

## FAQ Kommunalen Datenschutz 2.0

(Stand Januar 2024)

Die niedersächsischen Kommunen erbringen als lokale Verwaltungseinheiten vor Ort eine Vielzahl von Verwaltungsleistungen für die Bürgerinnen und Bürger, was mit der Verarbeitung unterschiedlichster personenbezogener Daten einhergeht. Dabei stellen sich in der täglichen Praxis häufig Fragen, die einen datenschutzrechtlichen Bezug aufweisen. Zu den Aufgaben des Landesbeauftragten für den Datenschutz Niedersachsen zählt auch die Beratung in datenschutzrechtlichen Belangen. Die nachfolgenden FAQ geben die Antworten auf häufig gestellte Fragen zum Datenschutz im Alltag der kommunalen Praxis und sollen den niedersächsischen Kommunen Unterstützung bieten.

### Inhalt

I. Allgemeines.....	3
1. Welche Vorschriften sind anzuwenden? .....	3
2. Müssen Kommunen eine/n Datenschutzbeauftragte/n bestellen?.....	3
3. Welche Aufgaben hat eine/ein Datenschutzbeauftragte/r (DSB)?.....	3
4. Wer trägt die Verantwortung für die Verarbeitung von personenbezogenen Daten in der Kommune? .....	4
5. Was sind personenbezogene Daten?.....	4
6. Welche personenbezogenen Daten verarbeitet eine Kommune?.....	4
7. Was sind besondere Kategorien personenbezogener Daten?.....	4
8. Was versteht man unter Datenverarbeitung? .....	4
9. Wann ist die Verarbeitung von personenbezogenen Daten erlaubt? .....	4
10. Wann kann eine Datenverarbeitung auf eine Einwilligung gestützt werden?.....	5
11. Muss eine Einwilligung schriftlich erteilt werden?.....	6
12. Was ist das Verzeichnis von Verarbeitungstätigkeiten? .....	6
13. Was muss in dieses Verzeichnis aufgenommen werden?.....	6
14. Was ist eine Datenschutz-Folgenabschätzung (DSFA)? .....	7
15. Wann ist eine DSFA durchzuführen?.....	7
16. Was ist eine Auftragsverarbeitung? .....	7
II. Betroffenenrechte .....	8
1. Welche Informationspflichten hat die Kommune gegenüber den betroffenen Personen? .....	8
2. Welche Speicher- und Löschrufen gelten für personenbezogene Daten in Kommunen? .....	8
3. Was ist bei einer Auskunft nach Artikel 15 DSGVO zu beachten? .....	8
III. Datenschutz in der Ratsarbeit .....	9
1. Was ist beim Einsatz von Rats- bzw. Bürgerinformationssystemen zu beachten?.....	9
2. Dürfen Kommunen ein „Livestreaming“ von Ratssitzungen durchführen?.....	9
3. Wird die Verarbeitung personenbezogener Daten durch ein Ratsmitglied stets der Kommune zugerechnet?.....	10



IV. Datenschutz für den sozialpsychiatrischen Dienst.....	10
1. Wo ist die Datenverarbeitung für den sozialpsychiatrischen Dienst geregelt? .....	10
2. Dürfen die Abgeordneten der kommunalen Vertretung in die Behandlungsakten des sozialpsychiatrischen Dienstes Einsicht nehmen? .....	10
3. Darf die Hauptverwaltungsbeamtin bzw. der Hauptverwaltungsbeamte Einsicht in die Behandlungsakten des sozialpsychiatrischen Dienstes Einsicht nehmen? .....	10
V. Datenschutz im Arbeitsalltag .....	11
1. E-Mail-Versand an mehrere Personen .....	11
2. Veröffentlichungen von Dokumenten.....	11
3. Was ist bei der Gewährung von Akteneinsicht zu beachten? .....	11

