www.manz.at/rfg

RECHT & FINANZEN FÜR GEMEINDEN

RFG

Neues zum Bettelverbot 118!

Herausgeber Walter Leiss, Alois Steinbichler
Schriftleitung und Redaktion Markus Achatz, Peter Pilz
Redaktion Alexander Enzinger, Christoph Grabenwarter, Ferdinand Kerschner, Wolfgang Meister, Katharina Pabel, Alfred Riedl, Ursula Stingl-Lösch

September 2017 03

93 – 148

Schwerpunkt

Rechnungslegung und Risikomanagement

Übersicht

Beiträge

ISSN 1993-8098 Österreichische Post AG PZ 06Z036884 P Verlag Manz, Gutheil Schoder Gasse 17, 1230 Wien

MANZ

Neues Datenschutzrecht für Gemeinden

RFG 2017/27
DSG 2018; DSGVO
Zustimmung; Datenschutzbeauftragte; Datenverarbeitungsregister; Betroffenenrechte

Der Datenschutz wird mit Mai 2018 in rechtlicher Hinsicht auf völlig neue Beine gestellt. Die damit einhergehenden Änderungen und neuen Anforderungen befinden sich derzeit in aller Munde und haben auch Auswirkungen auf die Gemeindepraxis. Der Beitrag versucht, möglichst ohne rechtstheoretische Ausschweifungen die wichtigsten Neuerungen für die Gemeinden herauszuarbeiten.

Von Martin Führer

Inhaltsübersicht:

A. Einleitung

Mit 25. 5. 2018 tritt die Datenschutz-Grundverordnung (DSGVO)[1] der Europäischen Union in Geltung. Gleichzeitig ist trotz der direkten Anwendbarkeit der DSGVO ein neues nationales Datenschutzgesetz notwendig. Das Datenschutz-Anpassungsgesetz 2018,[2] das zeitgleich in Kraft tritt, passierte bereits den Nationalrat und wird in diesem Beitrag der Einfachheit halber als *„DSG 2018"* bezeichnet.

B. (Keine) Geldbußen für Gemeinden

1. Öffentliche Stellen von den Geldbußen ausgenommen

Obwohl in der DSGVO ganz am Schluss geregelt, drängt sich derzeit ein Thema markant in die mediale Berichterstattung und Diskussion: die massiv angehobenen Geldbußen. Waren die Höchststrafen bisher im fünfstelligen Bereich angesiedelt, führen die nunmehr vorgesehenen Grenzen (10 bzw 20 Millionen Euro oder 2% bzw 4% des weltweiten Jahresumsatzes) zu einer gewissen Sensibilisierung – oder gar Nervosität – in Unternehmerkreisen. Abgesehen davon ist von der Übertragung der Strafbefugnis von den Bezirksverwaltungsbehörden auf die Datenschutzbehörde auch ein Anstieg der Anzahl der ausgesprochenen Strafen zu erwarten.

Für den öffentlichen Bereich eröffnet die DSGVO die Möglichkeit, diesen gänzlich von der Verhängung von Geldbußen auszunehmen.[3] Der österr Gesetzgeber hat davon Gebrauch gemacht.[4] Gegen *„Behörden und öffentliche Stellen"* können demnach **keine Geldbußen** verhängt werden.

2. Gilt das auch für Unternehmen im Eigentum der Gemeinden?

Gemeinde und Gemeindeverbände fallen daher unter diese Ausnahme. Spannender ist die Frage, ob auch von der Gemeinde betriebene Unternehmen – etwa eine in ihrem Eigentum stehende GmbH – umfasst sind. Dies va vor dem Hintergrund, dass gegen juristische Personen generell Geldbußen verhängt werden können.

Ebenso wenig wie die Behörde ist auch die *„öffentliche Stelle"* in der DSGVO definiert. Mangels geeigneter Definition ist ein Blick in andere Vorschriften zu werfen. Um zu ergründen, was der europäische Gesetzgeber unter einer *„öffentlichen Stelle"* versteht, kann an das Vergaberecht angeknüpft werden. Dort ist der Begriff des *„öffentlichen Auftraggebers"* bereits definiert.[5] Neben dem Staat und den Gebietskörperschaften sind auch sog *„Einrichtungen des öffentlichen Rechts"* ausschreibungspflichtig.[6] Das sind Einrichtungen mit Rechtspersönlichkeit, die

- im Allgemeininteresse liegende Aufgaben nicht gewerblicher Art erfüllen und
- – grob formuliert – vom Staat oder den Gebietskörperschaften *„beherrscht"* werden.

