen aus der täglichen Praxis der kommunalen Mandatsträger – ohne Anspruch auf Vollständigkeit.

1. Wie wird der Begriff „personenbezogene Daten“ definiert?

Gemäß Art. 4 Nr. 1 DS-GVO sind dies alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (sogenannte „betroffene Person“) beziehen (z. B. Name, Geburtsdatum, Familienstand, Anschrift, Foto oder Video einer Person). Solange ein Rückschluss auf eine Person möglich ist, gelten Daten als personenbezogen.

2. Was versteht man unter Datenverarbeitung?

Gemäß Art. 4 Nr. 2 DS-GVO versteht man unter Datenverarbeitung u.a. das Erheben, die Speicherung, die Offenlegung (z. B. Übermittlung) sowie das Löschen personenbezogener Daten.

3. Wer ist für die Verarbeitung personenbezogener Daten verantwortlich?

Die Tätigkeit der Vertretung, die gemäß § 7 Abs. 1 KVG LSA ein Organ der Kommune ist, wird der Kommune zugerechnet. Sofern ein Mitglied der Vertretung personenbezogene Daten im Rahmen der Ratstätigkeit verarbeitet, wird dies der Vertretung und somit der Kommune zugerechnet.

Abzugrenzen hiervon ist der Fall, in dem ein Mitglied der Vertretung offenkundig privat oder bei seiner Tätigkeit als Parteimitglied (z. B. im Rahmen des Wahlkampfs) personenbezogene Daten verarbeitet. In diesem Fall wird das Handeln nicht der Kommune zugerechnet, sondern dem Mitglied der Vertretung als Privatperson.

4. Wie kommen Mandatsträger mit personenbezogenen Daten in Berührung?

Kommunale Mandatsträger erlangen im Rahmen ihrer Mandatstätigkeit regelmäßig Kenntnis von personenbezogenen Daten und verarbeiten diese möglicherweise anderweitig. So können beispielsweise Sitzungsunterlagen personenbezogene Daten von Einwohnern enthalten oder es werden im Rahmen einer Gremiendiskussion personenbezogene Daten preisgegeben. Beinhalten die Sitzungsunterlagen Daten, die Rückschlüsse auf eine bestimmte Person zulassen (relevant ist dies insbesondere bei Grundstücksangelegenheiten, im Zusammenhang mit Personalangelegenheiten oder bei Vergabeentscheidungen etc.), so müssen diese Daten vor der Veröffentlichung der Unterlagen z. B. in einem Bürgerinformationssystem anonymisiert oder geschwärzt werden.

5. Wie gelangen Mandatsträger an die für ihre politische Arbeit notwendigen Informationen?

Die Verwaltung bereitet die Sitzungen durch die Aufstellung und öffentliche Bekanntmachung der Tagesordnung vor. Die Tagesordnung muss den Mitgliedern der Vertretung zugeleitet werden. Die Form der Übersendung kann in der Geschäftsordnung der Vertretung geregelt werden und schriftlich oder elektronisch (z. B. per E-Mail oder über ein Ratsinformationssystem) erfolgen. Die Verwaltung hat darauf zu achten, dass der Versand der Unterlagen in einer Form erfolgt, die vor der Einsicht oder dem Zugriff Dritter geschützt ist.

6. Was ist unter dem Begriff der Amtsverschwiegenheit zu verstehen?

Eine datenschutzrechtlich bedeutsame Regelung enthält § 32 Abs. 2 KVG LSA. Hiermit werden die in ein Ehrenamt oder zu einer sonstigen ehrenamtlichen Tätigkeit Berufene zur Amtsverschwiegenheit verpflichtet. Das bedeutet, dass sie niemandem Auskunft über Dinge erteilen dürfen, die sie im Rahmen ihrer Tätigkeit erfahren haben und die der Geheimhaltung unterliegen.

Sie sind verpflichtet personenbezogene Daten, zu denen Sie Zugang haben, nur zu dem Zweck zu verarbeiten, der für ihre Aufgabenerfüllung vorgesehen ist. Geben kommunale Mandatsträger z. B. personenbezogene Daten, die sie von der Verwaltung erhalten haben, an sogenannte Dritte (z. B. Bekannte, Partei, Presse etc.) weiter, so kann dies in Einzelfällen eine bußgeldbewährte Ordnungswidrigkeit (§ 32 DSAG LSA) bzw. in manchen Fällen sogar eine Straftat (§ 33 DSAG) darstellen. Die Verschwiegenheitspflicht gilt auch nach Beendigung der ehrenamtlichen Tätigkeit.