## I. Allgemeines

### 1. Welche Vorschriften sind anzuwenden?

Für die Verarbeitung personenbezogener Daten durch Kommunen finden neben den allgemeinen Bestimmungen der Datenschutz-Grundverordnung (DSGVO) vor allem das Niedersächsische Datenschutzgesetz (NDSG) sowie spezialgesetzliche Regelungen, die sich im jeweiligen Fachrecht befinden, Anwendung. Es gilt das sogenannte Verbot mit Erlaubnisvorbehalt. Die Verarbeitung personenbezogener Daten ist demnach nur zulässig, wenn das NDSG oder eine andere Rechtsvorschrift dies ausdrücklich vorsieht (vgl. Frage 9). Ausnahmeweise kann die Verarbeitung auf die Einwilligung der betroffenen Person gestützt werden (vgl. Frage 10).

### 2. Müssen Kommunen eine/n Datenschutzbeauftragte/n bestellen?

Ja, dieses Erfordernis ergibt sich aus Artikel 37 Absatz 1 Buchstabe a) DSGVO.

Beachten Sie, dass die Kontaktdaten der/des Datenschutzbeauftragten veröffentlicht werden müssen und eine Mitteilung an den Landesbeauftragten für den Datenschutz Niedersachsen erfolgen muss, Artikel 37 Absatz 7 DSGVO. Der Landesbeauftragte für den Datenschutz bietet hierfür einen Online-Service an. Das Meldeportal ist unter folgender Adresse erreichbar: [nds.dsb-meldung.de](https://nds.dsb-meldung.de).

Sofern vorhanden, kann die Veröffentlichung auf der Homepage der Kommune mittels Nutzung einer Funktionsadresse wie z.B. [Datenschutz@musterschule.de](mailto:Datenschutz@musterschule.de) erfolgen.

### 3. Welche Aufgaben hat eine/ein Datenschutzbeauftragte/r (DSB)?

Jede öffentliche Stelle und damit auch jede Kommune hat gemäß Artikel 37 Absatz 1 Buchstabe a) DSGVO eine bzw. einen 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 eine gemeinsame bzw. einen gemeinsamen DSB bestellen. Ebenso kann die Aufgabe der bzw. des DSB auf einen externen Dienstleister übertragen werden. Den DSB obliegen gemäß Artikel 39 Absatz 1 DSGVO u. a. folgende Aufgaben:

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

Eine weitere wichtige Aufgabe der DSB besteht darin, dass sie auf der örtlichen Ebene als Ansprechpartnerin bzw. Ansprechpartner für Fragen des Datenschutzes zur Verfügung stehen. Artikel 37 Absatz 7 DSGVO sieht daher die Veröffentlichung der Kontaktdaten der bzw. des DSB vor. Bürgerinnen und Bürger, die sich durch die öffentliche Stelle in ihrem Recht

auf informationelle Selbstbestimmung verletzt fühlen, können sich direkt an die bzw. den DSB wenden. Dasselbe gilt für die Bediensteten der Behörde sowie für Ratsmitglieder.

#### 4. Wer trägt die Verantwortung für die Verarbeitung von personenbezogenen Daten in der Kommune?

Die Hauptverwaltungsbeamtin bzw. der Hauptverwaltungsbeamte ist für die Einhaltung der Vorschriften bezüglich der Verarbeitung personenbezogener Daten innerhalb der Kommune verantwortlich.

#### 5. Was sind personenbezogene Daten?

Gemäß Artikel 4 Nummer 1 DSGVO sind dies alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (sogenannte „betroffene Person“) beziehen. Solange ein Rückschluss auf eine Person möglich ist, gelten Daten als personenbezogene Daten.

#### 6. Welche personenbezogenen Daten verarbeitet eine Kommune?

Die Kommune verarbeitet vornehmlich personenbezogene Daten von Einwohnerinnen und Einwohnern sowie von eigenen Beschäftigten.

