Unsere Freiheiten:
Daten nützen - Daten schützen

Datenschutz bei Gemeinden

Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Der Landesbeauftragte für den Datenschutz
und die Informationsfreiheit Baden-Württemberg
Dr. Stefan Brink
MitautorInnen: Anneke Graner, Alvar Freude, Dr. Peter Nägele, Frank Feucht

Königstraße 10a
70173 Stuttgart

Telefon: (07 11) 61 55 41-0
Telefax: (07 11) 61 55 41-15

E-Mail: poststelle@lfdi.bwl.de
Homepage: https://www.baden-wuerttemberg.datenschutz.de/

Schutzbedürftige Daten sollten nicht unverschlüsselt per E-Mail oder via Telefax übertragen werden.
PGP-Fingerprint: E4FA 428C B315 2248 83BB F6FB 0FC3 48A6 4A32 5962

Zur besseren Lesbarkeit wird bei verallgemeinernden Substantiven lediglich das bestimmende Geschlecht genannt. Selbstverständlich richtet sich diese Broschüre an die Angehörigen aller Geschlechter.

Stand: Dezember 2019

Zum Geleit

Die Datenschutzgrundverordnung (DS-GVO) ist seit dem 25. Mai 2018 geltendes Recht in Deutschland und in allen anderen Mitgliedstaaten der Europäischen Union.

Für viele Gemeinden in Baden-Württemberg stellt die Umsetzung der alten und neuen Anforderungen des Datenschutzrechts eine große Herausforderung dar, die vielerorts mit großem Engagement und guten Ergebnissen gemeistert wird.

Ein Ergebnis der jüngsten Umfrage unserer Dienststelle bei allen Gemeinden in Baden-Württemberg ist allerdings, dass Gemeinden mehr Unterstützung bei der datenschutzrechtlichen Bewertung von Sachverhalten wünschen - und benötigen. Hier zu helfen, sieht der Landesbeauftragte als eine eigene, zentrale Aufgabe an.

Häufig lassen sich datenschutzrechtliche Fragestellungen mit Grundkenntnissen des Datenschutzrechts beantworten. Diese Broschüre soll hier einen grundlegenden Beitrag leisten. Ziel ist es, den Gemeinden eine klare und gut verständliche Orientierung zu vermitteln, was es zu beachten gilt, wenn sie als verantwortliche Stellen personenbezogene Daten verarbeiten.

Diese Hilfestellung wendet sich aber nicht nur an die Kommunen. Vielen Bürgerinnen und Bürgern, die von der Verarbeitung ihrer Daten durch Gemeinden betroffen sind, ist unklar, welche Rechte und Möglichkeiten, ihnen das (neue) Datenschutzrecht zur Verfügung stellt. Deshalb sind klare Hinweise zu den Betroffenenrechten ein wichtiger Bestandteil dieser Broschüre.

Wir hoffen, dass wir mit den nachfolgenden Informationen den Gemeinden zielführende Hinweise für den Datenschutz in der kommunalen Praxis geben und allen Betroffenen aufzeigen können, welche Möglichkeiten und Rechte sie haben, eine recht- und zweckmäßige Verarbeitung ihrer Daten in den Kommunen sicherzustellen.

Mit freundlichen Grüßen
Ihr
Stefan Brink
Landesbeauftragter für den Datenschutz und
die Informationsfreiheit Baden-Württemberg

Abkürzungsverzeichnis

AG	Aktiengesellschaft
BDSG	Bundesdatenschutzgesetz
BMG	Bundesmeldegesetz
CDN	Content-Delivery-Networks
DSFA	Datenschutz-Folgenabschätzung
DSK	Datenschutzkonferenz des Bundes und der Länder
DS-GVO	Datenschutz-Grundverordnung
DV	Datenverarbeitung
EG	Erwägungsgrund der Datenschutz-Grundverordnung
EuGH	Europäischer Gerichtshof
GemO	Gemeindeordnung
GmbH	Gesellschaft mit beschränkter Haftung
JI-Richtlinie	Europäische Datenschutz-Richtlinie im Bereich von Justiz und Inneres
KunstUrhG	Kunsturhebergesetz
KVN	Kommunales Verwaltungsnetz
LBO	Landesbauordnung
LDA	Bayerisches Landesamt für Datenschutzaufsicht
LDSG	Landesdatenschutzgesetz
LDSG a.F.	Landesdatenschutzgesetz alte Fassung
LDSG n.F.	Landesdatenschutzgesetz neue Fassung (= LDSG)
LDSG JB	Landesdatenschutzgesetz für Justiz- und Bußgeldbehörden
LfDI	Landesbeauftragter für den Datenschutz und die Informationsfreiheit
LIFG	Landesinformationsfreiheitsgesetz
PolG	Polizeigesetz
SDK	Software-Development-Kit
SGB	Sozialgesetzbuch

1. Verantwortlicher

Wer ist Verantwortlicher?

Legaldefinition

Nach der Legaldefinition in Art. 4 Nr. 7 DS-GVO ist Verantwortlicher für die Verarbeitung personenbezogener Daten die Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Grundsatz

Gemeinde als Gebietskörperschaft, vertreten durch den Bürgermeister

Soweit es um die Verarbeitung personenbezogener Daten durch Gemeinden in Baden-Württemberg geht, ist Verantwortlicher grundsätzlich die jeweilige Gemeinde als Gebietskörperschaft, vertreten durch den Bürgermeister. Die Gemeinde ist verantwortliche Stelle für ihre Verwaltungsorgane Gemeinderat und Bürgermeister sowie für alle ihre nichtselbstständigen organisatorischen Untergliederungen.

Abgrenzungskriterium eigene Rechtspersönlichkeit

Bei einer ersten Annäherung an die Frage der Verantwortlichkeit kann man darauf abstellen, ob der Bereich/die Organisationseinheit, die personenbezogene Daten verarbeitet, rechtlich zur Gemeinde gehört (keine eigene Rechtspersönlichkeit), oder ob die Datenverarbeitung durch eine Einrichtung/Stelle mit eigener Rechtspersönlichkeit erfolgt, wie etwa durch eine kommunale Stiftung oder ein kommunales Unternehmen in Form einer GmbH. Stellen mit eigener Rechtspersönlichkeit sind selbst verantwortliche Stelle für die Verarbeitung personenbezogener Daten.

Ausnahmen

Abweichende Regelungen durch Rechtsvorschriften

Der Grundsatz, dass die Verarbeitung personenbezogener Daten durch Verwaltungsorgane und deren organisatorischen Untergliederungen der Gemeinde als verantwortliche Stelle zuzuordnen sind, gilt jedoch nur, soweit keine besonderen, insoweit vorrangigen Rechtsvorschriften die Verantwortlichkeit im gemeindlichen Bereich anders regeln.

Ausnahmen aufgrund der Gesamtschau aller Regelungen.

Auch kann eine nichtselbstständige Einrichtung einer Gemeinde selbst Verantwortlicher sein, wenn dies nicht ausdrücklich geregelt ist. Hier ist insbesondere darauf abzustellen, ob diese Einrichtung in der Gesamtschau aller insoweit relevanten Regelungen eigenverantwortlich über Zwecke und Mittel der Datenverarbeitung entscheiden.

Anwendungsbeispiele

Sozialämter und Jugendämter

Für Sozialämter und Jugendämter regelt § 67 Abs. 4 SGB X ausdrücklich, dass wenn eine Gebietskörperschaft Leistungsträger ist, der Verantwortliche der Organisationseinheit, die eine Aufgabe nach einem der besonderen Teile des Sozialgesetzbuches funktional durchführt, Verantwortlicher ist. Diese Regelung gilt auch für die Verarbeitung personenbezogener Daten. In solchen Fällen ist das Sozialamt der Gemeinde oder das Jugendamt der Gemeinde, vertreten durch den Bürgermeister, verantwortliche Stelle im datenschutzrechtlichen Sinne.

Eigenbetriebe

Eigenbetriebe haben zwar keine eigene Rechtspersönlichkeit. Das Eigenbetriebsgesetz räumt jedoch die Möglichkeit ein, Eigenbetrieben im großen Umfang eigene Entscheidungskompetenzen zu übertragen. Es ist somit für den jeweiligen Einzelfall zu prüfen, ob ein Eigenbetrieb grundsätzlich selbst eigenverantwortlich über Mittel und Zweck der Datenverarbeitung entscheidet. Ist dies der Fall, ist der Eigenbetrieb selbst verantwortliche Stelle (und nicht die Gemeinde als Gebietskörperschaft).

Beispiel Gemeinde als verantwortliche Stelle für Eigenbetrieb

In kleinen Gemeinden, die etwa die Wasserversorgung oder die Abwasserbeseitigung als Eigenbetrieb führen, die Betriebsleitung aus gemeindlichen Mitarbeitern besteht, die auch Aufgaben für den Eigenbetrieb wahrnehmen und technische Mittel der Gemeinde einsetzen (wie beispielsweise durch Rückgriff auf die gemeindliche IT-Infrastruktur) und der Eigenbetrieb die wesentlichen Entscheidungen über die Verarbeitung personenbezogener Daten nicht eigenständig trifft, ist die Gemeinde als Gebietskörperschaft verantwortliche Stelle.

Beispiel Eigenbetreib als verantwortliche Stelle

Große Eigenbetriebe, die eine Vielzahl eigener Beschäftigter haben, über eine eigene IT-Infrastruktur verfügen und denen weitreichende Entscheidungskompetenzen bei der Verarbeitung personenbezogener Daten im laufenden Betrieb eingeräumt wurden, dürften hingegen regelmäßig selbst verantwortliche Stelle für die Verarbeitung personenbezogener Daten sein.

Feuerwehren

Nach dem Feuerwehrgesetz Baden-Württemberg ist die Feuerwehr eine Einrichtung der Gemeinde ohne eigene Rechtspersönlichkeit. Soweit es um personenbezogene Daten geht, liegt die Entscheidungskompetenz über Mittel und Zweck von Datenverarbeitungen regelmäßig bei der Gemeinde und nicht bei der Feuerwehr selbst. Mithin ist für den Bereich der Feuerwehr die Gemeinde verantwortliche Stelle für Verarbeitung personenbezogener Daten.

Personalvertretungen

Entscheidend sind die Absicht der Personalvertretung, eigenständig Daten von Beschäftigten zu verarbeiten, die tatsächliche Verarbeitungssituation und der Grad der Einordnung des Personalrats in der Gemeinde. Somit ist auch hier der jeweilige Einzelfall zu würdigen. Es kann jedoch davon ausgegangen werden, dass im gemeindlichen Bereich im Regelfall der Personalrat keine eigene verantwortliche Stelle ist.

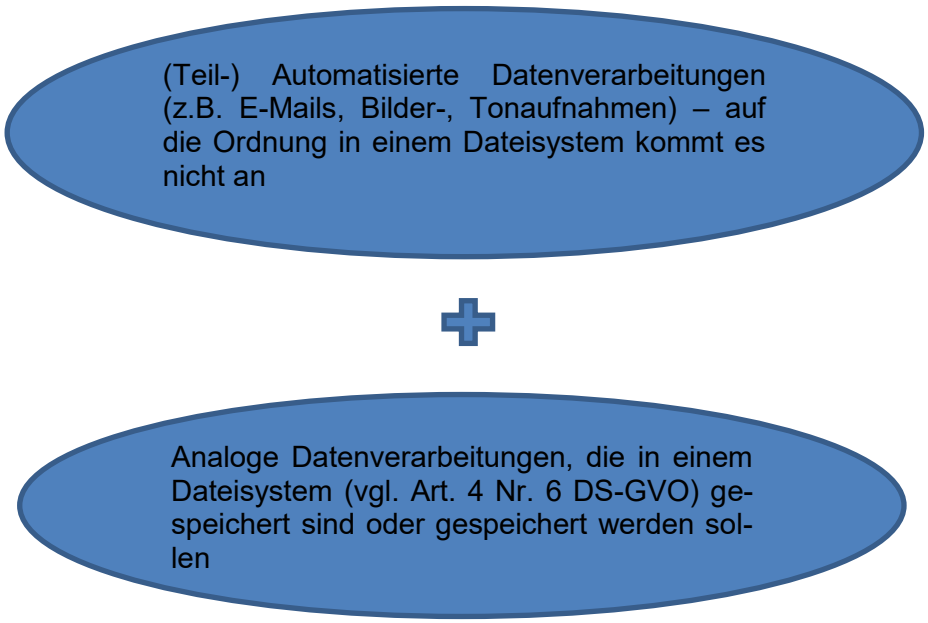
2. Anwendungsbereich DS-GVO

Grundlegendes

Technikneutraler Ansatz des Datenschutzrechts

Der (sachliche) Anwendungsbereich der Datenschutz-Grundverordnung umfasst nach Art. 2 Abs. 1 DS-GVO die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Nicht hiervon erfasst sind nach EG 15 DS-GVO lediglich "Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien geordnet sind".

Übersicht Anwendungsbereich



Strukturierte Behördenakten

Strukturierte Behördenakten – ob elektronisch oder in Papierform geführt – unterfallen daher vollumfänglich den Regelungen der Datenschutz-Grundverordnung. Dies ist auch bei den Betroffenenrechten von Bedeutung, wie etwa dem Auskunftsrecht.

Verhältnis DS-GVO zu nationalem Recht

Grundsatz: Anwendungsvorrang des EU-Rechts
-> **DS-GVO ist grundsätzlich immer vor nationalen Regeln anzuwenden**

1. Ausnahme:
Tätigkeiten, die **nicht** in den **sachlichen Anwendungsbereich** der Verordnung fallen (Art. 2 Abs. 2 DS-GVO)

- Behörden bei der Verfolgung von Straftaten und bei Gefahrenabwehr (Polizei, Strafgerichte, Staatsanwälte, Behörden, die Ordnungswidrigkeiten verfolgen), s.u.
- Außen- und Sicherheitspolitik
- Ausübung persönlicher und familiärer Tätigkeiten

2. Ausnahme:
DS-GVO räumt dem nationalen Gesetzgeber Gestaltungsspielraum ein über sog. **Öffnungsklauseln**
(für öffentlichen Bereich besonders bedeutsam: Art. 6 Abs. 3 in Verbindung mit Abs. 1 Buchst. e DS-GVO)

Verhältnis DS-GVO und JI-Richtlinie

Straftaten und Ordnungswidrigkeiten

Gemäß Art. 2 Abs. 2 Buchst. d DS-GVO und § 2 Abs. 1 Nr. 3 und 4 LDSG gelten die DS-GVO und das LDSG nicht für Verarbeitungen personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten und Ordnungswidrigkeiten durch Polizei, Gerichte, Staatsanwaltschaften, Justizministerium, Justizvollzugsbehörden und andere Behörden, die für die Verfolgung von Ordnungswidrigkeiten zuständig sind.

Landesdatenschutzgesetz für Justiz- und Bußgeldbehörden

Für die genannten Verarbeitungen personenbezogener Daten gilt das am 6. Juni 2019 in Kraft getretene Landesdatenschutzgesetz für Justiz- und Bußgeldbehörden (LDSG-JB). Das bedeutet in der Praxis, dass innerhalb eines Amtes oder einer Behörde einer Gemeinde (z.B. der Straßenverkehrsbehörde) zu fragen ist, in welchem Aufgabenbereich die fragliche Datenverarbeitung stattfindet. Die Bußgeldstelle innerhalb einer größeren Behördeneinheit unterliegt demnach der JI-Richtlinie bzw. dem LDSG-JB, die reine Verwaltungsabteilung dagegen der DS-GVO.

Datenschutz im Polizeibereich

Den Gemeinden kommt gem. § 62 Abs. 4 S. 1 PolG auch die Funktion als Ortspolizeibehörden zu. Ortspolizeibehörden als allgemeine Polizeibehörden unterfallen nicht dem Anwendungsbereich der DS-GVO (Art. 2 Abs. 2 Buchst. d), sondern der JI-Richtlinie. Die JI-Richtlinie bedarf der Umsetzung in nationales Recht. Zum jetzigen Zeitpunkt (Stand Oktober 2019) ist die Novellierung des Polizeigesetzes Baden-Württemberg noch nicht beschlossen worden. Bis dahin gilt gem. § 30 Abs. 1 LDSG n.F. das bis zum 20. Juni 2018 geltende Landesdatenschutzgesetz als Übergangsbestimmung weiter.

Ausfüllende nationale Normen

Öffnungsklauseln

Öffnungsklauseln, die nationale Datenschutzregeln zulassen, gibt es in der DS-GVO nicht nur bei den Rechtsgrundlagen (z.B. Art. 6 Abs. 1 Buchst. e DS-GVO), sondern bei einer Vielzahl an Bereichen (so gem. Art. 23 DS-GVO auch bei den Informationspflichten und Betroffenenrechten).

Grundsatz: Rechtsregime LDSG

Für Gemeinden kann sich die Frage stellen, welche ausfüllenden Normen für sie gelten. Diese Frage beantwortet § 2 LDSG. Nach § 2 Abs. 1 gilt das LDSG für die öffentlichen Stellen des Landes Baden-Württemberg, es sei denn die Absätze 2 bis 7 regeln etwas anderes.

Ausnahme Wettbewerb

Etwas anderes regelt § 2 Abs. 6 LDSG, wonach für öffentliche Stellen des Landes das BDSG gilt, wenn und soweit sie als Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb teilnehmen.

Teilnahme am Wettbewerb

EuGH-Urteil zur Wettbewerbsteilnahme

Für die Frage, wann in diesem Zusammenhang eine öffentliche Stelle am Wettbewerb teilnimmt – also wirtschaftlich tätig wird –, gibt der Europäische Gerichtshof Orientierung (Urteil vom 12. Juli 2012, C-138/11, Rn. 35 ff.). Danach ist eine wirtschaftliche Tätigkeit jede Tätigkeit, die darin besteht, Güter oder Dienstleistungen auf einem bestimmten Markt anzubieten. Soweit eine öffentliche Einheit eine wirtschaftliche Tätigkeit ausübt, die von der Ausübung ihrer hoheitlichen Befugnisse losgelöst werden kann, handelt sie in Bezug auf diese Tätigkeit als Unternehmen.

Definition „Wettbewerb“

Am Wettbewerb nehmen also Gemeinden dann teil, wenn sie Leistungen erbringen, die auch von privaten Anbietern erbracht werden oder erbracht werden können. Dabei kommt es nicht darauf an, ob der Leistungserbringung eine Gewinnerzielungsabsicht zu Grunde liegt.

Definition „Markt“

Bei der Bestimmung des Begriffs „Markt“ vertreten wir ein weites Definitionsverständnis. So unterscheiden wir z.B. bei Bädern nicht nach ihrer Art (Freibad, Hallenbad, Thermalbad), sondern legen den Oberbegriff „Bäderbetrieb“ als Bezugspunkt für den Begriff des „Marktes“ fest. Auch in räumlicher Hinsicht ist der Begriff des „Marktes“ weit zu verstehen, letztlich ist jedoch eine Einzelfallbetrachtung entscheidend.

Anwendungsbeispiel Stadtwerke

Beispielsfall Stadtwerke:
Die Stadtwerke sind in einer juristischen Person des Privatrechts (z.B. GmbH) organisiert, die Anteile werden aber zu 100% von der Kommune gehalten. Gemäß § 2 Abs. 2 LDSG gilt diese Stadtwerke GmbH damit als öffentliche Stelle, die Anwendbarkeit des LDSG gemäß § 2 Abs. 1 LDSG ist somit eröffnet.

In unserem Beispielsfall nimmt die Strom-Sparte dieser Stadtwerke-GmbH am Wettbewerb teil. Insoweit gilt für die Strom-Sparte (anders als z.B. die Sparte Wasser) gemäß § 2 Abs. 6 LDSG das BDSG. Dies hat u.a. Auswirkungen auf die Bestellung des (betrieblichen) Datenschutzbeauftragten und auf die Möglichkeit der Verhängung von Bußgeldern (siehe § 28 LDSG).

3. Personenbezogene Daten

Legaldefinition

Die DS-GVO ist nach ihrem Art. 2 Abs. 1 nur anwendbar, wenn Gegenstand der Verarbeitung personenbezogene Daten gemäß der Legaldefinition nach Art. 4 Nr. 1 DS-GVO sind.

Artikel 4
Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

1 . „personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Grundlegendes

Natürliche Person

Personenbezogene Daten sind nur solche Informationen, die sich auf eine natürliche Person beziehen. Auch Nicht-EU-Bürger fallen hierunter, wenn ihre Daten durch baden-württembergische Gemeinden als Verantwortliche verarbeitet werden.

Daten Verstorbener

Daten Verstorbener sind gemäß EG 27 DS-GVO keine personenbezogenen Daten. Allerdings können bestimmte Daten eines Verstorbenen einen Bezug zu einer lebenden Person haben und insoweit Personenbezug aufweisen (z.B. Information bezüglich des Vorliegens einer Erbkrankheit beim Verstorbenen).

Juristische Personen

Daten von juristischen Personen (wie etwa eingetragene Vereine oder Unternehmen, die in Form einer GmbH oder AG geführt werden) sind keine personenbezogenen Daten im Sinne datenschutzrechtlicher Vorschriften. Das bedeutet, dass juristische Personen sich nicht selbst auf das Grundrecht auf informationelle Selbstbestimmung berufen können. Wenn sie jedoch als Verantwortliche personenbezogene Daten von natürlichen Personen verarbeiten, müssen sie datenschutzrechtliche Bestimmungen hinreichend beachten.

Informationen, die sich auf eine identifizierte natürliche Person beziehen, wie z.B. Namen, Anschriften oder Geburtsdaten, bedürfen keines Hinzuziehens weiterer Informationen, sondern lassen die Identität der Person unmittelbar aus der Information folgen.

Unmittelbarer Personenbezug

Lediglich identifizierbar ist eine betroffene Person, wenn die Information für sich genommen nicht ausreicht, um sie einer Person zuzuordnen, dies aber durch Hinzuziehen weiterer Informationen möglich ist. In diesem Zusammenhang ist umstritten, ob es allein auf das Wissen der verantwortlichen Stelle ankommt (subjektive oder relative Theorie) oder ob das Wissen Dritter zu berücksichtigen ist, also ob irgendjemand den Personenbezug herstellen kann (objektive oder absolute Theorie).

Mittelbarer Personenbezug

Wir vertreten diesbezüglich einen verschärft subjektiven Ansatz, wonach lediglich das tatsächliche Wissen der verantwortlichen Stelle zu berücksichtigen ist. Nicht erforderlich ist unserer Ansicht nach jedoch, dass sich alle zur Identifizierung der betreffenden Person erforderlichen Informationen in den Händen einer einzigen Person befinden. Der Verantwortliche muss sich das Wissen Dritter dann zurechnen lassen, welches er in rechtlich zulässiger Weise oder vernünftigerweise hinzuziehen könnte (siehe Urteil des EuGH vom 19.10.2016, C-582/14).

Verschärft subjektiver Ansatz

Unter „vernünftigerweise“ ist der vertretbare und verhältnismäßige Aufwand der Beschaffung von Zusatzinformationen, wie Arbeitskraft, Kosten und Zeit zu verstehen. Die Herstellung des Personenbezugs muss also nicht tatsächlich erfolgt sein, die (legale) Möglichkeit reicht aus.

Definition „vernünftigerweise“

Beispiel aus der Praxis

Fall:
Ein Student bittet eine baden-württembergische Gemeinde für seine Bachelor-Arbeit um Übermittlung von Flurstücksnummern von Grundstücken auf dem Gebiet der Gemeinde. Die Gemeinde fragt, ob es sich dabei um personenbezogene Daten handelt.

Praxisfall

Antwort:
Nach dem von uns vertretenen verschärft subjektiven Ansatz, handelt es sich bei den Flurstücksnummern aus Sicht der Gemeinde als verantwortlicher Stelle um personenbezogene Daten, da sie mit ihrem Wissen (etwa Informationen über die ihre Baurechtsbehörde verfügt) die Eigentümer identifizieren kann.

Gemeinde als Verantwortliche

Für den Studenten stellen die Flurstücksnummern jedoch grundsätzlich keine personenbezogenen Daten dar, da er nicht ohne weiteres einen legalen Zugang zu Zusatzinformationen hat, mit Hilfe derer er den Personenbezug herstellen kann. Für den Zugang zu den Eigentümerverhältnissen über das Liegenschaftskataster und das Grundbuchamt bräuchte er ein berechtigtes Interesse. Auch sind in unserem Fall keine Anhaltspunkte ersichtlich, nach denen vernünftigerweise das Wissen Dritter hinzugezogen werden kann, mit Hilfe dessen ein Personenbezug hergestellt werden könnte.

Student als Verantwortlicher

4. Rechtsgrundlagen

Grundlegendes

Rechtmäßigkeitsprinzip

Jede Verarbeitung personenbezogener Daten bedarf einer Rechtsgrundlage (Rechtmäßigkeitsprinzip). Dies ergibt sich aus Art. 5 Abs. 1 Buchst. a DS-GVO („Personenbezogene Daten müssen auf rechtmäßige Weise […] verarbeitet werden.“) und Art. 6 Abs. 1 DS-GVO („Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist […]“).

Prinzip der Erforderlichkeit

Ergänzt wird dieses Rechtmäßigkeitsprinzip durch das Prinzip der Erforderlichkeit: mit Ausnahme der Einwilligung (Art. 6 Abs. 1 Buchst. a DS-GVO) setzen alle Erlaubnistatbestände voraus, dass die Datenverarbeitung im jeweiligen Zusammenhang erforderlich ist.

Legaldefinition Verarbeitung

Artikel 4
Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

2. „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

Tatbestandsmerkmal „Erforderlichkeit“

Alle Erlaubnistatbestände des Art. 6 Abs. 1 DS-GVO – außer der Einwilligung (Buchst. a) – setzen voraus, dass die Verarbeitung im Hinblick auf ein gewisses Ziel „erforderlich“ ist.

EuGH Urteil

EuGH Urteil vom 16.12.2008 – AZ: C-524/06: Der Begriff der Erforderlichkeit ist ein „autonomer Begriff des Gemeinschaftsrechts“, weil er keinen variablen Inhalt in den Mitgliedstaaten haben darf, das heißt, dass die Auslegung nicht nach deutschem Recht erfolgen darf.

Kriterien, ob eine Datenverarbeitung erforderlich ist, sind

Kriterien

- ein legitimer Zweck (vgl. EG 39 S. 6)
- die Beschränkung auf das Notwendige (<-> Dienliche / Förderliche), vgl. EG 39 S. 7
- eine Prüfung von für den Betroffenen günstigeren Alternativen (mildestes Mittel, vgl. EG 39 S. 9)

Die Voraussetzung der Erforderlichkeit stellt sicher, dass der Verantwortliche ein vorgegebenes Ziel nicht zum Anlass nimmt, überschießend personenbezogene Daten zu verarbeiten. Der zulässige Umfang ist anhand des Verarbeitungszwecks zu ermitteln.

Keine überschießende Datenverarbeitung

5. Die Einwilligung

Rechtsgrundlage

Eine wirksame Einwilligung ist gemäß Art. 6 Abs. 1 Buchst. a DS-GVO eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten.

Art. 6 Abs. 1 Buchst. a DS-GVO

Legaldefinition Einwilligung

Artikel 4
Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

11. „Einwilligung" der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist

Einwilligungsvoraussetzungen

Ob eine Einwilligung tatsächlich eine gültige Rechtsgrundlage für eine Datenverarbeitung darstellt, hängt davon ab, ob sie die Voraussetzungen erfüllt, die die DS-GVO postuliert. Eine wirksame Einwilligung muss

Freiwilligkeit, Bestimmtheit, Informiertheit und Unmissverständlichkeit

- freiwillig,
- bestimmt,
- informiert und
- unmissverständlich

sein.

Freiwilligkeit

Eine Einwilligung ist dann freiwillig, wenn die betroffene Person „eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden" (EG 42, letzter Satz).

Echte oder freie Wahl

Vermeidung von Zwangssituationen

Dabei meint „Nachteil“ nicht notgedrungen den Verlust eines Vorteils, denn es geht nicht darum, für den Betroffenen einen rechtlichen Anspruch auf eine Leistung durchzusetzen, sondern lediglich Zwangssituationen zu vermeiden.

Strukturelles Ungleichgewicht

Maßgeblich sind immer die konkreten Umstände des Einzelfalls. Arbeiten Behörden mit Einwilligungen als Rechtsgrundlage für ihre Datenverarbeitung, ist das Merkmal der Freiwilligkeit besonders sorgfältig zu prüfen. Denn im Verhältnis Behörde – Bürger liegt ein strukturelles Ungleichgewicht, welches die Freiwilligkeit einer Willensbekundung des Bürgers grundsätzlich in Frage stellt (EG 43).

Empfehlung: gesetzlich normierte Grundlage

Die Verarbeitung auf Basis einer Einwilligung sollte im gemeindlichen Bereich nur ausnahmsweise erfolgen. Wenn möglich, ist die Datenverarbeitung auf eine gesetzlich normierte Grundlage zu stützen.

Einwilligungs- oder Einsichtsfähigkeit

Freiwilligkeit liegt auch nur dann vor, wenn eine hinreichende Fähigkeit zur Erfassung des Sachverhalts und der Folgen hinsichtlich einer Einwilligung vorhanden ist (Einwilligungs- oder Einsichtsfähigkeit). Eine feste Altersgrenze für die Einwilligungsfähigkeit ist nur in Art. 8 DS-GVO bereichsspezifisch für Dienste der Informationsgesellschaft geregelt (Vollendung des 16. Lebensjahres). Art. 8 DS-GVO kommt aber jenseits seiner Regelungsmaterie indizieller Charakter zu.

Minderjährige: Faustformel 16

Zwar ist bei Minderjährigen die Prüfung des Vorliegens der Einwilligungsfähigkeit letztlich immer eine Frage des Einzelfalls. Jedoch ist dabei ein wichtiges Kriterium für die Einsichtsfähigkeit von Minderjährigen deren Fähigkeit, den tatsächlichen Sachverhalt und die Konsequenzen der Verarbeitung ihrer personenbezogenen Daten zu erfassen. Grundsätzlich gilt die Faustformel, dass Einsichtsfähigkeit mit Vollendung des 16. Lebensjahrs vorliegt. Wird die Einsichtsfähigkeit eines Minderjährigen von einer Gemeinde nach einer Prüfung des Einzelfalls nicht angenommen, müssen die Personensorgeberechtigten (etwa die Eltern) die Einwilligung für den Minderjährigen abgeben.

Bestimmtheit

Bezug auf konkrete Verarbeitungsformen

Der Zweck der Datenverarbeitung muss bestimmt sein. Eine Einwilligung muss sich somit auf eine bestimmte Verarbeitung der personenbezogenen Daten beziehen (wie etwa Erheben, Speichern, Verwenden oder Offenlegen).

Informiertheit

Zweck der Datenverarbeitung

Die betroffene Person muss (mindestens) wissen, wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen (EG 42).

Umfang der Einwilligung

Die betroffene Person muss erkennen können, dass und in welchem Umfang sie ihre Einwilligung erteilt (EG 42).

Beispiel Umfang

Beispiel:
Bei einer geplanten Veröffentlichung der personenbezogenen Daten ist es in diesem Zusammenhang bedeutsam, ob die Veröffentlichung lediglich in einem Printmedium und/oder im Internet erfolgt.

Kongruenz mit Informationspflichten

Bei der Informiertheit der Einwilligung sind die Voraussetzungen für das Vorliegen eines gültigen Rechtsgrunds für eine Datenverarbeitung teilweise kongruent mit den Informationspflichten aus Art. 13 DS-GVO.

Hinweis auf Widerrufsmöglichkeit

Die betroffene Person muss darüber belehrt werden, dass sie jederzeit ihre Einwilligung widerrufen kann (Art. 7 Abs. 3 S. 3 DS-GVO).

Keine rückwirkende Wirkung eines Widerrufs

Der Widerruf der Einwilligung berührt die Rechtmäßigkeit der Verarbeitung jedoch nicht rückwirkend (Art. 7 Abs. 3 S. 2 DS-GVO).

Prüfung, ob Löschpflicht besteht

Ein Widerruf verpflichtet aber – bei Fehlen eines alternativen Erlaubnistatbestandes – grundsätzlich zur Löschung der gespeicherten Daten (Art. 17 Abs. 1 Buchst. b DS-GVO).

Unmissverständlichkeit

Definition „unmissverständlich“

„Unmissverständlich“ ist eine eindeutige bestätigende Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung ihrer Daten einverstanden ist. Auch aktive konkludente Willensbekundungen (wie Nicken) fallen darunter. Stillschweigen oder Untätigkeit hingegen können keine Einwilligung darstellen (EG 32 S. 3).

