

# Teil I: „Darf ich das?“

## 1. Die Zulässigkeitsprüfung

### Schlagwörter

- Geht es eigentlich auch ohne Einwilligung?
- Brauchen wir als Gemeinde immer eine gesetzliche Grundlage?
- Wir *müssen* die Daten ja verarbeiten – *dürfen* wir das dann auch?

### Ausgangslage

Die mit Abstand am meisten gestellte Frage im Datenschutzrecht ist gleichzeitig auch die zentrale Frage: „*Darf ich das (mit den Daten machen)?*“ Das gilt auch für den Gemeindebereich. Die Antwort darauf ist die sogenannte datenschutzrechtliche Zulässigkeitsprüfung. Die Juristen vergeben für bestimmte Handlungsabfolgen gerne eigene Namen. Hinter diesem Begriff versteckt sich ein Konstrukt an Prüfschritten, die Klarheit bringen sollen, ob die jeweilige Datenverarbeitung zulässig ist oder nicht.

Das Wesen der Zulässigkeitsprüfung kennt für den Gemeindebereich keine Besonderheiten, weshalb zunächst ein paar allgemeine Ausführungen ihre Berechtigung haben, die in weiterer Folge durch Beispiele veranschaulicht werden. Im Wesentlichen sollten schon damit alle datenschutzrechtlichen Zulässigkeitsfragen in der Gemeindepraxis geklärt werden können. Zumindest werden die jeweiligen Bürgermeister bzw. Gemeindebediensteten ein erstes Gespür dafür entwickeln können, ob die Daten für das jeweilige Vorhaben verarbeitet, übermittelt und gespeichert werden dürfen oder nicht.

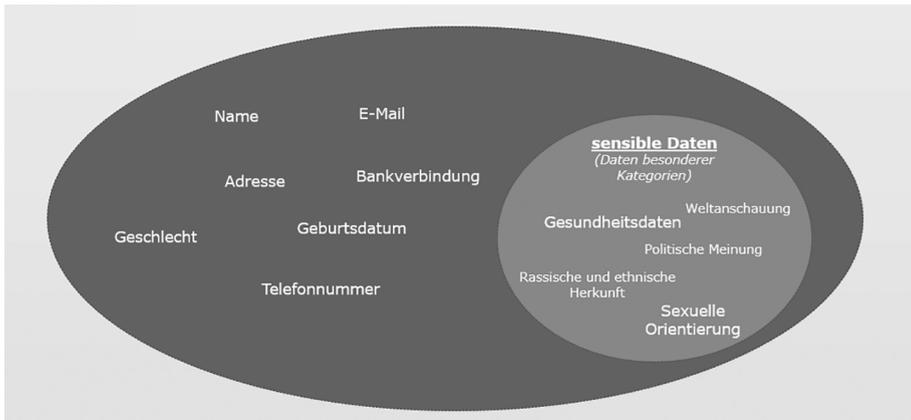
### Kurzfassung

1. Wir haben einen **Rechtfertigungsgrund**. ✓
2. Wir halten die **datenschutzrechtlichen Grundsätze** ein. ✓

Ist beides gegeben, ist die Datenverarbeitung zulässig.

### 1.1. Alles ist verboten, außer es ist erlaubt

Ausgangspunkt jeder Zulässigkeitsprüfung ist das sogenannte **Verbotsprinzip**. Demnach sollte man sich Folgendes in Erinnerung rufen: **Es ist alles verboten, außer es ist (gesondert) erlaubt**. Dies ist insofern von Bedeutung, weil die oft reflexartig herangezogene Rechtfertigung „*es steht nirgendwo, dass ich das nicht darf*“ im datenschutzrechtlichen Kontext gerade nicht zum Erfolg verhilft. Es muss – umgekehrt – geradezu „*irgendwo stehen*“, dass man das, was man vorhat, mit den Daten tun darf. Insofern ist das Datenschutzrecht – überspitzt formuliert – strenger als das Strafrecht, in welchem der obige Reflex seine Berechtigung hat.