#### 7. Was sind besondere Kategorien personenbezogener Daten?

Besondere Kategorien personenbezogener Daten werden auch als sensible Daten bezeichnet. Dabei handelt es sich um Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgeht sowie genetische oder biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person (vgl. Artikel 9 Absatz 1 DSGVO). Diese personenbezogenen Daten unterliegen einem grundsätzlichen Verarbeitungsverbot und dürfen nur unter besonderen Voraussetzungen verarbeitet werden (vgl. Artikel 9 Absatz 2 DSGVO).

#### 8. Was versteht man unter Datenverarbeitung?

Nach Artikel 4 Nummer 2 DSGVO ist Datenverarbeitung das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung, der Abgleich, die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung personenbezogener Daten (Zum Begriff der Verarbeitungstätigkeit siehe Frage 13).

#### 9. Wann ist die Verarbeitung von personenbezogenen Daten erlaubt?

Eine Verarbeitung von personenbezogenen Daten ist nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten ausnahmsweise eingewilligt hat.

Die nachfolgende Übersicht listet Rechtsgrundlagen auf, die in den jeweiligen Bereichen am häufigsten zur Anwendung kommen. Sie ist nicht abschließend.

- **Ausländerrecht:** §§ 86 ff. Aufenthaltsgesetz, §§ 61a – 76a Aufenthaltsverordnung (insbesondere §§ 63, 67 AufenthV)
- **Asylrecht:** §§ 7, 8 Asylgesetz
- **Beschäftigtendatenschutz:** § 88 Nds. Beamtengesetz und § 12 NDSG
- **Gewerberecht:** § 11 Gewerbeordnung
- **Melderecht:** §§ 3, 24, 33 - 52 Bundesmeldegesetz
- **Öffentliches Gesundheitswesen:** §§ 12, 16, 20, 23a, 25, 27, 28a, 30 Infektionsschutzgesetz
- **Passrecht:** §§ 16 - 18 Paßgesetz (PaßG), §§ 22-22a PaßG
- **Personalausweisrecht:** §§ 14-20 Personalausweisgesetz (PAuswG) sowie §§ 23-26 PAuswG
- **Personenstandsrecht:** §§ 5, 15, 21, 31 Personenstandsgesetz
- **Sozialrecht:** Grundlegende Regelungen finden sich in § 35 Sozialgesetzbuch I (SGB) sowie §§ 67 ff. SGB X – in den übrigen SGB finden sich weitergehende Regelungen, die berücksichtigt werden müssen, so zum Beispiel für den Bereich Kinder- und Jugendhilfe in §§ 61 ff. SGB VIII.
- **Wahlrecht:** § 11 Niedersächsisches Kommunalwahlgesetz

## 10. Wann kann eine Datenverarbeitung auf eine Einwilligung gestützt werden?

Grundsätzlich stützt sich die Verarbeitung personenbezogener Daten durch öffentliche Stellen auf gesetzliche Rechtsgrundlagen. Die Verarbeitung personenbezogener Daten auf Einwilligungsbasis ist die Ausnahme und ist nur in besonderen Konstellationen möglich.

Artikel 7 und 8 DSGVO enthalten Bedingungen für die Einwilligung. Sie muss informiert erfolgen, d.h. der betroffenen Person muss bekannt sein, zu welchem Zweck sie erteilt wird und wozu die Daten genutzt werden.

Des Weiteren muss ein Hinweis auf die Widerrufsmöglichkeit für die Zukunft enthalten sein und die Einwilligung muss freiwillig erfolgen. Die Freiwilligkeit setzt voraus, dass die betroffenen Personen die Einwilligung verweigern können, ohne Nachteile zu erleiden (vgl. Erwägungsgrund 42 und Artikel 7 Absatz 4 DSGVO). Um die Freiwilligkeit zu gewährleisten, können der betroffenen Person Alternativen angeboten werden. Da die Kommune bei der Verarbeitung personenbezogener Daten regelmäßig in einem sogenannten Über-

/Unterordnungsverhältnis zu der betroffenen Bürgerin bzw. dem betroffenen Bürger steht, muss anhand aller Umstände geprüft werden, ob die Einwilligung freiwillig erteilt wurde (vgl. Erwägungsgrund 43 zur DSGVO).