Beispiel elektronische Erklärung

Beispiel:
Eine elektronisch abgegebene Erklärung ist eine eindeutige bestätigende Handlung, wenn die betroffene Person beim Besuch einer Internetseite selbst ein Kästchen auf einer Internetseite anklickt. Keine eindeutige Erklärung liegt hingegen vor, wenn ein Kästchen bereits angekreuzt ist und die betroffene Person das Kreuzchen nicht herausnimmt. Untätigkeit ist keine unmissverständliche bestätigende Handlung (vgl. EG 32).

Nachweispflicht

Ausprägung der Rechenschaftspflicht

Die Nachweispflicht ist eine spezifische Ausprägung der Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO. Beruht die Datenverarbeitung auf einer Einwilligung, so muss die verantwortliche (öffentliche) Stelle nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat (Art. 7 Abs. 1 DS-GVO).

Empfehlung: Schriftlichkeit

Ein Schriftformerfordernis für die Einwilligung sieht die DS-GVO zwar nicht vor, im Hinblick auf die Nachweispflicht des Verantwortlichen ist sie aber nach wie vor zu empfehlen.

Fortgeltung von Einwilligungen nach altem Datenschutzrecht

Grundsatz der Fortgeltung rechtswirksamer Alt-Einwilligungen

Einwilligungen, die vor Wirksamwerden der DS-GVO erteilt wurden, gelten fort (Alt-Einwilligungen), sofern sie den Bedingungen der DS-GVO entsprechen (EG 171 S. 3). Rechtswirksame Alt-Einwilligungen erfüllen grundsätzlich diese Bedingungen.

Keine Informationspflichten bei Alt-Einwilligungen

Informationspflichten nach Artikel 13 DS-GVO müssen für die Rechtswirksamkeit von Alt-Einwilligungen nicht erfüllt sein, da sie keine Bedingungen im Sinne des genannten Erwägungsgrundes 171 S. 3 darstellen.

Beispiel elektronische Einwilligungen

Beispiel:
Nicht mehr den Bedingungen der DS-GVO entsprechen Einwilligungen, die elektronisch im Internet über ein bereits vorangekreuztes Kästchen erteilt wurden, gelten nicht fort (siehe EG 32).

Keine Fortgeltung von Alt-Einwilligungen bei Missachtung des Kopplungsverbots

Auch ist das „Kopplungsverbot“(Art. 7 Absatz 4 DS-GVO i.V.m. Erwägungsgrund 43 DS-GVO) zu beachten. Wurde in der Vergangenheit die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig gemacht, die für die Erfüllung des Vertrags nicht erforderlich war, gilt diese Einwilligung nicht weiter fort.

Verhältnis zu anderen Erlaubnistatbeständen

Für Rechtmäßigkeit der Datenverarbeitung muss ein Erlaubnistatbestand erfüllt sein

Rechtmäßig ist eine Datenverarbeitung gemäß Art. 6 Abs. 1 DS-GVO, wenn „mindestens“ einer der in Abs. 1 aufgeführten Erlaubnistatbestände erfüllt ist. Eine Datenverarbeitung lässt sich also auch auf mehrere Rechtsgrundlagen stützen. D.h., dass der Verantwortliche zusätzlich eine Einwilligung einholen darf, auch wenn bereits ein gesetzlicher Rechtsgrund nach Abs. 1 Buchst. b bis f einschlägig ist.

Kein Suggerieren einer fehlenden Entscheidungsmacht

Indem eine Einwilligung vom Betroffenen eingeholt wird, wird diesem jedoch signalisiert, dass es für die Zulässigkeit der DV gerade auf sein Einverständnis ankommen soll. Dann aber wäre es widersprüchlich, bei Verweigerung oder Unwirksamkeit der Einwilligung doch wieder auf den gesetzlichen Erlaubnistatbestand zurückzugreifen. Im Ergebnis darf dem Betroffenen keine Entscheidungsmacht suggeriert werden, die so gar nicht besteht (Grundsatz der Fairness und Transparenz, Art. 5 Abs. 1 Buchst. a). Zulässig wäre, bei Einholung einer Einwilligung auf den gesetzlichen Erlaubnistatbestand hinzuweisen.

Andere Rechtsauffassungen

Hinweis:
Der LfDI Baden-Württemberg vertritt an dieser Stelle eine andere Meinung als die Datenschutzkonferenz (DSK), welche in ihrem Kurzpapier Nr. 20 („Einwilligung nach der DS-GVO“) davon ausgeht, dass eine unwirksame Einwilligung nicht durch ein Stützen auf eine andere Rechtsgrundlage ersetzt werden kann.

Praxisfall Fotos bei Bürgerempfang

Beispiel aus der Praxis:
Anlässlich eines öffentlichen Bürgerempfangs, auf dem Fotos gemacht und danach veröffentlicht werden sollen, fragt eine Gemeinde, ob man von allen abgebildeten Personen eine Einwilligung einholen muss.

Öffentlichkeitsarbeit gemeindliche Aufgabe

Antwort:
Die Öffentlichkeitsarbeit öffentlicher Stellen gehört nach unserer Rechtsauffassung zu den diesen zugewiesenen Aufgaben. Sowohl das Fotografieren (=Erheben) als auch die Veröffentlichung von Lichtbildern richtet sich nach § 4 LDSG.

Sinngemäße Anwendung Kunsturhebergesetz

Wir halten es für vertretbar, im Rahmen der Erforderlichkeitsprüfung den § 23 Absatz 1 Nummer 2 oder 3 KunstUrhG jedenfalls entsprechend anzuwenden. Je eher sich eine Vielzahl von Personen als "Beiwerk" oder im Rahmen von Übersichtsaufnahmen auf dem Bild befindet, desto eher wird eine Veröffentlichung ohne Einwilligung zulässig sein. Je eher einzelne Personen hervorgehoben präsentiert werden, desto eher bedarf es einer Einwilligung der Betroffenen.

Abbildungen von Kindern

In besonderem Maß gilt dies, wenn es sich um Abbildungen von Kindern handelt. Im Zweifel sollte die öffentliche Stelle Personen entweder um Einwilligung bitten oder sie unkenntlich machen (z. B. verpixeln).

Informationspflicht

Da das Fotografieren eine Datenerhebung darstellt, ist zudem die Informationspflicht gemäß Artikel 13 DS-GVO zu beachten.

Einwilligung im Beschäftigungskontext

Normierte Konstellationen

In Umsetzung der Öffnungsklausel des Art. 88 Abs. 1 DS-GVO erklärt § 15 Abs. 3 und Abs. 6 LDSG für die dort aufgeführten Konstellationen (Erhebung personenbezogener Daten des Bewerbers beim bisherigen Dienstherrn im Rahmen der Begründung eines Dienst-/Arbeitsverhältnisses; Verarbeitung biometrischer Daten zu Authentifizierungszwecken), dass die Einwilligung auch im Beschäftigtenverhältnis möglich ist.

Voraussetzungen für andere Konstellationen

Auch neben diesen explizit aufgeführten Konstellationen ist eine Einwilligung als Rechtsgrundlage für eine Datenverarbeitung im Beschäftigtenkontext grundsätzlich zulässig. Hierbei sind allerdings zwei Punkte zu berücksichtigen:

Keine Umgehung des Erforderlichkeitsvorbehalts

Zum einen soll der Erforderlichkeitsvorbehalt des § 15 Abs. 1 LDSG nicht umgangen werden – also mittels der Einwilligung „durch die Hintertür“ personenbezogene Daten erhoben oder verarbeitet werden, die eigentlich für die Durchführung des Arbeitsverhältnisses an sich nicht notwendig sind.

Berücksichtigung des persönlichen Abhängigkeitsverhältnisses

Zum anderen ist die persönliche Abhängigkeit der Beschäftigten im Rahmen der „Freiwilligkeit der Einwilligung“ zu berücksichtigen. Aufgrund der im Beschäftigungsverhältnis bestehenden Abhängigkeit der beschäftigten Person sind an die Einwilligung besondere Anforderungen zu stellen und die Umstände, unter denen die Einwilligung erteilt worden ist, speziell zu berücksichtigen.

Empfehlung Schriftform

Zwar sieht § 15 LDSG (im Gegensatz zu § 26 BDSG) keine Schriftform für die Einwilligung im Beschäftigtenkontext vor, sie ist jedoch aus Gründen der Nachweisbarkeit zu empfehlen.

Aufklärung über konkrete Tragweite einer Einwilligungserklärung

Damit die Einwilligung als Rechtsgrundlage herangezogen kann, muss die betroffene Person hinreichend bestimmt und transparent über die konkrete Tragweite ihrer Entscheidung aufgeklärt werden. Die einzelnen Verwendungszwecke sind deshalb ausdrücklich festzulegen und in Textform zu bezeichnen und aufzulisten. Schließlich ist explizit auf die Freiwilligkeit der Erteilung der Einwilligung und die Sanktionslosigkeit bei ihrer Verweigerung hinzuweisen sowie auf die jederzeitige Möglichkeit des Widerrufs und dessen Folgen (Art. 7 Abs. 3 DS-GVO).

Einwilligung nur bei Zusatzleistungen möglich

Die aufsichtsrechtliche Praxis zeigt, dass es nicht selten an der notwendigen Freiwilligkeit der Einwilligung fehlt. Eine Einwilligung ist deshalb nur in Konstellationen möglich, die nicht das Arbeitsverhältnis als solches, sondern nur Zusatzleistungen des Arbeitgebers betreffen (wie z.B. bei der Gestattung privater Nutzung der IuK oder dienstlicher Fahrzeuge, Telefone und EDV-Geräte, der Einführung eines betrieblichen Gesundheitsmanagements zur Gesundheitsförderung oder der Aufnahme in Geburtstagslisten).

Hingegen ist die Verarbeitung personenbezogener Daten von Beschäftigten, welche zur Eingehung, Durchführung, Beendigung oder Abwicklung des Beschäftigungsverhältnisses erforderlich sind, nur auf § 15 Abs. 1 LDSG als gesetzliche Grundlage zu stützen, sodass es eines Rückgriffs auf eine Einwilligung gar nicht bedarf und davon sogar abzuraten ist.

Keine Einwilligung im Rahmen des eigentlichen Beschäftigungsverhältnisses

6. Der Vertrag

Rechtsgrundlage

Nach Art. 6 Abs. 1 Buchst. b DS-GVO darf eine Verarbeitung personenbezogener Daten zu vertraglichen Zwecken erfolgen.

Art. 6 Abs. 1 Buchst. b DS-GVO

Art. 6 Abs. 1 Buchst. b DS-GVO

„Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:
[…] die Verarbeitung ist für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgt; […]“

Erforderlichkeit

Eine Datenverarbeitung ist erforderlich, wenn sie für die Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgt. Erfasst werden auch öffentlich-rechtliche Verträge.

Vertragserfüllung oder vorvertragliche Maßnahmen

Anwendungsbeispiele

- Anmeldung zu einer kommunalen Musikschule
- Anmeldung zu einem Kurs der VHS (in kommunaler Trägerschaft)
- Anmeldung bei einem kommunalen Kindergarten

Abgrenzungshilfe

Bei Abgrenzungsschwierigkeiten kann die Fragestellung hilfreich sein, ob eine autonom getroffene Entscheidung der betroffenen Person vorliegt, mit der Gemeinde ein Schuldverhältnis einzugehen und in diesem Zusammenhang auch die damit erforderliche Datenverarbeitung in Gang zu setzen.

Schuldverhältnis

7. Die rechtliche Verpflichtung

Rechtsgrundlage

Rechtsgrundlage für die Verarbeitung personenbezogener Daten kann eine rechtlichen Verpflichtung sein (Art. 6 Abs. 1 Buchst. c DS-GVO).

Art. 6 Abs. 1 Buchst. c DS-GVO

Art. 6 Abs. 1 Buchst. c DS-GVO

„Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:
[…]die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt; […]“

Öffnungsklausel

Art. 6 Abs. 1 Buchst. c DS-GVO ist in Verbindung mit Art. 6 Abs. 3 DS-GVO eine Öffnungsklausel. Sieht die DS-GVO für eine bestimmte Regelungsmaterie eine Öffnungsklausel vor, darf der nationale Gesetzgeber für diesen Bereich die Datenverarbeitung nach nationalem (Bundes-/ oder Landes-) Recht regeln. Zur Beurteilung datenschutzrechtlicher Fragestellungen sind somit die Datenschutz-Grundverordnung und die Regelungen im nationalen Datenschutzrecht im Zusammenhang zu lesen und anzuwenden.

Mit Recht des Mitgliedstaates sind alle Gesetze im materiellen Sinne (Parlamentsgesetze, Rechtsverordnungen, Verwaltungsvorschriften, kommunale Satzungen, Urteile des EuGH, auch Dienstvereinbarungen) gemeint. Diese Regelungen müssen dabei klar und präzise die Verarbeitungsvoraussetzungen (einschließlich Verarbeitungszwecke) beschreiben und zur Erfüllung einer Aufgabe dienen, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die der Gemeinde übertragen wurde.

Anwendung deutscher Rechtsordnung

Art. 6 Abs. 1 Buchst. c DS-GVO bezieht sich auf die Erfüllung rechtlicher Verpflichtungen aus Rechtsvorschriften und nicht auf Rechtsgeschäfte (vgl. Buchst. b)

Rechtsgeschäfte nicht umfasst

Erforderlichkeit bei Rechtsverpflichtungen

Die Datenverarbeitung muss zur Erfüllung einer Rechtspflicht erforderlich sein. D.h. diese kann nicht erfüllt werden, ohne dass das Datum verarbeitet würde. Dies ist dann der Fall, wenn die Gemeinde unmittelbar zu einer Datenverarbeitung (wie Speicherung oder Offenlegung) rechtlich verpflichtet ist. Es gilt aber auch dann, wenn die Pflichterfüllung die Datenverarbeitung zwingend voraussetzt.

Rechtspflicht kann nicht ohne Datenverarbeitung erfüllt werden

8. Schutz lebenswichtiger Interessen

Rechtsgrundlage

Gemäß Art. 6 Abs. 1 Buchst. d DS-GVO kann die Datenverarbeitung zum Schutz lebenswichtiger Interessen eine Rechtsgrundlage darstellen.

Art. 6 Abs. 1 Buchstabe d DS-GVO

Art. 6 Abs. 1 Buchst. d DS-GVO

„Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:
[…]die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen; […]“

Grundlegendes

Voraussetzung ist somit, dass „lebenswichtige Interessen der betroffenen oder einer anderen natürlichen Person“ geschützt werden müssen.

Voraussetzung

Lebenswichtige Interessen sind in erster Linie der Schutz des Lebens und der körperlichen Unversehrtheit (vgl. EG 112).

Definition „lebenswichtige Interessen“

Häufig werden dann Gesundheitsdaten betroffen sein und Art. 9 Abs. 2 Buchst. c DS-GVO vorrangig anwendbar. Andere typischen Konstellationen wie der Schutz vor gefährlichen Krankheiten und Infektionen werden vorrangig von Art. 9 Abs. 2 Buchst. i DS-GVO erfasst.

Anwendungsbereich

Die praktische Bedeutung dieses Erlaubnistatbestandes für Gemeinden dürfte deshalb gering sein.

Geringe praktische Bedeutung

9. Öffentliche Gewalt

Rechtsgrundlage

Die Verarbeitung personenbezogener Daten zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, kann gemäß Art. 6 Abs. 1 Buchst. e DS-GVO rechtmäßig sein.

Art. 6 Abs. 1 Buchst. e DS-GVO

Art. 6 Abs. 1 Buchst. e DS-GVO

„Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:
[…]die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde; […]“

Grundlegendes

Art. 6 Abs. 1 Buchst. e DS-GVO (i.V.m. Art. 6 Abs. 3 DS-GVO) stellt für die öffentlichen Stellen den zentralen Erlaubnistatbestand zur Verarbeitung personenbezogener Daten dar.

Zentraler Erlaubnistatbestand für Gemeinden

Im Verhältnis zur rechtlichen Verpflichtung (Art. 6 Abs. 1 Buchst. c DS-GVO) stellt eine Datenverarbeitung, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, für Gemeinden die speziellere Ermächtigungsgrundlage dar.

Verhältnis zur rechtlichen Verpflichtung

Allerdings handelt es sich bei Art. 6 Abs. 1 Buchst. e DS-GVO um keine eigenständige Rechtsgrundlage, sondern gem. Art. 6 Abs. 3 DS-GVO (Öffnungsklausel) ist diese durch Unionsrecht / Recht des jeweiligen Mitgliedstaates festzulegen.

Anwendung deutscher Rechtsordnung

Der baden-württembergische Landesgesetzgeber hat dies zum Beispiel im LDSG (vgl. § 4 LDSG) umgesetzt. Dabei ist zu beachten, dass das LDSG gem. § 2 Abs. 3 subsidiär (nachrangig) ist zu „besonderen Rechtsvorschriften des Bundes oder des Landes“, die auf personenbezogene Daten anzuwenden sind.

Subsidiarität LDSG

Voraussetzungen

Nach Art. 6 Abs. 1 Buchst. e DS-GVO ist eine Datenverarbeitung dann rechtmäßig, wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist,

- die im öffentlichen Interesse liegt (Variante 1) oder
- in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde (Variante 2).

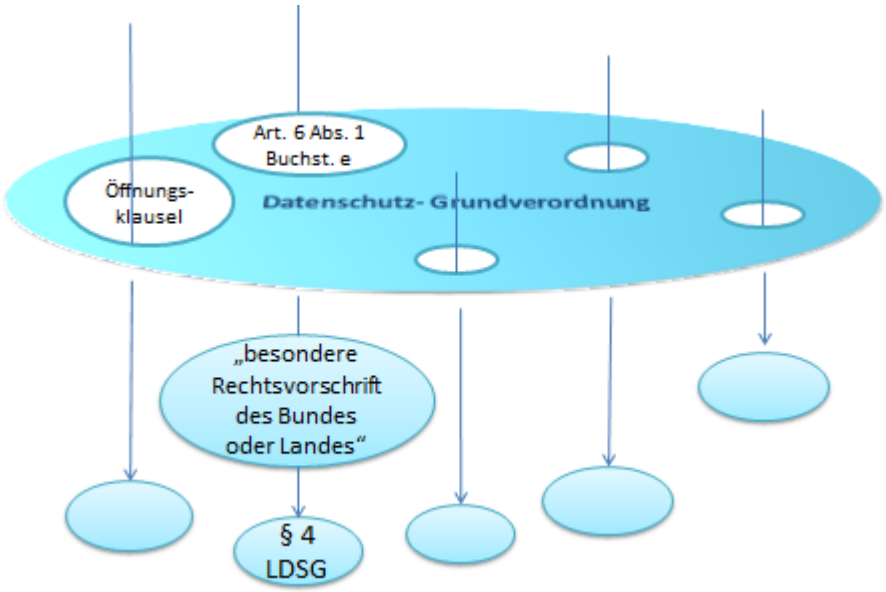
Beispiele für Variante 1 sind insbesondere aus dem Bereich der freiwilligen Aufgaben einer Gemeinde zu nennen, wie der Betrieb einer öffentlichen Bibliothek oder eines Schwimmbades. Es gilt in diesem Zusammenhang der Grundsatz der Allzuständigkeit der Gemeinde (§ 2 Abs. 1 GemO), vorausgesetzt eine öffentlichen Aufgabe liegt vor.

Beispiel öffentliches Interesse

Variante 2 beschreibt die klassisch hoheitlichen Tätigkeiten einer öffentlichen Stelle, die aufgrund rechtlich festgelegter Aufgaben durchgeführt werden müssen.

Beispiel Ausübung öffentlicher Gewalt

Öffnungsklausel und Subsidiaritätsprinzip



Die Rechtsgrundlage für eine Datenverarbeitung im gemeindlichen Bereich ist demnach Art. 6 Abs. 1 Buchst. e DS-GVO in Verbindung mit

- einem Fachgesetz (überwiegend im Bereich der Pflichtaufgaben) oder
- § 4 LDSG (überwiegend im freiwilligen Bereich).

Je nach zu Grunde liegenden Sachverhalt sind zusätzlich weitere Rechtsvorschriften beachtlich, wie beispielsweise Art. 9 DS-GVO, soweit besonders sensible Daten verarbeitet werden.

10. Wahrung berechtigter Interessen

Rechtsgrundlage

Die Rechtsgrundlage für eine Datenverarbeitung zur Wahrung berechtigter Interessen des Verantwortlichen oder von Dritten findet sich in Art. 6 Abs. 1 Buchst. f DS-GVO geregelt.

Art. 6 Abs. 1 Buchst. f DS-GVO

Art. 6 Abs. 1 Buchst. f DS-GVO

„Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:
[…]die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.
Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.“

Anwendungsbeschränkung

Gemäß Art. 6 Abs. 1 Unterabsatz 2 DS-GVO ist Art. 6 Abs. 1 Buchst. f DS-GVO nicht für die von Behörden in Erfüllung ihrer Aufgabe vorgenommenen Datenverarbeitung anwendbar. Gemeint sind an dieser Stelle sowohl die Pflicht- als auch die freiwilligen Aufgaben, die eine Gemeinde erfüllt.

Nicht für behördliche Aufgabenerfüllung

Anwendungsbereich Gemeinden

Etwas anderes gilt, wenn Behörden in gleicher Weise wie private Akteure am Privatrechtsverkehr teilnehmen. Wenn zum Beispiel eine Gemeinde als Eigentümerin von Immobilien also ausstehende privatrechtliche Miet- und Pachtzinsen eintreibt, handelt sie gerade nicht auf Grundlage eines Sonderrechts, das sich von denen im Verhältnis zwischen Privatpersonen geltenden Regeln unterscheidet.

Privatrechtsverkehr

Auch der EG 47 Satz 5 DS-GVO widerspricht hier im konkreten Fall nicht der Anwendbarkeit des Art. 6 Abs. 1 Buchst. f DS-GVO. Für die Aufgabenerfüllung einer Beitreibung privatrechtlicher Forderungen im vorliegenden Beispiel kann die Kommune eben gerade nicht die Schaffung eines Sonderrechts durch den (nationalen) Gesetzgeber erwarten, da ein solches in einer privatrechtlichen Beziehung zwischen Vermieterin und Mieter im Hinblick auf die bestehenden Bestimmungen des Bürgerlichen Gesetzbuches gar nicht erforderlich ist.

Kein Sonderrecht bei privatrechtlichen Beziehungen

11. Besonders sensible Daten

Rechtsvorschrift

Art. 9 DS-GVO

Art. 9 DS-GVO regelt die Verarbeitung besonderer Kategorien von besonders sensiblen personenbezogenen Daten.

Grundlegendes

Voraussetzungen Art. 6 DS-GVO müssen zusätzlich erfüllt sein

Zusätzlich zu den speziellen Anforderungen an eine Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 DS-GVO sollen gemäß EG 51 Satz 5 die allgemeinen Grundsätze und andere Bestimmungen der DSGVO gelten, insbesondere hinsichtlich der Bedingungen für eine rechtmäßige Verarbeitung (Art. 6 DS-GVO). Dies hat zur Folge, dass Art. 9 DS-GVO Art. 6 DS-GVO nicht verdrängt, sondern dessen Voraussetzungen zusätzlich zu denen des Art. 6 DSGVO vorliegen müssen.

12. Zweckänderung

Rechtsvorschrift

Art. 6 Abs. 4 DS-GVO regelt den Fall, dass eine verantwortliche Stelle personenbezogene Daten zu einem anderen Zweck verarbeiten will, als zu dem sie ursprünglich erhoben wurden.

Art. 6 Abs. 4 DS-GVO

Grundlegendes

Wenn die zweckändernde Weiterverarbeitung nicht auf einer Einwilligung oder auf einer qualifizierten Rechtsvorschrift der Union oder der Mitgliedstaaten beruht, stellt Art. 6 Abs. 4 DS-GVO Kriterien für eine dann durchzuführende Kompatibilitätsprüfung des ursprünglichen mit dem neuen Zweck der Datenverarbeitung auf. Zu der in Art. 6 Abs. 4 DS-GVO genannten Kompatibilitätsprüfung kommt man demnach nur wenn im Einzelfall keine Einwilligung bei der betroffenen Person eingeholt wurde und keine entsprechende nationale gesetzliche Regelung vorliegt.

Voraussetzungen Kompatibilitätsprüfung: Keine Einwilligung und keine gesetzliche Regelung

Ist die (Weiter-)Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, so können im Recht der Mitgliedstaaten die Aufgaben und Zwecke bestimmt werden, für die eine Weiterverarbeitung als vereinbar und rechtmäßig erachtet wird (Art. 6 Abs. 4 DS-GVO, EG 50 S. 3).

Öffentliches Interesse oder öffentliche Gewalt

Spezielle Fachgesetze, die die Übermittlung von personenbezogenen Daten regeln, wie z.B. §§ 34 und 37 BMG sind solche „Rechtsvorschriften der Mitgliedstaaten“ und insoweit können ungeachtet der Vereinbarkeit der Zwecke personenbezogene Daten (weiter-) verarbeitet werden (bei § 34 BMG in Form der Übermittlung, bei § 37 BMG in Form der Weitergabe von Meldedaten). Rechtsgrundlage für die (zweckändernde) Datenverarbeitung ist hier also das einschlägige Fachgesetz.

Vorrang von Fachgesetzen

Nach der Gesetzesbegründung zu § 5 LDSG sind von den Regelungen zur Zulässigkeit der Verarbeitung zu anderen Zwecken nicht nur die Fälle der Weiterverarbeitung zu anderen Zwecken innerhalb der verantwortlichen Stelle erfasst, sondern auch die Fälle der Datenübermittlung, soweit diese zu einem anderen als dem Erhebungszweck erfolgt und nicht auf Spezialgesetze gestützt werden kann.

Datenübermittlungen

Explizit gilt § 5 LDSG nicht für die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DS-GVO.

Ausnahme besonders sensible Daten

Sollte keine der genannten Vorschriften einschlägig sein, ist anhand der in Art. 6 Abs. 4 DS-GVO genannten Kriterien eine Kompatibilitätsprüfung durchzuführen.

Kompatibilitätsprüfung nach Art. 6 Abs. 4 DS-GVO

13. Prüfungsschema Rechtsmäßigkeit

Prüfungsschemata Rechtmäßigkeit einer Verarbeitung personenbezogener Daten

Vorprüfung:
Ist der Anwendungsbereich nach Art. 2 DS-GVO eröffnet?
Liegt ein personenbezogenes Datum vor?

1. In welcher Form liegt eine Verarbeitung personenbezogener Daten vor (Erheben, Offenlegen, Veröffentlichen, …)?

2. Welches Datum wird verarbeitet (Name, Religionszugehörigkeit, Beruf, …)?

   Wird ein sensibles Datum nach Art. 9 DS-GVO verarbeitet?

3. Welcher gesetzlicher Rechtsgrund aus Art. 6 Abs. 1 (b bis f) DS-GVO ist einschlägig?

   Müssen ggf. die Voraussetzungen des Art. 9 DS-GVO zusätzlich beachtet werden?

4. Bei Art. 6 c und e DS-GVO:
   Was ist die ausfüllende/ergänzende nationale Norm?
   (§ 4 LDSG oder besondere Rechtsvorschriften über die Verarbeitung personenbezogener Daten)

5. Ist die Erforderlichkeit beim gesetzlichen Rechtsgrund gegeben?

6. Wenn nein:
   Prüfung, ob Einwilligung eingeholt werden kann.

   Dabei ist zu beachten, dass nicht alle Sachverhalte einwilligungsfähig sind.

7. Wenn ein einwilligungsfähiger Sachverhalt vorliegt, Einwilligung als Rechtsgrundlage einholen.

14. Verarbeitungsverzeichnis

Rechtsvorschrift

Das Führen eines Verzeichnisses über Verarbeitungstätigkeiten ist in Art. 30 DS-GVO geregelt.

Art. 30 DS-GVO

Grundlegendes

Jede Gemeinde in Baden-Württemberg, unabhängig wie groß sie ist, muss ein Verarbeitungsverzeichnis erstellen, führen und regelmäßig aktualisieren. Die Ausnahme des Art. 30 Abs. 5 DS-GVO ist auf Gemeinden nicht anwendbar.

Verarbeitungsverzeichnis Pflicht

Innerhalb der Gemeinde sollte eine Organisationseinheit/Person bestimmt werden, der die Erstellung, das Führen und Aktualisieren des Verarbeitungsverzeichnisses obliegt. Es muss sichergestellt werden, dass diese von veränderten oder neuen Verarbeitungstätigkeiten zeitnah erfährt, um das Verarbeitungsverzeichnis aktuell zu halten.

Festlegung, wer Verarbeitungsverzeichnis führt

Auch Auftragsverarbeiter müssen ein Verarbeitungsverzeichnis führen, das alle Kategorien der im Auftrag des Verantwortlichen durchgeführten Verarbeitungstätigkeiten enthält, sowie die weiteren in Art. 30 Abs. 2 DS-GVO aufgeführten Angaben.

Auftragsverarbeiter

Inhalt

In das Verarbeitungsverzeichnis müssen (ganz oder teilweise) automatisierte Verarbeitungstätigkeiten sowie nichtautomatisierte Verarbeitungstätigkeiten (soweit personenbezogene Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen) aufgenommen werden

Verarbeitungstätigkeiten

Für jede einzelne Verarbeitungstätigkeit ist eine Beschreibung nach Maßgabe des Art. 30 DS-GVO anzufertigen. Das Verarbeitungsverzeichnis soll alle Verarbeitungstätigkeiten konkret abbilden, jedoch nicht zu kleinteilig sein.

Beschreibung

Als Verarbeitungstätigkeit wird im Allgemeinen ein Geschäftsprozess auf geeignetem Abstraktionsniveau verstanden. Der Begriff der „Verarbeitungstätigkeit“ umfasst alle Verarbeitungsschritte, Vorgänge und Vorgangsreihen, die einem gemeinsamen Zweck dienen.

Definition „Verarbeitungstätigkeit“

Es ist daher nicht zu jedem einzelnen Verarbeitungsschritt oder zu einer Vorgangsreihe ein eigener Verzeichniseintrag zu erstellen. Vielmehr ist ein zusammenfassender Verzeichniseintrag für die durch den Zweck verbundene Verarbeitungstätigkeit ausreichend.

Zusammenfassender Verzeichniseintrag

Verarbeitungsschritte, die nur untergeordnete Hilfsfunktion haben und damit keinem eigenen neuen Zweck, sondern letztlich nur dem Zweck der eigentlichen Verarbeitungstätigkeit dienen, müssen nicht gesondert aufgeführt werden.

Keine Aufnahme von Hilfsfunktion

Form

Das Verzeichnis ist schriftlich zu führen. Dies schließt auch ein elektronisches Format ein (Art. 30 Abs. 3 DS-GVO).

Schriftlich

Wegen der Unterschiede bei den eingesetzten Verfahren wird das Verarbeitungsverzeichnis in der Praxis notwendigerweise aus einer Reihe von Einzelverzeichnissen bestehen.

Einzelverzeichnisse

Beispiele

Beispiele für Verarbeitungszwecke (Art. 30 Abs. 1 Buchst. b DS-GVO):

Verarbeitungszwecke

- Personalaktenführung/Stammdaten
- Lohn-, Gehalts- und Bezügeabrechnung
- Arbeitszeiterfassung
- Urlaubsdatei
- Bewerbungsverfahren
- Nutzungsprotokollierungen IT/Internet/E-Mail
- Telefondatenerfassung
- Firmenparkplatzverwaltung
- Meldewesen (Melderegister)
- Wahlen (Wählerverzeichnis)
- Videoüberwachung an Arbeitsplätzen, in Schulen etc.
- Schülerverwaltung, Unterrichtsplanung, Zeugniserstellung
- Beschaffung/Einkauf sowie Finanzbuchhaltung
- Antragsbearbeitung (Bauanträge, Wohngeldanträge etc.)
- Rats- und Bürgerinformationssysteme
- Fahrerlaubnisregister und Fahrzeugregister
- Amtsärztliche Untersuchungen

Kategorien „Betroffene Personen“ und „personenbezogene Daten“

Beispiele für die Kategorie personenbezogene Daten in Verbindung mit der Kategorie Beschäftigungsverhältnisse (Art. 30 Abs. 1 Buchst. c DS-GVO):

- Mitarbeiter-Stammdaten mit Adressdaten, Geburtsdatum, Bankverbindung, Steuermerkmale, Lohngruppe, Arbeitszeit, bisherige Tätigkeitsbereiche, Qualifikationen
- Bewerbungen mit Kontaktdaten, Qualifikationsdaten, Tätigkeiten
- Arbeitszeugnisse, Leistungsdaten, Beurteilungsdaten
- Abmahnungen mit Adressdaten, Arbeitsverhalten, Leistungsdaten
- Betriebsarztuntersuchungen mit Adressdaten, Gesundheitsdaten
- Stundenplan als Einsatzplan für Lehrkräfte
- Videoüberwachung an Arbeitsplätzen

Kategorien von Empfängern

Beispiele für Kategorien von Empfängern im Zusammenhang mit Lohn- und Gehaltsabrechnungen (Art. 30 Abs. 1 Buchst. d DS-GVO):

- Banken
- Sozialversicherungsträger
- Finanzämter
- unternehmensinterne andere Datenempfänger (z.B. Betriebsrat, Fachvorgesetzte)
- ggf. Gläubiger bei Lohn-/Gehaltspfändungen
- ggf. Träger der Betriebsrente
- ggf. Auftragsverarbeiter

Mustervorlage

Eine Mustervorlage für ein ausgefülltes Verarbeitungsverzeichnis ist dieser Informationsschrift als Anlage beigefügt.