7. *Was passiert mit personenbezogenen Daten, wenn diese für die Mandatstätigkeit nicht mehr notwendig sind, weil der Vorgang abgeschlossen ist?*

Personenbezogene Daten sind zu löschen, wenn die Daten für den Zweck, zu dem sie verarbeitet wurden, nicht mehr erforderlich sind und Aufbewahrungsfristen nicht entgegenstehen (Art. 17 DS-GVO). Dies ist beispielsweise der Fall, sobald der Sitzungsgegenstand abschließend behandelt worden ist.

8. *Wie ist mit Sitzungsniederschriften zu verfahren?*

Vor der Veröffentlichung von Verlaufs- oder Ergebnisprotokollen über öffentliche Sitzungen ist darauf zu achten, dass diese keine personenbezogenen Daten von Einwohnern enthalten. Niederschriften nicht-öffentlicher Sitzungen sind nur denjenigen Mitgliedern der Vertretung zuzusenden, die an der Sitzung teilgenommen haben bzw. hätten teilnehmen dürfen.

9. *Dürfen Mandatsträger Sitzungsunterlagen an Dritte weitergeben?*

Nein, das ist nicht zulässig.

Grundsätzlich sind Mandatsträger dazu verpflichtet, alle Unterlagen, die personenbezogene Daten enthalten, vor dem Zugriff durch Dritte zu schützen. Sitzungsunterlagen sind ausschließlich für den Verwaltungsgebrauch bzw. für ihre Arbeit als Mitglied der Vertretung bestimmt.

Dies betrifft auch die Mitteilung über den Inhalt entsprechender Unterlagen. Als Dritte einzustufen sind beispielsweise Familienmitglieder, Beschäftigte des eigenen Betriebes, Kollegen außerhalb der Vertretung oder in Aufsichtsgremien, Vereinsmitglieder wie Sport- und Kulturvereine, Freundeskreise dieser Einrichtungen, Bekannte, Nachbarn sowie Mitglieder der eigenen Partei.

Endet das Mandat, so müssen alle verbliebenen Unterlagen an die Verwaltung zurückgegeben bzw. datenschutzgerecht vernichtet werden.

10. *Haben stellvertretende Ausschussmitglieder dieselben Rechte auf Information wie die ordentlichen Ausschussmitglieder?*

Im Verhinderungsfall übergibt das Ausschussmitglied die Sitzungsunterlagen üblicherweise an seine Vertreterin oder seinen Vertreter und erhält sie nach der Sitzung wieder zurück. Fällt ein Ausschussmitglied derartig kurzfristig aus, dass es die Sitzungsunterlagen persönlich nicht mehr rechtzeitig an seine Vertretung weitergeben kann, so kann sich diese die Unterlagen bei ihrer Fraktion besorgen. Der Fraktion steht immer ein kompletter Satz der jeweiligen Sitzungsunterlagen zur Verfügung.

Soweit in der Kommune ein Ratsinformationssystem verwendet wird, können den Vertretern im Vertretungsfall auch entsprechende Zugriffsrechte eingeräumt werden.

11. *Dürfen Daten von Mandatsträgern durch die Verwaltung bekannt gegeben werden?*

Beabsichtigt die Kommune die Veröffentlichung personenbezogener Daten von kommunalen Mandatsträgern, die über Vor- und Zuname hinausgehen, so bedarf es der vorherigen Einwilligung der betroffenen Mandatsträger. Das ist auch der Fall, wenn die Daten anlässlich der Kommunalwahl bereits öffentlich bekannt gemacht worden sind.

12. *Haben Mandatsträger die Möglichkeit, Auskunft über die über sie gespeicherten Daten bei der Verwaltung zu bekommen?*

Art. 15 DS-GVO regelt das Recht auf Auskunft über die personenbezogenen Daten der um Auskunft ersuchenden Person, die eine verantwortliche Stelle verarbeitet. Dieses Recht steht auch den Mandatsträgern gegenüber der Verwaltung zu. Die Daten verarbeitende Stelle muss ihnen auf Antrag Auskünfte erteilen über die zu ihrer Person gespeicherten Daten. Dieser Auskunftsanspruch ist ein wesentlicher Bestandteil ihres Rechts auf informationelle Selbstbestimmung.