1) Verordnung (EU) 2016/679 des EP und des Rates vom 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG, ABl L 2016/119, 1.
2) BG, mit dem das B-VG geändert, das Datenschutzgesetz erlassen und das Datenschutzgesetz 2000 aufgehoben wird, BGBl I 2017/120.
3) Art 83 Abs 7 DSGVO.
4) § 30 Abs 5 DSG 2018.
5) (Vergaberechts-)RL 2014/24/EU, ABl L 2014/94, 65.
6) Art 2 Abs 1 RL 2014/24/EU des EP und des Rates vom 26. 2. 2014 über die öffentliche Auftragsvergabe und zur Aufhebung der RL 2004/18/EG.

Beispiele

Beispiele für Tätigkeiten *„im Allgemeininteresse“* sind der Betrieb von Spitälern, Altersheimen, Kindergärten, Bildungseinrichtungen oder auch die Errichtung von gewerblichen Bauten für private Unternehmen zur Betriebsansiedelung; nicht hingegen etwa ein Thermalbad, eine Sauna oder ein Hotel.[7)]

Die Brücke kann geschlagen werden: Ist ein solches Unternehmen ausschreibungspflichtig, ist es gleichzeitig von der Verhängung von Geldbußen ausgenommen. Die Prüfung hat dabei stets im Einzelfall zu erfolgen.

3. Keine Geldbußen …

… und warum Sie trotzdem weiterlesen sollten:

Zunächst, weil die Ausnahme nur die Verhängung von **Geldbußen** betrifft. **Schadenersatzansprüche** gegen die Gemeinden – etwa wenn Schäden durch die unterlassene Bestellung eines Datenschutzbeauftragten (mit)entstehen – können die betroffenen Personen davon unabhängig stellen. Jede betroffene Person hat zudem das Recht, ihre **Betroffenenrechte** mit Klage gegen einen Verantwortlichen durchzusetzen.[8)] Auch ohne Geldbuße können gerichtliche Verfahren und Beschwerdeverfahren vor der Datenschutzbehörde beträchtliche Kosten verursachen, die nicht immer von der Gegenseite zu ersetzen sind.

Weiters wurden der Datenschutzbehörde sog „Abhilfebefugnisse“[9)] eingeräumt. Sie wird daher ermächtigt, Verwarnungen auszusprechen, Anweisungen zu erteilen oder etwa Beschränkungen der Verarbeitung sowie Löschungen von Daten anzuordnen.

Praxistipp

Neben den finanziellen Aspekten ist schließlich aber – als Pendant zur Reputation im wirtschaftlichen Wettbewerb – die politische Auseinandersetzung nach bekannt gewordenen Datenschutzverletzungen äußerst unangenehm.

Abgesehen davon sind einzelne öffentliche Unternehmen, die nicht unter die obige Ausnahme fallen (etwa weil sie gewerblich tätig sind), nicht vor Geldbußen gefeit. Dies kann auch insofern für Gemeindemitarbeiter beachtlich sein, wenn sie Führungspositionen bekleiden. Neben deren aktiven Handlungen können auch mangelnde Überwachung und Kontrolle Geldbußen nach sich ziehen.

Beispiel

Vorschriften der DSGVO werden von Mitarbeitern des Unternehmens verletzt, weil intern verabsäumt wurde, entsprechende Datenschutzrichtlinien aufzusetzen.

C. Was bleibt gleich?

Auch in einem Beitrag, der die Änderungen, die eine neue Rechtslage mit sich bringt, beleuchten soll, ist die Information, welche Punkte gleich bleiben, eine dankbare. Va dann, wenn der bisherigen Rechtslage im Vergleich zur aktuellen Sensibilisierung einer eher untergeordnete Rolle beigemessen wurde.