Eine wirksame Einwilligung stellt zum Beispiel die Einwilligung in die Anfertigung von Fotografien im Rahmen der Öffentlichkeitsarbeit der Kommune oder im Zusammenhang kommunaler Feste, Ehrungen oder Preisverleihungen dar.

### 11. Muss eine Einwilligung schriftlich erteilt werden?

Die Kommune muss im Zweifel nachweisen können, dass die betroffene Person in die Verarbeitung eingewilligt hat (Artikel 7 Absatz 1 DSGVO). Daher ist es ratsam, Einwilligungen nur schriftlich einzuholen. Im Falle der Verarbeitung besonderer Kategorien personenbezogener Daten auf Einwilligungsbasis setzt Artikel 9 Absatz 2 Buchstabe a) DSGVO eine ausdrückliche Einwilligung voraus. Zur Erfüllung der Rechenschaftspflichten (Artikel 5 Absatz 2 DSGVO) und zur Nachweisführung, dass eine Einwilligung vorgelegen hat, sollte diese schriftlich eingeholt werden.

### 12. Was ist das Verzeichnis von Verarbeitungstätigkeiten?

Das Verzeichnis von Verarbeitungstätigkeiten (VVT) dient als wesentliche Grundlage für eine strukturierte Datenschutzdokumentation und hilft dem Verantwortlichen dabei, gemäß Artikel 5 Absatz 2 DSGVO nachzuweisen, dass die Vorgaben aus der DSGVO eingehalten werden (Rechenschaftspflicht). Im VVT müssen alle Verarbeitungstätigkeiten beschrieben werden, die in der Kommune durchgeführt werden. Die Inhalte des VVT sind gesetzlich vorgeschrieben und finden sich in Artikel 30 DSGVO.

### 13. Was muss in dieses Verzeichnis aufgenommen werden?

Jede Verarbeitungstätigkeit muss sich im Verzeichnis von Verarbeitungstätigkeiten wiederfinden. Der Begriff der Verarbeitungstätigkeit orientiert sich an dem der Datenverarbeitung des Artikel 4 Nummer 2 DSGVO. Er ist aber nicht zwingend mit ihm gleichzusetzen. Einzelne Datenverarbeitungsvorgänge können zu einer Gruppe oder einzelnen Phasen zusammengefasst werden. Dabei sind bezüglich jeder Verarbeitungstätigkeit der Name und die Kontaktdaten des Verantwortlichen sowie des Datenschutzbeauftragten, der Zweck der Verarbeitung, eine Beschreibung der Kategorien der betroffenen Personen, der verarbeiteten personenbezogenen Daten, etwaiger Empfänger der personenbezogenen Daten im Falle einer Übermittlung, etwaige Drittlandübermittlungen, Löschrufen sowie eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 DSGVO aufzuführen.

Im Rahmen der durchgeführten Kommunalprüfung ist deutlich geworden, dass auch kleinere Kommunen mindestens 50 Verarbeitungstätigkeiten wahrnehmen.

## 14. Was ist eine Datenschutz-Folgenabschätzung (DSFA)?

Die DSFA (Artikel 35 DSGVO) dient der Bewertung von Risiken, die durch die Verarbeitung personenbezogener Daten entstehen und zu einer Rechtsverletzung der betroffenen Personen führen können. Sie befasst sich insbesondere mit Abhilfemaßnahmen, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Verordnung nachgewiesen werden kann (Artikel 35 Absätze 1 und 7 DSGVO).