13. *Kann Mandatsträgern die Auskunft verweigert werden?*

§ 11 DSAG LSA regelt für bestimmte Ausnahmetatbestände Beschränkungen des Rechts auf Auskunft. Die Auskunft kann demnach u.a. dann verweigert werden, wenn die Auskunftserteilung die öffentliche Sicherheit gefährden würde oder dem Wohl des Bundes bzw. der Länder Nachteile entstünden. Die Auskunft darf zudem verweigert werden, wenn die Auskunft dazu führen würde, dass ein Sachverhalt aufgedeckt würde, der nach einer Rechtsvorschrift oder wegen der Rechte und Freiheiten einer anderen Person geheim zu halten ist. Ein weiterer Hinderungsgrund der Auskunftserteilung besteht dann, wenn dies zur Verfolgung von Straftaten oder Ordnungswidrigkeiten erforderlich ist.

14. *Welche Informationen über Stellenbewerbungen dürfen Rats- bzw. Ausschussmitglieder im Rahmen eines Stellenbesetzungsverfahrens erhalten?*

Gemäß § 45 Abs. 5 Nr. 1 KVG LSA beschließt die Vertretung oder ein beschließender Ausschuss im Einvernehmen mit dem Hauptverwaltungsbeamten über die Ernennung, Einstellung, Versetzung in den Ruhestand und Entlassung mit Ausnahme der Entlassung innerhalb oder mit Ablauf der Probezeit von Beschäftigten der Kommune, soweit durch Hauptsatzung dem Hauptverwaltungsbeamten nicht die Entscheidung übertragen wurde oder diese zur laufenden Verwaltung gehört.

Im Rahmen des Auswahlverfahrens hat die Verwaltung die datenschutzrechtlichen Grundsätze der Erforderlichkeit und der Datensparsamkeit zu beachten. Das heißt, es dürfen nur die Daten aus den Bewerbungsunterlagen verarbeitet und an das für die Entscheidung zuständige Gremium weitergeleitet werden, die für die jeweilige Entscheidungsfindung erforderlich sind.

Maßgeblich hierfür ist dabei das in der Ausschreibung genannte Anforderungsprofil für den zu besetzenden Arbeitsplatz/Dienstposten unter Berücksichtigung der Kriterien der Bestenauslese (Art. 33 Abs. 2 des Grundgesetzes).

15. *Sind für die Änderung des Stellenplans personenbezogene Daten zu erheben?*

Eine Änderung des Stellenplans kommt grundsätzlich ohne die Erhebung personenbezogener Daten aus. Lediglich der Vollzug, also die konkrete Besetzung der Stelle, kann die Weitergabe von Personaldaten an das zuständige Gremium erforderlich machen.

16. *Darf ein Mandatsträger eine betriebsbezogene Aufstellung der Gewerbesteuerzahlungen aller Gewerbebetriebe in der Kommune erhalten, um mit der örtlichen Presse über die anstehende Neufestsetzung der Gewerbesteuerhebesätze diskutieren zu können?*

Nein, dies ist unzulässig.

Auch wenn es sich bei betriebsbezogenen Daten nicht immer um personenbezogene Daten handelt, sind diese Daten regelmäßig durch anderweitige Rechtsvorschriften geschützt. So ist in der Abgabenordnung (AO) das Steuergeheimnis besonders geschützt (§ 30 AO). Danach ist die Weitergabe der Daten im vorliegenden Fall u. a. nur dann möglich, wenn diese Daten für ein Verwaltungsverfahren benötigt werden. Allenfalls könnten anonymisierte Daten, wie z. B. Zahlen über das Gesamtaufkommen an Gewerbesteuer der vergangenen Jahre, weitergegeben werden (vgl. auch § 4 Abs. 2 Nr. 2 des Pressegesetzes des Landes Sachsen-Anhalt).

17. *Darf ein Mandatsträger eine Adressliste aller Sozialhilfeempfänger der Kommunen erhalten, um diese über eine geplante Initiative zum freien Eintritt für Sozialhilfeempfänger in alle kommunalen Einrichtungen zu informieren?*

Nein, dies ist nicht zulässig, da diese Daten dem Sozialgeheimnis gemäß § 35 SGB I i.V.m. §§ 67 ff. SGB X unterliegen. Die Daten dürfen nur mit vorheriger Einwilligung der betroffenen Personen weitergegeben werden, da sie nicht zu dem Zweck verwendet werden sollen, für den sie ursprünglich erhoben wurden (Grundsatz der Zweckbindung). Zudem ist auch kein gesetzlicher Grund für die Datenweitergabe gegeben (§ 35 des SGB I in Verbindung mit § 67b SGB X).

Das Ziel, die betroffenen Personen zu informieren, kann über die örtliche Presse, einen Informationsstand oder Flugblätter erreicht werden.