Vorlagepflicht und Einsichtsrechte

Vorlage Aufsichtsbehörde

Eine auf Antrag für jedermann zugängliche Übersicht der Verfahren, mit denen personenbezogene Daten verarbeitet werden, ist in der DS-GVO nicht mehr vorgesehen. Sie müssen jedoch den Aufsichtsbehörden (und somit auch unserer Dienststelle) jederzeit auf Anfrage zur Verfügung gestellt werden (Art. 30 Abs. 4 DS-GVO; EG 82).

LIFG

Wie andere amtliche Informationen unterliegt das Verzeichnis dem allgemeinen Informationszugangsanspruch nach dem Landesinformationsfreiheitsgesetz, so dass Auskunftsbegehren über den Inhalt der Verzeichnisse nach § 1 Abs. 2 LIFG und ggf. nach Maßgabe der Ablehnungsgründe in §§ 4 bis 6 und 9 Abs. 3 LIFG zu beurteilen sind.

15. Auftragsverarbeitung

Legaldefinition

Artikel 4
Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

8. „Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Rechtsvorschrift

Die Auftragsverarbeitung ist grundsätzlich in Art. 28 DS-GVO und EG 81 geregelt.

Art. 28 DS-GVO, EG 81

Wesen der Auftragsverarbeitung

Auch in der öffentlichen Verwaltung ist das Einsetzen von Auftragsverarbeitern (dies sind häufig spezialisierte Dienstleister) weit verbreitet. Dabei charakterisiert es den Auftragsverarbeiter, dass er nicht selbst über Zweck und Mittel der Datenverarbeitung entscheidet, sondern er lediglich als „verlängerter Arm“ der öffentlichen Stelle tätig wird. Es bleibt dabei, dass der Auftragsverarbeiter den Weisungen des Verantwortlichen unterworfen ist (Art. 29 DS-GVO).

Keine Entscheidung über Mittel und Zweck der Datenverarbeitung

Auswahlkriterien Auftragsverarbeiter

Für die Auswahl des Auftragsverarbeiters stellt Art. 28 Abs. 1 DS-GVO in klare Kriterien auf. Der Verantwortliche darf nur mit Auftragsverarbeitern zusammenarbeiten, die geeignete technische und organisatorische Maßnahmen bei der Datenverarbeitung sowie den Schutz der Betroffenenrechte garantieren können. In der Praxis stellt sich diese rechtliche Vorgabe als oftmals schwierig dar.

Eignung des Auftragsverarbeiters

Denn spezialisierte Dienstleister werden als Auftragsverarbeiter häufig aufgrund ihrer hohen Fachexpertise hinzugezogen, sodass ein Gefälle bei den technischen Kenntnissen und Fähigkeiten die Regel ist. Eine Gemeinde als verantwortliche Stelle sollte sich insbesondere vor Vertragsschluss mit dem Auftragsverarbeiter dessen Datensicherheitskonzept vorlegen lassen, das den Anforderungen des Art. 32 DS-GVO genügen muss. Dabei gilt, je sensibler die Daten sind, desto umfangreicher müssen die Datensicherungsmaßnahmen sein.

Datensicherheitskonzept des Auftragsverarbeiters

Gemeinde Adressat von Betroffenenrechte

Die DS-GVO nimmt den Auftragnehmer weitaus stärker in die Pflicht zur Einhaltung des Datenschutzrechts wie früher das LDSG a.F. Jedoch werden die datenschutzrechtlichen Pflichten des Verantwortlichen nicht abgeschwächt durch das Hinzuziehen eines Auftragsverarbeiters. Der Verantwortliche bleibt alleiniger Adressat der Betroffenenrechte (vgl. Art. 12 ff. DS-GVO). Er kann sich jedoch nach Maßgabe des Art. 28 Abs. 3 Buchst. e DS-GVO durch den Auftragsverarbeiter unterstützen lassen.

Vertrag über Auftragsverarbeitung

Schriftlicher Vertrag, auch elektronisch

Wie bisher muss der Auftragsverarbeiter einen Vertrag über die weisungsgebundene Tätigkeit abschließen (Art. 28 Abs. 3 DS-GVO), der schriftlich oder – neu – in elektronischer Form abgefasst werden kann (Art. 28 Abs. 9 DS-GVO).

Vertragsinhalt

Für den notwendigen Inhalt des Vertrags gilt weitestgehend das Gleiche wie bisher (Aufzählung des notwendigen Inhalts in Art. 28 Abs. 3 DS-GVO). Ein wichtiger Bestandteil ist jedoch vor allem die Darstellung der erforderlichen Maßnahmen zur Sicherheit der Verarbeitung nach Art. 32 DS-GVO (Art. 28 Abs. 3 Buchst. c DS-GVO).

Rechtsgrundlage für Datenübermittlung an Auftragsverarbeiter

Der Vertrag nach Art. 28 Abs. 3 DS-GVO bildet die Rechtsgrundlage für die Datenübermittlung zwischen Verantwortlichem und Auftragsverarbeiter. Der Auftragsverarbeiter ist im Verhältnis zum Verantwortlichen nicht „Dritter“ im Sinne des Art. 4 Nr. 10 DSGVO, sondern „Empfänger“ im Sinne des Art. 4 Nr. 9 DSGVO.

Formulierungshilfe

Eine Formulierungshilfe für einen Vertrag zur Auftragsverarbeitung kann unserer Internetseite entnommen werden.

Abgrenzung Verantwortlicher und Auftragsverarbeiter

Für die Abgrenzung zwischen Verantwortlichem und Auftragsverarbeiter nach der DS-GVO empfiehlt es sich, auf die anhand der Datenschutz-Richtlinie 95/46/EG von der Artikel-29-Datenschutzgruppe herausgearbeiteten Kriterien abzustellen:

Abgrenzungskriterien

- Ausführliche, dem Auftragsverarbeiter wenig Spielraum gebende Weisungen sind ein Indiz für eine Auftragsverarbeitung.
- Eine vertraglich vorgesehene und tatsächlich ausgeführte permanente Beaufsichtigung seitens des Auftraggebers ist ein Indiz für eine vollständige alleinige Kontrolle über die Verarbeitungsvorgänge und damit für eine Auftragsverarbeitung.
- Die traditionelle Rolle und Fachkompetenz des Dienstleisters kann eine entscheidende Rolle bei der Einstufung spielen. Rechtsanwälte verarbeiten personenbezogene Daten zwar aufgrund eines Mandats des Klienten, der Schwerpunkt dürfte jedoch weiterhin auf der berufsständisch verankerten unabhängigen Tätigkeit liegen. Gleiches gilt grundsätzlich für Rechnungsprüfer und Steuerberater. Generell sind sie ähnlich den Rechtsanwälten als Verantwortliche einzuordnen und sollen daher nur ausnahmsweise bei klar umrissenen und ausführlichen Weisungen unterliegenden Tätigkeiten als Auftragsverarbeiter einzustufen sein.

Vermeidung des Begriffs „Funktionsübertragung“

Bisher wurde nach deutschem Recht als Gegenbegriff zur weisungsgebundenen Auftragsverarbeitung der Begriff der „Funktionsübertragung“ verwendet. Für die Zukunft sollte man den Begriff der Funktionsübertragung jedoch vermeiden, denn die DS-GVO hat bezüglich des Hinzuziehens anderer Stellen, die im Interesse des Verantwortlichen eine Datenverarbeitung vornehmen, andere Vorstellungen. Entweder handeln diese als völlig eigenständige Verantwortliche oder als Auftragsverarbeiter.

Haftung durch Auftragsverarbeiter

Haftung bei Pflichtverletzung

Gemäß Art. 82 Abs. 2 S. 2 DS-GVO haftet der Auftragsverarbeiter für den durch eine Datenverarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten nicht nachgekommen ist oder entgegen der Anweisung des Verantwortlichen (respektive der Gemeinde) gehandelt hat.

Zulässigkeitseinschränkungen

Einschränkungen durch fachspezifische Regelungen

Die Zulässigkeit einer Auftragsverarbeitung kann im öffentlichen Bereich durch nationales Recht eingeschränkt (Öffnungsklausel Art. 6 Abs. 2 und 3 DS-GVO) sein. Überlegen öffentliche Stellen, Auftragsverarbeiter hinzuzuziehen, sollten sie vorab prüfen, ob fachspezifische Regelungen dies beschränken oder sogar ausschließen.

Beispiele

Beispiele für einschränkende Regelungen:

- Patientendaten gemäß § 48 Landeskrankenhausgesetz
- Sozialdaten gemäß § 80 SGB X
- Personalaktendaten gemäß § 85a Landesbeamtengesetz
- Steuerdaten gemäß § 30 Abs. 9 Abgabenordnung

Anpassung bestehender Verträge

Bestehende Verträge zur Auftragsverarbeitung sind an die Anforderungen des Art. 28 Abs. 3 DSGVO anzupassen. Dabei sind vor allem folgende Punkte zu prüfen:

Fragen zur Ermittlung eines Anpassungsbedarfs

- Werden der Gemeinde als Auftraggeber wirksame Kontrollrechte eingeräumt (Art. 28 Abs. 3 Satz 2 Buchst. h DSGVO)?
- Werden der Gemeinde wirksame Weisungsrechte eingeräumt?
- Ist die Beauftragung von Unterauftragsverarbeitern vertraglich geregelt (Art. 28 Abs. 3 Satz 2 Buchst d und Art. 28 Abs. 2 und 4 DSGVO)?
- Hat der Auftragnehmer einen Datenschutzbeauftragten und einen gemeindlichen Ansprechpartner bei auftretenden Problemen?
- Bestehen ausreichende Mitwirkungspflichten des Auftragnehmers bei der Erfüllung der Rechte der betroffenen Person gemäß Art. 28 Abs. 3 Satz 2 Buchst. e DSGVO (wie etwa auf Auskunft, Löschung oder Widerspruch) und bei Verletzungen des Schutzes personenbezogener Daten sowie ggf. einer erforderlichen Datenschutz-Folgenabschätzung (Art. 28 Abs. 3 Satz 2 Buchst. f DSGVO)?
- Sind Haftungsbeschränkungen zum Nachteil der Gemeinde im Vertrag enthalten?

Übersicht über die wichtigsten Neuerungen und Pflichten des Auftragsverarbeiters

Vorliegend eine Übersicht über die wichtigsten Neuerungen und Pflichten des Auftragsverarbeiters
(nicht abschließend):

1) **Rechtmäßigen Weisungen des Auftraggebers folgen**: Verstößt ein Auftragsverarbeiter gegen die Pflicht zur weisungsgebundenen Verarbeitung, indem er die Zwecke und Mittel selbst bestimmt, gilt er nach Art. 28 Abs. 10 DS-GVO insoweit selbst als Verantwortlicher (mit allen rechtlichen Folgen, z.B. auch zur Erfüllung der Betroffenenrechte).
2) **Haftungsregeln** (Art. 82 DS-GVO): Demnach drohen dem Auftragsverarbeiter bei Verstößen auch Schadensersatzforderungen von Betroffenen.
3) **Führen eines Verarbeitungsverzeichnisses** (Art. 30 Abs. 2 DS-GVO): für alle Kategorien der im Auftrag des Verantwortlichen durchgeführten Verarbeitungstätigkeiten.
4) **Meldepflicht bei Datenpannen** (Art. 33 Abs. 2 DS-GVO) an den Verantwortlichen
5) **ggf. Benennen eines Datenschutzbeauftragten** (Art. 37 DS-GVO)
6) **Umsetzung geeigneter technischer und organisatorischer Maßnahmen** für ein angemessenes Schutzniveau (Art. 32 DS-GVO)

16.Datenschutz-Folgenabschätzung

Rechtsvorschrift

Für die Datenschutz-Folgenabschätzung (DSFA) sind die Art. 35 und 36 DS-GVO grundlegend. Zudem sind die EG 84, 89 bis 96 zu berücksichtigen.

Art. 35 und 36DS-GVO sowie EG 84, 89 bis 96

Bedeutung

Die Datenschutz-Folgenabschätzung ist das im Planungsstadium einer beabsichtigten Verarbeitung personenbezogener Daten vorgesehene Instrument der DS-GVO zur Risikoanalyse und -bewertung und damit ein wesentlicher Teil des Datenschutz-Managementsystems.

Instrument zur Risikoanalyse und -bewertung

Eine geplante Datenverarbeitung mit voraussichtlich hohen Risiken für die Rechte und Freiheiten natürlicher Personen bedarf nach den Datenschutzgrundsätzen der DS-GVO zwingend präventiver Maßnahmen vor der Verarbeitung personenbezogener Daten. Die DSFA trägt daher wesentlich zur Minimierung von Datenschutzrisiken bei.

Minimierung von Datenschutzrisiken

Beiziehung unserer Dienststelle

Bei hohen Risiken, denen nicht durch technisch-organisatorische oder andere Maßnahmen abgeholfen werden kann, muss gemäß Art. 36 DS-GVO unsere Dienststelle beigezogen werden.

Bei hohen Risiken, denen nicht abgeholfen werden kann: Hinzuziehung LfDI

Aufsichtsbehördliche Liste mit Regelfällen

Eine nicht abschließende, sog. Muss- und Muss-nicht-Listen mit Regelfällen, wann eine DSFA notwendig ist auf unserer Internetseite (https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Liste-von-Verarbeitungsvorgängen-nach-Art.-35-Abs.-4-DS-GVO-LfDI-BW.pdf) abrufbar. Die Liste wurde zwar für den nicht-öffentlichen Bereich erstellt, kann jedoch auch für den öffentlichen Bereich verwendet werden.

Muss- und Muss-nicht-Listen

Schwellwertanalyse

Findet sich die geplante Verarbeitung nicht in den Muss- oder Muss-nicht-Listen der Aufsichtsbehörden, kann mit einer Schwellwertanalyse die Notwendigkeit einer DSFA ermittelt werden. Diese erfolgt nach Artikel 35 Absatz 4 DS-GVO in Verbindung mit dem Working-Paper 248 der Artikel 29-Gruppe.

Wenn Verarbeitung nicht in Muss- und Muss-nicht-Listen, dann Schwellwertanalyse

Kriterien Schwellwertanalyse

Die Kriterien der Schwellwertanalyse sind:

1. Bewerten oder Einstufen
2. Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
3. Systematische Überwachung
4. Vertrauliche Daten oder höchst persönliche Daten, insbesondere nach Art. 9 DS-GVO
5. Datenverarbeitung in großem Umfang
6. Abgleichen oder Zusammenführen von Datensätzen
7. Daten zu schutzbedürftigen Betroffenen
8. Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen
9. Hürde für den Betroffenen, ein Recht auszuüben bzw. einen Dienst nutzen zu können

Kriterien zur Feststellung, ob hohes Risiko vorliegt

Sind zwei oder mehr dieser Kriterien erfüllt, so ist vielfach ein hohes Risiko gegeben und eine DSFA durch den Verantwortlichen durchzuführen. Eine DSFA kann aber auch dann erforderlich sein, wenn nur ein Kriterium erfüllt wird.

Dokumentation der DSFA

Kommt die Schwellwertanalyse zu dem Schluss, dass keine DSFA durchgeführt werden muss, ist dennoch eine Dokumentation über die Risiken und die Entscheidungsgründe durchzuführen.

Vorgehensweise bei DSFA

Phasen einer DSFA

Jede Verarbeitungstätigkeit muss vor der Datenerhebung und vor wesentlichen Änderungen auf ihr Risikopotenzial geprüft werden. Danach folgen grob die Phasen der Beschreibung der Verarbeitung, der rechtlichen Grundlagen, der Risikobeurteilung/-bewertung und der Abhilfemaßnahmen für die erkannten Risiken.

DSK-Kurzpapier

Eine DSFA ist ein umfangreicher Prozess, bei dem alle Datenflüsse und Verarbeitungen zu betrachten und in einer Risikoabschätzung zu bewerten sind. Ein detaillierter Ablauf wird in dem DSK Kurzpapier Nr. 5 beschrieben.

Beispiele und Anhaltspunkte für eine DSFA

LDA Bayern

Ein Beispiel einer DSFA, angelehnt an die internationalen Normen der ISO/IEC 27000-Reihe und der ISO/IEC 29134, ist unter https://www.lda.bayern.de/de/thema_dsfa.html abrufbar.

Fraunhofer-Institut

Auch das White Paper Datenschutz-Folgenabschätzung des Forum Privatheit des Fraunhofer-Instituts für System- und Innovationsforschung kann wesentliche Anhaltspunkte für ein konkretes Vorgehen geben.

Bitkom

Zudem kann der Leitfaden zu Risk-Assessment und Datenschutz-Folgenabschätzung der Orientierung dienen.

Beratung durch LfDI

Für schwierige Rechts-, Auslegungs- und Anwendungsfragen steht unsere Dienststelle den baden-württembergischen Gemeinden beratend zur Seite.

Mögliche Folgen einer Nichtdurchführung

Bußgelder bei Rechtsregime BDSG

Wird trotz hoher Risiken keine DSFA durchgeführt, drohen dem Verantwortlichen grundsätzlich Bußgelder durch die jeweilige Aufsichtsbehörde. Im kommunalen Bereich ist dies nur der Fall, wenn eine verantwortliche Stelle dem Rechtsregime des BDSG unterliegt. Dies gilt grundsätzlich nicht, soweit Gemeinden als Gebietskörperschaften verantwortliche Stellen sind.

Bußgelder gegen Mitarbeiter

Bußgelder können auch bei Verstößen, die einzelnen Mitarbeitern (und nicht der Gemeinde) zuzurechnen sind, verhängt werden.

Anordnung oder Untersagung

Unsere Dienststelle kann eine DSFA anordnen oder eine Datenverarbeitung ohne DSFA untersagen.

Veröffentlichungen und zivil-rechtliche Forderungen

Nicht zuletzt kann dies Folgen für das Ansehen einer verantwortlichen Stelle haben, da die Aufsichtsbehörden verhängte Bußgelder, Anordnungen und sonstige Maßnahmen veröffentlichen können. Außerdem kann eine fehlende DSFA eventuell zivilrechtliche Forderungen nach sich ziehen.

17. Betroffene

Grundlegendes

Definition „Betroffener“

Betroffen im datenschutzrechtlichen Sinne ist eine natürliche Person, deren personenbezogene Daten von einem Dritten (wie einem Verein, einem Unternehmen oder einer Gemeinde) verarbeitet werden. Nicht unmittelbar betroffen ist eine Person, wenn Datenverarbeitungen Andere und nicht die eigene Person betreffen. Nur Betroffene im datenschutzrechtlichem Sinne (und deren Vertretungsbefugte) können ihre eigenen Rechte wahrnehmen.

Natürliche Personen

Das informationelle Selbstbestimmungsrecht in der Ausgestaltung der Datenschutz-Grundverordnung gilt für natürliche Personen.

Juristische Personen

Keine natürlichen Personen sind juristische Personen (wie beispielsweise Unternehmen, die in Form einer GmbH oder AG geführt werden, oder Vereine). Juristische Personen sind keine Träger des Rechts auf informationelle Selbstbestimmung, müssen jedoch datenschutzrechtliche Vorschriften beachten, wenn sie als Verantwortliche personenbezogene Daten verarbeiten.

Verstorbene

Auch Verstorbene sind keine natürlichen Personen im Sinne datenschutzrechtlicher Vorschriften, da das Grundrecht auf informationelle Selbstbestimmung mit dem Tode des jeweils Betroffenen erlischt. Anders verhält es sich beispielsweise mit der Menschenwürde, die auch nach dem Tode einer Person fortwirkt (postmortale Wirkung).

Vertretungsbefugnis

Gesetzliche Regelungen oder Vollmacht

Immer wieder wenden sich Personen für andere (wie Ehepartner oder volljährige Kinder) an unsere Dienststelle, die aus datenschutzrechtlicher Sicht über die erforderliche Einsichts- und Handlungsfähigkeit verfügen, und somit grundsätzlich selbst datenschutzrechtliche Erklärungen abzugeben haben. Personen, die nicht selbst Betroffene sind, sondern für andere tätig werden wollen, benötigen eine Vertretungsbefugnis. Diese kann sich etwa aufgrund gesetzlicher Regelungen ergeben, wie beispielsweise bei einem für ein Kleinkind personensorgeberechtigtes Elternteil oder aufgrund einer wirksamen Vollmacht, die etwa einem Rechtsanwalt oder einem Ehepartner erteilt wurde. Für Betroffene handelnde Personen haben ihre Vertretungsbefugnis anzuzeigen und müssen diese auf Anforderung belegen können.

Vollmacht

Allgemein muss einer schriftlichen Vollmacht eindeutig und klar zu entnehmen sein, wer für den Betroffenen in datenschutzrechtlichen Angelegenheiten vertretungsbefugt ist.

Minderjährige

Bei Minderjährigen ist zu beachten, dass sich bei datenschutzrechtlichen Erklärungen der Entscheidungsspielraum der Eltern (oder anderen Personensorgeberechtigten) in dem Maße verringert, in dem die Einsichtsfähigkeit der Minderjährigen zunimmt. Dabei kommt es im jeweiligen Einzelfall darauf an, ob Minderjährige in der Lage sind, die Konsequenzen der Verwendung ihrer Daten zu übersehen und sie sich insoweit hierzu verbindlich äußern können. Im Sinne einer Regelannahme kann mit Vollendung des 16. Lebensjahres grundsätzlich davon ausgegangen werden, dass die erforderliche Einsichtsfähigkeit vorliegt.

Hinweisgeber

Keine Betroffeneneigenschaft

Hinweisgeber sind Personen, denen es nicht um die Verarbeitung ihrer eigenen Daten geht und die auch keine Vertretungsbefugnis für andere Personen haben. Es fehlt ihnen deshalb an der Betroffeneneigenschaft. Im Rahmen unserer gesetzlichen Aufgaben und mit Blick auf die Vielzahl von Eingaben sowie anhängigen datenschutzrechtlichen Verfahren äußert sich unsere Dienststelle grundsätzlich nur gegenüber datenschutzrechtlich Betroffenen und den datenschutzrechtlich verantwortlichen Stellen, nicht jedoch gegenüber Dritten (wie Hinweisgebern). Das bedeutet, dass wir Dritten in der Regel weder mitteilen, ob wir eine datenschutzrechtliche Prüfung vornehmen, noch äußern wir uns gegebenenfalls zu dem Ergebnis einer datenschutzrechtlichen Prüfung. Vielmehr informieren wir die Allgemeinheit über entsprechende Sachverhalte (wie beispielsweise mittels Pressemitteilung oder Beitrag in unserem Tätigkeitsbericht), falls dies aus unserer Sicht im Einzelfall geboten ist.

Allgemeine Fragen und Hinweise zum Datenschutzrecht

Hinweise oder Anhaltspunkte für Rechtsverletzungen

Mit allgemeinen Eingaben zum Datenschutzrecht, denen weder eine Beratungsanfrage einer verantwortlichen Gemeinde noch eine Beschwerde eines datenschutzrechtlichen Betroffenen zu Grunde liegt, können wir uns aufgrund des anhaltend hohen Arbeitsaufkommens oft nur nachrangig befassen. Auch können wir nicht immer dann tätig werden, wenn aufgrund eines Vorbringens eine Verletzung von datenschutzrechtlichen Vorschriften theoretisch nicht kategorisch ausgeschlossen werden kann. Vielmehr bedarf es grundsätzlich konkreter Hinweise oder zumindest substanzieller Anhaltspunkte für eine eventuelle unzulässige Verarbeitung von personenbezogenen Daten.

18. Betroffenenrechte

Grundlegendes

Rechte und Rechtsvorschriften

Datenschutzrechtlich Betroffene haben eine Vielzahl von Rechten. Es gibt Informationsrechte

- bei der Datenerhebung (Art. 13 u. 14 DS-GVO) und
- beim Vorliegen von bestimmten Datenpannen (Art. 34 DS-GVO).

Des Weiteren müssen Gemeinden auf Antrag von Betroffenen tätig werden, wie etwa bei Anträgen auf

- Auskunft (Artikel 15 DS-GVO),
- Berichtigung (Artikel 16 DS-GVO),
- Löschung (Artikel 17 DS-GVO) oder
- Einschränkung der Verarbeitung (Art. 18 DS-GVO).

Auch gehören hierzu

- das Recht auf Datenübertragbarkeit (Art. 20 DS-GVO),
- das Widerspruchsrecht des Betroffenen (Art. 21 DS-GVO) und
- Regelungen zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling (Art. 22 DS-GVO).

Einschaltung behördlicher Datenschutzbeauftragter

Zudem können Betroffene sich an gemeindliche Datenschutzbeauftragte mit der Bitte um Beratung und Unterstützung wenden, soweit es ihnen um die Verarbeitung ihrer Daten geht (Art. 38 Abs. 4 DS-GVO).

Anrufung LfDI

Des Weiteren können sie unsere Dienststelle einschalten, wenn sie der Auffassung sind, die Verarbeitung ihrer Daten durch eine Gemeinde verletze sie in ihren Rechten (§ 25 Abs. 3 LDSG).

Broschüre „Betroffenenrechte“ des LfDI

Weitere Informationen zu Betroffenenrechten können der Broschüre „Betroffenenrechte“ unserer Dienststelle entnommen werden.

Art. 12 DS-GVO als Generalklausel

Sinn und Zweck von Art. 12 DS-GVO

Art. 12 DS-GVO regelt für bestimmte Sachverhalte (Art. 13 bis 22 und 34 DS-GVO) allgemeine Vorgaben für die Unterrichtung von Betroffenen durch Gemeinden und enthält Verfahrensregeln bei der Ausübung von Betroffenenrechten.

Einfache Ausübung von Betroffenenrechten und Transparenz

Art. 12 Abs. 1 DS-GVO verpflichtet eine Gemeinde (und zwar bereits bevor eine Datenverarbeitung stattfindet), geeignete Maßnahmen für eine transparente Informationspolitik der Gemeinde zu treffen, um Betroffenen die Ausübung ihrer Rechte zu erleichtern.

Vorbereitung erforderlich

Um den datenschutzrechtlichen Anforderungen an die Wahrung der Betroffenenrechte hinreichend Rechnung tragen zu können, hat eine

Gemeinde bereits im Voraus klare interne Regelungen zu Zuständigkeiten, Abläufen und Prozessen sowie damit verbundene erforderliche technische und organisatorische Maßnahmen zu treffen.

Form und Sprache

Informationen, Hinweise und Mitteilungen an Betroffene sind in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache abzufassen. Dabei ist ein adressatenorientierter Maßstab anzulegen. Dies gilt besonders, wenn Informationen an Kinder gerichtet sind. Die Übermittlung entsprechender Inhalte kann grundsätzlich schriftlich, elektronisch und falls vom Betroffenen verlangt, auch mündlich erfolgen.

Präzise

Präzise bedeutet, Informationen vollständig sowie inhaltlich richtig und dennoch so kurz wie möglich abzufassen.

Transparent

Transparent sind Informationen, die vom Betroffenen ohne weiteres nachvollzogen werden können.

Verständlich

Verständlichkeit setzt u. a. voraus, dass der Betroffene den Inhalt und die Bedeutung der Informationen erfassen kann.

Leicht zugänglich

Leicht zugänglich sind Informationen, die der Betroffene sich mit dem ihm zur Verfügung stehenden Mitteln ohne zusätzlichen Aufwand erschließen kann. Hierunter fällt auch die Barrierefreiheit von Informationen.

Einfache, kurze Sätze

Zu einer einfachen und klaren Sprache gehört die Vermeidung von Fachbegriffen und Fremdwörtern. Hiervon sind zudem einfache und kurze Sätze umfasst.

Identifizierung eines Betroffenen

Datensparsamkeit

Eine Gemeinde ist verpflichtet, alle ihr möglichen und vertretbaren Mittel zu nutzen, um einen Betroffenen zu identifizieren. Dabei ist das Gebot der Datensparsamkeit zu beachten. Das heißt, es dürfen nur die und nur so viele Daten vom Betroffenen erhoben werden, wie zu seiner Identifizierung erforderlich sind (kein Datenüberschuss). Reichen einer Gemeinde die ihr vorliegenden Informationen nicht aus, um einen Betroffenen eindeutig zu identifizieren, kann sie weitere Informationen von diesem anfordern.

Folgen unzureichender Identifizierung

Wenn eine Identifizierung nicht möglich ist, hat die Gemeinde

- die betroffene Person hierüber zu informieren, soweit ihr dies möglich ist, und
- diese aufzufordern, zusätzliche Informationen bereitzustellen, die eine eindeutige Identifizierung ermöglichen.

Dies setzt jedoch begründete Zweifel im Einzelfall voraus.

Fristlauf nach Identifizierung

Wenn zusätzliche Informationen zur eindeutigen Identifizierung des Betroffenen erforderlich sind, beginnt die Monatsfrist zur Bearbeitung des Antrags erst dann zu laufen, wenn der Gemeinde die zusätzlich angeforderten Nachweise vorliegen.

Kein gemeindliches Tätigwerden

Ist eine Gemeinde letztlich nicht in der Lage, den Betroffenen hinreichend klar zu identifizieren, kann sie sich weigern, aufgrund von Anträgen gemäß Art. 15 bis 22 DS-GVO tätig zu werden.

Definition „glaubhaft“

Glaubhaft machen setzt voraus, dass eine Gemeinde in nachvollziehbarer Weise darlegen kann, warum es ihr nicht möglich ist, eine Person hinreichend klar zu identifizieren und welche Schritte sie ohne Erfolg eingeleitet hat, dem abzuhelfen.

Praxisfall

Gemeinden führen in Verwaltungsverfahren mit Betroffenen oftmals über einen längeren Zeitraum hinweg auf postalischem Wege einen regen Schriftwechsel. In einem Fall forderte bei einem Auskunftsverlangen eine Gemeinde den Betroffenen auf, entweder eine Personalausweiskopie vorzulegen oder persönlich zu erscheinen, um sich hinreichend zu identifizieren. Und das, obwohl der Betroffene der Gemeindeverwaltung persönlich bekannt war. Warum die Gemeinde auf einmal Zweifel an der Identität des Betroffenen hatte, konnte uns nicht darlegt werden. Vor diesem Hintergrund konnten wir insoweit auch nicht erkennen, dass weitere Informationen für eine Identifizierung erforderlich waren.

Frist

Grundsatz unverzüglich

Gemeinden müssen entsprechend Art. 12 Absatz 3 DS-GVO betroffenen Person in der Regel unverzüglich (das bedeutet ohne schuldhaftes Zögern) Informationen über die auf einen Antrag gemäß den Art. 15 bis 22 DS-GVO ergriffenen Maßnahmen zur Verfügung zu stellen, grundsätzlich jedoch spätestens innerhalb eines Monats nach Eingang des Antrags. Dies erfordert seitens der Gemeinden, dass sie sich auf den möglichen Eingang entsprechender Anträge hinreichend vorbereiten und bei der Informationserteilung ein straffes Zeitmanagement walten lassen müssen.

Fristverlängerung

Die Monatsfrist kann um zwei weitere Monate verlängert werden, wenn dies aufgrund der Komplexität des Antrags des Betroffenen und in der Gesamtschau der Anzahl aller ihr vorliegender datenschutzrechtlicher Anträge (nicht nur die des Betroffenen) erforderlich ist. Betroffene sind innerhalb eines Monats über eine Fristverlängerung und die Gründe hierfür zu informieren. Grundsätzlich sollte diese Information auf dem gleichen Weg erfolgen, wie der Antrag des Betroffenen.

Information bei Untätigkeit

Gründe darlegen und auf Rechtsbehelfe hinweisen

Nicht jeder Antrag eines Betroffenen erfordert, dass eine Gemeinde sich inhaltlich näher mit diesem befasst. Dies kann etwa der Fall sein, wenn ein Antragsteller nicht hinreichend klar identifiziert werden kann oder ein exzessiver Antrag vorliegt. Wenn eine Gemeinde untätig bleibt, muss sie gemäß Artikel 12 Abs. 4 DS-GVO den Antragsteller über die Gründe hierfür und die Möglichkeit der Beschwerde bei unserer Dienststelle oder des Einlegens eines gerichtlichen Rechtsbehelfs informieren. Grundsätzlich sollte diese Information auf dem gleichen Weg erfolgen, wie der Antrag des Betroffenen.