## 15. Wann ist eine DSFA durchzuführen?

Die DSFA ist durchzuführen, wenn die Form der Verarbeitung auf Grund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

Eine Auflistung mit Verarbeitungstätigkeiten, für die in jedem Fall eine DSFA durchzuführen ist, finden Sie hier:

[https://lfd.niedersachsen.de/startseite/datenschutzreform/ds\\_gvo/liste\\_von\\_verarbeitungsvorgaengen\\_nach\\_art\\_35\\_abs\\_4\\_ds\\_gvo/muss-listen-zur-datenschutz-folgenabschätzung-179663.html](https://lfd.niedersachsen.de/startseite/datenschutzreform/ds_gvo/liste_von_verarbeitungsvorgaengen_nach_art_35_abs_4_ds_gvo/muss-listen-zur-datenschutz-folgenabschätzung-179663.html)

## 16. Was ist eine Auftragsverarbeitung?

Eine datenverarbeitende öffentliche Stelle (hier: die Kommune) beauftragt einen Dritten (Auftragsverarbeiter - AV) personenbezogene Daten für sie weisungsgebunden zu verarbeiten (vgl. Artikel 28 DSGVO). Der AV wird nur als „verlängerter Arm“ der Kommune tätig. In diesem Fall bedarf es für die Übermittlung personenbezogener Daten von der Kommune an den AV keiner Rechtsgrundlage. Hat der AV einen eigenen Entscheidungsspielraum bzgl. des „Ob“ oder „Wie“ der Datenverarbeitung, liegt keine Auftragsverarbeitung vor. Insbesondere, wenn der AV personenbezogene Daten zu eigenen Zwecken verarbeitet, sind die Grenzen von Artikel 28 DSGVO überschritten.

Ein Beispiel für eine Auftragsverarbeitung ist die Auslagerung der eigenen Datenhaltung auf Servern einer anderen Stelle.

Eine Auftragsverarbeitung setzt zudem einen schriftlichen Vertrag zwischen der Kommune und dem AV voraus. Die Mindestinhalte dieses Vertrags sind in Artikel 28 Absatz 3 DSGVO aufgeführt.

Eine Formulierungshilfe für einen Auftragsvertragsvertrag sowie weitere Hinweise finden Sie hier:

[https://lfd.niedersachsen.de/startseite/themen/auftragsverarbeitung\\_nach\\_art\\_28\\_ds\\_gvo/auftragsverarbeitung-nach-art-28-ds-gvo-179673.html](https://lfd.niedersachsen.de/startseite/themen/auftragsverarbeitung_nach_art_28_ds_gvo/auftragsverarbeitung-nach-art-28-ds-gvo-179673.html)

## II. Betroffenenrechte

### 1. Welche Informationspflichten hat die Kommune gegenüber den betroffenen Personen?

Der Grundsatz der Transparenz bei der Verarbeitung personenbezogener Daten in Artikel 5 Absatz 1 Buchstabe a) DSGVO wird durch eine ganze Reihe von Informationspflichten des Verantwortlichen gegenüber der betroffenen Person konkretisiert.

Die zentralen Informationspflichten in den Artikeln 13 und 14 DSGVO enthalten jeweils einen Katalog mit Pflichtinhalten für die Information je nach Art der Datenverarbeitung. Artikel 12 DSGVO enthält außerdem allgemeine Anforderungen an die Zugänglichkeit und Verständlichkeit der Information.

Die wichtigsten weiteren Informationspflichten sind:

- Information über Widerrufsrecht bei der Einwilligung (Artikel 7 Absatz 3 DSGVO),
- Informationspflicht bei Erhebung der Daten bei der betroffenen Person (Artikel 13 Absatz 1 DSGVO),
- Informationspflicht, wenn die Daten nicht bei der betroffenen Person erhoben werden (Artikel 14 Absatz 1 DSGVO),
- Informationspflicht bei Zweckänderung (Artikel 13 Absatz 3 DSGVO und Artikel 14 Absatz 4 DSGVO),
- Benachrichtigungspflicht bei Datenschutzverletzungen (Artikel 34 DSGVO),
- Veröffentlichung der Kontaktdaten des Datenschutzbeauftragten (Artikel 37 DSGVO).