18. *Darf die Verwaltung anlässlich wiederholt aufgetretener Sachbeschädigungen an öffentlichen Gebäuden eine Videoüberwachungsanlage installieren?*

Öffentlich zugängliche Bereiche dürfen unter den Voraussetzungen des § 8 DSAG durch optisch-elektronische Einrichtungen (Videoüberwachung) beobachtet werden. Jedoch bevor die Überwachungstechnik eingesetzt wird, ist – neben einer eingehenden Prüfung der Geeignetheit und Erforderlichkeit sowie einer Abwägung mit möglichen widerstreitenden Interessen – eine Vielzahl von Formvorschriften zu beachten.

So muss z. B. vor dem Einsatz einer systematischen und umfangreichen Videoüberwachung regelmäßig eine sogenannte Datenschutz-Folgenabschätzung durchgeführt werden (Art. 35 Abs. 1 DS-GVO). Sofern Beschäftigte der öffentlichen Stelle von der Videobeobachtung betroffen sind, darf keine Verhaltens- und Leistungskontrolle stattfinden. Das gilt auch für das Betreten und das Verlassen des Grundstücks bei Dienstbeginn und -ende.

Weitere Hinweise zum Thema Videoüberwachung enthält das Kurzpapier Nr. 15 der unabhängigen Datenschutzbehörden des Bundes und der Länder, das unter folgendem Link abrufbar ist: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_15.pdf .

19. *Dürfen personenbezogene Daten im Rahmen von Bauleitverfahren veröffentlicht werden?*

Im Rahmen der Bauleitplanung können während der Beteiligung der Öffentlichkeit Stellungnahmen abgegeben werden. Diese werden bei der weiteren Beratung der Bebauungspläne von den zuständigen kommunalen Gremien in die Entscheidung miteinbezogen.

Viele Kommunen veröffentlichen die eingegangenen Stellungnahmen über ihre Webseite. Dabei ist jedoch zu berücksichtigen, dass weder die baurechtlichen Vorschriften noch die allgemeinen datenschutzrechtlichen Bestimmungen die Offenlegung von personenbezogenen Daten zulassen.

Vor diesem Hintergrund müssen die Kommunen sicherstellen, dass bei der Veröffentlichung der Stellungnahmen kein Personenbezug mehr vorhanden ist. Dies setzt voraus, dass sämtliche Daten, die Rückschlüsse auf eine bestimmte Person zulassen (z. B. Vorname, Name, Anschrift, Unterschrift) geschwärzt bzw. anonymisiert werden, bevor eingereichte Dokumente über die Webseite für die Allgemeinheit zugänglich gemacht werden.

20. *Darf sich ein Mandatsträger als Kandidat für die Kommunalwahl im Zuge des Kommunalwahlkampfes personenbezogene Daten der Erstwähler in der Kommune von der Verwaltung geben lassen?*

Gemäß § 50 Abs. 1 Bundesmeldegesetz (BMG) darf die Meldebehörde Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen im Zusammenhang mit Wahlen und Abstimmungen auf staatlicher und kommunaler Ebene in den sechs einer Wahl oder Abstimmung vorangehenden Monaten Auskunft aus dem Melderegister über die in § 44 Absatz 1 Satz 1 BMG bezeichneten Daten von Gruppen von Wahlberechtigten erteilen, soweit für deren Zusammensetzung das Lebensalter bestimmend ist. Die Geburtsdaten der Wahlberechtigten dürfen dabei nicht mitgeteilt werden. Die Person oder Stelle, der die Daten übermittelt werden, darf diese nur für die Werbung bei einer Wahl oder Abstimmung verwenden und hat sie spätestens einen Monat nach der Wahl oder Abstimmung zu löschen oder zu vernichten.

Hieraus folgt, dass eine Partei oder Wählergruppe oder ein einzelner Mandatsträger, sofern er Träger eines Wahlvorschlages ist (dies wäre der Fall, wenn er keiner Partei oder Wählergruppe angehört bzw. sein Handeln keiner Partei oder Wählergruppe zugeordnet werden kann), unter den zuvor genannten Voraussetzungen berechtigt ist bzw. sind, entsprechende Daten von der Meldebehörde anzufordern und zu Wahlwerbezwecken zu nutzen.

Sofern ein Mandatsträger einer Partei oder Wählergruppe angehört, bestehen datenschutzrechtlich keine Bedenken, wenn ihm die Partei oder Wählergruppe die von der Meldebehörde erhaltenen Daten der Personen übermittelt, die in seinem Wahlkreis wahlberechtigt sind.

Die nachfolgenden Daten dürfen gemäß § 44 Abs. 1 Satz 1 BMG von der Meldebehörde übermittelt werden:

- Familienname,

- Vornamen,
- Doktorgrad und die
- derzeitigen Anschriften.