Kostenfreiheit

Grundsatz Kostenfreiheit

Art. 12 Abs. 5 S. 1 DS-GVO regelt, dass Informationen gemäß den Artikeln 13 und 14 DS-GVO (Informationspflichten bei Datenerhebungen) sowie alle Mitteilungen und Maßnahmen gemäß den Artikeln 15 bis 22 DS-GVO (Auskunft, Berichtung, Löschung usw.) und Artikel 34 DS-GVO (Informationspflichten bei Datenpannen) grundsätzlich kostenfrei zur Verfügung gestellt werden. Ausnahmen von der Kostenfreiheit gibt es bei mehrfacher Anforderung von Datenkopien sowie offenkundig unbegründeten und exzessiven Anträgen.

Unbegründete und exzessive Anträge

Entgelt oder Weigerung, tätig zu werden

Bei offenkundig unbegründeten oder exzessiven Anträgen hat eine Gemeinde nach Art. 12 Abs. 5 S. 2 DS-GVO die Wahlmöglichkeit, entweder ein angemessenes Entgelt zu verlangen oder sich zu weigern, tätig zu werden. Den Nachweis für die Unbegründetheit oder das Vorliegen eines Exzesses hat die Gemeinde zu führen.

Offenkundig unbegründet

Offenkundig unbegründet ist ein Antrag, wenn die Voraussetzungen für das jeweilige Betroffenenrecht offensichtlich nicht vorliegen.

Exzessiv

Exzessiv ist ein Antrag, der häufig wiederholt wird. Exzessiv kann auch ein rechtsmissbräuchlicher Antrag sein, der etwa zum Ziel hat, eine Gemeinde allgemein bei ihrer Aufgabenerfüllung zu behindern oder zu stören.

Mögliche Vorgehensweise bei Anträgen und Beschwerden

In vielen Fällen bietet sich bei der Geltendmachung von Betroffenenrechten sowie bei Beschwerden folgende Vorgehensweise an:

1. **Gemeinde**
   Anträge und Beschwerden sollten zunächst bei der Gemeinde als für die Datenverarbeitung verantwortlicher Stelle eingereicht bzw. eingelegt werden.

2. **Behördlicher Datenschutzbeauftragter**
   Den behördlichen Datenschutzbeauftragten der Gemeinde um Beratung und Unterstützung bitten, wenn diese nicht oder nur unzureichend tätig wird.

3. **Landesbeauftragter für den Datenschutz und die Informationsfreiheit**
   Einschaltung unserer Dienststelle als datenschutzrechtliche Aufsichtsbehörde, wenn die Gemeinde dem Anliegen nicht oder nicht hinreichend abhilft und aus Sicht des Betroffenen insoweit eine Rechtsverletzung vorliegen könnte.

4. **Gerichtlicher Rechtsbehelf**
   Eine weitere Möglichkeit kann je nach Sachverhalt und Intension des Betroffenen – unabhängig von der Einschaltung unserer Dienststelle – das Einlegen eines gerichtlichen Rechtsbehelfs sein.

Verantwortliche Gemeinde

Erste Anlaufstelle Gemeinde

Anträge und Beschwerden von Betroffenen sollten zunächst an die für die Datenverarbeitung verantwortliche Gemeinde gerichtet werden. In Fällen, in denen sich Betroffene mit Beschwerden direkt an unsere Dienststelle wenden, ohne sich zuvor an die für die Datenverarbeitung verantwortliche Stelle zu wenden, kommt es immer wieder vor, dass sich Anliegen nach Kontaktaufnahme mit der Gemeinde zügig regeln lassen. Dies gilt insbesondere, wenn dem Anliegen ein Missverständnis oder ein einfacher Fehler in der Einzelfallbearbeitung zu Grunde liegt. Wenden Betroffene sich in solchen Fällen unmittelbar an die Gemeinde, lassen sich entsprechende Sachverhalte in aller Regel schnell und einfach unmittelbar mit der für die Datenverarbeitung verantwortlichen Stelle klären.

Mögliche Rechtsverletzung darlegen

Nur wenn eine Gemeinde nachvollziehen kann, was für ein Antrag mit welchem Inhalt gestellt wird oder warum sich ein Betroffener in seinen Rechten verletzt fühlt bzw. von welchem Recht er wie Gebrauch machen möchte, kann sie auch im Sinne des Betroffenen tätig werden und den entsprechenden Sachverhalt prüfen. Deshalb sollte der zu Grunde liegende Sachverhalt vom Betroffenen mit einfachen, verständlichen und zutreffenden Worten geschildert bzw. dargelegt werden. Dem Vorbringen sollte u. a. entnommen werden können, warum möglicherweise eine Rechtsverletzung vorliegt sowie genau beschreiben werden, was man von der Gemeinde erwartet/fordert.

Empfehlung Schriftform

Wegen der späteren Nachprüfbarkeit empfehlen wir Betroffenen, Anträge schriftlich zu stellen (auch wenn die Schriftform nicht erforderlich ist) und eine Mehrfertigung des Antrages zu den eigenen Unterlagen zu nehmen.

Musterbrief

In unserem Internetauftritt ist auf der Seite „Datenschutzthemen“ in der Kategorie „Betroffenenrechte“ ein Musterbrief für ein Erstanschreiben an einen Verantwortlichen abrufbar (https://www.baden-wuerttemberg.datenschutz.de/datenschutzthemen/).

Behördliche Datenschutzbeauftragte

Unterstützung und Beratung für Betroffene

Datenschutzrechtlich Betroffene können gemäß Art. 38 Abs. 4 DS-GVO sich an behördliche Datenschutzbeauftragte mit allen Fragen wenden und diese zu Rate ziehen, soweit es um die Verarbeitung ihrer personenbezogenen Daten und die Wahrnehmung ihrer diesbezüglichen Rechte geht.

Empfehlung Schriftform

Grundsätzlich empfiehlt es sich auch hier, eine entsprechende Anfrage schriftlich einzureichen und dabei möglichst genau zu beschreiben, worum es geht.

Gerichtlicher Rechtsbehelf

Rechtsbeistand konsultieren

Unabhängig davon, ob sich ein Betroffener an unsere Dienststelle wendet, kann dieser in Erwägung ziehen, seine Rechte auch gerichtlich durchzusetzen. Vor Beschreitung des Rechtswegs empfehlen wir, sich vorher von einem Rechtsbeistand (beispielsweise einem Rechtsanwalt) rechtlich beraten zu lassen, um nach Möglichkeit unnötige Kosten und zeitlichen Aufwand zu vermeiden.

Verwaltungsverfahren

Anrufung LfDI hat keine unmittelbare Auswirkung auf Verwaltungsverfahren.

Bei laufenden Verwaltungsverfahren ist zu beachten, dass die Anrufung unserer Dienststelle (formloser Rechtsbehelf) keine unmittelbare Auswirkung auf diese hat. Dies gilt auch für Fristen in Verwaltungsverfahren und mögliche Folgen bei Fristversäumnissen. So sind beispielsweise trotz Anrufung unserer Dienststelle Zahlungsfristen in Verwaltungsverfahren beachtlich und können bei Nichtbeachtung Folgen bis hin zur Vollstreckung nach sich ziehen.

Spezifischer Rechtbehelf für Verwaltungsverfahren einlegen

Häufig ergeht in einem Verwaltungsverfahren ein Verwaltungsakt (wie beispielsweise bei Gebührenbescheiden). Gegen Verwaltungsakte kann Widerspruch eingelegt werden. Wird dem Widerspruch von der Widerspruchsbehörde (in der Regel die Gemeinde selbst) nicht abgeholfen, ist es möglich, Klage vor dem Verwaltungsgericht einzulegen. In der Regel haben Verwaltungsakte am Ende eine Rechtsmittelbelehrung, der näheres hierzu entnommen werden kann.

Landesbeauftragter für den Datenschutz und die Informationsfreiheit

Betroffene können LfDI bei Rechtsverletzungen anrufen

Jede betroffene Person hat unabhängig davon, welche der oben genannten Maßnahmen sie ergreift, das Recht auf Beschwerde bei unserer Dienststelle, wenn sie der Ansicht ist, bei der Verarbeitung von Daten über ihre Person in ihren Rechten verletzt worden zu sein. Auf unserer Internetseite ist ein Online-Beschwerdeformular eingestellt, das Betroffene verwenden oder an dem sie sich bei der Einreichung einer Beschwerde orientieren können (https://www.baden-wuerttemberg.datenschutz.de/online-beschwerde/).

Rechte von Betroffenen gegenüber LfDI

Die Anrufung unserer Dienstelle vermittelt einem Betroffenen, der aufgrund der Verarbeitung seiner Daten eine Verletzung seiner Rechte geltend macht, einen Anspruch auf Entgegennahme seiner Eingabe, eine sachliche Prüfung (hinsichtlich einer möglichen Verletzung seines informationellen Selbstbestimmungsrechts) und eine Antwort unserer Dienststelle. Einen Anspruch von Betroffenen auf eine bestimmte Vorgehensweise oder ein bestimmtes Ergebnis gegenüber unserer Dienststelle gibt es hingegen nicht. Unabhängig davon ist es Betroffenen, die unsere Dienststelle angerufen haben, selbstverständlich unbenommen, weitere in unserer Rechtsordnung für den jeweiligen Sachverhalt vorgesehene Rechtsbehelfe einzulegen.

Einholung Stellungnahme bei Gemeinden

In vielen Fällen ist bei der datenschutzrechtlichen Prüfung von Sachverhalten die Einholung einer gemeindlichen Stellungnahme erforderlich, oft unter Nennung des Namens des Betroffenen und Angabe seiner Adressdaten. Die Nennung von Namen und Adressdaten bei der Einholung einer Stellungnahme erfolgt in der Regel nur, wenn der Betroffene hierzu zuvor sein Einverständnis erteilt hat. Nach Eingang der angeforderten Stellungnahme beurteilen wir das Anliegen des Betroffenen in datenschutzrechtlicher Hinsicht und teilen danach diesem und der verantwortlichen Gemeinde das Ergebnis unserer Prüfung mit.

Mögliches Fehlverhalten von Gemeindemitarbeitern

Immer wieder erreichen unsere Dienststelle Eingaben, die ein mögliches persönliches Fehlverhalten von Gemeindemitarbeitern (und nicht eine rechtswidrige Datenverarbeitung der verantwortlichen Gemeinde) rügen. Hier ist grundsätzlich eine Dienstaufsichtsbeschwerde der richtige Rechtsbehelf, auch wenn das Fehlverhalten mit einem Verstoß gegen datenschutzrechtliche Vorschriften begründet wird. Ziel einer Dienstaufsichtsbeschwerde ist es, dienstaufsichtsrechtliche Maßnahmen gegen bestimmte Personen zu veranlassen. Dienstaufsichtsbeschwerden gegen Gemeindemitarbeiter sind bei der jeweiligen Gemeinde einzureichen.

Zivil-, verwaltungs- oder strafrechtlichen Fragestellungen

Auch verzeichnen wir mitunter Eingänge mit rein zivil-, verwaltungs- oder strafrechtlichen Fragestellungen. Wir bitten zu beachten, dass wir uns mit solchen Sachverhalten ohne einen relevanten datenschutzrechtlichen Bezug nicht ohne weiteres näher befassen können.

19. Auskunftsrecht des Betroffenen

Wesentliche rechtliche Regelungen

Grundlegende rechtliche Regelungen zum Auskunftsrecht von Betroffenen finden sich u. a. in Art. 12 und 15 DS-GVO, EG 63 u. 64 sowie § 9 LDSG

Art. 12 u. 15 DS-GVO, EG 63 u. 64, § 9 LDSG

Grundlegendes

Sinn und Zweck

Das Auskunftsrecht ist das zentrale Betroffenenrecht. Nach Art. 15 Absatz 1 DS-GVO haben betroffene Personen das Recht auf Auskunft, ob und ggf. welche Daten eine Gemeinde über sie speichert. Dieser Auskunftsanspruch soll Betroffene in die Lage versetzen, zu beurteilen, welche konkreten Daten über ihre Person gespeichert werden und diese Datenverarbeitungen auf ihre Rechtmäßigkeit hin zu überprüfen.

Informiertheit

Darüber hinaus hat eine Gemeinde bei einer Datenauskunft über weitere Punkte zu informieren (sog. Metadaten). Denn nur wer hinreichend über eine Verarbeitung seiner Daten durch eine Gemeinde informiert ist, kann diese überprüfen und falls geboten, weitere datenschutzrechtliche Ansprüche geltend machen. Das Auskunftsrecht ist für Betroffene der Ausgangspunkt für die Inanspruchnahme von weiteren Rechten, wie etwa auf Berichtigung, Löschung oder Einschränkung der Verarbeitung („Sperrung“).

Verhältnis zu anderen Auskunfts- und Einsichtsrechten

Das datenschutzrechtliche Auskunftsrecht steht grundsätzlich unabhängig von und neben anderen Auskunfts- und Einsichtsrechten, wie beispielsweise dem Anspruch auf Einsichtnahme in die eigene Patientenakte oder die eigene Personalakte.

Antragsberechtigung und Form des Auskunftsverlangens

Antragsberechtigt ist jede natürliche Person, unabhängig von ihrem Wohnsitz. Betroffene können Auskunftsverlangen mündlich oder schriftlich stellen. Wir empfehlen, Auskunftsverlangen schriftlich zu stellen und eine Kopie zu den Unterlagen zu nehmen, um Missverständnisse nach Möglichkeit zu vermeiden und später ggf. einen entsprechenden Nachweis führen zu können.

Muster „Auskunftsantrag“

Ein Muster für einen Auskunftsantrag nach Artikel 15 DS-GVO, das Betroffene verwenden oder an dem sie sich orientieren können, ist in unserem Internetauftritt in der Rubrik „Sonstige Dokumente und Hinweise“ eingestellt.

Umfang und Inhalt des Auskunftsanspruchs

Umfang

Der Auskunftsanspruch umfasst eine Bestätigung, ob eine Gemeinde Daten über den Antragsteller verarbeitet. Falls nein, ist eine sogenannte Negativauskunft zu erteilen. Falls ja, ist dem Antragsteller vom Verantwortlichen mitzuteilen, welche personenbezogenen Daten konkret verarbeitet werden. Eine Auflistung der Kategorien von Daten reicht nicht aus. Vielmehr ist konkret darzulegen, welche Daten im Einzelnen gespeichert werden. Es genügt also beispielsweise nicht, mitzuteilen, dass die Kategorie „Nachname" gespeichert wird, sondern es ist konkret anzugeben, welcher Nachname (genaue Schreibweise) verarbeitet wird. Zudem ist das Recht auf eine Datenkopie zu beachten. Über bereits gelöschte Daten muss keine Auskunft erteilt werden. Auch hat ein Betroffener keinen Anspruch darauf, dass gespeicherte Daten extra für eine Auskunftserteilung aufbereitet werden.

Metadaten

Bei einem Auskunftsverlangen sind von der Gemeinde über die gespeicherten personenbezogenen Daten hinaus noch weitere Informationen (sog. Metadaten) mitzuteilen, wie etwa

- Verarbeitungszwecke,
- Kategorien personenbezogener Daten mit Gruppenbezeichnungen (wie etwa Melde- oder Steuerdaten),
- Empfänger bzw. Kategorien von Empfängern, die diese Daten bereits erhalten haben oder künftig noch erhalten werden,
- geplante Speicherdauer falls möglich, andernfalls die Kriterien für die Festlegung der Speicherdauer,
- Rechte auf Berichtigung, Löschung oder Einschränkung der Verarbeitung,
- Widerspruchsrecht gegen diese Verarbeitung nach Art. 21 DSGVO,
- Beschwerderecht bei unserer Dienststelle oder
- Herkunft der Daten, soweit diese nicht bei der betroffenen Person selbst erhoben wurden.

Verarbeitungszweck

Die Zwecke der Datenverarbeitung sind konkret und in für den Betroffenen nachvollziehbarer Weise anzugeben.

Speicherdauer

Bei der Speicherdauer ist zu beachten, dass der Hinweis, eine Speicherung erfolgt, solange diese rechtmäßig ist, nicht ausreicht. Vielmehr sind, soweit möglich, konkrete Speicherfristen zu benennen. Nur ausnahmsweise kann auf bestimmte Kriterien hingewiesen werden, von denen die Speicherfristen abhängen. Bei gesetzlichen Löschfristen ist über diese unter Angabe der entsprechenden Rechtsnormen zu informieren.

Betroffenenrechte

Es handelt sich hier um eine generelle Hinweispflicht. Das heißt, es sind die genannten Betroffenenrechte aufzuführen, unabhängig davon, ob diese dem Betroffenen zum Zeitpunkt der Auskunftserteilung auch tatsächlich zustehen.

Dritterhebung

Bei einer Datenerhebung bei Dritten hat eine Gemeinde alle verfügbaren Informationen über die Herkunft der Daten aufzuführen.

Automatisierte Entscheidungsfindung

Der automatisierten (rein technischen) Verarbeitung bei der Entscheidungsfindung und dem Profiling kommt im gemeindlichen Bereich keine große Bedeutung zu. Wenn dies jedoch ausnahmsweise der Fall sein sollte und fachbereichsspezifische Vorschriften nichts anderes regeln, ist hierüber zu informieren.

Art und Weise der Auskunftserteilung sowie Unentgeltlichkeit

Die Auskunftserteilung kann je nach Sachverhalt schriftlich, elektronisch oder auf Wunsch des Antragstellers mündlich erfolgen. Wird der Auskunftsantrag elektronisch gestellt, ist die Auskunft in einem gängigen elektronischen Format zu erteilen (zum Beispiel PDF-Format), sofern im Auskunftsersuchen nichts anderes angegeben ist. Die Auskunftserteilung hat in einer verständlichen und nachvollziehbaren Form sowie in einer klaren und einfachen Sprache zu erfolgen. Grundsätzlich erfolgt die Auskunftserteilung unentgeltlich.

Zweifel an der Identität des Antragstellers

Hat eine Gemeinde begründete Zweifel an der Identität der natürlichen Person, die einen Auskunftsantrag stellt, so kann sie nach Art. 12 Abs. 6 DS-GVO zusätzliche Informationen anfordern, die zur Bestätigung der Identität erforderlich sind. Ggf. muss eine Gemeinde darlegen können, warum sie Zweifel an der Identität des Antragsstellers hat. Bei elektronischen Auskunftsersuchen und begründeten Zweifeln an der Identität kann etwa die Angabe einer postalischen Anschrift erbeten werden.

Verständliches und nachvollziehbares Auskunftsersuchen

Betroffene können formlos und ohne Begründung von einer Gemeinde eine Datenauskunft verlangen. Erforderlich sind jedoch Angaben, die es ermöglichen, die auskunftsersuchende Person zu identifizieren. Hierzu gehören unter anderem der Namen des Antragstellers und seine Kontaktdaten. Je präziser ein Auskunftsersuchen formuliert ist, desto weniger Nachfragen sind seitens einer Gemeinde erforderlich und desto schneller kann ein entsprechender Antrag bearbeitet werden. Es sollte von Betroffenen deshalb möglichst genau angegeben werden, über welche Daten oder Verarbeitungsvorgänge Auskunft begehrt wird. Bei personenbezogenen Daten, die nicht in automatisierten oder teilautomatisierten Verfahren verarbeitet werden, sollten Angaben gemacht werden, die das Auffinden dieser Daten ermöglicht. Ansonsten kann dies möglicherweise ein unverhältnismäßig hoher Aufwand sein und letztendlich einen Grund darstellen, eine Auskunft abzulehnen.

Frist für Auskunftserteilung

Grundsatz unverzügliche Auskunftserteilung

Auskunftserteilungen müssen gemäß Art. 12 Abs. 3 DS-GVO unverzüglich erfolgen, spätestens aber innerhalb eines Monats. In begründeten Fällen kann die Monatsfrist um zwei Monate überschritten werden. Die Verarbeitung großer Mengen von Informationen über die betroffene Person kann eine Fristverlängerung begründen. Über eine Fristverlängerung ist der Antragsteller innerhalb eines Monats nach Antragseingang zu informieren. Eine Gemeinde hat, wie jede andere verantwortliche Stelle, im Voraus geeignete technische und organisatorische Maßnahmen zu treffen, damit eine Auskunft gemäß Art. 15 DS-GVO zeitnah und in verständlicher Form erteilt werden kann.

Fristversäumnisse in der Praxis

Bei unserer Dienststelle gehen regelmäßig Beschwerden von Antragsstellern ein, deren Auskunftsanträge nicht innerhalb der rechtlichen Vorgaben, insbesondere innerhalb der vorgesehenen Fristen, bearbeitet wurden. Auch wenn zuzugeben ist, dass der umfassende Auskunftsanspruch von Betroffenen eine große Herausforderung für Gemeinden sein kann, ist ein Überziehen dieser Fristen, teilweise um Monate, nicht hinnehmbar. Insbesondere dann nicht, wenn Gemeinden sich nicht ausreichend auf mögliche Auskunftsanträge vorbereitet haben und Auskunftserteilungen nicht nachhaltig bearbeitet werden. Unsere Dienststelle wird in solchen Fällen künftig verstärkt von ihren Abhilfebefugnissen Gebrauch machen.

Datenkopie

Umfang des Rechts auf eine Datenkopie

Eine Gemeinde stellt gemäß Art. 15 Abs. 3 DS-GVO dem Betroffenen kostenfrei eine Kopie seiner personenbezogenen Daten zur Verfügung. Diese Regelung bezieht sich auf sämtliche personenbezogenen Daten, die zu beauskunften sind. Jedoch umfasst der Auskunftsanspruch und somit auch der Anspruch auf eine Datenkopie nicht sämtliche internen Vorgänge oder Kopien des Schriftverkehrs mit der betroffenen Person, die dieser bereits bekannt sind. Auch wird kein Anspruch auf Kopien begründet, die lediglich den Kontext bilden und keine personenbezogenen Daten enthalten.

Beschränkungen des Rechts auf eine Datenkopie

Das Recht auf eine Datenkopie darf nach Art. 15 Abs. 4 DS-GVO Rechte und Freiheiten anderer Personen nicht beeinträchtigen. Dies können beispielsweise Daten von anderen natürlichen Personen oder Betriebs- und Geschäftsgeheimnisse sein. Gegebenenfalls sind Daten, die Rechte und Freiheiten anderer Personen beinträchtigen, in geeigneter Art und Weise unkenntlich zu machen. Werden mehrere Datenkopien beantragt, kann hierfür ein angemessenes Entgelt auf der Grundlage der angefallenen Verwaltungskosten verlangt werden.

Rechtsmissbräuchliche Auskunftsverlangen

Exzessive Anträge

Exzessiv im Sinne von Artikel 12 Absatz 5 Satz 2 DS-GVO ist ein Auskunftsantrag nach Artikel 15 DS-GVO, wenn diesem ein rechtsmissbräuchliches Verhalten des Antragsstellers zu Grunde liegt. Dies kann insbesondere bei häufigen Wiederholungen des Auskunftsersuchens innerhalb eines kurzen Zeitraums der Fall sein. Rechtsmissbräuchlich kann zudem ein Antrag sein, wenn ein Antragsteller vorrangig das Ziel verfolgt, eine Gemeinde zu schädigen oder bei der Wahrnehmung ihrer Aufgaben zu behindern.

Beweislast liegt bei Gemeinde

Eine Gemeinde trägt die Beweislast für den exzessiven Charakter eines Auskunftsantrags. Die begründete Feststellung, dass ein Antrag exzessiv ist, kann nur für den jeweiligen Einzelfall erfolgen. Der Einwand des Rechtsmissbrauchs kann nicht alleine darauf gestützt werden, dass der Antragssteller seinen Anspruch auf vollständige Auskunft nicht reduziert oder ihm eine bestimmte politische oder religiöse Weltanschauung zugeschrieben wird.

Beispiel Reichsbürger

So begründet alleine der Umstand, dass ein Antrag auf Datenauskunft möglicherweise von einem sog. Reichsbürger gestellt wurde, noch kein exzessives Verhalten. Vielmehr ist im Rahmen einer Einzelfallprüfung aufgrund des konkreten Vorbringens des Auskunftsersuchenden festzustellen und zu dokumentieren, warum aus Sicht der Gemeinde ein Rechtsmissbrauch vorliegt. Auskunftsersuchen von sog. Reichsbürgern wie auch von anderen Personen, die offensichtlich vorrangig das Ziel haben, eine Verwaltung allgemein bei ihrer Aufgabenerfüllung zu behindern oder zu stören, können rechtsmissbräuchlich sein.

Folgen des Rechtsmissbrauchs

Gemäß Artikel 12 Absatz 5 Satz 2 DS-GVO kann bei einem Antrag auf Auskunft, der als exzessiv zu qualifizieren ist, entweder ein angemessenes Entgelt verlangt werden oder die Gemeinde kann sich weigern, eine Auskunft zu erteilen.

Beschränkungen des Auskunftsrechts

Beschränkungen des Auskunftsrechts sind in § 9 LDSG geregelt. So ist in dessen Absatz 1 aufgeführt, dass eine Auskunftsunterteilung abgelehnt werden kann, wenn entsprechende Informationen unter anderem

Beschränkungsgründe

- die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten,
- die Verhütung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung gefährden,
- die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche beeinträchtigen würden sowie
- nach einer Rechtsvorschrift oder zum Schutze der betroffenen Person oder der Rechte und Freiheiten anderer Personen geheim gehalten werden müssen.

Des Weiteren kann eine Auskunft unterbleiben, solange personenbezogene Daten ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind und eine Verarbeitung zu anderen Zwecken ausgeschlossen ist.

Präzisierung des Auskunftsverlangens

Nach § 9 Absatz 2 LDSG kann sich eine Gemeinde auf die Benennung der Verarbeitungsvorgänge und der Art der verarbeiteten Daten beschränken und die Präzisierung eines Auskunftsersuchens verlangen, wenn sie eine große Menge von Informationen über die betroffene Person verarbeitet.

Große Menge von Informationen

Die Voraussetzung, dass eine große Menge von Informationen über eine auskunftsersuchende Person verarbeitet wird, dürfte in vielen Fällen erfüllt sein. Selbst eine kleinere Gemeinde kann große Mengen von Informationen über eine Person verarbeiten, beispielsweise wenn diese dort wohnhaft war oder noch ist.

Ablehnung wegen unzumutbarer Aufwands

Wenn dem Verlangen auf Präzisierung nicht nachgekommen wird, kann gemäß § 9 Absatz 2 LDSG eine Datenauskunft verweigert werden, soweit diese einen unzumutbaren Aufwand für die Gemeinde auslöst. Die Ablehnung einer Datenauskunft wegen eines unzumutbaren Aufwands stellt allerdings eine hohe Hürde dar.

Definition „unzumutbarer Aufwand“

Unzumutbar bzw. unverhältnismäßig ist ein Aufwand, wenn eine Gemeinde aufgrund eines Auskunftsersuchens mit Blick auf die benötigte Zeit für die Bearbeitung und eine damit verbundene Bindung von Arbeitskraft von Beschäftigten über einen längeren Zeitraum nicht mehr ihren Aufgaben im erforderlichen Umfang nachkommen kann und das Schutzbedürfnis des Betroffenen an einer Auskunftserteilung nicht überwiegt (Interessen- und Güterabwägung). Bei der Feststellung, ob eine Auskunftserteilung unzumutbar ist, ist auf die Funktionsfähigkeit der Gemeinde als Ganzes bzw. einzelner organisatorischer Untergliederungen (wie Behörden und Ämter) abzustellen, und nicht auf die Belastung einzelner Mitarbeiter.

Hinreichende Vorbereitung auf Auskunftsersuchen

Zu beachten ist, dass eine Gemeinde eine Auskunft auch nur dann mit der Begründung, diese verursache einen unzumutbaren Aufwand, verweigern kann, wenn sie im Vorfeld bereits die ihr möglichen organisatorischen und technischen Maßnahmen zur Aufwandsreduzierung ergriffen hat und in der Lage ist, dies gegebenenfalls nachzuweisen. Im Ergebnis ist eine Auskunftsverweigerung wegen eines unzumutbaren Aufwand nur innerhalb sehr enger Grenzen und mit einer tragenden und objektiv nachvollziehbaren Begründung im Einzelfall möglich. Dies gilt grundsätzlich auch für alle anderen Betroffenenrechte, denen mit Hinweis auf einen unzumutbaren Aufwand nicht oder nicht im vollen Umfang nachgekommen werden soll.

Folgen der Ablehnung eines Auskunftsersuchens

Begründung

Die Ablehnung einer Auskunftserteilung ist grundsätzlich zu begründen. Dies ergibt sich aus § 9 Abs. 4 S. 1 LDSG und Art. 12 Abs. 4 DS-GVO.

Beschwerdemöglichkeit beim LfDI

Die betroffene Person ist auf die Beschwerdemöglichkeit bei unserer Dienststelle hinzuweisen. Dies ist in § 9 Abs. 4 S. 3 LDSG und Art. 12 Abs. 4 DS-GVO geregelt.

Gerichtlicher Rechtsbehelf

Auch ist über die Möglichkeit, einen gerichtlichen Rechtsbehelf einzulegen, zu informieren.

Mögliche Auskunftserteilung an den LfDI

Die betroffene Person kann nach § 9 Abs. 5 LDSG im Falle einer abgelehnten Auskunft verlangen, dass die Auskunft unserer Dienststelle erteilt wird (soweit nicht die zuständige oberste Landesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde). Unsere Mitteilung an den Betroffenen über das Ergebnis der datenschutzrechtlichen Prüfung darf keine Rückschlüsse auf den Erkenntnisstand der öffentlichen Stelle zulassen, sofern diese nicht zustimmt.

20. Recht auf Berichtigung

Wesentliche rechtliche Regelungen

Grundlegende rechtliche Regelungen zum Recht auf Berichtigung finden sich u. a. in Art. 12, 16 und 19 DS-GVO sowie EG 65.

Art. 12, 16 und 19 DS-GVO und EG 65

Grundlegendes

Sinn und Zweck

Das Recht auf Berichtigung nach Art. 16 DS-GVO ist ein Ausfluss des Grundsatzes der Datenrichtigkeit (Art. 5 Abs. 1 Buchst. d DS-GVO). Personenbezogene Daten müssen inhaltlich richtig, aktuell und vollständig sein. Betroffene können mit diesem Recht die Verarbeitung inhaltlich falscher und nicht aktueller sowie unvollständiger Daten über ihre Person und damit verbundene Nachteile verhindern.

Unentgeltlichkeit

Die Berichtigung durch die Gemeinden erfolgt unentgeltlich, es sei denn, es liegt ein unbegründeter oder exzessiver Antrag vor.

Identität Antragsteller

Bei begründeten Zweifeln an der Identität des Antragsstellers kann eine Gemeinde weitere Informationen anfordern. Dabei ist der Grundsatz der Datensparsamkeit zu beachten

Weigerung Tätigwerden

Bei unbegründeten oder exzessiven Anträgen sowie wenn eine eindeutige Identifikation des Antragstellers nicht möglich ist, können Gemeinden sich weigern, tätig zu werden.

Unrichtige personenbezogene Daten

Nur Tatsachen können unrichtig sein

Ein personenbezogenes Datum muss objektiv unrichtig sein. Unrichtig kann nur eine Tatsache sein. Somit sind Werturteile und Meinungen von einem Berichtigungsanspruch ausgenommen, da diese grundsätzlich keinem empirischen Beweis zugänglich sind. Betroffene sollten bei einem Antrag auf Berichtigung in nachvollziehbarer Weise darlegen, aufgrund welcher objektiv überprüfbaren Tatsachen ein Datum aus ihrer Sicht unrichtig ist

Werturteile und Meinungen

Es ist nicht immer einfach zu bestimmen, ob die in Frage stehenden personenbezogenen Daten ein Werturteil oder eine Meinung darstellen. In aller Regel zeichnen sich Werturteile und Meinungen dadurch aus, dass sie naturgemäß das subjektive Empfinden und die subjektive Wahrnehmung einer Person darstellen. Solange es sich bei den Informationen um Werturteile oder Meinungsäußerungen handelt, kann deren Unrichtigkeit nur schwerlich angegriffen werden. Eine Berichtigung ist in diesen Fällen somit nicht möglich.

Maßgeblich ist Prüfungszeitpunkt

Maßgeblich ist, ob ein Datum zum Prüfungszeitpunkt richtig ist oder nicht. Nicht bedeutsam für einen Berichtigungsanspruch ist hingegen, ob ein personenbezogenes Datum zum Zeitpunkt der Speicherung richtig war oder aufgrund welcher Umstände sich eine Unrichtigkeit einstellte.