Die sensiblen Daten werden bewusst als Teilmenge aller personenbezogenen Daten dargestellt, um zu betonen, dass nicht nur die sensiblen Daten den Schutz der DSGVO genießen.

## 2.2. Sonderfall Fotos

Eine einfache Frage mit einer gar nicht so einfachen Antwort: **Sind Fotos sensible Daten?**

---

### Beispiel

Fotos von Gemeindebediensteten auf der Homepage

---

Reflexartig würde man diese Frage zunächst verneinen, immerhin sind Fotos nicht in der Auflistung der DSGVO genannt. Allerdings: Auch aus Fotos sind einige Informationen abzuleiten, die in den sensiblen Bereich fallen. Man denke etwa an einfache Porträtfotos von Brillenträgern (Sehschwäche als Gesundheitsdatum). Dennoch hat die DSGVO (wenn auch nur in einem Erwägungsgrund) festgehalten, dass Lichtbilder **nicht grundsätzlich als Verarbeitung besonderer Kategorien** von Daten angesehen werden sollten. Anderes könnte etwa gelten, wenn das Foto selbst wiederum besonders sensible Informationen beinhaltet (zB Brille; Hautfarbe als Hinweis auf die Herkunft) oder wenn sich der Verarbeitungszweck gerade auf den sensiblen Bereich bezieht. Auch handle es sich um kein „*biometrisches*“ Datum, sofern die Lichtbilder nicht mit technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person möglich machen.

Auch die Rechtsprechung geht in diese Richtung. Für die normalen Fotos (Porträtfotos für die Homepage, Veranstaltungsfotos etc) dürfte demnach feststehen, dass sie *keine sensiblen Daten* darstellen. Warum das wichtig ist? Siehe sogleich.

## 3.2. Statistische Auswertungen/Unternehmens- und Vereinsdaten

Weites darf in Erinnerung gerufen werden, dass die DSGVO nur personenbezogene Daten – und hier auch nur jene der *natürlichen* Personen – schützt. Personenbezogene Daten juristischer Personen sind nicht umfasst, können aber – bei entsprechender Relevanz – als Geschäfts- oder Betriebsgeheimnis geschützt sein.

---

### Beispiel

Allgemeine Office-Mailadressen, Vereinsanschriften etc unterliegen nicht der DSGVO. Sie müssen daher auch nicht nach bestimmten Fristen gelöscht oder bei Auskunftsbegehren durchsucht werden. Sind jedoch die Kontaktpersonen (Ansprechpartner) der Unternehmen oder Vereine gespeichert, handelt es sich wieder um personenbezogene Daten natürlicher Personen.

---

### Exkurs

Das österreichische Datenschutzgesetz schützt in seinem Grundrecht auf Datenschutz (§ 1 DSG) auch die juristischen Personen („Jedermann“). Ein Kommentar zu den (verfehlten) Bemühungen, diese Bestimmung (mit Verfassungsmehrheit) an die DSGVO anzupassen, kann ebenso unterbleiben wie zum Verhältnis der beiden (sich widersprechenden) Bestimmungen. Klar ist jedenfalls, dass den juristischen Personen kein Antragsrecht hinsichtlich Löschung und Auskunft im Anwendungsbereich der DSGVO zukommt, diese aber allenfalls Beschwerde an die DSB wegen Verletzung des Grundrechts auf Datenschutz erheben könnten.

---

Werden personenbezogene Daten natürlicher Personen verarbeitet, kann eine **Anonymisierung** einen Ausweg aus der DSGVO bieten. Insbesondere, wenn die Rückschlüsse und Erkenntnisse aus diesen Daten weiterverwendet werden sollen, empfiehlt sich die Entfernung des Personenbezugs (Anonymisierung), um die Daten nicht gänzlich aus dem Bestand löschen zu müssen.