Diese sogenannte „Melderegisterauskunft in besonderen Fällen“ bezieht sich auf klar umgrenzte Bevölkerungsgruppen eines bestimmten Lebensalters. Es ist also unzulässig, wenn ein Verzeichnis der Bürger „zwischen 16 und 100 Jahren“ angefordert wird. Damit bekäme man eine Aufstellung aller wahlberechtigten Einwohner der Kommune. Fordert man hingegen eine Liste aller Senioren über 60 Jahren an, so ist dies zulässig, da es sich um eine begrenzte Gruppe von Personen handelt.

Die betroffenen Personen haben gemäß § 50 Abs. 5 BMG das Recht, einer Übermittlung ihrer Daten an Parteien, Wählergruppen und andere Träger von Wahlvorschlägen zu widersprechen. Auf diese Möglichkeit ist bei der melderechtlichen Anmeldung und einmal jährlich durch öffentliche Bekanntmachung hinzuweisen. Diese Meldedaten werden dann nicht übermittelt.

Eine Partei oder Wählergruppe muss die Daten spätestens einen Monat nach der Wahl löschen oder an die Meldebehörde zurückgeben. Gleiches gilt für die Mandatsträger, wenn sie beispielsweise Daten von ihrer Partei erhalten haben.

21. Dürfen Mandatsträger außerhalb der Sechsmonatsfrist vor Wahlen mit Hilfe der sogenannten „Gruppenauskunft“ gemäß § 46 BMG Daten aus dem Melderegister erhalten?

Nein, dies ist nicht zulässig. Eine Gruppenauskunft darf nur erteilt werden, wenn sie im öffentlichen Interesse liegt. Unter öffentlichem Interesse ist vor allem das Interesse der Allgemeinheit zu verstehen, das über das Individualinteresse einzelner Personen oder Gruppen weit hinausgeht.

Deshalb sind Gruppenauskünfte außerhalb der „Wahlkampfzeit“ an Parteien und Wählergruppen in aller Regel unzulässig – umso mehr gilt dies für Auskünfte an Mandatsträger als Einzelperson.

22. Dürfen Meldedaten im Zusammenhang mit Alters- bzw. Ehejubiläen verarbeitet werden?

Verlangen Mandatsträger, Presse oder Rundfunk Auskunft aus dem Melderegister über Alters- oder Ehejubiläen von Einwohnern, darf die Meldebehörde gemäß § 50 Abs. 2 BMG Auskunft über die nachfolgenden Daten erteilen:

- Familienname,
- Vornamen,
- Doktorgrad,
- Anschrift sowie

- Datum und Art des Jubiläums.

Unter Altersjubiläen versteht man den 70. Geburtstag, jeden fünften weiteren Geburtstag sowie ab dem 100. Geburtstag jeden folgenden. Zu den Ehejubiläen zählen das 50. sowie jedes folgende.

Die betroffenen Personen haben gemäß § 50 Abs. 5 BMG das Recht, dieser Übermittlung zu widersprechen. Auf diese Möglichkeit ist bei der melderechtlichen Anmeldung und einmal jährlich durch öffentliche Bekanntmachung hinzuweisen.

23. Dürfen Mandatsträger auch weitergehende Informationen über einzelne Personen einholen?

Die sogenannte erweiterte Melderegisterauskunft gemäß § 45 Abs. 1 BMG ist nur an Personen zulässig, die ein berechtigtes Interesse glaubhaft machen können. Die Rechtsprechung hat ein berechtigtes Interesse definiert als „ein nach vernünftiger Abwägung durch die Sachlage gerechtfertigtes Interesse, das rechtlicher, wirtschaftlicher oder ideeller Natur sein kann und das von der Rechtsordnung anerkannt ist“. Ein berechtigtes Interesse ist also nahezu jedes Interesse außerhalb der reinen Neugier.

Wenn der Mandatsträger ein solches berechtigtes Interesse glaubhaft machen kann, darf die Meldebehörde zu einer bestimmten Person die nachfolgenden Daten mitteilen:

- frühere Namen,
- Geburtsdatum und Geburtsort sowie bei Geburt im Ausland auch den Staat,
- Familienstand, beschränkt auf die Angabe, ob verheiratet oder eine Lebenspartnerschaft führend oder nicht,
- derzeitige Staatsangehörigkeiten,
- frühere Anschriften,
- Einzugsdatum und Auszugsdatum,
- Familienname und Vornamen sowie Anschrift der gesetzlichen Vertreterin bzw. des gesetzlichen Vertreters,
- Familienname und Vornamen sowie Anschrift der Ehegattin bzw. des Ehegatten oder der Lebenspartnerin bzw. des Lebenspartners sowie
- Sterbedatum und Sterbeort sowie bei Versterben im Ausland auch den Staat.