Unverzügliche Berichtigung

Die Berichtigung von Daten durch Gemeinden muss „unverzüglich" erfolgen. Jedoch muss der Verantwortliche die Möglichkeit haben, das Vorliegen der Voraussetzungen des Berichtigungsanspruchs zu prüfen. Dabei ist zu beachten, dass die Frist nach Art. 12 Abs. 4 DS-GVO „spätestens nach einem Monat" bereits eine Ausnahme darstellt.

Einschränkung der Verarbeitung

Für den Zeitraum, in dem eine Gemeinde prüft, ob ein Berichtigungsanspruch gegeben ist, hat der Betroffene das Recht, die Einschränkung der Verarbeitung des zu prüfenden Datums nach Art. 18 Abs. 1 Buchst. a DS-GVO zu verlangen.

Praxisfälle

Immer wieder tragen Betroffene vor, dass aus ihrer Sicht Daten über ihre Person unrichtig sind. Dabei sind für eine datenschutzrechtliche Prüfung, ob ein Berichtigungsanspruch gegeben ist, häufig zunächst rein verwaltungsrechtliche Feststellungen bedeutsam. In der Regel sind personenbezogene Daten, die aufgrund von fachbereichsspezifischen Vorschriften (wie etwa dem Bundesmeldegesetz, dem Personenstandsgesetz oder der Gewerbeordnung) ermittelt bzw. festgelegt wurden, auch aus datenschutzrechtlicher Sicht richtig (siehe nachfolgendes Beispiel).

Beispiel Feststellung der Hauptwohnung

Bei mehreren Wohnungen ist melderechtlich festzustellen, welche Wohnung Hauptwohnung ist. Das Ergebnis entsprechender Prüfungen durch Meldebehörden führt bei Betroffenen mitunter zu Unverständnis. Welche Wohnung Hauptwohnung ist, ist zunächst eine melderechtliche Fragestellung. Wenn eine Meldebehörde bei einer Prüfung die entsprechenden einschlägigen melderechtlichen Vorschriften hinreichend beachtet, ist dieses Datum „Hauptwohnung" auch aus datenschutzrechtlicher Sicht richtig. Auf die subjektive Wahrnehmung und Einschätzung des Betroffenen, wo er seiner Auffassung nach seinen Lebensmittelpunkt und seine Hauptwohnung hat, kommt es insoweit nicht an.

Unvollständige personenbezogene Daten

Voraussetzungen

Unvollständig können nur Daten sein, die eine Gemeinde bereits verarbeitet. Maßstab für die Feststellung der Unvollständigkeit ist die rechtliche Verpflichtung einer Gemeinde, für einen bestimmten Zweck bestimmte Daten (Datensatz) zu verarbeiten, und ob insoweit ein einzelnes Datum rechtswidrig nicht verarbeitet wird.

Unverzügliche Berichtigung

Zwar fehlt dem Wortlaut von Art. 16 S. 2 DS-GVO das Wort „unverzüglich". Dennoch hat nach Sinn und Zweck dieser Regelung (u. a. faire und transparente Verarbeitung) auch bei unvollständigen Daten eine Berichtigung unverzüglich zu erfolgen.

Nachberichtspflicht

Information etwaiger Empfänger bei Offenlegung

Gem. Art. 19 DS-GVO muss eine Gemeinde im Falle der Berichtigung etwaige Empfänger, denen sie die berichtigten Daten zuvor offengelegt hat, informieren. Keine entsprechende Informationspflicht besteht, wenn dies unmöglich oder mit einem unverhältnismäßigen Aufwand verbunden ist. Auf Verlangen des Betroffenen muss ihm die Gemeinde mitteilen, welche Empfänger seine entsprechenden Daten erhalten haben.

Ausübung des Rechts auf Berichtigung

Betroffener

Adressat Gemeinde

Wenn Betroffene ihr Recht auf Berichtigung ausüben wollen, sollten sie zunächst die verantwortliche Gemeinde darüber informieren, dass sie die Richtigkeit bzw. die Vollständigkeit der Daten anzweifeln und Berichtigung verlangen.

Nachvollziehbarer und begründeter Antrag

Betroffene sollten bei einem entsprechenden Antrag

- klar und deutlich angeben, was sie für unrichtig oder unvollständig halten,
- erklären, auf welche Weise die Gemeinde die Daten berichtigen soll und
- soweit möglich, den Nachweis erbringen, warum diese Daten fehlerhaft sind.

Empfehlung: Schriftlichkeit

Ein Berichtigungsverlangen kann mündlich oder schriftlich geltend gemacht werden. Wir empfehlen jedoch, zum besseren gegenseitigen Verständnis und der Schaffung eines Nachweises ein mündliches Berichtigungsverlangen schriftlich nachzureichen.

Gemeinde

Auseinandersetzung mit Betroffenenvorbringen

Wenn eine Gemeinde aufgefordert wird, personenbezogene Daten zu berichtigen, sollte diese zunächst sorgfältig prüfen und feststellen, ob die Daten richtig und vollständig sind. Dabei sollte sie sich mit den vom Betroffenen vorgetragenen Argumenten und vorgelegen Nachweisen umfassend auseinandersetzen.

Information des Betroffenen

Nach erfolgter Prüfung hat die Gemeinde sich mit dem Betroffenen in Kontakt zu setzen und

- diesem entweder mitzuteilen, dass und wie seine personenbezogenen Daten berichtigt, gelöscht oder ergänzt wurden,
- oder aber ihn zu informieren, dass eine Berichtigung nicht erfolgte und die Gründe darzulegen, weshalb davon ausgegangen wird, dass die entsprechenden Daten richtig sind und kein Handlungsbedarf besteht.

21. Recht auf Löschung

Wesentliche rechtliche Regelungen

Grundlegende rechtliche Regelungen zum Recht auf Löschung („Recht auf Vergessenwerden“) finden sich u. a. in Art. 12 und 17 DS-GVO, EG 65 und 66 sowie § 10 LDSG

Art. 12 u. 17 DS-GVO, EG 65 u. 66 sowie § 10 LDSG

Grundlegendes

Löschen im Sinne der DS-GVO bedeutet, es ist irreversibel sicherzustellen, dass personenbezogene Daten nicht Gegenstand der allgemeinen Datenverarbeitung einer Gemeinde sind.

Definition „löschen“

Ein Betroffener kann gemäß Art. 17 Abs. 1 DS-GVO von einer Gemeinde die Löschung seiner Daten verlangen, u. a. wenn

- die Gemeinde die Daten nicht weiter zu ihrer Aufgabenerfüllung benötigt,
- er seine Einwilligung in die Datenverarbeitung widerrufen hat,
- er der Verarbeitung seiner Daten widersprochen hat und sein Interesse, das eine Verarbeitung seiner Daten unterbleibt, das Interessen der Gemeinde an der Datenverarbeitung überwiegt,
- die Gemeinde die Daten unrechtmäßig verarbeitet oder
- die Gemeinde rechtlich verpflichtet ist, die Daten zu löschen.

Voraussetzungen für Löschverlangen

Soweit in einschlägigen Rechtsvorschriften konkrete Aufbewahrungs- bzw. Löschfristen normiert sind, sind diese beachtlich. Ansonsten muss eine Gemeinde eine Löschfrist für die jeweilige Datenverarbeitung festlegen. Dabei hat eine Gemeinde darzulegen, welche Daten zur Erfüllung welcher konkreten Aufgabe aus welchem Grund wie lange zu speichern sind. Wenn ihr dies nicht möglich ist, hat sie die entsprechenden Daten unverzüglich zu löschen.

Löschfristen

Liegen die Voraussetzungen für eine Löschung personenbezogener Daten vor, sind diese von der Gemeinde unverzüglich zu löschen und zwar unabhängig von einem Löschverlangen des Betroffenen. Eine sich aus Art. 17 Abs. 1 DS-GVO ergebende Löschungspflicht verlangt von einer Gemeinde nur die Löschung der in ihrer Verantwortungssphäre gespeicherten Daten.

Unverzügliche Löschung, unabhängig von einem Löschverlangen

Eine Löschpflicht besteht auch dann, wenn vom Betroffenen nach Art. 21 DS-GVO erfolgreich Widerspruch eingelegt wurde. Unter dieser Prämisse ist eine Datenverarbeitung zu beenden und die entsprechenden Daten sind zu löschen.

Löschpflicht bei erfolgreichem Widerspruch

Frist für die Beantwortung eines Löschverlangens

Grundsätzlich Monatsfrist

Eine Gemeinde muss Antragstellern grundsätzlich innerhalb eines Monats auf ein Löschverlangen antworten. Unter bestimmten Voraussetzungen kann eine Gemeinde die Bearbeitungsfrist um bis zu zwei weitere Monate verlängern. Dann muss sie jedoch dem Antragsteller dies und die Gründe für die Fristverlängerung innerhalb eines Monats nach Antragseingang mitteilen.

Identifizierung Antragsteller

Falls eine eindeutige Identifizierung des Antragstellers nicht ohne weiteres möglich ist, darf eine Gemeinde Zusatzinformationen verlangen. Hierbei hat sie jedoch den Grundsatz der Datensparsamkeit zu beachten. Es dürfen nur solche und so viele Information verlangt werden, wie zur Identifizierung erforderlich sind. Wenn zusätzliche Informationen zur eindeutigen Identifizierung erforderlich sind, beginnt die Monatsfrist zur Bearbeitung des Löschantrags erst dann zu laufen, wenn der Gemeinde die die zusätzlich angeforderten Nachweise vorliegen.

Ausnahmen und Beschränkungen von der Löschpflicht

Ausnahmegründe

Nach Artikel 17 Absatz 3 DS-GVO besteht u. a. keine Löschpflicht, wenn personenbezogene Daten

- zur Ausübung des Rechts auf freie Meinungsäußerung und Information,
- zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die der Gemeinde übertragen wurde,
- für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke,
- für statistische Zwecke oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen

erforderlich sind.

Abwägung zwischen Recht auf freie Meinungsäußerung und Recht auf Löschung

Das Recht auf freie Meinungsäußerung kann nicht nur die Presse, sondern grundsätzlich jede natürliche Person für sich geltend machen. Insoweit ist die Erforderlichkeit einer Datenspeicherung zur Ausübung des Rechts auf freie Meinungsäußerung mit dem Anspruch des Betroffenen auf Löschung gegeneinander abzuwägen. Wobei es nach Auffassung unserer Dienststelle in der kommunalen Praxis ausreicht, bereits vorliegende Informationen zu berücksichtigen, die das Recht auf freie Meinungsäußerung berühren könnten.

Beschränkungen der Löschpflicht

In § 10 LDSG sind Beschränkungen des Rechts auf Löschung geregelt. In Artikel 10 Absatz 1 LDSG ist normiert, dass die Bestimmungen des Landesarchivgesetzes zur Anbietungspflicht sowie sonstige gesetzliche oder satzungsmäßige Dokumentations- und Aufbewahrungspflichten von der Löschpflicht nach Art. 17 DS-GVO unberührt bleiben.

Schutzwürdige Interessen des Betroffenen gegen eine Löschung

Nach § 10 Abs. 2 LDSG unterbleibt eine Löschung, wenn Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen der betroffenen Person beeinträchtigt werden. Dafür kommt es in solchen Fällen zu einer Einschränkung der Verarbeitung nach Art. 18 DS-GVO. Die Gemeinde hat dann den Betroffenen über das Absehen von der Löschung und die Einschränkung der Verarbeitung zu unterrichten. Der Betroffene kann der Nichtlöschung jedoch widersprechen. Bei einem Widerspruch sind die Daten des Betroffenen zu löschen.

Unverhältnismäßig hoher Löschaufwand bei nichtautomatisierter Datenverarbeitung

Die Verarbeitung personenbezogener Daten ist gemäß § 10 Abs. 3 LDSG von einer Gemeinde auch dann einzuschränken, wenn eine Löschung bei einer nichtautomatisierter Datenverarbeitung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und das Interesse des Betroffenen an der Löschung als gering anzusehen ist. Somit ist zunächst festzustellen, ob in solchen Fällen eine Löschung nicht oder nur mit einem unverhältnismäßigen Aufwand möglich ist. Wenn diese Voraussetzung erfüllt ist, muss die Gemeinde das Interesse des Betroffenen an einer Datenlöschung feststellen. Nur wenn alle Voraussetzungen (nichtautomatisierte Datenverarbeitung, unverhältnismäßig hoher Aufwand und geringes Interesse des Betroffenen) erfüllt sind, kann eine Löschung unterbleiben.

Unbegründete oder exzessive Löschanträge

Die verantwortliche Stelle kann die Löschung von personenbezogenen Daten auch dann verweigern, wenn sie der Ansicht ist, dass das Verlangen offenkundig unbegründet oder exzessiv ist. Weitere Ausführungen hierzu können dem Abschnitt „Betroffenenrechte“ entnommen werden.

Unterrichtung anderer Stellen

Bei öffentlicher Bekanntmachung

Sollte eine Gemeinde Daten von Betroffenen öffentlich gemacht haben und sie nach Art. 17 Abs. 1 DS-GVO zur Datenlöschung verpflichtet sein, so hat sie gem. Art. 17 Abs. 2 DS-GVO grundsätzlich andere verantwortliche Stellen zu informieren, dass ein Betroffener die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien bzw. Replikationen der entsprechenden Daten verlangt hat.

Spurentilgung im Internet

Dieses „Recht auf Vergessenwerden“ bezieht sich auf die Tilgung (von Spuren) der personenbezogenen Daten, die durch Veröffentlichungen von Gemeinden, insbesondere im Internet, allgemein zugänglich sind. Es verpflichtet eine Gemeinde, weitere Verantwortliche, die die zu löschenden Daten (noch) verarbeiten, über ein Verlangen des Betroffenen nach Löschung von Links, Kopien oder Replikationen zu informieren. Wobei Art. 17 Abs. 2 DS-GVO lediglich eine Informationspflicht der Gemeinde ist und keine eigene Pflicht darstellt, für die Lö-

schung der Daten des Betroffenen im ganzen Internet selbst zu sorgen.

Ausnahmen von der Informationspflicht

Von einer Information anderer verantwortlicher Stellen kann eine Gemeinde absehen, wenn die Benachrichtigung dieser unmöglich ist oder einen unverhältnismäßigen Aufwand darstellen würde. Auf Verlangen des Betroffenen muss eine Gemeinde jedoch diesem mitteilen, ob seine Daten an andere Stellen übermittelt wurden, so dass er möglicherweise selbst tätig werden oder andere Schritte einleiten kann.

Unterrichtung des Betroffenen

Information über Nichtlöschung

Wenn eine Gemeinde zu dem Ergebnis gelangt, dass personenbezogene Daten nicht gelöscht werden müssen und dies daher unterlässt, muss der Antragsteller gem. Art. 12 Abs. 4 DS-GVO hierüber – einschließlich der entsprechenden Gründe und des Beschwerderechts bei unserer Dienststelle sowie die Möglichkeit des Einlegens eines gerichtlichen Rechtsbehelfs – informiert werden.

22. Recht auf Einschränkung der Verarbeitung

Wesentliche rechtliche Regelungen

Grundlegende rechtliche Regelungen zum Recht auf Einschränkung der Verarbeitung finden sich u. a. in Art. 12, 18 und 19 DS-GVO sowie EG 67.

Art. 12, 18 und 19 DS-GVO, EG 67

Grundlegendes

Das Recht auf Einschränkung nach Art. 18 DS-GVO soll einen vorübergehenden Ausgleich zwischen den Interessen des Betroffenen und der Gemeinde bei der Datenverarbeitung schaffen.

Sinn und Zweck

Begrifflich entspricht die Einschränkung der Verarbeitung einer Sperrung. Das bedeutet, Daten werden zwar nicht gelöscht, dürfen außer der Speicherung jedoch grundsätzlich nicht mehr anderweitig verarbeitet werden.

Begriff „Einschränkung“

Betroffene können eine Gemeinde auffordern, die Verarbeitung Ihrer Daten einzuschränken,

- wenn sie die Rechtmäßigkeit der Verarbeitung ihrer Daten bezweifeln,
- die Datenverarbeitung unrechtmäßig ist, sie jedoch eine Löschung ihrer Daten verhindern wollen,
- die Daten für gemeindliche Zwecke nicht mehr gebraucht werden, sie diese jedoch für die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigen oder
- sie Widerspruch gegen die Verarbeitung gemäß Artikel 21 Abs. 1 DS-GVO eingelegt haben, und noch nicht feststeht, ob die berechtigten Gründe der Gemeinde oder ihre eigenen überwiegen.

Voraussetzungen für Einschränkungsverlangen

Bei Zweifel an der Rechtmäßigkeit der Datenverarbeitung ist die Datenverarbeitung einzuschränken, bis die Gemeinde eine Überprüfung vornehmen konnte. Kann die Gemeinde die Rechtmäßigkeit nicht nachweisen, hat eine Datenverarbeitung zu unterbleiben.

Folgen bei Zweifel an der Rechtmäßigkeit

Zweifel können sich sowohl auf die Richtigkeit der verarbeitenden Daten als auch auf die Zulässigkeit der Datenverarbeitung beziehen.

Begriff „Zweifel“

Ein einfaches Bestreiten der Rechtmäßigkeit durch den Betroffenen reicht nicht aus. Vielmehr hat er in nachvollziehbarer Weise begründet darzulegen, weshalb er Zweifel an der Rechtmäßigkeit hat.

Begründete Darlegung durch Betroffenen

Für die Annahme einer rechtlichen Auseinandersetzung muss zumindest eine hinreichende Wahrscheinlichkeit bestehen.

Rechtsstreitigkeiten

Die Einschränkung der Datenverarbeitung und eine Unterrichtung des Betroffenen bzw. anderer Stellen erfolgt unentgeltlich, es sei denn, es liegt ein offenkundig unbegründeter oder exzessiver Antrag des Betroffenen vor. Bei Zweifel an der Identität des Betroffenen kann eine Gemeinde zusätzliche Informationen anfordern. Näheres hierzu kann den allgemeinen Ausführungen zu den Betroffenenrechten entnommen werden.

Kostenfreiheit und Identifizierung

Das Recht auf Einschränkung der Verarbeitung ist eng mit den Betroffenenrechten, die Richtigkeit der Daten zu bestreiten (Art. 16 DS-GVO) und dem Widerspruchsrecht (Art. 21 DS-GVO) verbunden.

Einschränkungsmethoden

Methoden zur Einschränkung der Datenverarbeitung werden in EG 67 beispielhaft genannt (unter anderem die zeitweise Verschiebung der Daten in ein anderes IT-System, die Zugriffsmöglichkeiten durch andere Nutzer beschränken und die vorübergehende Entfernung der Daten von einer Webseite).

EG 67

Datenverarbeitung bei vorliegender Einschränkung

Liegt einer der Gründe aus Art. 18 Abs. 1 DS-GVO vor, dürfen die einschlägigen Daten (abgesehen von der immer zugelassenen Speicherung) gemäß Art. 18 Abs. 2 DS-GVO nur noch verarbeitet werden

- mit Einwilligung des Betroffenen,
- zur Geltendmachung von Rechtsansprüchen (auch des Verantwortlichen),
- zum Schutz der Rechte einer anderen Person oder
- aufgrund eines wichtigen öffentlichen Interesses.

Gründe für Weiterverarbeitung

Informationspflicht bei Aufhebung der Einschränkung

Entscheidet sich eine Gemeinde, eine vorhandene Einschränkung der Verarbeitung aufzuheben und die Daten wieder vollständig zu verarbeiten, muss sie den Betroffenen zuvor gemäß Art. 18 Abs. 3 DS-GVO hierüber informieren.

Information des Betroffenen über Aufhebung

Nachberichtspflicht

Mitteilung an Empfänger

Eine Gemeinde muss nach Art. 19 DS-GVO allen Empfängern, denen personenbezogenen Daten offengelegt wurden, eine Einschränkung der Verarbeitung nach Art. 18 mitteilen. Dies gilt nicht, wenn eine Mitteilung sich als unmöglich erweist oder mit einem unverhältnismäßigen Aufwand verbunden ist.

Mitteilung von Empfängern an Betroffenen

Wenn der Betroffene es verlangt, hat die Gemeinde ihn über diese Empfänger zu unterrichten, damit er ggf. seine Rechte (wie etwa auf eine weitere Einschränkung) gegenüber anderen verantwortlichen Stellen effektiv wahrnehmen kann.

23. Recht auf Datenübertragbarkeit

Wesentliche rechtliche Regelungen

Art. 20 DS-GVO und EG 68

Grundlegende rechtliche Regelungen zum Recht auf Datenübertragbarkeit finden sich in Art. 20 DS-GVO und EG 68

Grundlegendes

Voraussetzungen

Das Recht auf Datenübertragbarkeit nach Art. 20 DS-GVO ist dem Auskunftsrecht nach Art. 15 DS-GVO grundsätzlich ähnlich. Ein wesentlicher Unterschied ist jedoch, dass dieses Recht nur auf solche Daten anwendbar ist,

- die elektronisch vorgehalten werden,
- die der Betroffene selbst der Gemeinde zur Verfügung gestellt hat,
- Beschränkungen auf die Rechtsgrundlagen „Einwilligung“ und „Vertrag“ sowie
- die Datenverarbeitung mithilfe automatisierter Verfahren erfolgt.

Bedeutung für den gemeindlichen Bereich

Nachrangige Bedeutung für Gemeinden

Bei dem Großteil der Datenverarbeitungen durch Gemeinden greift dieses Recht nicht, da es sich auf die Verarbeitung personenbezogener Daten beschränkt, die auf Einwilligungen oder Verträge beruhen.

Gilt nicht bei öffentlicher Aufgabe

Zudem ist für den gemeindlichen Bereich Art. 20 Abs. 3 S. 2 DS-GVO von Bedeutung. Dieser regelt, dass das Recht auf Datenübertragbarkeit nicht gilt, soweit die Verarbeitung zur Wahrnehmung einer öffentlichen Aufgabe oder in Ausübung öffentlicher Gewalt erforderlich ist. Das bedeutet, soweit Betroffene auf freiwilliger Basis (Einwilligung) oder aufgrund eines öffentlich-rechtlichen Vertrags personenbezogene Daten bereitgestellt haben und eine Gemeinde bei der Datenverarbeitung im öffentlich-rechtlichen Bereich tätig wird, keine Rechtspflicht auf Datenübertragung besteht.

Prüfschema für Betroffene

Betroffene können ihr Recht auf Datenübertragbarkeit jederzeit wirksam geltend machen, wenn sie

- personenbezogene Daten einer Gemeinde zur Verfügung stellen,
- die elektronisch in automatisierten Verfahren verarbeitet werden,
- die Datenverarbeitung auf ihrer Einwilligung beruht oder
- die Daten als Teil eines Vertrags verarbeitet werden, den sie mit der Gemeinde geschlossen haben und
- die Gemeinde bei der Verarbeitung der Daten nicht im öffentlich-rechtlichen Bereich tätig wird.

Abgrenzung nicht-öffentlich-rechtlicher Bereich

Nicht im öffentlich-rechtlichen Bereich tätig wird eine Gemeinde beispielsweise dann, wenn sie gemeindeeigene Wohnungen wie jeder andere Anbieter auf dem Wohnungsmarkt privatrechtlich vermietet.

Rechtsfolgen bei wirksamen Antrag auf Datenübertragung

Gängiges maschinenlesbares Format und Übermittlung an andere Stellen

Wenn die entsprechenden Voraussetzungen erfüllt sind, haben Betroffene das Recht, Daten über ihre Person, die sie der Gemeinde selbst bereitgestellt haben, in einem gängigen und maschinenlesbaren Format von dieser zu erhalten. Zudem können Betroffene eine Gemeinde auffordern, solche Daten direkt an eine andere Stelle zu übermitteln. Eine Gemeinde ist hierzu dann verpflichtet, wenn dies für sie technisch machbar ist.

24. Widerspruchsrecht

Wesentliche rechtliche Regelungen

Art. 12 und 21 DS-GVO sowie EG 69

Grundlegende rechtliche Regelungen zum Widerspruchsrecht finden sich in Art. 12 und 21 DS-GVO sowie EG 69.

Grundlegendes

Sinn und Zweck

Das Widerspruchsrecht nach Art. 21 Abs. 1 S. 1 DS-GVO soll es Betroffenen in besonders gelagerten Einzelfällen ermöglichen, eine atypische, ihre Person betreffende Situation geltend zu machen. Die Gemeinde hat dann eine eingehende Prüfung und ggf. Abwägung durchzuführen, die auch die konkreten Umstände und Interessen des Betroffenen umfasst.

Voraussetzungen

Betroffene haben das Recht, der Verarbeitung ihrer eigenen Daten zu widersprechen. Dabei ist zu beachten, dass dieses Widerspruchsrecht nicht voraussetzungslos ist. Eine Voraussetzung ist, dass die Datenverarbeitung aufgrund von Artikel 6 Absatz 1 Buchstabe e (Aufgabenwahrnehmung im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt) oder Buchstabe f (berechtigtes Interesse der Gemeinde) DS-GVO erfolgt. Eine weitere Voraussetzung ist, dass beim Betroffenen hinsichtlich der Daten, die von ihm verarbeitet werden sollen, eine besondere Situation vorliegt.

Einlegungsfrist für Widerspruch

Ein Widerspruch kann jederzeit, also auch nach Beginn der Datenverarbeitung eingelegt werden. Ist die Datenverarbeitung jedoch bereits beendet, kann ein Widerspruch keine rechtliche Wirkung mehr entfalten.

Besondere Situation

Atypische Situation des Betroffenen

Wenn ein Betroffener von seinem Widerspruchsrecht Gebrauch macht, muss er das Vorliegen einer besonders gelagerten Situation geltend machen können. Das bedeutet, dass das Widerspruchsrecht nur in solchen Einzelfällen greift, in denen beim Betroffenen ganz besondere Umstände vorliegen, die in seiner Person begründet sind, und aufgrund dieser für ihn eine Situation besteht, die sich in nachvollziehbarer und objektiver Weise deutlich von einer „normalen“, durchschnittlichen Situation von anderen Betroffenen abhebt. Im Ergebnis muss beim Betroffenen eine atypische Situation gegeben sein, die seinem persönlichen Interesse, dass eine Verarbeitung seiner Daten unterbleibt, ein überragendes Gewicht verleiht.

Damit die für die Datenverarbeitung verantwortliche Gemeinde feststellen kann, ob in dem von ihr zu prüfenden Einzelfall eine besondere Situation vorliegt, hat der Betroffene ihr dies gegenüber glaubhaft und in einer plausibel nachvollziehbaren Art und Weise darzulegen und nachzuweisen.

Darlegungspflicht des Betroffenen

Bei der Prüfung, ob eine besondere Situation vorliegt, ist zu beachten ist, dass es hier nicht auf die subjektive Einschätzung des Betroffenen ankommt, sondern vielmehr ein eindeutiger Sachverhalt vorliegen muss, aus dem sich die besondere Situation des Betroffenen nach einem objektiven Maßstab ergibt.

Objektiver Maßstab

Zwar können weder dem Wortlaut von Artikel 21 DS-GVO noch den insoweit auch heranzuziehenden Erwägungsgrund 69 konkret entnommen werden, wann genau eine solche besondere Situation vorliegt. Es kann jedoch davon ausgegangen werden, dass dies der Fall ist, wenn im jeweiligen Einzelfall für den Betroffenen im Vergleich zu anderen Betroffenen durch eine Datenverarbeitung eine besondere Gefährdungslage oder eine vom Normalfall abweichende, besonders hohe Eingriffsqualität und -tiefe gegeben ist, die den Betroffenen in seinen Grundrechten oder Grundfreiheiten in einem besonderen Maße bedrohen. Dies ist insbesondere der Fall, wenn eine durch eine Verarbeitung seiner Daten beim Betroffenen Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen besteht.

Begriff „besondere Situation“

Gründe für Datenverarbeitung trotz Widerspruchs

Wenn eine Gemeinde aufgrund der Mitteilungen des Betroffenen festgestellt hat, dass für seine Person eine besondere Situation im Sinne von Artikel 21 Absatz 1 Satz 1 DS-GVO vorliegt, ist eine Datenverarbeitung nicht von vornherein ausgeschlossen. Trotz eingelegten Widerspruchs können personenbezogene Daten des Betroffenen verarbeitet werden, wenn

Verarbeitungsgründe trotz eingelegten Widerspruchs

- keine besondere Situation,
- überwiegende schutzwürdige Gründe für die gemeindliche Datenverarbeitung vorliegen oder
- die Verarbeitung personenbezogener Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erfolgt.

Gegebenenfalls muss eine Gemeinde darlegen und begründen können, welche zwingenden schutzwürdigen Gründe für eine Datenverarbeitung das (sich aus der besonderen Situation ergebende) Interesse des Betroffenen, dass keine Daten von ihm verarbeitet werden, überwiegen und diese Gründe auch Vorrang vor den Grundrechten und Grundfreiheiten des Betroffenen haben. Hierzu hat die verantwortliche Stelle eine Interessen- und Güterabwägung vorzunehmen. Bei den zwingend schutzwürdigen Gründen kann es sich sowohl um ein überwiegendes Interesse der Gemeinde, als auch um ein überwiegendes Interesse

Überwiegende schutzwürdige Gründe für eine Datenverarbeitung

Dritter an der Verarbeitung der personenbezogenen Daten handeln.

Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen

Die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen beschränkt sich nicht auf die gerichtliche Verfolgung von Rechtsansprüchen, sondern schließt auch außergerichtliche Verfahren ein. Die theoretische Möglichkeit von Rechtsstreitigkeiten reicht nicht aus. Soweit es um mögliche künftige Rechtsstreitigkeiten handelt, muss zumindest im Rahmen einer Prognose wahrscheinlich sein, dass es hierzu kommen wird.

Rechtsfolgen eines erfolgreichen Widerspruchs

Datenlöschung

Wurde erfolgreich Widerspruch eingelegt, ist die Datenverarbeitung zu beenden und die entsprechenden Daten sind zu löschen.

Nicht erfolgreich ist ein Widerspruch, wenn keine besondere Situation vorliegt oder bei Vorliegen einer besonderen Situation, die Gemeinde ausreichende Gründe für eine Fortführung der Datenverarbeitung nachweisen kann.

25. Recht auf nicht-automatisierte Datenverarbeitung (einschließlich Profiling)

Wesentliche rechtliche Regelungen

Art. 12 u. Art. 22 DS-GVO, EG 71 u. 72.

Grundlegende rechtliche Regelungen zum Recht auf nicht-automatisierte Datenverarbeitung finden sich in Art. 12 und Art. 22 DS-GVO sowie in den EG 71 u. 72.

Grundlegendes

Sinn und Zweck

Dem Recht auf eine nicht-automatisierte Datenverarbeitung (einschließlich Profiling) gemäß Art. 22 DS-GVO soll verhindern, dass es bei einer rein technischen Verarbeitung personenbezogener Daten zu rechtserheblichen oder nachteiligen Entscheidungen für Betroffene kommt. Entsprechende Konstellationen sind überwiegend im nicht-öffentlichen Bereich vorzufinden (wie beispielsweise bei der Beantragung eines Kredits oder bei Finanzdienstleistungen). Wenn jedoch eine Gemeinde vorprogrammierte Kriterien und Algorithmen bei einer Datenverarbeitung anwendet oder eine Profilbildung vornehmen sollte, ist auch hier der Anwendungsbereich des Rechts auf nicht-automatisierte Datenverarbeitung eröffnet.

Definitionen

Automatisierte Datenverarbeitung

Eine automatisierte Datenverarbeitung liegt vor, wenn Entscheidungen ohne jegliche menschliche Einflussnahme getroffen werden.

Profiling

Profiling bedeutet, dass personenbezogene Daten automatisiert verarbeitet werden, um Kriterien in Bezug auf eine natürliche Person zu analysieren, zu bewerten oder vorherzusagen. Beispiele für solche Kriterien sind die Arbeitsleistung oder die Gesundheit einer Person.

Grundsätzliches Verbot mit Ausnahmen

Grundsatz mit weitreichenden Ausnahmen

Zwar dürfen verantwortliche Stellen grundsätzlich keine Entscheidungen treffen, die ausschließlich auf einer automatisierter Verarbeitung basieren, wenn diese die gesetzlichen Rechte von Betroffenen oder andere gleich wichtige Angelegenheiten berühren. Das grundsätzliche Verbot einer ausschließlich automatisierten Datenverarbeitung kennt jedoch weitreichende Ausnahmen.