---

### Beispiele

- Alter und Geschlecht der eine Gemeindeförderung in Anspruch nehmenden Personen zur Abschätzung eines zukünftigen Wohnbedarfs
  - Statistische Auswertung der gewährten Fördermittel, um dies bei der Budgetplanung berücksichtigen zu können
- 

## 3.3. Geburtstagsliste im Büro – die privaten Daten

Zahlreiche Menschen – zumindest die beneidenswert aufmerksamen – führen Listen von Geburtstagen nahestehender Personen. Dies dient in der Regel aus-

## 5.1. Prüfschritt 1 – das Interesse (der Gemeinde oder Dritter)

Zunächst ist zu prüfen, ob überhaupt ein Interesse der Gemeinde vorliegt. Als Hilfe dient die Kontrollfrage „*Warum wollen wir das eigentlich machen?*“ Kann schon diese Frage nicht beantwortet werden, ist die Prüfung hiermit vorbei. Die Datenverarbeitung wäre unzulässig.

Ein Interesse ist etwa das Bestreben im weiteren Sinne, das die Gemeinde – oder ein Dritter – an einer Verarbeitung haben kann, oder der Nutzen, der daraus gezogen wird. Erforderlich ist demnach ein real vorhandenes Interesse, etwas, das den aktuellen Tätigkeiten oder aber Vorteilen, mit denen in sehr naher Zukunft gerechnet wird, entspricht.

## 5.2. Prüfschritt 2 – das berechnigte Interesse (der Gemeinde oder Dritter)

Das Interesse an der Verarbeitung muss auch ein *berechnigtes* iSd DSGVO sein. Grob formuliert muss das Interesse von der Gesellschaft als legitim anerkannt sein. Das wird in den meisten Fällen kein Problem darstellen, zumal die DSGVO etwa ausdrücklich das – datenschutzrechtlich traditionell heiklere – Direktmarketing als Beispiel für ein berechnigtes Interesse anführt. Auch die Datenschutzkommission hat heiklere Bereiche (Bonitätsprüfung bei der Kreditvergabe) schon früh als grundsätzlich berechnigt anerkannt.

---

### Beispiel

Das Interesse der Gemeinde an der Förderung des Bürgerwohls und der Aufrechterhaltung einer ordnungsgemäßen Bürger-Gemeinde-Beziehung ist jedenfalls ein berechnigtes.

---

Ausreichend ist auch, dass zwar nicht die Gemeinde selbst, aber (irgend-)ein Dritter ein Interesse an der Verarbeitung durch die Gemeinde hat.

---

### Beispiel

Die Gemeinde als Vermieter von Gemeindewohnungen hat selbst kaum Interesse an der Anbringung des Namens des Mieters auf dem Schild der Gegensprechanlage (gerade sie weiß als Vertragspartei ohnehin, welcher Mieter zu welcher Top-Nummer gehört). Als Interesse Dritter kann aber die notwendige Kenntnis von Rettungskräften und sonstigen Einsatz- oder Zustelldienste genannt werden.

---

## 6.1. In Kenntnis der Sachlage

Die Betroffenen müssen wissen, wozu sie ihre Zustimmung erteilen. Im Detail kann das durchaus zu Problemen führen, etwa dann, wenn die Einwilligungserklärung zu unbestimmt bzw zu allgemein gehalten ist. Eine Vorab-Zustimmung zur generellen Veröffentlichung von Lichtbildern etwa – ohne einzuschränken, welche Daten bzw Fotos in welchen Medien wann und von wem veröffentlicht werden – wird zu unbestimmt sein.

---

### Beispiel

Sich auf eine Generalzustimmung zu Beginn des Kindergartenjahres zu verlassen, ist demnach nicht zu empfehlen. Die Einholung einer Zustimmung abgestimmt auf die jeweilige Veranstaltung ist ratsam. Dies führt in der Regel auch zur erhöhten Bereitschaft, tatsächlich zuzustimmen.