Allerdings muss der Mandatsträger das berechtigte Interesse bezogen auf jedes einzelne der vorstehenden Daten glaubhaft machen, sonst darf ihm die Meldebehörde diese Auskunft nicht mitteilen. Die Meldebehörde hat die betroffene Person außerdem darüber zu informieren, dass sie dem Mandatsträger eine erweiterte Melderegisterauskunft erteilt hat.

24. *Wer kann Mandatsträgern bei Fragen zum Datenschutz helfen?*

Jede öffentliche Stelle und damit auch jede Kommune hat gemäß Art. 37 Abs. 1 Buchstabe a) DS-GVO einen Datenschutzbeauftragten (DSB) zu bestellen. Die Bestellung hat unabhängig von der Mitarbeiterzahl der öffentlichen Stelle zu erfolgen.

Es ist auch möglich, dass z. B. mehrere kleinere Gemeinden einen gemeinsamen DSB bestellen. Ebenso kann die Aufgabe des DSB auf einen externen Dienstleister übertragen werden. Dem DSB obliegen gemäß Art. 39 Abs. 1 DS-GVO u. a. folgende Aufgaben:

- Unterrichtung und Beratung des Verantwortlichen, seiner Auftragsverarbeiter sowie der mit der Verarbeitung personenbezogener Daten befassten Beschäftigten,
- Überwachung der Einhaltung der datenschutzrechtlichen Vorschriften,
- Zusammenarbeit mit der Datenschutzaufsichtsbehörde.

Eine weitere wichtige Aufgabe des DSB besteht darin, dass er auf der örtlichen Ebene als Ansprechpartner für Fragen des Datenschutzes zur Verfügung steht. Artikel 37 Abs. 7 DS-GVO sieht daher die Veröffentlichung der Kontaktdaten der bzw. des DSB vor. Einwohner, die sich durch die öffentliche Stelle in ihrem Recht auf informationelle Selbstbestimmung verletzt fühlen, können sich direkt an den DSB wenden. Dasselbe gilt für die Bediensteten der Behörde sowie für die Mitglieder der Vertretung.

25. *Dürfen Mandatsträger während einer Ratssitzung gefilmt werden?*

Grundsätzlich dürfen öffentliche Sitzungen der Vertretung per Video übertragen werden. Voraussetzung dafür ist, dass die Hauptsatzung der Kommune eine entsprechende Regelung enthält.

Allerdings haben Mandatsträger auch die Möglichkeit zu verlangen, dass ihre Redebeiträge nicht im Internet bzw. im Fernsehen übertragen werden (detailliertere Ausführungen unter *„III. Livestreaming von Ratssitzungen“*).

26. *Dürfen Mandatsträger Daten zur Ratsarbeit auf ihrem Handy oder Tablet verarbeiten?*

Grundsätzlich wird davon aus Gründen der Datensicherheit abgeraten. Erfahrungsgemäß sind nur wenige Nutzer mobiler Endgeräte selbst in der Lage, diese hinreichend sicher zu administrieren. Der Einsatz privater Endgeräte (sog. Bring Your Own Device, BYOD-Ansatz) sollte daher aus datenschutzrechtlicher Sicht nur erfolgen, wenn die privaten Endgeräte lediglich als Web-Endgerät genutzt werden und gewährleistet ist, dass die eigentliche Anwendung und Datenverarbeitung (Speicherung, Transformation, Nutzersteuerung durch Rechte-Rollen-Konzepte usw.) ausschließlich auf einem gesicherten Server der Kommune und nicht lokal auf dem mobilen Endgerät erfolgt. Die Nutzung des privaten Endgerätes würde somit lediglich in der reduzierten Funktion ähnlich einem Terminal für die Ein- und Ausgabe genutzt werden (detaillierte Ausführungen unter *„IV. Sicherer Einsatz technischer Geräte in der Gremienarbeit“*).

II. Rats- und Bürgerinformationssysteme

Tagesordnungen, Vorlagen und amtliche Niederschriften öffentlicher Sitzungen werden im Rahmen der gesetzlichen Vorgaben von den Kommunen veröffentlicht. Im Rahmen der Abwicklung des Sitzungsdienstes arbeiten viele Kommunen mit Rats- und Bürgerinformationssystemen. Die Ratsinformationssysteme sind geschlossene Systeme, auf welche nur die Mitglieder der Vertretung bzw. Ausschussmitglieder Zugriff haben. Ihre Nutzung ist daher aus datenschutzrechtlicher Sicht unproblematisch.