Ausnahmen können vorliegen, wenn eine Entscheidung

Ausnahmegründe

- für die Zwecke eines Vertrags zwischen dem Betroffenen und der verantwortlichen Stelle erforderlich oder
- gesetzlich erlaubt (wie zur Verhinderung von Betrug oder Steuerhinterziehung) ist,
- sowie wenn diese auf der ausdrücklichen Einwilligung des Betroffenen basiert.

Rechte von Betroffenen

Grundsätzlich haben Betroffene das Recht

Betroffenenrechte

- nicht einer Entscheidung unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung basiert, wenn die Entscheidung Ihre gesetzlichen Rechte oder sie in ähnlicher Weise erheblich beeinträchtigt,
- die Gründe für Entscheidungen, die aufgrund automatisierter Verarbeitung getroffen wurde sowie die möglichen Konsequenzen der Entscheidungen zu verstehen, und
- sich gegen eine Profilerstellung in bestimmten Situationen zu wehren.

26. Informationspflichten

Wesentliche rechtliche Regelungen

Art. 12 bis 14 DS-GVO, EG 60 bis 62, §§ 8 u. 16 LDSG

Grundlegende rechtliche Regelungen zu den Informationspflichten einer Gemeinde respektive den Informationsrechten von Betroffenen finden sich in den Art. 12 bis 14 DS-GVO, EG 60 bis 62 und §§ 8 u. 16 LDSG

Grundlegendes

Sinn und Zweck

Die Informationspflicht der Gemeinde bzw. das Informationsrecht der Betroffenen bei der Datenerhebung soll eine faire und transparente Verarbeitung personenbezogener Daten gewährleisten.

Informationspflicht nur bei Datenerhebung

Die Informationspflichten nach Art. 13 und 14 DS-GVO werden (nur) ausgelöst, wenn eine Datenerhebung vorliegt. Der Begriff des Erhebens personenbezogener Daten im Sinne der genannten Vorschriften ist umstritten.

Begriff „Datenerhebung“

Nach unserer Rechtsauffassung setzt eine Datenerhebung in diesem Zusammenhang ein aktives Handeln einer Gemeinde mit dem Ziel voraus, über bestimmte Daten als verantwortliche Stelle Kenntnis zur erlangen oder über diese verfügen zu können.

Im Zweifelsfall informieren

Wenn eine Gemeinde unsicher ist, ob sie einer Informationspflicht unterliegt, empfehlen wir, Betroffene vorsorglich entsprechend Art. 13 bzw. 14 DS-GVO zu informieren.

Beispiel aufgedrängte Daten

Bei aufgedrängten personenbezogenen Daten ist die Voraussetzung des Erhebens nach Art. 13 und 14 DS-GVO nicht erfüllt. Aufgedrängt sind Informationen, deren Erhalt die Gemeinde nicht gefordert und auch sonst nichts aktiv zur deren Erhalt beigetragen hat (wie etwa die unaufgeforderte Übergabe einer Visitenkarte). Bei aufgedrängten Daten entfällt eine Informationspflicht nach Art. 13 DS-GVO (Direkterhebung).

Direkterhebung oder Dritterhebung

Allgemein ist bei der Informationspflicht zwischen der Erhebung von personenbezogenen Daten beim Betroffenen selbst (Direkterhebung, Art. 13 DS-GVO) und der Datenerhebung bei einem Dritten (Dritterhebung, Art. 14 DS-GVO) zu unterscheiden.

Begriff „Direkterhebung“

Zu einer Direkterhebung zählen insbesondere Daten, die die betroffene Person bewusst einer Gemeinde offenbart, die Gemeinde hierzu aufgefordert bzw. die entsprechenden Rand- und Rahmenbedingungen für eine Datenverarbeitung geschaffen hat (wie etwa durch Zurverfügungstellung eines Formulars oder durch das Stellen von Fragen eines Gemeindemitarbeiters in einem Gespräch im Rahmen eines Verwaltungsverfahrens.).

Direkterhebungsgrundsatz

Ein klar formulierter Direkterhebungsgrundsatz ist in der DS-GVO nicht zu finden. Gleichwohl ergibt sich dieser aus den in Art. 5 Abs. 1 DS-GVO formulieren Grundsätzen „Verarbeitung nach Treu und Glauben“ (Buchst. a) und „Datenminimierung“ (Buchst. c). Das bedeutet, Gemeinden haben personenbezogene Daten nach Möglichkeit direkt bei den betroffenen Personen zu erheben.

Ausnahmen von der Direkterhebung

Etwas anderes gilt, wenn bereichsspezifische Vorschriften eine Datenerhebung bei Dritten vorsehen (vgl. Formulierung in Art. 14 Abs. 5 Buchst. c DS-GVO), sowie wenn eine Datenerhebung beim Betroffenen unmöglich ist oder nur mit einem unverhältnismäßig hohen Aufwand erfolgen kann.

Begriff „Dritterhebung“

Eine Dritterhebung liegt vor, wenn die Gemeinde personenbezogene Daten nicht vom Betroffenen selbst, sondern von einem Dritten erlangt. Mögliche Quellen für Dritterhebungen können private und öffentliche Stellen, allgemein zugängliche Quellen oder auch Privatpersonen sein. Beispiele für eine Dritterhebung sind, wenn eine Gemeinde Daten über eine Person bei einer Behörde oder im Internet erhebt.

Die Hinweise mit den entsprechenden Informationen nach Art. 13 und 14 DS-GVO werden häufig als Datenschutzhinweis, Datenschutzbestimmungen oder Datenschutzerklärung bezeichnet.

Verarbeitungsverzeichnis

Viele Informationen, die Gemeinden im Rahmen ihrer Informationspflicht Betroffenen mitzuteilen haben, decken sich mit Angaben im nach Art. 30 DS-GVO zu führenden Verarbeitungsverzeichnis. Ein den datenschutzrechtlichen Anforderungen entsprechendes Verarbeitungsverzeichnis bildet somit nicht nur die Grundlage, dass eine Gemeinde ihren Informationspflichten hinreichend nachkommen kann, sondern erleichtert dies auch erheblich.

Zeitpunkt der Information

Direkterhebung

Erhebungszeitpunkt

Bei Direkterhebungen (Art. 13 DS-GVO) sind bestimmte Informationen „zum Zeitpunkt der Erhebung dieser Daten“ zu übermitteln.

Dritterhebung

Grundsatz ein Monat

Bei Dritterhebungen (Art. 14 DS-GVO) hat eine entsprechende Information grundsätzlich spätestens innerhalb eines Monats zu erfolgen.

Kommunikation mit Betroffenen

Werden die von Dritten erhobenen Daten zur Kommunikation mit dem Betroffenen verwendet, erfolgt eine Information spätestens zum Zeitpunkt der ersten Mitteilung an diesen.

Offenlegung gegenüber anderem Empfänger

Bei einer Offenlegung von bei Dritten erhobenen Daten gegenüber einem anderen Empfänger, erfolgt eine Information des Betroffenen spätestens zum Zeitpunkt der ersten Offenlegung gegenüber dem anderen Empfänger.

Art und Weise sowie Unentgeltlichkeit der Informationsbereitstellung

Leicht zugänglich, gut verständlich und unentgeltlich.

Eine Informationsbereitstellung hat in einer für den Betroffenen leicht zugänglichen Form zu erfolgen. Die Informationen sind einer klaren und einfachen Sprache zu halten. Dabei ist darauf zu achten, dass der Betroffene sich nicht aus einer Flut von anderen Informationen selbst die relevanten Informationen über die Verarbeitung seiner personenbezogenen Daten heraussuchen muss. Die Informationen werden grundsätzlich unentgeltlich zur Verfügung gestellt.

Pflicht zur Mitteilung

Gemeinden sind verpflichtet, Informationen gem. Art. 13 und 14 DSGVO bei Vorliegen der entsprechenden Voraussetzungen dem Betroffenen von sich aus mitzuteilen. Dies bedeutet, dass eine Gemeinde von sich aus tätig werden muss, um der betroffenen Person die vorgesehenen Information bereitzustellen oder sie aktiv in nachvollziehbarer Weise zu der Stelle zu leiten, wo die entsprechenden Angaben zur Verfügung stehen (wie etwa Aushändigung eines Informationsblatts, Hinweis auf einen Internetlink oder die Bereitstellung eines QR-Codes).

Medienbruch

Die von der Gemeinde insgesamt mitzuteilenden Informationen müssen nicht zwangsläufig mit demselben Medium zur Verfügung gestellt werden. Werden beispielsweise Daten direkt beim Betroffenen mittels eines Formulars in Papierform erhoben, kann grundsätzlich eine (ergänzende) Information auch durch einen Hinweis auf eine entsprechende gemeindliche Internetseite erfolgen. Weitere Möglichkeiten sind in diesem Zusammenhang, die Informationen im Bearbeitungsbereich der gemeindlichen Mitarbeiter auszuhängen/auszustellen oder dem Betroffenen ein Informationsblatt zu übergeben.

Nutzung verschiedener Kanäle der Informationsvermittlung

Grundsätzlich sollten mehrere Kanäle der Informationsvermittlung genutzt und dabei die Informationskanäle ausgewählt werden, die den Betroffenen voraussichtlich auch zur Verfügung stehen. Dabei ist auf den jeweiligen Einzelfall abzustellen (wie etwa Lebensalter, bekannte Einschränkungen oder Lebensumstände).

Informationsinhalte

Unterschiede zwischen Direkt- und Dritterhebung

Bei einer Direkterhebung sind die mitzuteilenden Informationen abschließend in Art. 13 Abs. 1 und 2 DS-GVO, bei einer Dritterhebung in Art. 14 Abs. 1 und 2 DS-GVO aufgeführt. Die Informationen, die verpflichtend mitzuteilen sind, sind weitgehend deckungsgleich, es gibt aber auch Unterschiede.

Direkterhebung

Grundinformationen

Bei einer Direkterhebung durch Gemeinden ist nach Art. 13 Abs. 1 DS-GVO über Folgendes zu informieren:

a) Gemeindenamen, gesetzlicher Vertreter und gemeindliche Kontaktdaten,
b) Kontaktdaten des gemeindlichen Datenschutzbeauftragten,
c) die Zwecke der Datenverarbeitung und die Rechtsgrundlage,
d) wenn die Datenverarbeitung auf einem berechtigen Interesse beruht, das berechtigte Interesse der Gemeinde oder eines Dritten,
e) ggf. Datenempfänger bzw. Kategorien von Datenempfängern sowie
f) ggf. die Absicht der Gemeinde personenbezogene an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder Fehlen eines Angemessenheitsbeschlusses bzw. einen Verweis auf geeignete oder angemessene Garantien und die Möglichkeit , wie eine Kopie von diesen zu erhalten ist oder diese verfügbar sind.

Zusatzinformationen

Zudem ist bei einer Direkterhebung nach Art. 13 Absatz 2 DS-GVO zu informieren

a) über die Speicherdauer und falls dies nicht möglich ist, über die Kriterien für die Festlegung der Speicherdauer,
b) über bestimmte Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung und Datenübertragbarkeit),
c) über das Recht, eine Einwilligung jederzeit zu widerrufen zu können und dass die Rechtmäßigkeit der Datenverarbeitung bis zum Widerruf bestehen bleibt,
d) über das Beschwerderecht bei unserer Dienststelle,
e) ob die Bereitstellung personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob der Betroffene verpflichtet ist, die Daten über seine Person bereitzustellen, und welche Folgen eine Nichtbereitstellung haben kann sowie
f) über bestimmte Informationen bei einer automatisierten Entscheidungsfindung einschließlich Profiling.

Dritterhebung

Grundinformationen

Bei einer Dritterhebung durch eine Gemeinde ist nach Art. 14 Abs. 1 DS-GVO über Folgendes zu informieren:

a) Gemeindenamen, gesetzlicher Vertreter und gemeindliche Kontaktdaten,
b) die Kontaktdaten des Datenschutzbeauftragten;
c) die Zwecke der Datenverarbeitung und die Rechtsgrundlage,
d) die Kategorien personenbezogener Daten, die verarbeitet werden;
e) ggf. die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und
f) ggf. die Absicht der Gemeinde, personenbezogene Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder Fehlen eines Angemessenheitsbeschlusses bzw. einen Verweis auf geeignete oder angemessene Garantien und die Möglichkeit , wie eine Kopie von diesen zu erhalten ist oder diese verfügbar sind.

Zusatzinformationen

Zudem ist bei einer Dritterhebung nach Art. 14 Absatz 2 DS-GVO zu informieren

a) über die Speicherdauer und falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,
b) ggf. über die berechtigten Interessen, die von der Gemeinde oder einem Dritten verfolgt werden,
c) über bestimmte Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung und Datenübertragbarkeit)
d) über das Recht, eine Einwilligung jederzeit widerrufen zu können und dass die Rechtmäßigkeit der Datenverarbeitung bis zum Widerruf bestehen bleibt,
e) über das Beschwerderecht bei unserer Dienststelle,
f) aus welcher Quelle die personenbezogenen Daten stammen und ggf., ob sie aus öffentlich zugänglichen Quellen stammen und
g) über bestimmte Informationen bei einer automatisierten Entscheidungsfindung einschließlich Profiling.

Datenweiterverarbeitung

Zweckänderung

Soweit eine Gemeinde beabsichtigt, personenbezogene Daten für einen anderen Zweck als den ursprünglich erhobenen Zweck weiterzuverarbeiten (Zweckänderung), so hat sie den Betroffenen gem. Art. 13 Abs. 3 DS-GVO (Direkterhebung) bzw. Art. 14 Abs. 4 DS-GVO (Dritterhebung) erneut zu informieren. Die Information muss vor der Weiterverarbeitung erfolgen und umfasst alle relevanten Punkte über den anderen (neuen) Zweck (dies schließt u. a. die Rechtsgrundlage der Datenverarbeitung und die Speicherdauer für diesen Zweck ein) sowie alle Informationen nach Art. 13 Abs. 2 DS-GVO bzw. Art. 14 Abs. 2 DS-GVO.

Hinweise

Kontaktdaten Gemeinde

Die Kontaktdaten der Gemeinde müssen eine (ladungsfähige) Anschrift der Gemeinde sowie die elektronische und telefonische Erreichbarkeit der Gemeinde umfassen.

Kontaktdaten Datenschutzbeauftragter

Bei den Kontaktdaten des gemeindlichen Datenschutzbeauftragten halten wir grundsätzlich die Nennung einer funktionalen E-Mail Adresse (wie etwa Datenschutz@beispielsgemeinde.de) und Angabe der Postanschrift des gemeindlichen Datenschutzbeauftragten mit Blick auf die rechtlichen Vorgaben für ausreichend. Dies gilt insbesondere, wenn eine Gemeinde einen internen Datenschutzbeauftragten ernannt hat.

Externe Datenschutzbeauftragte

Betroffene teilen unserer Dienststelle jedoch immer wieder mit, dass externe gemeindliche Datenschutzbeauftragte für sie nicht oder nur sehr schwer erreichbar sind. Wir empfehlen deshalb dringend, umfassend anzugeben, wie und wann externe Datenschutzbeauftragte von Gemeinden erreichbar sind.

Zweck nachvollziehbar formulieren

Die Zwecke der Datenverarbeitung sind konkret und für den Betroffenen in nachvollziehbarer Weise anzugeben.

Präzise Benennung von Rechtsgrundlagen

Wenn eine Datenverarbeitung auf Rechtsvorschriften gestützt wird, sind diese präzise anzugeben. Ein allgemeiner Hinweis auf eine Datenerhebung im Rahmen rechtlicher Regelungen oder die bloße Benennung von Gesetzen oder Verordnungen (wie etwa Bundesmeldegesetz oder Meldeverordnung) reicht nicht aus.

Empfänger von Daten

Wer Empfänger von Daten ist, ist in Art. 4 Nr. 9 DS-GVO legal definiert.

Speicherdauer

Die Speicherdauer ist soweit möglich als konkreter Zeitraum anzugeben. Bei gesetzlichen Löschfristen ist über diese unter Angabe der entsprechenden Rechtsnorm zu informieren.

Betroffenenrechte

Es handelt sich hier um eine generelle Hinweispflicht. Das heißt, es sind alle genannten Betroffenenrechte aufzuführen, unabhängig davon, ob diese dem Betroffenen zum Zeitpunkt der Auskunftserteilung auch tatsächlich zustehen.

Automatisierte Entscheidungsfindung

Der automatisierten (rein technischen) Verarbeitung bei der Entscheidungsfindung (einschließlich Profiling) kommt im gemeindlichen Bereich keine große Bedeutung zu. Wenn dies jedoch ausnahmsweise der Fall sein sollte und fachbereichsspezifische Vorschriften nichts anderes regeln, ist hierüber zu informieren.

Ausnahmen von der Informationspflicht

Überblick

Grundsätzlich besteht eine gesetzliche Verpflichtung der Daten verarbeitenden Gemeinde, Betroffenen die oben genannten Informationen zu erteilen. Jedoch gibt es auch Situationen, in denen eine Gemeinde von einer Informationserteilung absehen kann/muss. Es gibt Ausnahmen, die nur für Direkterhebungen (Art. 13 Abs. 4 DS-GVO), nur für Drittehrhebungen (Art. 14 Abs. 5 DS-GVO) oder für beide Bereiche (§§ 8 und 16 LDSG) gelten.

EG 62 nur bei Dritterhebung anwendbar

Nach Erwägungsgrund 62 erübrigt sich die Pflicht, Informationen zur Verfügung zu stellen, wenn die betroffene Person die Information bereits hat, die Speicherung oder Offenlegung der personenbezogenen Daten geregelt ist oder sich die Unterrichtung der betroffenen Person als unmöglich erweist oder mit einem unverhältnismäßigen Aufwand verbunden ist. Es ist zu beachten, dass Erwägungsgrund 62 in seiner konkreten Formulierung ausschließlich in Art. 14 DS-GVO zum Ausdruck kommt. Die Annahme, Erwägungsgrund 62 könnte bei Direkterhebungen ergänzend zu der Ausnahme in Art. 13 Abs. 4 DS-GVO hinzugezogen werden, halten wir europarechtlich für nicht zulässig.

Ausnahmen nur bei Direkterhebungen

Informationen liegen bereits vor

Eine Informationspflicht besteht gem. Art. 13 Abs. 4 DS-GVO nicht, wenn und soweit der Betroffene bereits über die entsprechenden Informationen verfügt.

Ausnahmen nur bei Dritterhebungen

Ausnahmegründe Art. 14 Abs. 5 DS-GVO

Ausnahmen von der Informationspflicht bei Dritterhebungen sind u. a. im Art. 14 Abs. 5 DS-GVO geregelt. Dementsprechend besteht etwa dann keine Informationspflicht, wenn

- Betroffene bereits über die Informationen verfügen und sich seit der letzten Verarbeitung nichts geändert hat,
- es unmöglich ist oder einen „unverhältnismäßigen Aufwand“ erfordern würde, diese Informationen zu erteilen, oder
- die Informationserteilung an Betroffene dazu führen würde, dass es unmöglich wird, personenbezogene Daten für die Verarbeitungsziele noch zu nutzen oder die Ziele der Verarbeitung ernsthaft beeinträchtigen werden.

Ausnahmen für Direkt- und Dritterhebungen

In den §§ 8 und 16 Abs. 1 LDSG sind Ausnahmen von der Informationspflicht sowohl für Direkt- als auch für Dritterhebungen geregelt.

Gem. § 8 LDSG besteht u. a. keine Informationspflicht, wenn eine entsprechende Information,

Ausnahmegründe § 8 LDSG

- die öffentliche Sicherheit,
- die Verhütung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung,
- die Geltendmachung, Ausübung oder Verteidigung von zivilrechtlicher Ansprüche gefährden würden oder
- die Daten und Tatsache der Verarbeitung nach einer Rechtsvorschrift oder zum Schutz der betroffenen Person oder der Rechte oder Freiheiten anderer Personen geheim gehalten werden müssen.

In § 16 LDSG ist geregelt, dass bei der Verarbeitung personenbezogener Daten im Zusammenhang mit öffentlichen Auszeichnungen und Ehrungen keine Informationspflichten bestehen.

Ausnahme öffentliche Auszeichnungen und Ehrungen

Besonderheiten bei der Direkterhebung für Sozialleistungsträger

Besonderheiten bei der Direkterhebung nach Art. 13 DSGVO für Sozialleistungsträger können folgendem Link entnommen werden: https://www.baden-wuerttemberg.datenschutz.de/besonderheiten-zur-informationspflicht-nach-artikel-13-der-datenschutz-grundverordnung-fuer-sozialleistungstraeger/

27.Gemeinderat

Grundlegendes

Gemeindliches Hauptorgan

Der Gemeinderat ist nach § 24 Absatz 1 GemO die Vertretung der Bürger und das Hauptorgan der Gemeinde. Er legt die Grundsätze für die Verwaltung fest und entscheidet über alle Angelegenheiten der Gemeinde, soweit nicht der Bürgermeister kraft Gesetzes zuständig ist. Als Hauptorgan kommt dem Gemeinderat die kommunalpolitische Führung zu, indem er die „Leitlinien" der Gemeindepolitik festlegt. Im Rahmen seiner Aufgabenerfüllung verarbeitet der Gemeinderat eine Vielzahl personenbezogener Daten, darunter auch besonders sensible.

Verantwortliche Stelle für Datenverarbeitungen des Gemeinderats

Gemeinde als Gebietskörperschaft

Verantwortliche Stelle ist die Gemeinde als Gebietskörperschaft (vertreten durch den Bürgermeister). Die datenschutzrechtliche Verantwortung einer Gemeinde umfasst auch die Tätigkeit seines Hauptorgans Gemeinderat und die Verarbeitung personenbezogener Daten durch Mitglieder des Gemeinderats.

Ausnahme unbefugte Verwendung für private Zwecke

Etwas anderes ergibt sich nur, wenn Mitglieder des Gemeinderats personenbezogene Daten, von denen sie im Rahmen ihrer ehrenamtlichen Tätigkeit Kenntnis erlangt haben, unbefugt für andere Zwecke, beispielsweise private Zwecke, verwenden. In diesen Fällen ist zu prüfen, ob es sich um einen sog. Exzess handelt, der dem Gemeinderatsmitglied nicht als ehrenamtlich Tätigen, sondern als Privatperson zuzuordnen ist. Unter bestimmten Voraussetzungen kann eine solche rechtswidrige Datenverarbeitung bußgeldpflichtig sein, da diese einem Gemeinderatsmitglied als Privatperson (und nicht der Gemeinde) zuzurechnen ist.

Verschwiegenheitspflicht von Gemeinderatsmitgliedern

Verschwiegenheitspflicht umfasst hinreichende Beachtung des Datenschutzes

Mitglieder des Gemeinderats erhalten mitunter sehr weitgehende Informationen über persönliche Verhältnisse und Lebensumstände von Personen. Als ehrenamtlich Tätige sind sie nach § 17 Absatz 2 GemO zur Verschwiegenheit über alle Angelegenheiten verpflichtet, deren Geheimhaltung gesetzlich vorgeschrieben, besonders angeordnet oder ihrer Natur nach erforderlich ist. Hierunter fällt selbstverständlich auch die hinreichende Beachtung von datenschutzrechtlichen Vorschriften, wie dass personenbezogene Daten nicht unbefugt Dritten offenbart werden dürfen. Die Verschwiegenheitspflicht besteht auch nach Beendigung der ehrenamtlichen Tätigkeit als Gemein-

deratsmitglied fort.

Sitzungs- und Beschlussvorlagen für den Gemeinderat

Vorlagen mit personenbezogenen Daten soweit erforderlich und kein Entgegenstehen berechtigter Interessen Einzelner

In § 34 Absatz 1 GemO ist geregelt, dass der Bürgermeister den Gemeinderat mit angemessener Frist einberuft und diesem rechtzeitig vor dem Sitzungstag die Verhandlungsgegenstände mitteilt und dabei die für die Verhandlung erforderlichen Unterlagen (auch mit personenbezogenen Daten) beifügt, soweit dem nicht das öffentliche Wohl oder berechtigte Interessen Einzelner entgegenstehen. Erforderlich in diesem Sinne sind alle Unterlagen, die zur Vorbereitung der Mitglieder des Gemeinderates auf die Sitzung, die Bildung einer vorläufigen Meinung und zur Besprechung in den Fraktionen benötigt werden.

Definition „berechtigtes Interesse“

Unter einem berechtigten Interesse ist jedes rechtlich geschützte und anerkannte Interesse eines Betroffenen zu verstehen, wie beispielsweise die Vermeidung des Bekanntwerdens persönlicher Verhältnisse, sofern nach allgemeiner vernünftiger Abwägung ein individuelles Schutzbedürfnis erkennbar ist.

Keine Vorschrift für Übermittlung an Dritte

Eine Übermittlung personenbezogener Daten an Dritte, wie die sog. Saalöffentlichkeit und/oder Internetöffentlichkeit, ist vom Regelungsgehalt dieser Vorschrift nicht umfasst.

Löschung nach Aufgabenerfüllung

Zudem hat eine Gemeinde darauf hinzuweisen, dass Unterlagen mit personenbezogenen Daten, die zu Aufgabenerfüllung des Gemeinderats nicht mehr benötigt werden, datenschutzgerecht zu löschen sind. Bei Unterlagen in Papierform bietet es sich an, dass diese Unterlagen an die Gemeindeverwaltung zurückgegeben und von dieser vernichtet werden. Elektronische Daten, die von Gemeinderatsmitgliedern gespeichert wurden, sind unwiederbringlich zu löschen.

Informationsrecht des Gemeinderats

Beurteilungsmaßstab Erforderlichkeit zur Aufgabenerfüllung

Auch steht dem Gemeinderat (als Kollegialorgan) unter bestimmten Voraussetzungen ein umfassendes Informationsrecht zu (vgl. § 24 Abs. 3 GemO). Das Informationsrecht des Gemeinderats bezieht sich dabei auch auf Angelegenheiten, die zum gesetzlichen Aufgabenbereich des Bürgermeisters gehören, also auch auf Weisungsaufgaben. Datenschutzrechtlicher Beurteilungsmaßstab, wie weit das Informationsrecht des Gemeinderats in Bezug den Erhalt personenbezogener Daten reicht, ist die Erforderlichkeit der entsprechenden Informationen für die Wahrnehmung der Funktion des Gemeinderats.

Öffentlichkeit von Gemeinderatsitzungen

Öffentlichkeitsgrundsatz

Sitzungen des Gemeinderats sind nach § 35 Absatz 1 Satz 1 GemO grundsätzlich öffentlich. Dies bedeutet, dass jedermann zu den Gemeinderatssitzungen Zutritt hat (sog. Saalöffentlichkeit). Die Öffentlichkeit von Gemeinderatssitzungen gehört zu den wesentlichen Grundsätzen der Gemeindeverwaltung.

Nicht-öffentliche Sitzungen

Es ist jedoch nicht ausgeschlossen, dass das berechtigte Interesse Einzelner, dass keine Daten von ihnen in Gemeinderatsitzungen veröffentlicht werden, eine Beratung und Beschlussfassung in nicht-öffentlicher Sitzung erfordern können, falls auf die Herstellung eines Personenbezugs nicht verzichtet werden kann.

Abwägung zwischen Öffentlichkeitsgrundsatz und berechtigten Interessen Einzelner

Dies wäre ggf. von der verantwortlichen Gemeinde im Rahmen einer Abwägung zwischen dem Öffentlichkeitsgrundsatz und dem Schutzinteresse des jeweiligen Betroffenen zu prüfen und festzustellen. Klassische Beispiele für Tagesordnungspunkte, die in einer nicht-öffentlichen Sitzung zu behandeln sind, sind unter anderem Personalangelegenheiten oder Anträge auf Stundung und Erlass von Abgabepflichtigen.

Namensnennung nur bei Erforderlichkeit

Die Nennung des Namens einer natürlichen Person in einer öffentlichen Gemeinderatssitzung muss auch zur gemeindlichen Aufgabenerfüllung erforderlich sein. Es muss also mindestens ein tragender Sachgrund vorliegen, warum es nicht ausreicht, dass der Gemeinderat sich bei seinen (öffentlichen) Beratungen und Beschlussfassungen auf reine Sachverhaltserörterungen (ohne Personenbezug) beschränken kann. Wenn die Herstellung eines Personenbezugs während einer Gemeinderatssitzung erforderlich sein sollte, ist von der Gemeinde zu prüfen, ob berechtigte Interessen der insoweit Betroffenen berührt sind, die eine Beratung und Beschlussfassung in nicht-öffentlicher Sitzung erfordern.

Auslage von Beratungsunterlagen im Sitzungsraum

Rechtsgrundlage für Auslage mit personenbezogenen Daten erforderlich

In der kommunalen Praxis ist es durchaus üblich, für den Gemeinderat bestimmte Sitzungsunterlagen für die Saalöffentlichkeit auszulegen. In der Regel sind damit Zwecke wie ein transparenteres Verwaltungshandeln, eine bessere Bürgerbeteiligung oder eine höhere Akzeptanz von Entscheidungen verbunden. Auch wenn diesen Zielen nach unserer Auffassung große Bedeutung zukommt, so ist dennoch zu beachten, dass soweit die Sitzungsunterlagen personenbezogene Daten beinhalten, eine Rechtsgrundlage für diese Form der Veröffentlichung benötigt wird.

Keine einschlägigen Rechtsvorschriften

Dabei ist zu beachten, dass die §§ 34 Absatz 1 Satz 1 (Einberufung der Sitzung unter Beifügung der erforderlichen Unterlagen), 35 Absatz 1 Satz 1 (Öffentlichkeit der Sitzungen) und 41 b Absatz 3 Satz 1 (Auslage von Sitzungsunterlagen) GemO keine Vorschriften sind, die selbst eine öffentliche Auslegung von Sitzungsunterlagen mit personenbezogenen Daten erlauben.

Keine unbefugte Veröffentlichung personenbezogener Daten bei Auslage

Zwar regelt § 41 b Absatz 3 Satz 1 GemO, dass Beratungsunterlagen in öffentlichen Sitzungen im Sitzungsraum für die Zuhörer auszulegen sind. Gemäß Satz 2 dieser Vorschrift ist jedoch durch geeignete Maßnahmen sicherzustellen, dass hierdurch personenbezogene Daten nicht unbefugt offenbart werden. Der Gesetzesbegründung hierzu kann unter anderem entnommen werden, dass bei der Auslegung von Beratungsunterlagen im Sitzungsraum personenbezogene Daten zu schützen sind. „Eine Auslage von Beratungsunterlagen für öffentliche Sitzungen muss nicht erfolgen, wenn dies [zum Schutz personenbezogener Daten] nicht ohne erheblichen Aufwand oder erhebliche Veränderung der Sitzungsunterlagen erfolgen kann."

Beratungsanfragen von Gemeinderatsfraktionen oder einzelnen Mitgliedern des Gemeinderats

Unterschiedliche Rechtsauffassungen innerhalb der Gemeinde sind zunächst auch innerhalb dieser zu klären

Immer wieder wenden sich Gemeinderatsfraktionen oder einzelne Mitglieder des Gemeinderats mit der Bitte um datenschutzrechtliche Beratung oder sonstiges Tätigwerden an unsere Dienstelle, insbesondere wenn sie eine andere Rechtsauffassung als der Bürgermeister oder die Gemeindeverwaltung vertreten. Dabei geht es meist nicht um die Verarbeitung ihrer Daten, sondern um allgemeines Datenschutz- und teilweise um reines Verwaltungsrecht. Hier ist zu beachten, dass der Gemeinderat und seine Untergliederungen integraler Teil der Gebietskörperschaft Gemeinde sind. Zwar berät unsere Dienststelle Gemeinden als verantwortliche Stellen, wir sind jedoch keine Vermittlungs- oder Mediationsstelle bei Unstimmigkeiten oder unterschiedlichen Rechtsauffassungen innerhalb der verantwortlichen Stelle Gemeinde, wie etwa bei Meinungsverschiedenheiten zwischen Gemeinderat und Gemeindeverwaltung.

Hervorgehobene Bedeutung des Bürgermeister bei internen Unstimmigkeiten

In solchen Fällen könnte es eine Erwägung der Gemeinde als verantwortlicher Stelle sein, den behördlichen Datenschutzbeauftragten zur Beratung und Unterstützung und ggf. das Rechtsamt hinzuziehen. Letztlich kommt in solchen Fällen dem Bürgermeister mit Blick auf seine kommunalverfassungsrechtlich exponierten Stellung als Leiter der Gemeindeverwaltung, Vorsitzender des Gemeinderats und gesetzlicher Vertreter der Gemeinde (vgl. § 42 Absatz 1 GemO) bei der Klärung gemeindeinterner Unstimmigkeiten und entsprechender datenschutzrechtlichen Fragestellungen eine hervorgehobene Bedeutung zu.