### 2. Welche Speicher- und Löschfristen gelten für personenbezogene Daten in Kommunen?

Artikel 17 DSGVO regelt das Recht der betroffenen Person auf Löschung ihrer personenbezogenen Daten, wenn einer der dort genannten Gründe des Artikel 17 Absatz 1 DSGVO vorliegt (Beispiel: Die Daten sind für den Zweck, zu dem sie verarbeitet wurden, nicht mehr erforderlich.). Allerdings sind bestehende gesetzliche Aufbewahrungsfristen zu berücksichtigen.

### 3. Was ist bei einer Auskunft nach Artikel 15 DSGVO zu beachten?

Die von der Verarbeitung personenbezogener Daten betroffene Person hat nach Artikel 15 DSGVO ein umfangreiches Recht auf Auskunft. Dies umfasst auch eine Bestätigung, dass keine personenbezogenen Daten verarbeitet werden. Einer Begründung bedarf das Auskunftersuchen nicht.

In der Praxis werden häufig von Verantwortlichen standardmäßig Nachweise zur Identität der um Auskunft bittenden Person angefordert. Dies ist nur zulässig, wenn Zweifel an der Identität bestehen. In diesem Fall dürfen weitergehende Angaben, die eine Zuordnung ermöglichen, erfragt werden. Hierbei ist zu beachten, dass nur erforderliche zusätzliche Daten erfragt werden. Sofern sich aus den gespeicherten Unterlagen bereits die auf dem Ersuchen genannte Adresse ergibt und die Auskunft an diese gesandt werden soll, ist eine Beantwortung

möglich. Die Kommune muss in der Lage sein, die Zweifel an der Identität der Antragstellerin oder des Antragstellers mitteilen zu können.

Der Umfang der zu erteilenden Auskunft ergibt sich grundsätzlich aus Artikel 15 Absatz 1 DSGVO und ist konkret auf die zu der betreffenden Person verarbeiteten Daten zu beziehen. Es ist nicht ausreichend, in der Auskunft mitzuteilen, dass Adressdaten gespeichert und an andere öffentliche Stellen übermittelt werden. Vielmehr sind die konkreten personenbezogenen Daten (Erika Mustermann, Musterstraße 1, 12345 Musterort) und deren Empfänger (Stadtverwaltung xy) anzugeben. Die auskunftersuchende Person muss die Möglichkeit haben zu prüfen, ob die gespeicherten Daten inhaltlich richtig sind und welche Stelle diese erhalten hat.

Des Weiteren können die Betroffenen eine Kopie der verarbeiteten personenbezogenen Daten (Artikel 15 Absatz 3 DSGVO) beantragen. Die erste Kopie ist kostenfrei zur Verfügung zu stellen (Artikel 15 Absatz 3 DSGVO).

Die für eine Antwort einzuhaltende Monatsfrist ergibt sich aus Artikel 12 Absatz 3 DSGVO.

### III. Datenschutz in der Ratsarbeit

#### 1. Was ist beim Einsatz von Rats- bzw. Bürgerinformationssystemen zu beachten?

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 Rats- 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. Werden hierzu Schwärzungen mit Softwareprodukten vorgenommen, ist sicherzustellen, dass diese beim Aufruf des Dokumentes nicht rückgängig gemacht werden können.

#### 2. Dürfen Kommunen ein „Livestreaming“ von Ratssitzungen durchführen?

Einige Kommunen möchten öffentliche Sitzungen im Internet über ihre Homepage (z.B. Live-Streaming) oder auf örtlichen TV-Sendern übertragen lassen. Im Zuge dieser Übertragungen werden personenbezogene Daten verarbeitet. In Niedersachsen findet sich die Rechtsgrundlage für die Übertragung von Bild- und Tonaufnahmen der Sitzung der Vertretung in § 64 Absatz 2 Satz 2 Niedersächsisches Kommunalverfassungsgesetz (NKomVG). Demnach sind Bild- und Tonaufnahmen von Mitgliedern der Vertretung mit dem Ziel der Berichterstattung zulässig, wenn die Hauptsatzung 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 Zuschauerinnen und Zuschauern der Ratssitzungen. Von diesen Personen muss immer vor Beginn der Bild- und/oder Tonaufnahmen eine Einwilligung eingeholt werden. Doch auch die Mandatsträgerinnen und Mandatsträger haben die Möglichkeit zu verlangen, dass

ihre Redebeiträge nicht zum Zwecke der Berichterstattung aufgenommen oder im Internet bzw. im Fernsehen übertragen werden (§ 64 Absatz 2 Satz 3 NKomVG).