Die Bürgerinformationssysteme hingegen sind öffentliche Systeme, auf die jedermann online zugreifen kann. Die dort eingestellten Unterlagen dürfen deshalb keine personenbezogenen Daten enthalten. Erforderlichenfalls sind die Unterlagen zu anonymisieren.

III. Livestreaming von Ratssitzungen

Einige Kommunen möchten öffentliche Sitzungen im Internet über ihre Webseite (z. B. Live-Streaming) oder auf regionalen TV-Sendern übertragen lassen. Im Zuge dieser Übertragungen werden personenbezogene Daten verarbeitet. In Sachsen-Anhalt findet sich die Rechtsgrundlage für die Übertragung von Bild- und Tonaufnahmen der Sitzung der Vertretung in § 52 Abs. 5 S. 1 KVG LSA. Demnach sind Bild- und Tonaufnahmen von Mitgliedern der Vertretung mit dem Ziel der Berichterstattung zulässig, wenn die Geschäftsordnung der Kommune eine entsprechende Regelung enthält.

Aus datenschutzrechtlicher Sicht ist insbesondere zu beachten, dass keine Aufnahmen von Personen gemacht werden, die nicht Mitglieder der Vertretung sind, also zum Beispiel von Zuschauern der Ratssitzungen. Von diesen Personen ist vor Beginn der Bild- und/oder Tonaufnahmen eine Einwilligung einzuholen. Auch die Mandatsträger haben die Möglichkeit zu verlangen, dass ihre Redebeiträge nicht im Internet bzw. im Fernsehen übertragen werden.

VI. Sicherer Einsatz Technischer Geräte in der Gremienarbeit

Personenbezogene Daten müssen u. a. nach den Grundsätzen des Art. 5 Abs. 1 lit. f) sowie nach Art. 24, 25 und 32 DS-GVO in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet. Die Gewährleistung von Datensicherheit ist ein zentrales Prinzip des Datenschutzes und umfasst die Summe aller **T**echnischen und **O**rganisatorischen Sicherungs**M**aßnahmen (TOM), die erforderlich sind, um eine den Datenschutznormen entsprechende Datenverarbeitung sicher zu stellen und damit die Rechte und Freiheiten natürlicher Personen angemessen zu schützen. Es gilt, unbefugter oder unrechtmäßiger Verarbeitung und unbeabsichtigtem Verlust sowie unbeabsichtigter Zerstörung oder Schädigung vorzubeugen.

Kommen in der kommunalen Gremienarbeit technische Geräte zur Verarbeitung personenbezogener Daten zum Einsatz, sind demnach die erforderlichen angemessenen TOM zur Datensicherheit zu treffen. Dies ist Aufgabe des Verantwortlichen (und ggf. eines Auftragsverarbeiters), nicht die des Herstellers der Geräte, Systeme und Anwendungsprogramme. Die TOM trifft der Verantwortliche sowohl, wenn er die Mittel für die Verarbeitung festlegt als auch zum Zeitpunkt der eigentlichen Verarbeitung (Datenschutz durch Technikgestaltung, Art. 25 Abs. 1 DS-GVO). Zudem trifft er geeignete TOM, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten verarbeitet werden, die für den jeweiligen Verarbeitungszweck erforderlich sind (Datenschutz durch datenschutzfreundliche Voreinstellungen, Art. 25 Abs. 2 DS-GVO).

Bei der Auswahl der TOM ist zu beachten, dass dies unter Berücksichtigung des Risikos, also der Eintrittswahrscheinlichkeit und Schadenshöhe für die Rechte und Freiheiten natürlicher Personen, des Standes der Technik und der Implementierungskosten sowie der Art, Umstände und des Zwecks der Datenverarbeitung geschieht. Die Maßnahmen müssen wirksam und je nach den Abwägungsergebnissen angemessen sein. Dieser Schritt dient dazu, sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß den datenschutzrechtlichen Bestimmungen erfolgt. Schließlich müssen nach der Bestimmung der Maßnahmen das Restrisiko bewertet und die Maßnahmen ggf. konsolidiert werden.

Stellt die Verwaltung den Mandatsträgern die für ihre Tätigkeit benötigten vertraulichen Daten optimalerweise über ein Ratsinformationssystem zur Verfügung, trägt sie dementsprechend die Verantwortung für dessen datenschutzgerechte Ausgestaltung.