---

Auch die bloße Zustimmung zur Datenverarbeitung „zu Werbezwecken“ ist zu unbestimmt. Bei verallgemeinerbaren Datenverarbeitungen kann die Kenntnis der Sachlage auch durch eine umfassende Datenschutzerklärung auf der Webseite erfolgen (zB Cookie-Zustimmung; siehe zur Verwendung von Cookies auch Kapitel IV.1.).

## 6.2. Freiwilligkeit

Die Zustimmung muss freiwillig erfolgen. Der Zustimmungende soll sich frei entscheiden können, ob er die Einwilligung abgibt oder nicht. Das ist etwa dann **nicht** der Fall, wenn die Zustimmung an irgendetwas anderes gekoppelt ist, klassischerweise an die Erfüllung eines Vertrages.

Mit anderen Worten: Es muss für den Zustimmungenden immer die theoretische Möglichkeit geben, das ursprüngliche Ziel seiner Handlung (zB Vertragsabschluss, Bearbeitung seines Ansuchens) zu erreichen, *ohne* damit auch (automatisch) die Einwilligung zu erteilen.

Ist das entsprechende Formular (zB Antrag auf Förderung, Mitgliedsantrag bei Vereinen) allerdings richtig ausgestaltet (eigene Erklärung mit eigener Auswählbarkeit), kann die Zustimmung gültig in dessen Rahmen eingeholt werden. Wichtig ist dabei, dass ein aktives Handeln für die Einwilligung notwendig sein muss. Daher sind bereits vorausgewählte Checkboxen unzulässig.

---

### Beispiel

Bei einem Ansuchen auf Förderung besteht kein Einwand, die Zustimmung im jeweiligen Formular aufzunehmen. Sie muss allerdings mit einem eigenen Kästchen oder einer eigenen Unterschrift versehen werden und darf einer Erledigung des Ansuchens ohne Abgabe der Zustimmung nicht entgegenstehen.

---

## 2. Von der Verpflichtung zum Nutzen: Kann das Verarbeitungsverzeichnis auch Sinn machen?

### Schlagworte

- Hat das Verarbeitungsverzeichnis auch Sinn oder erfüllt es nur die Pflicht seines Daseins?
- Wie detailliert muss man es ausgestalten?

### Kurzfassung

Wie das Verzeichnis der Verarbeitungstätigkeiten ausgestaltet werden kann, dafür gibt es (wie oben ausgeführt) bereits zahlreiche Vorlagen. Wesentlich ist dabei nur, dass der Mindestinhalt enthalten ist: Für jede Datenverarbeitung sind Zweck, Art der Daten, Betroffenen- und Empfängerkategorien sowie (wenn möglich) allfällige Löschfristen anzugeben. Gemeinsam mit den allgemeinen Angaben (Name und Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten, technische und organisatorische Maßnahmen zur Datensicherheit) sind diese Informationen in eine schriftliche und ausdrückbare Form zu gießen, wobei keine näheren Anforderungen an das Format (zB Word, Excel, Datenbank) gestellt werden.

### 2.1. Eine mögliche Ausgestaltung

Die im Gemeindebereich kursierenden Verzeichnisse sind zumeist auf Word-Basis erstellt. Ohne dies als bessere Variante darstellen zu wollen, darf ein Auszug aus einem alternativen Format für ein Verarbeitungsverzeichnis dargetan und dessen Hintergründe erörtert werden:

Anträge auf finanzielle Unterstützungen								
Ansprechperson:								
Zweck der Verarbeitung:		Erfassung und Verarbeitung sämtlicher notwendiger personenbezogener Daten zur Bearbeitung einer finanziellen Unterstützung bzw eines Zuschusses und zusammenhängende Datenverarbeitungen						
Rechtsgrundlagen:		(vor-)vertragliche Verpflichtung, ggffalls Einwilligung, berechtigte Interessen (siehe Zweck)						
Verarbeitete Daten (Kategorien)	Empfänger (Kategorie)	Zweck der Übermittlung	Rechtsgrundlage Übermittlung	Löschfrist	Beginn Fristenlauf	Aufbewahrungspflicht	Applikation	Rolle
<b>Ansüchender</b>								
<i>Stammdaten</i>	1, 18, 31, 32, 33, 35, 38	Erfüllung einer gesetzlichen Verpflichtung	Gesetzliche Verpflichtung	7 Jahre	Ende des Geschäftsjahres, in welchem die Förderung vollendet bzw rückbezahlt wurde	BAO	Datenbank Förderungen f:\-Laufwerk	Förderwerber, Bürger
<i>Erweiterte Stammdaten, Kontaktdaten</i>								
<i>Auftragsdaten (Förderansuchen, insb Fördersumme)</i>								
<b>Dienststelle</b>								
<i>Sachbearbeiter</i>	-							MA
<b>*Anmerkungen:</b>								
Übermittlung Drittland/int. Org.:								

### Beispiel

Im ABGB existiert eine objektive Verjährungsfrist von 30 Jahren. Theoretisch ist daher möglich, dass ein ehemaliger Mitarbeiter im Zusammenhang mit einem Dienstunfall auch noch Jahre später an die Gemeinde herantritt. Die Frage ist, ob zur Abwehr eines solchen behaupteten Anspruchs alle Daten **über die gesetzlichen Aufbewahrungspflichten hinaus** aufbewahrt werden dürfen.

---

Eine über die Aufbewahrungspflicht (zB sieben Jahre) hinausgehende Verjährungsfrist (zB 30 Jahre) als Rechtfertigung für die Aufbewahrung heranzuziehen, ist zwar grundsätzlich denkbar, die Rechtsprechung dazu ist aber relativ streng. Zunächst wurde (wenn auch für den Telekommunikationsbereich) die Überschreitung einer gesetzlichen Aufbewahrungspflicht nur dann als gerechtfertigt erachtet, wenn es **konkrete Anhaltspunkte für befürchtete Verfahren** (zB Aufforderung durch den Bediensteten, strittige Beendigung des Mietverhältnisses betreffend eine Gemeindefwohnung) gibt. Diese Rechtsprechung wurde wenig später (wenn auch für den Bereich der Bewerbungen) etwas aufgeweicht, indem festgehalten wurde, dass schon der bloße Verweis auf ein bestimmtes Gesetz (dort: Gleichbehandlungsgesetz) für den Verantwortlichen für die längere Speicherung ausreichen könnte, weil und wenn er damit nachweisen kann, **welche konkreten zukünftigen Verfahren** auf welcher konkreten Grundlage und binnen welcher Frist er befürchtet (Näheres zu dieser Entscheidung siehe Kapitel IV.4.).

---

### Beispiel: Aufbewahrung „zu Dokumentationszwecken“

Der jüngeren Rechtsprechung der DSB ist zu entnehmen, dass die Aufbewahrung von personenbezogenen Daten zu Dokumentationszwecken durchaus von der Ausnahme der Löschpflicht „zur Geltendmachung, Ausübung und Verteidigung von Rechtsansprüchen“ gedeckt sein kann. Im Zuge der Ablehnung der Löschung ist dem Betroffenen jedoch genau zu begründen, **weshalb** man „aus Dokumentationszwecken“ die Daten weiterhin aufbewahren möchte. Eine inhaltsleere Begründung (dort: „aus sicher amtsbekanntem Gründen“) ist jedenfalls zu wenig.