Zu beachten ist, dass beim Einsatz von Videokonferenztechnik zum Zwecke der Teilnahme an Sitzungen (§ 64 Absätze 3 bis 5 NKomVG) die Übertragung von Bild und Ton in den Sitzungssaal zulässig ist. Hingegen kann dem darüberhinausgehenden Livestreaming widersprochen werden (§ 64 Abs. 4 in Verbindung mit § 64 Absatz 2 Satz 3 NKomVG).

### 3. Wird die Verarbeitung personenbezogener Daten durch ein Ratsmitglied stets der Kommune zugerechnet?

Sofern ein Ratsmitglied personenbezogene Daten im Rahmen der Ratstätigkeit verarbeitet, wird dies dem Rat und somit der Kommune zugerechnet.

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

## IV. Datenschutz für den sozialpsychiatrischen Dienst

### 1. Wo ist die Datenverarbeitung für den sozialpsychiatrischen Dienst geregelt?

In Niedersachsen ist die Arbeit des sozialpsychiatrischen Dienstes im Niedersächsischen Gesetz über die Hilfen und Schutzmaßnahmen für psychisch Kranke (NPsychKG) geregelt. Das Gesetz enthält auch Regelungen zum Datenschutz (§§ 32 bis 36 NPsychKG). Es wird im Gesetz zwischen der Verarbeitung von „normalen“ personenbezogenen Daten (§ 32 NPsychKG) und besonders schutzwürdigen Daten (§ 33 NPsychKG) unterschieden.

### 2. Dürfen die Abgeordneten der kommunalen Vertretung in die Behandlungsakten des sozialpsychiatrischen Dienstes Einsicht nehmen?

Nein. Anträgen auf Einsicht in die Behandlungsakten nach dem NKomVG steht die ärztliche Schweigepflicht entgegen. Diese schützt das besondere Vertrauensverhältnis zwischen erkrankten Personen und ärztlichem Fachpersonal. Weder das NPsychKG noch andere Rechtsgrundlagen enthalten Regelungen, die eine Offenlegung der Behandlungsakten gegenüber der kommunalen Vertretung rechtfertigen.

### 3. Darf die Hauptverwaltungsbeamtin bzw. der Hauptverwaltungsbeamte Einsicht in die Behandlungsakten des sozialpsychiatrischen Dienstes Einsicht nehmen?

Auch in diesem Fall ist eine Aktensicht nicht zulässig. Hier ist zu berücksichtigen, dass das NPsychKG die Wahrnehmung von Aufsichts- und Kontrollbefugnissen in § 32 NPsychKG regelt. Gesundheitsdaten unterliegen als besonders schutzwürdige Daten jedoch den Regelungen des § 33 NPsychKG, der keine Verarbeitung zu Aufsichts- und Kontrollzwecken vorsieht. Erkrankte Personen müssen dem ärztlichem Fachpersonal ihre physischen und psychischen Probleme anvertrauen dürfen, ohne befürchten zu müssen, dass Gesundheitsinformationen ungefragt Dritten preisgegeben werden. Andernfalls könnten sich erkrankte Personen entscheiden, ihre gesundheitlichen Probleme für sich zu behalten oder

sich gar nicht erst behandeln zu lassen. Insbesondere im Fall einer psychischen Erkrankung kann dies schwerwiegende Folgen für den Betroffenen haben.