Soweit mobile Endgeräte (z. B. Notebooks, Tablets oder Smartphones) für die Gremienarbeit zum Einsatz kommen, birgt dies je nach Netzanbindung, Betriebssystem und Anwendungsumgebung zusätzliche spezifische Gefährdungs-aspekte wie z. B. zusätzliche Sicherheitslücken oder technische Schwachstellen. Beim Einsatz dienstlicher Geräte müssen diese ebenso hinsichtlich ihrer Risikopotenziale bewertet werden, um die angemessenen wirksamen TOM festzulegen und umzusetzen.

Einen wertvollen grundlegenden Beitrag zur Datensicherheit können Kommunen leisten, indem sie den Mandatsträgern sichere und datenschutzkonform ausgestaltete Systeme zur Verfügung

stellen, die mittels einer zentral administrierten und gemanagten Einbindung der Geräte unter IT-fachlicher Kontrolle stehen. Die Bereitstellung und Administration der mobilen Endgeräte obliegen damit der Kommune. Zusätzlich ist eine Informationssicherheitsrichtlinie einschließlich der Datenschutzmaßnahmen und ein Datenschutzkonzept zur Durchsetzung der TOM erforderlich, die jeweils wegen der technischen Weiterentwicklung zyklisch fortzuschreiben sind.

Bedingt durch die Vielfalt möglicher Betriebssysteme, die Notwendigkeit des Vorhaltens und der aktuellen Konfiguration komplexerer Sicherheitsanwendungen (Firewall, Virenschutz, Verschlüsselung etc.) sowie ständig wechselnder und weiterentwickelter Angriffsszenarien auf Soft- und Hardwareschwachstellen sind der Erfahrung nach nur wenige Nutzer mobiler Endgeräte selbst in der Lage, diese hinreichend sicher zu administrieren.

Der Einsatz privater Endgeräte (sog. Bring Your Own Device, BYOD-Ansatz) sollte daher aus datenschutzrechtlicher Sicht nur erfolgen, wenn die privaten Endgeräte lediglich als Web-Endgerät genutzt werden und gewährleistet ist, dass die eigentliche Anwendung und Datenverarbeitung (Speicherung, Transformation, Nutzersteuerung durch Rechte-Rollen-Konzepte usw.) ausschließlich auf einem gesicherten Server der Kommune (oder auf dem Server eines Auftragsverarbeiters i. S. v. Art. 4 Nr. 8 DS-GVO) und nicht lokal auf dem mobilen Endgerät erfolgt. Die Nutzung des privaten Endgerätes würde somit lediglich in der reduzierten Funktion ähnlich einem Terminal für die Ein- und Ausgabe genutzt werden.

Soweit kommunale Mandatsträger für ihre Gremienarbeit vertrauliche Daten auf einem privaten Endgerät verarbeiten, geht die Verantwortung für deren Sicherheit und Integrität auf die jeweiligen Mandatsträger über. Sie sind dann selbst in der Pflicht, die erforderlichen Maßnahmen zur Datensicherheit zu treffen. Dies ist jedoch angesichts der genannten Risikopotenziale ausdrücklich nicht empfehlenswert.

V. Weiterführende Links

Zum Thema Datenschutz gibt es im Internet zahlreiche Websites mit unzähligen Informationen. Nachfolgend sei daher lediglich eine kleine Auswahl genannt:

- Auf unserer Internetseite www.kommunales-sachsen-anhalt.de stehen unter *SGSA / Mitgliederservice / Themengebiete / Allgemeine Verwaltung / Datenschutz* neben den Handreichungen „Datenschutz in Kommunalverwaltungen“, „Datenschutz für kommunale Mandatsträger“ und „Anfertigung und Veröffentlichung von Personenfotografien im öffentlichen Bereich“ weitere Informationen zum Datenschutz zum Download bereit.

- Auf der Internetseite stellt der Landesbeauftragte für den Datenschutz Sachsen-Anhalt https://datenschutz.sachsen-anhalt.de/landesbeauftragter/ stehen in der Rubrik *Recht* die landes- und bundesrechtlichen und internationale Vorschriften sowie Grundsatzurteile und weitere Rechtsprechung zum Datenschutz sowie in der Rubrik *Informationen* zahlreiche Informationsmaterialien zur Verfügung.

- Auf der Internetseite des Bundesbeauftragten für den Datenschutz und die Informationssicherheit https://www.bfdi.bund.de sind in der Rubrik *Bürgerinnen und Bürger* unter *Allgemeine Verwaltung* vielfältige Materialien eingestellt.

- Unter https://www.datenschutzkonferenz-online.de/, dem Webauftritt der Datenschutzkonferenz (DSK), dem Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder, steht in der Infothek umfangreiches Informationsmaterial wie Kurzpapiere, Orientierungshilfen oder Anwendungshinweise zum Download bereit.