---

### Beispiele: Mögliche Auftragsverarbeitungen

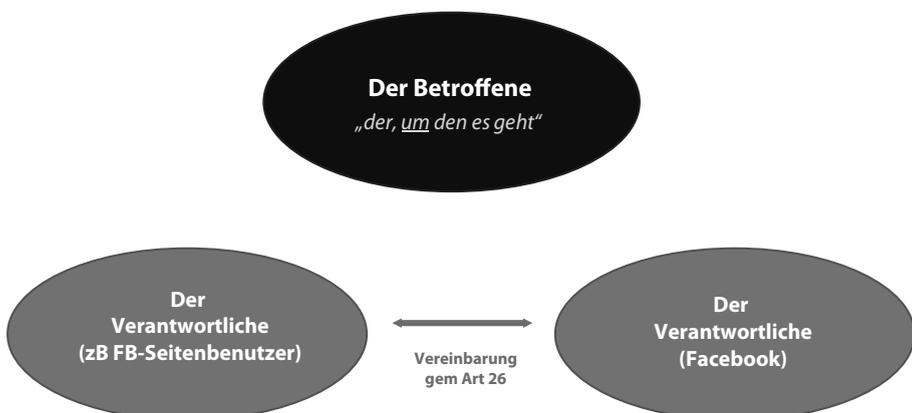
- Erledigung von Massenarbeiten (Versand von Mitteilungsblättern, Informationsbroschüren, Beitragsrechnungen etc auf der Basis eines vom Verantwortlichen zur Verfügung gestellten Adressenbestandes; Anfertigung von Namensschildern usw)
- Datenerfassung, Datenumsetzung und Scannen von Dokumenten
- Outsourcing im klassischen Sinn (zB Speicherung der Geschäftsunterlagen für die Dauer der steuerlichen Aufbewahrungspflicht durch einen Dritten)
- Auslagerung der Bürokommunikation (Beschaffung, Installation und Betreuung der entsprechenden Software, zB Textverarbeitung, E-Mail-Kommunikation)
- Cloud Computing
- Archivierung von Daten (zB Archivierung von maschinenlesbaren Datenträgern sowie von Altakten)
- Löschung bzw Vernichtung von Datenträgern/Dokumenten

## 8.2. Gemeinsam Verantwortliche

Entscheiden hingegen zwei (oder mehrere) Verantwortliche *gemeinsam* über Zwecke und Mittel der Verarbeitung, sind sie **gemeinsam Verantwortliche gem Art 26 DSGVO**. Dabei kommt es auf die **tatsächlichen Gegebenheiten**, also auf den faktischen Einfluss auf diese Entscheidung, an und nicht etwa darauf, wer in rechtlicher Hinsicht entscheiden darf/dürfte.

Die Abgrenzung zwischen Auftragsverarbeitung und gemeinsam Verantwortlichen ist schwierig zu ziehen. Entscheidend ist, ob der Auftragsverarbeiter irgendwann über Zwecke und (wesentliche Punkte der) Mittel mitentscheiden kann. Rechtsfolge einer gemeinsamen Verantwortlichkeit ist ebenso die Notwendigkeit des **Abschlusses einer Vereinbarung** – diesfalls einer gem Art 26 DSGVO.

Die Verantwortlichen agieren auf gleicher Ebene:



Gerne vergessen wird jedoch, dass auch den Bediensteten mitzuteilen ist, welche Daten zu welchem Zweck verarbeitet, wohin verschickt und wie lange gespeichert werden. Details dazu siehe Kapitel II.7. Dafür könnte für die Mitarbeiter eine eigene Datenschutzerklärung verfasst werden, die wie folgt eingeleitet werden könnte:

### **Muster: Datenschutzerklärung für Bedienstete**

Im Rahmen Ihres Arbeitsverhältnisses werden die von Ihnen zur Verfügung gestellten Daten (Stammdaten, Kontaktdaten, Lebenslauf, Notfallkontakte etc) sowie jene, die aufgrund des Dienstverhältnisses anfallen (zB Gehaltsdaten, Krankenstände, Pflegeurlaub), verarbeitet.

#### **Zweck der Datenverarbeitung**

Die Verarbeitung und Übermittlung der Daten erfolgt für die Lohn-, Gehalts-, Entgeltsverrechnung und Einhaltung von Aufzeichnungs-, Auskunfts- und Meldepflichten, soweit dies aufgrund von Gesetzen oder Normen kollektiver Rechtsgestaltung oder arbeitsvertraglichen Verpflichtungen jeweils erforderlich ist, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (zB Korrespondenz) in diesen Angelegenheiten.