1. Das Verbotsprinzip

„Alles ist verboten, außer es ist erlaubt“, lautet die einfache Formel, nach der zu beurteilen ist, ob Datenverarbeitungen den Schutz personenbezogener Daten verletzen. Es sind – und werden weiterhin sein – für jede Verarbeitung personenbezogener Daten geeignete Rechtfertigungsgründe zu finden.

2. Rechtfertigungsgründe

An möglichen Rechtfertigungsgründen standen bspw zur Verfügung:

- Zustimmung der Betroffenen
- Erfüllung eines gesetzlichen Auftrags
- Erfüllung einer vertraglichen Verpflichtung
- überwiegende Interessen des Auftraggebers[10)]

Für den **öffentlichen Bereich** steht zudem als Rechtfertigungsgrund nach wie vor

- die Wahrnehmung einer Aufgabe zur Verfügung, die
  - im öffentlichen Interesse liegt oder
  - in Ausübung einer hoheitlichen Gewalt erfolgt und der Gemeinde übertragen wurde.

Im Hoheitsbereich ist weiters das Legalitätsprinzip zu beachten, dh, Eingriffe dürfen nur auf Basis einer gesetzlichen Grundlage im Unionsrecht oder im nationalen Recht vorgenommen werden.

Bei der Prüfung der Rechtmäßigkeit der Datenverarbeitung bleibt – im Wesentlichen – alles gleich. Das gilt sowohl für die Systematik *(„Alles ist verboten, außer es ist erlaubt“)*, als auch für die einzelnen Rechtfertigungsgründe.

3. Datenschutzrechtliche Grundsätze

Schon bisher ist neben der Suche nach einem geeigneten Rechtfertigungsgrund zu prüfen, ob die datenschutzrechtlichen Grundsätze eingehalten werden. Die prominentesten Grundsätze: Zweckbindung und Verhältnismäßigkeit. Das ändert sich auch mit der DSGVO nicht.

Daten sind nach wie vor insofern und so lange zu verarbeiten, als dies notwendig ist, um den Zweck, der Erhebung und Verarbeitung zu Grunde liegt, zu erreichen **(Zweckbindung).** MaW: Werden Daten nicht mehr benötigt, um den ursprünglichen Zweck zu erreichen, und existiert keine Aufbewahrungspflicht/-frist, sind sie zu löschen. Und zwar schon bei jetziger Rechtslage – nicht erst durch das in der DSGVO verankerte (und in den Medien präsente) Recht auf Vergessenwerden. ➜

7) *Heid* in *Heid/Preslmayr,* Handbuch Vergaberecht[4] (2015) Rz 291, 293.
8) Art 79 DSGVO.
9) Art 58 Abs 2 DSGVO.
10) Im privaten Bereich und nur für nicht-sensible Daten.

Beispiel

Löschen der Daten von nicht aufgenommenen Bewerbern

Ebenso sind auch Eingriffe in das Recht auf Geheimhaltung nur im möglichst geringen Umfang, also mit dem gelindesten Mittel, zulässig **(Verhältnismäßigkeit).** Darüber hinausgehende Datenverarbeitungen sind unverhältnismäßig.

Beispiel

Wird beabsichtigt, das Download-Volumen von Mitarbeitern zu überwachen, ist es nicht notwendig, auch die ausgewählten Webseiten zu protokollieren. Ebenso kann eine Zutrittskontrolle auch mit anderen (gelinderen) Mitteln als durch eine Videoüberwachung erfolgen.

Die in der DSGVO teilweise neu angeführten Grundsätze der Transparenz, Fairness sowie Richtigkeit, Integrität und Verfügbarkeit (Verpflichtung zur ordnungsgemäßen Sicherung, Backups, redundante Systeme etc) sind keine Neuerfindungen, sondern waren entweder bereits bisher zu beachten oder leiten sich von den beiden zentralen Grundsätzen ab.