## V. Datenschutz im Arbeitsalltag

### 1. E-Mail-Versand an mehrere Personen

Eine E-Mail-Adresse stellt ein personenbezogenes Datum (Artikel 4 Nummer 1 DSGVO) dar, wenn sie einer natürlichen Person zugeordnet werden kann. Aus diesem Grund ist bei der Versendung an mehrere Empfängerinnen und Empfänger darauf zu achten, dass die E-Mail-Adressen nicht offengelegt werden. Eine häufig genutzte Möglichkeit ist, das Feld „bcc“ zu verwenden. Hier besteht jedoch das Risiko, dass die E-Mail-Adressen versehentlich in das Feld „an“ oder „cc“ eingetragen werden. Eine weitere Möglichkeit E-Mails ohne Offenlegung weiterer E-Mail-Adressen an eine große Anzahl von Personen zu versenden besteht in der Nutzung der Serien-E-Mail-Funktion. Hier werden für jede Empfängerin und jeden Empfänger einzelne E-Mails versandt. Dadurch werden mögliche Datenschutzverletzungen vermieden.

### 2. Veröffentlichungen von Dokumenten

Häufig werden Dokumente im Rahmen von Bauleitverfahren und anderen Verfahren in denen die Öffentlichkeit beteiligt wird über die Webseiten von Kommunen veröffentlicht. Hierbei handelt es sich um Planungsunterlagen sowie um Stellungnahmen von Interessierten. Die Stellungnahmen sind in die notwendigen Abwägungen einzubeziehen und werden auch veröffentlicht. Zu beachten ist, dass die Eingaben der Interessierten auch personenbezogene Angaben, beispielweise Name und Anschrift enthalten. Für die Veröffentlichung personenbezogener Daten benötigen Kommunen eine Rechtsgrundlage oder eine Einwilligung.

Eine rechtliche Grundlage für die Veröffentlichung personenbezogener Daten über das Internet ist nur in besonderen Ausnahmefällen vorhanden. Demnach setzt die Offenlegung der personenbezogenen Daten eine wirksame Einwilligung voraus. Diese wäre von den betroffenen Personen einzuholen. Es ist unzulässig ein Einverständnis zu unterstellen, weil jemand im Rahmen der Öffentlichkeitsbeteiligung eine Anregung abgegeben hat.

Des Weiteren ist zwischen den Dokumenten, die in den Akten der Kommune verbleiben, und denen die einer breiten Öffentlichkeit zugänglich gemacht werden zu unterscheiden.

Vor der Veröffentlichung von Dokumenten ist somit sicherzustellen, dass personenbezogene Daten geschwärzt oder auf andere Weise entfernt werden. Darüber hinaus ist sicherzustellen, dass die vorgenommene Anonymisierung nicht durch Dritte rückgängig gemacht werden kann.

### 3. Was ist bei der Gewährung von Akteneinsicht zu beachten?

Bei der Gewährung von Akteneinsicht ist zu beachten, dass personenbezogene Dritter grundsätzlich zu schwärzen sind. Als „Dritte“ werden Personen bezeichnet, die nicht Beteiligte des Verwaltungsverfahrens (§ 13 Verwaltungsverfahrensgesetz – VwVfG) sind, zum Beispiel Hinweisgeber. Deren personenbezogene Daten sind ihrem Wesen nach geheim zu halten. „Dritte“ sind regelmäßig nicht Teil des Verwaltungsverfahrens,



das zwischen Behörde und den Beteiligten geführt wird. Das durch § 29 Abs. 1 VwVfG geschützte Interesse des Antragstellers, die eigene Rechtsposition in einem konkreten Verwaltungsverfahren abzusichern oder zu verbessern, ist grundsätzlich nicht von der Kenntnis von Personen abhängig, die in dem Verfahren nicht als Beteiligte im Sinne des VwVfG gelten. Deren Geheimhaltungsinteressen sind in Form ihres Rechts auf informationelle Selbstbestimmung und über § 29 Abs. 2 VwVfG geschützt.