Eingaben von Gemeinderatsmitgliedern aufgrund nicht erhaltender personenbezogener Daten

Teilweise wenden sich Gemeinderatsmitglieder an unsere Dienststelle, da sie der Auffassung sind, dass sie aufgrund ihrer ehrenamtlichen Tätigkeit Anspruch auf bestimmte Informationen mit Personenbezug haben und diese zu Erfüllung ihrer Aufgaben auch erforderlich seien. Diese haben sie von der Gemeindeverwaltung jedoch nicht erhalten, teilweise auch unter Verweis auf das Datenschutzrecht. Ob der Gemeinderat als Kollegialorgan, eine Gemeinderatsfraktion oder einzelne Mitglieder des Gemeinderats einen Informationsanspruch haben, richtet sich zunächst nach kommunal-(verfassungs-)rechtlichen Vorschriften. Wenn es dabei um personenbezogene Daten geht, sind die heranzuziehenden kommunalrechtlichen Vorschriften in aller Regel sogenannte besondere Vorschriften, die auf personenbezogene Daten anzuwenden sind. Das bedeutet, dass wenn ein Informationsanspruch des Kollegialorgans Gemeinderat oder seiner Untergliederungen aufgrund kommunalrechtlicher Regelungen besteht, der Datenschutz einer entsprechenden Datenweitergabe grundsätzlich nicht entgegensteht.

Anforderungen an gemeindliche Beratungsanfragen

Bei Fragen kann sich eine Gemeinde als datenschutzrechtlich verantwortliche Stelle zur Beratung an unsere Dienststelle wenden. Hierzu ist es – wie auch bei anderen Beratungsanfragen – grundsätzlich erforderlich, dass die Gemeinde den zu Grunde liegenden Sachverhalt ausführlich schildert, das Ergebnis ihrer eigenen datenschutzrechtlichen Prüfung mitteilt und hierzu konkrete Fragen stellt. Bei der gemeindlichen Sachverhaltsfeststellung und -prüfung sollte der behördliche Datenschutzbeauftragte und soweit vorhanden das Rechtsamt eingebunden werden. Mitglieder des Gemeinderats, wie auch Mitarbeiter der Gemeindeverwaltung, können sich gerne an unsere Dienststelle wenden, wenn sie im Auftrag der Gemeinde als verantwortlicher Stelle anfragen.

Informationelles Selbstbestimmungsrecht von Gemeinderatsmitgliedern

Rechtsgrundlage für die Verarbeitung personenbezogener Daten von Gemeinderatsmitgliedern erforderlich

Anders verhält es sich, wenn ein Mitglied des Gemeinderats der Auffassung ist, dass die Gemeinde Daten über seine Person unrechtmäßig verarbeitet. Selbstverständlich sind auch Gemeinderatsmitglieder Träger des Rechts auf informationelle Selbstbestimmung. Werden personenbezogene Daten von Mitgliedern des Gemeinderats von einer Gemeinde verarbeitet, benötigt sie (wie auch bei der Verarbeitung von Beschäftigtendaten) hierfür eine Rechtsgrundlage.

Empfehlung Einwilligung schriftlich einzuholen

Soweit Datenverarbeitungen auf die Einwilligung eines Mitglieds des Gemeinderats gestützt werden, empfehlen wir, diese schriftlich einzuholen und zu Dokumentationszwecken zu den Akten zu nehmen. Gemeinderatsmitglieder, die sich aufgrund der Verarbeitung ihrer Daten in ihren Rechten verletzt fühlen, können sich als Betroffene jederzeit an unsere Dienststelle wenden.

Technische und organisatorische Maßnahmen

Eine Gemeinde hat als verantwortliche Stelle bei der Verarbeitung personenbezogener Daten durch den Gemeinderat unter anderem Folgende technische und organisatorische Maßnahmen hinreichend zu beachten:

Informiertheit von Gemeinderatsmitgliedern

Informationen zum Datenschutzrecht

Es ist wichtig, dass Mitglieder des Gemeinderats wissen, welche datenschutzrechtlichen Vorschriften bei ihrer ehrenamtlichen Tätigkeit zu beachten sind. Deshalb hat die Gemeinde die Gemeinderatsmitglieder (ähnlich wie bei Gemeindebediensteten) hierüber zu informieren. Wir empfehlen, zumindest die wichtigsten Punkt schriftlich zu fixieren.

Grundlegende Informationen zu Beginn der Amtszeit

Eine entsprechende Unterrichtung sollte zu Beginn einer neuen Amtsperiode des Gemeinderats erfolgen und bedarfsweise wiederholt werden. Hierzu gehören auch Hinweise, wie gegebenenfalls mit Datenpannen umzugehen ist, was bei Verlust oder Entsorgung eines privaten (mobilen) Endgeräts, dass auch für die Gemeinderatstätigkeit verwendet wurde, zu beachten ist oder welche Folgen das Ausscheiden aus dem Gemeinderat nach sich zieht.

Trennung Gemeinderatstätigkeit und andere Sphären

Enge datenschutzrechtliche Grenzen

Der strikten und klaren Trennung zwischen einer ehrenamtlichen Tätigkeit als Gemeinderat und anderen Sphären (wie privater oder beruflicher Bereich) kommt im Datenschutzrecht große Bedeutung zu. Mitunter verwenden Gemeinderatsmitglieder ihre privaten PCs und Laptops oder andere Endgeräte zur Speicherung von Dokumenten mit personenbezogenen Daten oder es werden seitens der Gemeindeverwaltung E-Mails mit personenbezogenen Daten an private oder berufliche E-Mail-Adressen von Gemeinderatsmitgliedern versandt. Das Datenschutzrecht setzt dem jedoch sehr enge Grenzen.

Verwendung gemeindlicher E-Mail-Adressen und Vermeidung des Einsatzes privater Endgeräte

Die Gemeinde hat die erforderlichen Maßnahmen zu ergreifen, um zu gewährleisten, dass nur Gemeinderatsmitglieder Kenntnis von personenbezogenen Daten erlangen und nicht unbefugte Dritte (wie etwa Familienmitglieder, Freunde, Arbeitskollegen). Deshalb sollten nach Möglichkeit unter anderem Gemeinderäte für ihre ehrenamtliche Tätigkeit gemeindliche E-Mail-Adressen erhalten und keine personenbezogenen Daten, die im Zusammenhang mit der ehrenamtlichen Tätigkeit stehen, auf privaten Endgeräte gespeichert werden.

Transparenz

Gemeinde darf Überblick über Datenverarbeitung nicht verlieren

Es muss für die Gemeinde nachvollziehbar sein, welches ihre Organe und deren Untergliederungen bzw. welche Personen, die in ihre Verantwortungssphäre fallen (wie etwa Gemeinderatsmitglieder oder Gemeindebedienstete), welche personenbezogenen Daten zu welchem Zweck in welcher Form auf welcher Rechtsgrundlage wie lange verarbeiten. Anderenfalls läuft die Gemeinde Gefahr, dass sie Betroffenenrechten, wie beispielsweise Auskunfts- oder Löschrecht, und anderen datenschutzrechtlichen Anforderungen nicht hinreichend gerecht werden kann. Um dies zu gewährleisen, hat sie die hierfür erforderlichen technischen und organisatorischen Maßnahmen zu treffen.

Löschkonzeption

Keine Schattenarchive mit personenbezogenen Daten bei Gemeinderatsmitgliedern

Wenn Gemeinderäte zur Aufgabenerfüllung Unterlagen mit personenbezogenen Daten erhalten, muss auch geregelt sein, wann, wie und von wem diese Unterlagen zu löschen sind. Für die Umsetzung eines Löschkonzepts eignet sich die Anwendung der Normen DIN 66398 und DIN 66399. Es dürfen bei Gemeinderatsmitgliedern keine Schattenarchive mit personenbezogenen Unterlagen für die Gemeinderatsarbeit entstehen, auch nicht in Papierform. Es sind Fälle bekannt, in denen alle Dokumente des Gemeinderats der letzten 15 Jahre (und teils noch länger) auf privaten PCs zu finden waren oder in Aktenordnern abgelegt wurden.

Restriktiver Maßstab bei Löschpflicht

Grundsätzlich ist ein sehr restriktiver Maßstab an die Löschpflicht von personenbezogenen Daten anzulegen, die von Gemeinderatsmitgliedern selbst außerhalb der gemeindlichen Sphäre gespeichert werden. Es ist nicht Aufgabe eines Gemeinderatsmitglieds, personenbezogene Daten für eine möglicherweise zu einem unbestimmten späteren Zeitpunkt erforderliche (Weiter-)Verwendung zu speichern. Sollte sich zu einem späteren Zeitpunkt herausstellen, dass für die gemeinderätliche Tätigkeit nochmals die gleichen personenbezogenen Daten benötigt werden, ist es Aufgabe der Gemeindeverwaltung, diese erneut den Mitgliedern des Gemeinderats zu Verfügung zu stellen.

Nutzung privater Endgeräte für ehrenamtliche Zwecke

Private Endgeräte grundsätzlich nur als Lesegeräte

Die Nutzung privater Endgeräte, wie PC und Laptops, durch Mitglieder des Gemeinderats sollte grundsätzlich nur erfolgen, wenn diese lediglich als Lesegeräte (Web-Endgerät) verwendet werden, ohne dass eine Datenspeicherung auf einem internen Speichermedium erfolgt.

Gefahr von Sicherheitslücken

Hintergrund hierfür ist, dass Sicherheitslücken schnell übersehen werden können und möglicherweise der Zugriff von weiteren Personen, beispielsweise durch Familienmitglieder, schwierig zu kontrollieren ist. Auch der Schutz vor Viren und Trojanern muss durch den Einsatz entsprechender sog. Security Tools gewährleistet sein, die dem Stand der Technik entsprechen. Löschfristen müssen (auch von Mitgliedern des Gemeinderats) beachtet werden. Gemeinderatsmitglieder müssen wissen, wie sie sich bei Verlust von privaten Endgeräten datenschutzgerecht verhalten. Es sind Regelungen zu treffen, was zu beachten ist, wenn private Endgeräte von Dritten gewartet und repariert oder entsorgt werden.

Umsetzung aller datenschutzrechtlichen Anforderungen in der Praxis schwierig

Es bedarf somit einer Vielzahl von Regelungen für den Einsatz privater Endgeräte für eine Gemeinderatstätigkeit. Grundsätzlich dürfte es sich in der gemeindlichen Praxis als schwierig erweisen, alle erforderlichen organisatorischen und technischen Maßnahmen hinreichend umzusetzen. Deshalb raten wir hiervon ab.

Geschützter Container auf privaten Endgeräten

Wenn private Endgeräte dennoch eingesetzt und dort personenbezogene Daten gespeichert werden sollen, ist die Speicherung von Gemeinderatsunterlagen in einem geschützten Container oder einer gleich wirksamen Schutzmaßnahme unabdingbar. Eine datenschutzgerechtere Alternative für den Einsatz privater Endgeräte stellen Tablets mit Mobile-Device-Management dar.

Tablets mit Mobile-Device-Management für Gemeinderatsmitglieder

Empfehlung Tablets mit Mobile-Device-Management zu verwenden

Grundsätzlich ist bei Einsatz eines Gremieninformationsportal die Verwendung von gemeindlichen Tablets mit Mobile-Device-Management zu empfehlen, die den Gemeinderatsmitgliedern zur Verfügung gestellt werden. Eine Speicherung von Dateien auf privaten Endgeräten ist damit obsolet. Löschfristen können zentral umgesetzt werden und für Dritte wird der Zugriff auf (vertrauliche) Dokumente erschwert. Bei der Verwendung von Tablets mit Mobile-Device-Management können auf einem verwalteten Gerät weiterhin Dokumente gespeichert und bearbeitet werden und bei einem Verlust kann das Gerät aus der Ferne geortet und gelöscht werden. Auch temporäre Dateien, die bei einem Dokumentendownload aus dem Ratsinformationssystem entstehen können, müssen bei dienstlichen Geräten nicht gesondert betrachtet werden. Zu beachten ist, einen geeigneten Speicherort für die Dokumente auszuwählen (eigener Server vs. Cloud), und als technische und organisatorische Maßnahmen zumindest ein Zugriffskonzept und eine Benutzerverwaltung zu erstellen und auch umzusetzen.

E-Mail-Kommunikation

Keine Verwendung privater oder beruflicher E-Mail-Adressen

Mitglieder des Gemeinderats erhalten zu ihrer Aufgabenerfüllung eine Vielzahl personenbezogener Daten, darunter solche, die Art. 9 DS-GVO (Verarbeitung besonders sensibler Daten) zuzuordnen sind. Die Kommunikation per E-Mail ist in den Gemeinden in vielen Bereichen inzwischen Standard. Gemeindemitarbeiter verfügen in aller Regel über eigene dienstliche E-Mail-Adressen. Bei Gemeinderatsmitgliedern ist dies, wie wir aus unserer Beratungs- und Aufsichtspraxis wissen, allerdings nicht immer der Fall. Bei der Übermittlung von personenbezogenen Daten an Gemeinderatsmitglieder werden mitunter deren private oder berufliche E-Mail-Adressen verwendet. Auf solche E-Mail-Adressen haben jedoch möglicherweise auch Dritte im familiären oder beruflichen Umfeld Zugriff, wie beispielsweise Familienmitglieder oder Arbeitskollegen. Die Verwendung privater oder beruflicher E-Mail-Adressen, um Gemeinderatsmitgliedern für die Ausübung ihrer ehrenamtlichen Tätigkeit personenbezogene Daten zu übermitteln, ist deshalb grundsätzlich nicht zulässig.

Nutzung gemeindlicher E-Mail-Adressen

Vielmehr sollte eine Gemeinde den Mitgliedern des Gemeinderats gemeindliche E-Mail-Adressen zur Verfügung stellen und die elektronische Kommunikation, soweit dabei personenbezogene Daten verarbeitet werden, ausschließlich über diese führen. Des Weiteren hat die Gemeinde durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass auf diese gemeindlichen E-Mail-Adressen auch nur das jeweilige Gemeinderatsmitglied Zugriff hat.

28. Internetauftritt

Grundlegendes

Rechtsgrundlage für Internetveröffentlichungen erforderlich

Nahezu jede Gemeinde in Baden-Württemberg betreibt eine oder mehrere eigene Internetseiten. Bei der Veröffentlichung von personenbezogenen Daten im Internet kommen für Gemeinden in der Mehrzahl der Fälle zwei Erlaubnistatbestände in Betracht: eine Rechtsvorschrift, die eine Internetveröffentlichung erlaubt, oder eine wirksame Einwilligung des Betroffenen.

Rechtsvorschrift

Soweit eine Gemeinde die Veröffentlichung von personenbezogenen Daten im Internet auf eine Rechtsvorschrift stützt, ist unter anderem zu beachten, dass es in diesem Zusammenhang nicht ausreicht, wenn eine entsprechende Rechtsvorschrift allgemein eine Veröffentlichung von bestimmten personenbezogenen Daten erlaubt, sie muss sich vielmehr ausdrücklich auf diese besondere Veröffentlichungsform (Internet) beziehen.

Einwilligung

Wirksame Einwilligungen setzen u. a. die hinreichende Informiertheit der Betroffenen voraus, die auch die besonderen Gefahren und Risiken von Internetveröffentlichungen (wie globale Verfügbarkeit, Verknüpfungsmöglichkeiten mit anderen Daten im Internet, Erfassung durch Suchmaschinen) umfassen.

Beiträge von und über andere Stellen

Verantwortung für Internetveröffentlichung auch bei Gemeinde

Viele Gemeinden veröffentlichen in ihrem Internetauftritt Beiträge mit personenbezogenen Daten, die andere Stellen erstellt haben. Ein Beispiel hierfür ist der Vereinsbereich. In solchen Fällen ist zu beachten, dass nicht nur die andere Stelle der Gemeinde einen Betrag mit personenbezogenen Daten zur Internetveröffentlichung zukommen lässt, sondern auch die Gemeinde selbst verantwortliche Stelle ist. Und zwar für die Veröffentlichung dieser Beiträge auf ihrer Internetseite.

Einwilligung als Rechtsgrundlage

Hierfür benötigt die Gemeinde eine Rechtsgrundlage, die ihr diese Vorgehensweise erlaubt. In aller Regel kommt hier nur eine wirksame Einwilligung der jeweils Betroffenen in Betracht. Grundsätzlich kann die andere Stelle eine Einwilligung des Betroffenen einholen, die (zumindest auch) eine gemeindliche Internetveröffentlichung umfasst.

Information andere Stelle über datenschutzrechtliche Anforderungen

Die Gemeinde hat die andere Stelle, deren Beiträge sie veröffentlicht, hinreichend klar über die datenschutzrechtlichen Anforderungen an eine wirksame Einwilligung bei Internetveröffentlichungen zu informieren und sich von dieser allgemein bestätigen zu lassen, dass für jedes einzelne personenbezogene Datum, das veröffentlicht werden soll, eine wirksame Einwilligung des jeweils Betroffenen vorliegt.

Stichproben, ob Einwilligungen bei anderer Stelle vorliegen

Es ist zwar nicht erforderlich, dass sich eine Gemeinde für jeden Einzelfall auch tatsächlich eine Einwilligung vorlegen lässt. Sie hat jedoch stichprobenweise zu überprüfen, ob der anderen Stelle auch tatsächlich entsprechende Einwilligungen vorliegen. Selbstverständlich ist es einer Gemeinde unbenommen, sich selbst von den Betroffenen eine Einwilligung für eine Internetveröffentlichung einzuholen.

Gemeinsame Verantwortung

Je nach konkreter Gestaltung im Einzelfall kann bei solchen Sachverhalten zudem Art. 26 DS-GVO Bedeutung zukommen, der regelt, was bei gemeinsam Verantwortlichen zu beachten ist.

Internetveröffentlichung von Tagesordnung und Beratungsunterlagen von öffentlichen Gemeinderatssitzungen

Keine unbefugte Offenbarung personenbezogener Daten

Gemäß § 41 b GemO sind unter bestimmten Voraussetzungen Tagesordnung (Abs. 2) und Beratungsunterlagen (Abs. 3) für öffentliche Gemeinderatssitzungen im Internet zu veröffentlichen. Jedoch ist dabei von einer Gemeinde sicherzustellen, dass dabei keine personenbezogenen Daten unbefugt offenbart werden. Das bedeutet, dass § 41 b Abs. 2 und 3 GemO selbst keine eigenständigen Erlaubnistatbestände für Internetveröffentlichungen personenbezogener Daten darstellen.

Gesetzesbegründung

In der Gesetzesbegründung zu § 41 b Abs. 2 GemO heißt es unter anderem: Die mit einer Internetveröffentlichung „verbundenen weitreichenden Verletzungen des Rechts auf informationelle Selbstbestimmung sind sorgfältig durch geeignete Maßnahmen, z.B. eine zuverlässige Anonymisierung der zu veröffentlichen Dokumente, zu vermeiden."

Begriff „unbefugt"

Unbefugt offenbart in diesem Sinne bedeutet, dass die Internetveröffentlichung personenbezogener Daten nicht auf eine Rechtsgrundlage gestützt werden kann.

Ausnahmen von der Veröffentlichungspflicht

Im Einzelfall kann von Veröffentlichungen im Internet abgesehen werden, wenn eine Anonymisierung personenbezogener Daten oder andere geeignete Maßnahmen nicht ohne erheblichen Aufwand oder erhebliche Veränderungen der Beratungsunterlagen möglich sind.

Gremienübertragungen im Internet

Keine Rechtsvorschrift als Erlaubnistatbestand

Gemeinden erkundigen sich bei unserer Dienststelle regelmäßig, unter welchen Voraussetzungen Gremiensitzungen im Internet übertragen werden dürfen. In Baden-Württemberg gibt es derzeit keine Rechtsvorschrift, die es einer Gemeinde erlauben würde, kommunale Gremiensitzungen ins Internet zu übertragen.

Regelung durch Gesetzgeber möglich

In diesem Zusammenhang ist zu beachten, dass der Gesetzgeber nach ständiger Rechtsprechung des Bundesverfassungsgerichts verpflichtet ist, die für Grundrechtseingriffe wesentlichen Regelungen normenklar durch ein formelles Gesetz zu treffen. Grundsätzlich ist der Gesetzgeber jedoch nicht daran gehindert, eine formellgesetzliche Rechtsgrundlage für die Übertragung von Gemeinderatssitzungen in das Internet, etwa in der Gemeindeordnung, zu schaffen.

Saalöffentlichkeit

Allgemeine Zugänglichkeit und hinreichend Platz für interessierte Bevölkerungskreise

Insbesondere stellt der Grundsatz der Öffentlichkeit von Gemeinderatssitzungen (§ 35 GemO) keine geeignete Rechtsgrundlage dar. Der Öffentlichkeitsgrundsatz ist bereits hinreichend beachtet, wenn die Sitzungen an einem Ort stattfinden, der allgemein zugänglich ist und Platz für interessierte Bevölkerungskreise bietet (sog. „Saalöffentlichkeit“). Eine weitere Ausdehnung der Öffentlichkeit, insbesondere auf die Internetöffentlichkeit, ist vom Öffentlichkeitsgrundsatz nicht abgedeckt.

Wirkungskreis Gemeinde

Auch ist zu beachten, dass in Gemeinderatssitzungen in aller Regel Angelegenheiten der örtlichen Gemeinschaft erörtert werden. Mit dem damit verbundenen Wirkungskreis einer Gemeinde ist eine global zugängliche Übertragung von Gemeinderatsitzungen nicht ohne weiteres in Einklang zu bringen.

Einwilligung

Einwilligung als Erlaubnistatbestand

Mangels eines anderen Erlaubnistatbestandes kann eine Internetveröffentlichung personenbezogener Daten im Zusammenhang mit Gemeinderatssitzungen nur auf eine wirksame Einwilligung des jeweils Betroffenen gestützt werden.

Rand- und Rahmenbedingungen für Einwilligung

Zwar sollten bei der Verarbeitung von personenbezogenen Daten durch öffentliche Stellen Einwilligungen (insbesondere bei schwerwiegenden Eingriffen in das Grundrecht auf informationelle Selbstbestimmung) nur eine untergeordnete Rolle spielen. Jedoch hält unsere Dienststelle es bei Internetübertragungen von Gemeinderatsitzungen (auch mit Blick auf das wichtige Ziel der Transparenz des Verwaltungshandelns) dennoch für zulässig, wenn Datenverarbeitungen auf der Grundlage freiwilliger Einwilligungserklärungen und unter Beachtung bestimmter Rand- und Rahmenbedingungen erfolgen.

Freie Wahlmöglichkeit

U. a. ist bei der Einholung einer Einwilligung bedeutsam, dass eine Willensbekundung nur freiwillig sein kann, wenn die betroffene Person „eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden“ (EG 42). Somit ist eine erteilte Einwilligung unwirksam, wenn der Betroffene keine wirklich freie Wahlmöglichkeit hat. Bei einem deutlichen Ungleichgewicht ist Unfreiwilligkeit zu unterstellen. Ob ein deutliches Ungleichgewicht vorliegt, kann nur im jeweiligen Einzelfall festgestellt werden.

Dokumentationspflicht

Es ist zu dokumentieren, aufgrund welcher Umstände und Erwägungen eine Gemeinde zu dem Ergebnis gelangt ist, dass das Merkmal der Freiwilligkeit vorliegt. Wir empfehlen, mit Hinblick auf die gemeindliche Beweislast, Einwilligungserklärungen schriftlich einzuholen und zu den Akten zu nehmen.

Betroffenengruppen

Betroffene keine homogene Gruppe

Soweit eine Gemeinde als verantwortliche Stelle beabsichtigt, im Rahmen von Internetübertragungen von Gemeinderatssitzungen personenbezogene Daten auf der Grundlage von Einwilligungen zu verarbeiten, ist von ihr auch das Vorliegen des Merkmals der Freiwilligkeit einer Einwilligungserklärung zu prüfen. Da die von einer Internetübertragung möglicherweise betroffenen natürlichen Personen keine homogene Gruppe darstellen, kann für eine erste Annäherung an das Merkmal der Freiwilligkeit eine Unterscheidung nach Betroffenengruppen (wie etwa Gemeinderatsmitglieder, Gemeindemitarbeiter, Vertreter kommunaler Gesellschaften und Bedienstete von anderen öffentlichen Stellen, externe Gutachter und Projektentwickler oder Saalöffentlichkeit) hilfreich sein.

Mitglieder des Gemeinderats

Einwilligung für gesamte Amtszeit möglich

Bei Mitgliedern des Gemeinderats sollte das Merkmal der Freiwilligkeit grundsätzlich gegeben sein. Es ist möglich, dass Gemeinderatsmitglieder Einwilligungserklärungen abgeben, die ihre gesamte Amtszeit umfassen. In der kommunalen Praxis gibt es Konstellationen, in denen nicht alle Mitglieder des Gemeinderats in die Verarbeitung ihrer Daten einwilligen wollen. Es ist durch technische und organisatorische Maßnahmen zu gewährleisten, dass nur von den Mitgliedern des Gemeinderats Bild- und Tonaufnahmen im Internet veröffentlicht werden, die hierin wirksam eingewilligt haben. Wenn einzelne Mitglieder des Gemeinderats eine erforderliche Einwilligung nicht erteilen, kann dies in der praktischen Umsetzung zu erheblichen Problemen führen.

Mitarbeiter der Gemeinde

Einwilligung bei Leitungs- und Führungsfunktionen

Bei Gemeindemitarbeitern ist das Vorliegen des Merkmals der Freiwilligkeit besonders sorgfältig zu prüfen. Bei Leitungs- und Führungsfunktion (wie etwa bei Amts-, Abteilungs- oder Projektleitungen) kann dieses Merkmal vorliegen. Bei anderen gemeindlichen Mitarbeitern ist die Regelannahme, dass aufgrund des bestehenden Beschäftigungs- bzw. Beamtenverhältnisses und des damit verbundenen Über- und Unterordnungsverhältnisses ein deutliches Ungleichgewicht und somit keine wirklich freie Wahlmöglichkeit der Bediensteten besteht. In diesen Fällen kann keine wirksame Einwilligung eingeholt werden. Abweichungen von dieser Regelannahme müssen von der verantwortlichen Gemeinde für den jeweiligen Bediensteten nachvollziehbar und schlüssig begründet werden können.

Vertreter kommunaler Gesellschaften und Bedienstete von anderen öffentlichen Stellen

Grundsätzlich gilt das Gleiche wie bei Bediensteten von Gemeindeverwaltungen. Unter diese Betroffenengruppe können unter anderem Geschäftsführer von kommunalen Gesellschaften, Revierförster oder Polizeibeamte subsumiert werden.

Externe Gutachter und Projektentwickler

Kein Ungleichgewicht bei Vergabeverfahren

Eine freie Wahlmöglichkeit von externen Gutachtern und Projektentwicklern im Sinne der DS-GVO kann beispielsweise dann gegeben sein, wenn eine Auftragserteilung aufgrund eines vorgeschalteten Vergabeverfahrens und somit nach den restriktiven Vorgaben des Vergaberechts erfolgte und deshalb davon ausgegangen werden kann, dass kein deutliches Ungleichgewicht vorliegt.

Saalöffentlichkeit

Keine Übertragung der Saalöffentlichkeit in Bild oder Ton

Eine Internetübertragung von Zuhörern in Bild und Ton ist in Hinblick auf die Anforderungen an eine Einwilligungserklärung datenschutzrechtlich besonders problematisch. Deshalb sollte hiervon Abstand genommen werden. Auch kann grundsätzlich nicht ausgeschlossen werden, dass eine Internetübertragung mit einem Abschreckungseffekt für Zuhörer verbunden ist und diese deshalb nicht an Gemeinderatsitzungen teilnehmen. Insbesondere kann eine laufende Kamera für Bürger eine Hemmschwelle darstellen, sich in sog. Bürgerfragestunden zu äußern. Deshalb sollten grundsätzlich weder Aufnahmen von Zuhörern noch von Bürgerfragestunden von Internetübertragungen umfasst sein.

Weitere Betroffene

Prüfung, ob freie Wahlmöglichkeit vorliegt

Allgemein ist im Rahmen einer Einzelfallprüfung festzustellen und darzulegen, warum eine echte freie Wahlmöglichkeit des jeweiligen Betroffenen und kein signifikantes Ungleichgewicht oder keine be-

deutsame strukturelle Ungleichheit vorliegt.

Podcast

Podcast als datenschutz- und praxisgerechter Lösungsansatz

Eine besonders datenschutzkonforme sowie intelligente und praxisgerechte Lösung kann ein Podcast mit Bild- und Tonaufzeichnungen aus Gemeinderatssitzungen sein. Bei entsprechender Umsetzung kann eine Gemeinde einen Podcast bereits im Laufe des auf die Sitzung folgenden Werktags auf ihren Internetseiten zum Abruf bereitstellen. Aufgrund des zumindest mehrstündigen zeitlichen Versatzes zwischen einer Gemeinderatssitzung und dem Einstellen des Podcasts in das Internet sollte eine Gemeinde grundsätzlich in der Lage sein, den Anforderungen des Datenschutzes hinreichend gerecht zu werden. Dennoch können sich interessierte Bürgerinnen und Bürger im Internet zeitnah und zudem zielgerichtet über den Verlauf von Gemeinderatssitzungen informieren.

Reichweitenanalyse, Web-Analytics, Remarketing, Tracking

In der Regel Personenbezug bei Analyse Nutzerverhalten

Viele Webseiten nutzen Werkzeuge von Drittanbietern zur Analyse des Nutzerverhaltens. Bei einigen (wie Google Analytics) ist damit die Weitergabe von umfangreichen individuellen und personenbezogenen Nutzungsdaten an Dritte verbunden. Auch wenn der Seitenbetreiber nur anonyme Statistiken erhält, sind die weitergegebenen Daten für den Betreiber des Analysedienstes oftmals individuell und personenbezogen. Dazu zählen nicht nur die IP-Adresse, sondern auch einzelne Personen identifizierende Merkmale, die z.B. über Cookies gespeichert werden.

Einwilligung im gemeindlichen Bereich nicht möglich

Während im nichtöffentlichen Bereich die Nutzung unter den hohen Hürden einer informierten, vorherigen, aktiven, freiwilligen, separaten und widerruflichen Einwilligung möglich ist (vgl. unsere FAQ zu Cookies und Tracking), haben öffentliche Stellen hinsichtlich der Freiwilligkeit der Einwilligung stets das Ober-/Unterordnungsverhältnis mit Blick auf ihre Eigenschaft als Hoheitsträger der Gemeinde zu betrachten. Daher scheidet eine Einwilligung im Bereich des Trackings bzw. der Weitergabe von Nutzungsdaten an Dritte grundsätzlich aus. Ferner ist für Hoheitsträger der Vorbehalt des Gesetzes zu beachten.

Reichweitenanalyse ohne Drittanbieter-Tracking

Gemeinden, die bisher zur Reichweiten-Analyse oder zum Remarketing einwilligungsbedürftige Dienste nutzen sollten daher umgehend auf datensparsame Alternativen wie lokal installierte Analyse-Tools wechseln.

Einbindung von Elementen Dritter

Üblicherweise Erhebung personenbezogener Daten

Dazu vergleichbar ist die Situation bei der Einbindung von anderen Elementen Dritter. Neben Reichweitenanalyse betrifft dies häufig Karten- und Übersetzungsdienste, Plugins von sozialen Netzwerken, Inhalte anderer Seiten oder Dateien von Content-Delivery-Networks (CDN) und ähnliches. Auch hier gilt, dass diese Einbindung üblicherweise damit verbunden ist, Dritten die Erhebung von personenbezogenen Daten zu ermöglichen, einschließlich der besuchten Seiten oder in Formularen eingegebenen Inhalten. Statt der Nutzung von CDNs sollten Gemeinden alle Dateien (wie Schriften oder JavaScript-Bibliotheken) selbst bereitstellen.

Verwendung eines gemeindlichen Proxy-Server

Für Kartendienste und ähnliches sollten daher bevorzugt solche anderer öffentlicher Stellen zum Einsatz kommen. Sollen Dienste wie OpenStreetmap genutzt werden, können die Daten auch über einen (Reverse-)Proxy der Gemeinde-Website geleitet werden, so dass Dritte keinen Zugriff auf Nutzerdaten erhalten.

Social Plugins

Soziale Netzwerke und Nutzerprofile

Plugins Sozialer Netzwerke sind Programme, die vom Hersteller dafür gedacht sind, dass der Verantwortliche sie in den eigenen Internetauftritt einbindet. Beispiele sind Plugins von Facebook (z.B. eingebettete Beiträge oder „Like-Button“), Google (z.B. Youtube-Videos), Twitter, u. v. a. mehr. Diese Plugins bewirken, dass der Hersteller über jeden Seitenbesuch und ggf. über weitere Interaktionen wie Formulareingaben auf der Internetseite informiert wird. Der Bezug zu konkreten Personen wird üblicherweise über Cookies oder ähnliche Mechanismen hergestellt.