Ihre beruflichen Kontaktdaten werden intern zur Kontaktaufnahme durch Kollegen an diese und – falls Sie Außenkontakt haben – auf der Webseite zur Kontaktaufnahme durch Kunden und Lieferanten veröffentlicht.

#### **Freiwillige Datenverarbeitung**

- a. Die Angabe Ihres Religionsbekenntnisses erfolgt freiwillig, wenn Sie entsprechende Rechte in Anspruch nehmen möchten.
- b. Die Angabe Ihrer Gewerkschaftszugehörigkeit erfolgt freiwillig, wenn Sie den Gewerkschaftsbeitrag über den Arbeitgeber abführen lassen.
- c. Die Angabe der Notfallkontakte erfolgt freiwillig.
- d. Die Veröffentlichung Ihres Fotos auf der Firmen-Website erfolgt freiwillig.

Die Datenverarbeitungen selbst sind natürlich dementsprechend auszugestalten.

## **4.2. Eine IT-Policy liest sowieso niemand?**

Die DSGVO schreibt nicht vor, dass bestimmte Richtlinien erstellt oder Handbücher ausgearbeitet werden müssen. Sie legt allerdings den Gemeinden die Pflicht auf, intern **geeignete technische und organisatorische Maßnahmen** (TOMs) zur Datensicherheit zu treffen. Als Teil dieser TOMs eignet sich jedoch die

## 2. Sind GPS-Tracker in Dienstfahrzeugen zulässig?

### 2.1. Zulässigkeitsprüfung im Schnellverfahren

Mithilfe von GPS-Trackern werden personenbezogene Daten der Bediensteten, vor allem deren Aufenthalte, Fahrtstrecken, Arbeitszeiten, aufgezeichnet und verarbeitet. Sihin führt, falls GPS-Tracker verwendet werden, kein Weg daran vorbei, für diese Verarbeitung einen Rechtfertigungsgrund zu suchen (vgl Kapitel I.1.). Mangels gesetzlicher Grundlage für das GPS-Tracking sowie Notwendigkeit zur Erfüllung des Dienstvertrages verbleiben nur zwei Rechtfertigungsgründe: eine Einwilligung oder berechtigte Interessen.

### 2.2. Können die Bediensteten überhaupt einwilligen?

Im Bereich des **Mitarbeiterdatenschutzes** kursieren immer wieder Meinungen, wonach eine Einwilligung im Rahmen des Dienstverhältnisses nicht zulässig sei, weil aufgrund des Abhängigkeitsverhältnisses eine freiwillige Zustimmung nicht möglich wäre. In dieser Allgemeinheit kann das nicht gelten gelassen werden, zumal in mehreren Bereichen (zB Urlaubsvereinbarung) freiwilliges Einvernehmen mit den Dienstnehmern herstellbar ist. Im Übrigen war in den ersten Entwürfen zur DSGVO noch ausdrücklich enthalten, dass die Einwilligung im Dienstverhältnis aufgrund der Drucktheorie nicht zulässig sei. Diese Bestimmung wurde nicht in Geltung gesetzt, woraus abzuleiten ist, dass auch der europäische Gesetzgeber davon ausgeht, dass eine Einwilligung zulässig erzielt werden kann.

Allerdings sollte in diesem Bereich besonders vorsichtig bei der Ausgestaltung der Einwilligungserklärung vorgegangen und jeder Anschein einer Drucksituation verhindert werden. In diesem Fall und bei entsprechenden Informationen kann die Einwilligung die GPS-Tracker rechtfertigen.

### 2.3. Welche berechtigten Interessen hat die Gemeinde am GPS-Tracking?

In dieser Fallkonstellation wird die Gemeinde als Vertragspartner des Dienstvertrages – und damit im privatwirtschaftlichen Bereich – tätig. Eine Rechtfertigung über die berechtigten Interessen ist somit denkbar.