Personenbezug bei Plugins

Wird der gemeindliche Internetauftritt durch einen im Sozialen Netzwerk des Plugin-Herstellers angemeldeten Nutzer besucht, wird er unmittelbar identifiziert und das Nutzungsverhalten auf der (gemeindlichen) Internetseite wird seinem Profil zugeordnet. Der Plugin-Hersteller erfährt dadurch, wer wann welche Unterseite der Website der Gemeinde besucht hat und was er dort getan hat. Beispiele können die für Schwangeren- oder AIDS-Beratung oder die für Fragen des Kirchenaustritts gedachten Unterseiten eines gemeindlichen Internetauftritts sein, sodass hier auch besondere Kategorien personenbezogener Daten nach Art. 9 DS-GVO betroffen sein können.

Erforderlichkeit zur Aufgabenerfüllung nicht ersichtlich

Für diese Datenweitergabe gibt es grundsätzlich keine Rechtsgrundlage. Daher sollten öffentliche Stellen keine Plugins sozialer Netzwerke in ihre Webseiten einbinden. Es ist nicht ohne weiteres ersichtlich, zur Erfüllung welcher gesetzlichen Aufgabe einer Gemeinde die Einbindung von Plugins Sozialer Netzwerke erforderlich sein soll. Wenn überhaupt kann nur eine Einwilligung einen Erlaubnistatbestand darstellen.

Anforderungen an eine Einwilligung

Gemeinden haben aber auch das Ober-/Unterordnungsverhältnis mit Blick auf ihre Eigenschaft als Hoheitsträger zu beachten, so dass eine rechtskonforme Einwilligung erfahrungsgemäß schwierig zu gestalten ist. Sollte eine Verarbeitung personenbezogener Daten im diesem Kontext trotz der öffentlichen Natur auf eine Einwilligung der Nutzer gestützt werden, so ist nicht nur, darauf zu achten, dass die Freiwilligkeit gewährleistet ist, sondern es sich auch um eine informierte, vorherige, aktive und separat erklärte Einwilligung handelt (vgl. FAQ Cookies und Tracking).

Umsetzung in der gemeindlichen Praxis

Wenn diese Bedingungen erfüllt sind, kann als Beispiel für eine praxisgerechte Umsetzung die 2-Klick-Lösung oder die 1-Klick-Lösung mit sogenannten Shariff-Buttons dienen.

Gemeinsame Verantwortung prüfen

Auch ist zu berücksichtigen, dass bei Plugins sozialer Netzwerks eine gemeinsame Verantwortung mit dem Hersteller bzw. Betreiber des sozialen Netzwerks bestehen kann. Ist dies der Fall, ist Art. 26 DS-GVO (Gemeinsam für die Verarbeitung Verantwortliche) zu beachten. Insbesondere ist nach Art. 26 DS-GVO eine Vereinbarung zur gemeinsamen Verantwortung abzuschließen, die u. a. die Wahrnehmung der Rechte der betroffenen Person regelt und beinhaltet, welcher Verantwortlicher welchen Informationspflichten gemäß den Artikeln 13 und 14 DS-GVO nachkommt.

Seiten innerhalb des sozialen Netzwerks

Gemeinsame Verantwortung liegt vor

Bei Seiten innerhalb eines Sozialen Netzwerks (wie etwa bei einer Facebook-Seite oder einem Twitter-Profil) liegt eine gemeinsame Verantwortung vor. Damit ist Art. 26 DS-GVO zu beachten. Zu Facebook hat die Datenschutzkonferenz von Bund und Ländern einen Fragenkatalog entwickelt, um die Rechtmäßigkeit des eigenen Auftritts hinterfragen zu können.

Dieser Fragenkatalog kann entsprechend für andere Dienste angewandt werden.

Datensicherheit

Schutz von Angriffen und Schwachstellenanalyse

Schutz nach dem Stand der Technik

Gemeindliche Internetseiten müssen nach dem Stand der Technik vor potentiellen Angriffen (beispielsweise SQL-Injection oder Cross-Site-Scripting etc.) gesichert sein. Für die Umsetzung ist Fachpersonal oder ein kompetenter externer Dienstleister notwendig. Ist dies nicht der Fall, ist es Angreifern unter Umständen möglich, auf personenbezogene Daten zuzugreifen bzw. Schadcode einzubinden, der dann auf den Rechnern der Besucher der Internetseite ausgeführt wird.

Regelmäßige Schwachstellenanalysen mit Ergebnisdokumentation

Leider gab es auch in Baden-Württemberg schon Fälle, bei denen derartige Schwachstellen auf Internetseiten von Gemeinden entdeckt wurden. Eine Gemeinde als verantwortliche Selle ist gefordert, regelmäßig zu prüfen (bzw. von unabhängigen Experten prüfen zu lassen), ob ihre Internetseiten Schwachstellen aufweisen und diese gegebenenfalls umgehend zu schließen. Mit Blick auf die bei den Gemeinden liegende Beweislast sollten entsprechende Überprüfungen mit Ergebnissen und sich eventuell anschließenden Maßnahmen dokumentiert werden.

Gesicherte Internetverbindung

Handlungsbedarf bei kleineren Gemeinden

Ein weiteres wichtiges Thema ist die Verschlüsselung von Internetseiten: Nur wenn Internetseiten über eine gesicherte HTTPS-Verbindung angeboten werden, sind die personenbezogenen Daten der Besucher der gemeindlichen Internetseiten während der Übertragung ausreichend geschützt. Eine Untersuchung unserer Dienststelle im Jahr 2018 hat ergeben, dass gerade bei kleineren Gemeinden in Baden-Württemberg in diesem Bereich noch Handlungsbedarf besteht: bei Gemeinden mit weniger als 30.000 Einwohnern sind viele Internetseiten noch nicht per HTTPS gesichert. Bei Gemeinden mit mehr Einwohnern sieht es hingegen besser aus und die Internetseiten großer Städte sind alle HTTPS-gesichert.

Zertifizierung für HTTPS-Sicherung kostenlos möglich

Dank Initiativen wie „Let's Encrypt" ist die für die HTTPS-Sicherung nötige Zertifizierung inzwischen kostenlos möglich. Finanzielle Gründe können also nicht mehr ins Spiel gebracht werden, wenn es um eine fehlende HTTPS-Sicherung einer Website geht. Vor diesem Hintergrund sind alle Gemeinden gefordert, zeitnah gesicherte Internetverbindungen einzurichten, soweit dies noch nicht geschehen ist. Wer ein Kontaktformular, Online-Formulare oder vergleichbares für Bürger bereitstellt, muss mindestens für diese Webseitenbereiche eine gesicherte HTTPS-Verbindung anbieten. Fehlt diese, muss unsere Dienststelle einschreiten.

E-Mail-Verkehr

Transportverschlüsselung erforderlich

Der Sicherheit bei der Kommunikation per E-Mail kommt eine entscheidende Bedeutung zu. In jedem Fall muss dafür gesorgt werden, dass die Mail-Kommunikation transportverschlüsselt erfolgt.

Innerhalb des KVN-Netzes (sowie gegebenenfalls zu Institutionen auf Landes- oder Bundesebene in anderen Netzen) findet eine Transport-Verschlüsselung bereits statt. Außerhalb dieser Netze für öffentliche Stellen ist die Transportverschlüsselung nicht durchgängig gewährleistet.

Einzelfallprüfung

Laut einem Transparenzbericht von Google kann aber bei europäischen und nord-amerikanischen E-Mail-Providern in der Regel von einer Transportverschlüsselung ausgegangen werden. Darüber hinaus gibt es Initiativen wie „E-Mail made in Germany“ (web.de, gmx, etc.), die eine Transportverschlüsselung sicherstellen. Im Zweifel wäre dies im Einzelfall zu prüfen. Dies gilt insbesondere dann, wenn es sich um sensible personenbezogene Daten nach Art. 9 DS-GVO, um große Datenmengen oder regelmäßige Übertragung personenbezogener Daten handelt.

Speicherung bei Dienstanbietern im Klartext

Zu beachten ist, dass eine Transportverschlüsselung ausschließlich während des Transports greift und die Inhalte der E-Mails bei den beteiligten Diensteanbietern im Klartext gespeichert werden. Auch innerhalb des KVN ist kein absoluter Schutz garantiert und je nach Risiko sind weitere Maßnahmen nötig.

Zustimmung von Betroffenen

Betroffene (wie Bürger), die mit einer Gemeinde per E-Mail kommunizieren, müssen sich diesen Risiken bewusst sein und dem Versandweg E-Mail zustimmen. Von einer Zustimmung ist auszugehen, wenn der Betroffene diesen Kommunikationsweg vorschlägt oder beginnt und ihn, nachdem die Gemeinde auf die Risiken und Alternativen hingewiesen hat, fortsetzt.

Ende-zu-Ende-Verschlüsslung außerhalb öffentlicher Verwaltungsnetze

Anders verhält es sich beim E-Mail-Verkehr mit personenbezogenen Daten zwischen öffentlichen Stellen, falls sich diese nicht im KVN (oder in anderen Netzen auf Landes- oder Bundesebene) befinden, sowie zwischen der Gemeinde und privaten Unternehmen/Vereinen. Sollten hier dauerhaft personenbezogene Daten ausgetauscht werden, ist eine Ende-zu-Ende-Verschlüsselung erforderlich. Bei sensiblen personenbezogenen Daten nach Art. 9 DS-GVO gilt dies immer, auch wenn nur im Einzelfall eine E-Mail versandt werden soll.

Alternativen zur Transportverschlüsselung

Alternativen können eine Ende-zu-Ende-Verschlüsselung per Webportal (wenn die Daten auch wirklich durchgängig bei der Speicherung auf dem Web-Portal Ende-zu-Ende-verschlüsselt vorliegen), OpenPGP, S/MIME oder Messenger sein. Gemeinden sollten sich befähigen, Ende-zu-Ende-Verschlüsselung nach gängigen Internet-Standards zu unterstützen.

29.Digitalisierung

Grundlegendes

Art. 32 DS-GVO normiert Anforderungen an die Datensicherheit

Die Digitalisierung stellt viele Gemeinden vor hohe Herausforderungen. Im Zuge der Umstellung von Verfahren wird dabei unter Zeitdruck oftmals auf notwendige technische und organisatorische Maßnahmen zur IT-Sicherheit verzichtet. Dabei stellt die Datenschutz-Grundverordnung in Artikel 32 deutliche Anforderungen an die Sicherheit der Verarbeitung. Personenbezogene Daten müssen auf allen Ebenen vor Zugriff und Veränderung von Dritten wie zum Beispiel durch starke Verschlüsselung geschützt werden und dürfen nicht (oftmals auch unabsichtlich) an Dritte weitergegeben werden. Gemeinden haben dabei jeweils ein angemessenes Schutzniveau einzuhalten.

Neben allgemeinen strategischen Themen beschäftigen viele Gemeinden aber auch diverse Einzelthemen. Auf ausgewählte Einzelthemen wird im Folgenden näher eingegangen.

IT-Grundschutz für Gemeinden

Das Bundesamt für Sicherheit in der Informationstechnik hat in seinen Internetauftritt Informationen zum IT-Grundschutz im gemeindlichen Bereich eingestellt (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Basis_Absicherung_Kommunalverwaltung.html).

Smart Cities

Verkehrs- und Bewegungsströme

In der Vergangenheit sind etliche Gemeinden mit ihren „Smart City"-Projektplänen an uns herangetreten. Häufig geht es dabei auch um die Frage, inwieweit Verkehrsströme bzw. Bewegungsströme von Bürgern analysiert werden dürfen. Technisch wird dabei i.d.R. auf ein Tracking von Mobiltelefonen zurückgegriffen. Dafür werden die von Mobiltelefonen ausgesendeten WLAN/Bluetooth-Signale genutzt. Da es sich bei den entsprechenden Adressen der Mobiltelefone (sog. MAC-Adressen) um personenbezogene Daten handelt, ist ein derartiges Tracking aus Datenschutzsicht problematisch.

Hinreichende unmittelbare Anonymisierung

Bei derartigen Vorhaben müssen personenbezogene Daten unmittelbar (noch in den Empfangsstationen und nicht in einem Backend) anonymisiert werden. Dies kann etwa durch die Anwendung einer kryptographischen Hashfunktion geschehen, wobei ein Zufallswert (sog. „Salt"-Wert) in die Berechnung einfließen muss, der spätestens alle 24 Stunden geändert (und keinesfalls gespeichert) wird. Des Weiteren ist darauf zu achten, dass Bewegungsmuster, etwa zu außergewöhnlichen Zeiten, nicht doch wieder einer Person zugeordnet werden können.

DSFA erforderlich

Die Durchführung einer Datenschutzfolgen-Abschätzung nach Art. 35 DS-GVO (sowie gegebenenfalls eine Konsultation unserer Dienststelle) ist bei einem derartigen Vorhaben in jedem Fall erforderlich.

Smartphone-Apps

Rechtmäßigkeit von Datenflüssen beim Einsatz von Software-Development-Kits

Bei Smartphone-Apps werden häufig Software-Development-Kits (SDK) von Drittanbietern eingesetzt. Diese beinhalten oftmals umfangreiche Datenflüsse zu den Herstellern. Verantwortliche müssen sicherstellen, dass nur rechtmäßige Datenflüsse stattfinden. Dies dürfte in der gemeindlichen Praxis nicht unproblematisch sein. Ggf. müssen Gemeinden in nachvollziehbarer Weise darlegen können, auf welche Rechtsgrundlage sie sich dabei stützen.

Einwilligung scheidet grundsätzlich aus

Die Ausführungen in unseren FAQ zu Cookies und Tracking können für Smartphone-Apps von Gemeinden nur begrenzt angewandt werden: öffentliche Stellen können grundsätzlich kein berechtigtes Interesse nach Artikel 6 Absatz 1 Buchstabe f DS-GVO geltend machen und haben hinsichtlich der Freiwilligkeit der Einwilligung stets das Ober-/Unterordnungsverhältnis zum Bürger mit Blick auf ihre Eigenschaft als Hoheitsträger zu betrachten. Daher scheidet eine Einwilligung im Bereich des Trackings bzw. der Weitergabe von Nutzungsdaten an Dritte auch bei Smartphone-Apps grundsätzlich aus.

Verschlüsselung von Datenträgern

Schutz vor Datenpannen

Eine der häufigsten Datenpannen, bei denen personenbezogene Daten in fremde Hände gelangen, ist der Verlust von USB-Sticks, Speicherkarten, externen Festplatten, Laptops oder ganzer PCs. Diese werden bei Einbrüchen gestohlen, im Zug vergessen oder gehen anderweitig verloren. Teilweise sind auf den Geräten besondere Daten nach Artikel 9 DS-GVO wie Medizindaten gespeichert. Wie können sich Gemeinden nun davor schützen, dass bei Diebstahl nicht auch noch eine große Datenpanne wird?

Verwendung von Verschlüsselungsverfahren

Die wichtigste Maßnahme zur Vorsorge ist relativ einfach umzusetzen: Verschlüsselung der Datenträger! Um den Zugriff auf sensible Daten zu verhindern, sollte dabei die gesamte Festplatte oder der gesamte Datenträger mittels „Full Disk Encryption“ verschlüsselt und per Passwort oder vergleichbarem Zugriffsschutz gesichert werden. Entsprechende Verfahren sind seit vielen Jahren Stand der Technik, aber die Hersteller konnten sich bisher nur bei Smartphones und Tablets dazu durchringen, sie standardmäßig zu aktivieren. Daher muss diese manuell aktiviert werden.

Datenträgerverschlüsselung ist in verschiedenen Sicherheitsstufen unter allen gängigen Desktop- und Server-Betriebssystemen verfügbar: Windows (BitLocker oder extern via VeraCrypt), macOS (FileVault) oder Linux (dm-crypt, LUKS) bringen entsprechende Verfahren seit Jahren mit. Es empfiehlt sich grundsätzlich – auch bei wenig sensiblen Daten – Festplatten zu verschlüsseln. Dies gilt insbesondere für Laptops, externen Festplatten, USB-Sticks und ähnlichem, da bei diesen ein erhöhtes Risiko des Verlusts besteht. Neben der Auswahl einer sicheren Verschlüsselungs-Software ist darauf zu achten, dass sichere Algorithmen und eine ausreichende Schlüssellänge sowie sichere Passwörter gewählt werden.

Verfügbarkeit in allen gängigen Betriebssystemen

Messenger-Dienste

Messenger mit Telefonnummer

Ein datenschutzrechtliches Problem bei der Nutzung von Messengern stellt der Zugriff auf alle Kontakte dar, der beispielsweise von dem gebräuchlichsten Messenger WhatsApp zum Abgleich der Kommunikationsteilnehmer benutzt wird. Dass die eigenen Kontakte mit Telefonnummern automatisch an einen Server übertragen werden und zusätzlich mit Dritten geteilt werden, ist nicht mit der DS-GVO vereinbar.

Grundsätzlich nicht zulässig

Zwischenweg

Ein weiterer oft genannter Messenger geht dabei einen Zwischenweg. Der Open-Source Messenger Signal verwendet zwar Telefonnummern für den Abgleich von Nutzern, diese werden aber nur gekürzt und als Hashwert übertragen. Die Hashwerte der gekürzten Telefonnummern werden abgeglichen und direkt wieder verworfen – ohne Speicherung auf dem Server.

Telefonnummer werden als Hashwert übertragen

Zusätzlich gibt es bei Signal noch den „Vertraulichen Absender“ („Sealed Sender“ https://signal.org/blog/sealed-sender/). Bei bekannten Kontakten wird automatisch der Absender einer Nachricht nur verschlüsselt mitübertragen – auf dem Kommunikationsweg ist nur der Empfänger sichtbar. Eine mögliche Verkettung von Transport-Metadaten wird deutlich erschwert und der Dienstanbieter hat per Voreinstellung keine Kenntnis darüber, wer mit wem kommuniziert.

Funktion „Vertraulicher Absender“

Messenger ohne Telefonnummer

Verwendung eines pseudonymen Accounts möglich

Dass es auch ohne Telefonnummer geht, zeigen die Schweizer Verwaltung und das Schweizerische Bundesamt für Informatik und Telekommunikation (https://netzpolitik.org/2019/schweizer-verwaltung-setzt-auf-threema-statt-whatsapp/ sowie https://www.inside-it.ch/articles/53634). Dort wird zukünftig der Messenger Threema zur Kommunikation zugelassen. Als einziges Kommunikationsmittel auf dem Smartphone auch für vertrauliche Dokumente. Dabei benötigt Threema für den Betrieb keine Telefonnummer, sondern kann auch mit einem pseudonymen Account betrieben werden.

Messenger-Software mit Malwarescanner und Antivirensoftware

Ein weiteres Beispiel kommt aus Frankreich (https://www.golem.de/news/statt-whatsapp-frankreich-wandert-in-die-matrix-1902-139167.html, https://matrix.org/blog/2018/04/26/matrix-and-riot-confirmed-as-the-basis-for-frances-secure-instant-messenger-app/). Dort wird das dezentrale Open-Source Messenger-Protokoll Matrix weiterentwickelt und für den Einsatz in allen Ministerien und Behörden vorbereitet. Die dazugehörige Messenger-Software enthält dabei sogar einen Malwarescanner und Antivirensoftware.

Gruppenchats

Sichtbarkeit von Telefonnummer problematisch

Gruppenchats sind eine separat zu betrachtende Thematik. Die offene Sichtbarkeit der im Verteiler registrierten Telefonnummern stellt beispielsweise bei der Verwendung von Messengern an Schulen ein Problem dar (https://www.heise.de/newsticker/meldung/WhatsApp-Messengernutzung-zwischen-Lehrern-und-Eltern-ist-eine-Grauzone-4311168.html). Hier wäre der französische Weg mit Matrix denkbar – mit pseudonymen Nutzerkonten und verschlüsselten Gruppenchats. Ob die (Pseudo-)Anonymität an Schulen auch erwünscht ist, ist dabei eine andere Frage.

Dezentrale versus zentrale Dienste

Einzelfallgestaltung entscheidend

Dezentrale selbst betriebene Dienste wie Matrix bieten viele Vorteile, sind aber nicht zwingend in jedem Fall besser. Firmen oder Gemeinden benötigen Fachkräfte mit entsprechenden Kenntnissen, um einen solchen Dienst überhaupt einrichten zu können. Wie schwierig es ist, solche Fachkräfte zu finden, zeigt sich bei dem Trend sämtliche Netzanwendungen zu Dienstleistern in die Cloud zu verlagern. Insofern kann ein professionell betreuter zentraler Dienst mehr Datenschutz bieten, als ein nach bestem Wissen aufgesetzter dezentraler Dienst. Andererseits können Gewährleistungsziele wie Verfügbarkeit, Vertraulichkeit und Integrität einen selbst betriebenen dezentralen Dienst notwendig machen.

Backups

Verschlüsselte Backups

Nicht zuletzt sollten noch die verschiedenen Möglichkeiten für Backups betrachtet werden. Unverschlüsselte Backups in der Cloud sind nicht zulässig. Bei einem lokalen, auf dem Gerät, gespeicherten Backup sollte regelmäßig eine Übertragung auf geeignete Backup-Medien erfolgen.

Bewertung

Messenger grundsätzlich datenschutzkonform einsetzbar

Eine klare Empfehlung kann aufgrund der vielschichtigen Probleme und Anforderungen leider nicht erfolgen (https://www.eff.org/deeplinks/2018/03/secure-messaging-more-secure-mess). Unsererseits spricht allerdings vieles dafür, dass Messenger datenschutzkonform einsetzbar sind und in der Regel sogar ein höheres Datenschutzniveau als E-Mails bieten.

Backups

Getrennte Systeme bei Backups

Für Angreifer sind Backups ein zentraler Angriffspunkt. Sie enthalten meist zentral Daten aller Art und sind der Notanker bei Datenverlust. Sie müssen deswegen besonders gut gesichert und vom sonstigen Netzwerk der Gemeinde weitgehend getrennt sein. So sollte die Authentifizierung unabhängig von den normalen Diensten ablaufen, damit erfolgreiche Angreifer auf die normalen Systeme keinen Zugriff auf die Backups erhalten. Insbesondere Verschlüsselungs-Schadsoftware versucht meist als erstes, Backups zu löschen oder anderweitig unbrauchbar zu machen. Dies lässt sich nur mit getrennten Systemen sinnvoll verhindern.

Bürgerportal/Bürger-App

Ausdifferenziertes Angebot

Immer mehr Gemeinden wollen ihren Bürgern ein sogenanntes Bürgerportal anbieten. Dies kann viele Angebote umfassen, wie eine Terminvereinbarung für das Bürgerbüro oder das Standesamt, eine Kfz-Zulassung, verschiedene Kultur- und Freizeittipps, Echtzeitinformationen zu Parkplatzmöglichkeiten und zur Verkehrslage, Nachbarschaftshilfe, Arzttermine und noch vieles mehr. Bei der Auflistung der Möglichkeiten wird schnell klar, dass Aussagen zum Datenschutz pauschal nicht möglich sind.

Empfehlung frühzeitige Einbindung LfDI

In der Vergangenheit gab es während der Planung und auch bei schon umgesetzten Projekten dieser Art grundsätzliche Bedenken von Betroffenen die unserer Dienststelle vorgetragen wurden und die in Einzelfällen dann zur Einstellung des gesamten Projekts geführt haben. Daher ist den Gemeinden eine frühzeitige Einbindung unserer Dienststelle dringend anzuraten.

Elektronische Schließsysteme

Immer häufiger werden elektronische Schließsysteme für eine teils mehrstufige Zutrittskontrolle in Gebäuden genutzt. Dabei spielen vor allem wirtschaftliche Gründe eine Rolle, wie beispielsweise ein verringerter Aufwand bei der Schlüssel- und Schließanlagenverwaltung, individuelle Zutrittsberechtigungen statt verschiedener Schlüssel und auch die Möglichkeit verlorene elektronische Schlüssel zentral sperren zu können, ohne die ganze Schließanlage tauschen zu müssen. Mit einem elektronischen Schließplan können für jede einzelne Türe elektronische Schlüsselberechtigungen zugewiesen werden.

Ereignisprotokoll

Die elektronischen Schließsysteme bieten meist auch die Möglichkeit, die Schlüsselnutzung mit einem Zeitstempel und der Schlüssel-ID des genutzten elektronischen Schlüssels in einem Ereignisprotokoll zu speichern. Die Speicherung erfolgt dabei typischerweise in einem Ringspeicher. Dabei werden beispielsweise die letzten 100 Ereignisse erfasst. Das Ereignisprotokoll kann dabei lokal im Schloss oder auch zentral in einem Server gespeichert werden. Denkbar sind auch verschiedene Protokollierungszonen, wie zum Beispiel die Eingangstür führt keine Protokollierung durch, aber die Sicherheitstür zu einem sensiblen Bereich protokolliert jedes Ereignis. Damit stellt sich direkt die Frage nach der Personenbeziehbarkeit der erfassten Daten.

Regelfall Personenbeziehbarkeit

In den meisten Fällen wird bei der Vergabe eines Schlüssels an Mitarbeiter die Schlüssel-ID zusammen mit dem Namen des Schlüsselinhabers vermerkt. Nur so kann im Verlustfall auch der entsprechende Schlüssel gesperrt oder eine missbräuchliche Nutzung erkannt werden. Die Schlüssel-ID ist also in der Regel personenbeziehbar.

Betroffenenrechte und Grundsatz der Datensparsamkeit

Bei Personenbeziehbarkeit müssen entsprechend die Anforderungen an die Betroffenenrechte erfüllt werden können (wie Auskunftsrecht oder Löschung). Zudem müssen die Anforderung an den Grundsatz der Datensparsamkeit erfüllt und technisch-organisatorische Maßnahmen zum Schutz der personenbezogenen Daten umgesetzt werden.

Erfassung von Zutrittsdaten nur in Ausnahmefällen

Das Erfassen der Zutrittsdaten ist zudem nur in Ausnahmefällen zulässig. Denkbar wäre es unter anderem bei der Verfolgung einer Straftat eines Bediensteten oder zur Gefahrenabwehr. Hier wäre allerdings zu unterscheiden, ob es sich um eine allgemeine Zugangstüre oder dem Zugang zu einem besonders schutzbedürftigen Bereich handelt. Dies wäre im Einzelfall mit den berechtigten Interessen der Betroffenen abzuwägen. Keinesfalls dürfen die Zutrittsdaten für eine (flächendeckende) Mitarbeiterüberwachung zweckentfremdet werden. Diese Zweckbindung wäre mittels technisch-organisatorischer Maßnahmen umzusetzen.

Regelfall keine Speicherung der Schlüsselnutzung

In der Regel sind elektronische Schließsysteme demnach so zu konfigurieren, dass keine Speicherung der Schlüsselnutzung stattfindet.

Dienstvereinbarung

Der Einsatz einer elektronischen Schließanlage sollte mittels einer Dienstvereinbarung geregelt und der Personalrat eingebunden werden. Demnach empfiehlt es sich, Kontrollrechte des Personalrats und des Datenschutzbeauftragten zu normieren. Ferner sollten die konkreten Zwecke der Speicherung festgelegt werden (zum Beispiel Durchsetzung des Hausrechts, Sicherheit und des Schutzes der Mitarbeiter oder Fehlerlokalisation). Auch sollte die Speicherdauer ausdrücklich geregelt werden.

Cloud-Dienste

Prüfung, ob datenschutzrechtliche Vorgaben hinreichend beachtet werden

Beim Einsatz von Cloud-Diensten sind die Gemeinden, die eine Software oder einen Dienst einsetzen, Verantwortliche im Sinne der DS-GVO. Sie haben alle datenschutzrechtlichen Vorgaben auch beim Einsatz von Drittsoftware zu prüfen und einzuhalten. Dies gilt umso mehr, wenn sensible Daten oder große Mengen oder gar die gesamte Dokumenten-Erstellung und -Bearbeitung darüber abgewickelt werden. Verantwortliche müssen also bei der Auswahl einer Software oder eines Dienstes prüfen, ob diese allen datenschutzrechtlichen Vorgaben gerecht wird, ob unerwünschte Datenübertragungen einschließlich Auswertung des Nutzerverhaltens erfolgen und die Rechtmäßigkeit der Verarbeitung sicherstellen. Kann diese Prüfung nicht erfolgen, etwa weil nicht alle Datenflüsse und Verarbeitungen ausreichend dokumentiert sind, kann eine solche Software nicht datenschutzkonform eingesetzt werden, schon weil die Datenverarbeitung nicht fair und transparent erfolgt (vgl. Artikel 5 DS-GVO).

Anhang

Verzeichnis von Verarbeitungstätigkeiten **Verantwortlicher** **gem. Artikel 30 Abs. 1 DSGVO**	Vorblatt

Angaben zum Verantwortlichen

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Name:	Gemeinde Musterstadt
Straße:	Musterstr. 1
Postleitzahl:	7777
Ort:	Musterstadt
Telefon:	0707/123-0
E-Mail-Adresse:	info@musterstadt.de
Internet-Adresse	www.musterstadt.de

Angaben zum ggf. gemeinsam mit diesem Verantwortlichen

Name:	
Straße:	
Postleitzahl:	
Ort:	
Telefon:	
E-Mail-Adresse:	

Angaben zum Vertreter des Verantwortlichen

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

[Hinweis LfDI: Die in Art. 30 Abs. 1 Satz 2 Buchst. a DSGVO genannten „Vertreter“ beziehen sich auf den Vertreter im Sinne von Art. 4 Nr. 17 DSGVO und sind damit für öffentliche Stellen nicht relevant. Aus aufsichtsbehördlicher Sicht ist die Angabe des operativ verantwortlichen Ansprechpartners wünschenswert. Dementsprechend sollte ein Eintrag unter „Ansprechpartner“ erfolgen.]

Name:	
Straße:	
Postleitzahl:	
Ort:	
Telefon:	
E-Mail-Adresse:	

Angaben zur Person des Datenschutzbeauftragten * (extern mit Anschrift)

* sofern gem. Artikel 37 DS-GVO benannt

Anrede:	Frau	Titel:	
Name, Vorname:	Simpson, Lisa		
Straße:			
Postleitzahl:			
Ort:			
Telefon:	0707/123-18		
E-Mail-Adresse:	datenschutz@musterstadt.de		

Verarbeitungstätigkeit: Benennung: **Bewerbungsunterlagen**	**lfd. Nr.:** **12**
Datum der Einführung: 25.05.2018	Datum der letzten Änderung: 02.09.2019

Verantwortliche Fachabteilung	Personalabteilung
Ansprechpartner	Herr Flanders
Telefon	0707/123-12
E-Mail-Adresse	personal@musterstadt.de
Zwecke der Verarbeitung (Art. 30 Abs. 1 S. 2 lit b)	Gewinnung von neuen Mitarbeiterinnen und Mitarbeitern
Optional: Name des eingesetzten Verfahrens	
Beschreibung der Kategorien betroffener Personen (Art. 30 Abs. 1 S. 2 lit. c)	☐ Beschäftigte ☐ Interessenten ☐ Lieferanten ☐ Kunden ☐ Patienten ☒ Bewerber ☐ ☐

Beschreibung der Kategorien von personenbezogenen Daten (Art. 30 Abs. 1 S. 2 lit. c)	☒ Name, Familienstand, Foto, Adressdaten, Geburtsdatum, ☒ Arbeitszeugnisse, Qualifikationen, Leistungsdaten, Beurteilungen ☐ Besondere Kategorien personenbezogener Daten (Art. 9): ☒ ggf. Schwerbehindertenbescheinigungen
Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden (Art. 30 Abs. 1 S. 2 lit. d)	☒ intern (Zugriffsberechtigte) Abteilung/ Funktion: - Mitarbeiter und Mitarbeiterinnen der Personalabteilung haben Zugriff; - Dienstvorgesetze - Personalvertretung und BfC
	☐ extern Empfängerkategorie
	☐ Drittland oder internationale Organisation (Kategorie)
ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation (Art. 30 Abs. 1 S. 2 lit. e)	☒Datenübermittlung findet nicht statt und ist auch nicht geplant ☐Datenübermittlung findet wie folgt statt:
Nennung der konkreten Datenempfänger	☐ Drittland oder internationale Organisation (Name)

Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannte Datenübermittlung handelt.	Dokumentation geeigneter Garantien
Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 S. 2 lit. f)	4 Monate nach Zugang der Absage

Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs.1 DSGVO (Art. 30 Abs. 1 S. 2 lit. g) *Siehe TOM-Beschreibung in den „Hinweisen zum Verzeichnis von Verarbeitungstätigkeiten“, Ziff. 6.7. und 6.8*

…… …… .....
Verantwortlicher Datum Unterschrift