D. Was wird neu?

1. Allgemeines

Zunächst halten mit der DSGVO **neue Begriffe** Einzug in die österr Rechtsordnung. Die bei datenschutzrechtlichen Sachverhalten mitspielenden Personen werden fortan so bezeichnet:

- Der für die **Verarbeitung Verantwortliche** = die natürliche oder juristische Person, die die Entscheidung über Zweck und Mittel der Datenverarbeitung trifft (frühere Bezeichnung: der Auftraggeber).
- Der **Auftragsverarbeiter** = die natürliche oder juristische Person, die die Daten tatsächlich verarbeitet (frühere Bezeichnung: der Dienstleister).
- Die **betroffene Person** = die natürliche Person, deren Daten verarbeitet werden (frühere Bezeichnung: der/die Betroffene).

Beispiele

- Für die Verarbeitung Verantwortliche: die Gemeinde für in ihrem Namen verarbeitete Daten
- Der Auftragsverarbeiter: ein von der Gemeinde beigezogenes IT-Dienstleistungsunternehmen
- Die betroffene Person: Gemeindemitarbeiter, Bürger, Vertragspartner

Neu ist weiters die **direkte Anwendbarkeit** der DSGVO. Wie eingangs dargetan, ist daher kein Umsetzungsgesetz notwendig. Lediglich Klarstellungen in einzelnen Details sollen mit dem DSG 2018 erfolgen. Relevant kann uU sein, dass fortan unerheblich ist, **wo** die Daten tatsächlich verarbeitet werden. Eine Verarbeitung bei IT-Dienstleistern außerhalb der EU unterliegt – wenn sie (grob gesagt) **für** einen Verantwortlichen in der EU durchgeführt wird – ebenfalls der DSGVO.

Die wesentlichen Änderungen der DSGVO betreffen nicht die Frage der Rechtmäßigkeit der Datenverarbeitung selbst, sondern die zahlreichen Verpflichtungen rund um die Datenverarbeitungen. Zuvor dürfen jedoch – entsprechend der obigen Nummerierung – zwei Ergänzungen dargetan werden:

2. Rechtfertigungsgründe – Nachschärfungen (nur) bei der Zustimmung

Die Zustimmung des Betroffenen ist nach wie vor eine der wichtigsten Rechtfertigungen für die Zulässigkeit einer Datenverarbeitung. Um als solche dienen zu können, muss sie allerdings gewisse Anforderungen erfüllen. Als Schlagworte dienen: die Abgabe der Zustimmung **in Kenntnis der Sachlage** und **freiwillig.**

Derjenige, der die Zustimmung abgibt, muss wissen, worin er einwilligt. Die Zustimmungserklärungen müssen daher so formuliert werden, dass der Einwilligende ersieht, **welche** Daten von **wem** zu **welchem Zweck** in **welcher Form** verarbeitet und gegebenenfalls **wohin** übermittelt werden.

Ebenso sind nur Zustimmungen zulässig, die **freiwillig** abgegeben wurden. Dabei wurde nicht etwa an physischen Zwang gedacht. Freiwillig bedeutet im Wesentlichen – und diesbezüglich wurde eine entsprechende Klarstellung **neu** in die DSGVO aufgenommen, – dass der Betroffene bei Verweigerung der Zustimmung keine Nachteile in der (Geschäfts-)Beziehung zum *„Verantwortlichen"* hat. Das wäre der Fall, wenn die Zustimmungserklärung in den AGB enthalten ist, weil diesfalls ein Vertragsabschluss ohne Zustimmungserklärung nicht möglich wäre. Das **Koppelungsverbot** untersagt Derartiges.

Klargestellt wurde weiters, dass für die Zustimmung ein **aktives Handeln** notwendig ist. Zustimmungen, die durch Stillschweigen oder bereits ausgewählte Checkboxen erfolgen, sind unzulässig. Eine Sonderregelung wird für Cookies gelten, was für jene Gemeinden interessant ist, auf deren Webseiten zustimmungspflichtige Cookies (zB Analysetools) implementiert sind. Die derzeit im Entwurf vorhandene *„ePrivacy-Verordnung"*[11] wird diesbezüglich eine Erleichterung vorsehen. Demnach soll – wenngleich sich dies nicht mit dem grundsätzlichen System der Zustimmungserklärung vereinbaren lässt – eine Zustimmung über die Browsereinstellung zulässig sein.

Die Zustimmung muss schon derzeit ohne Grund widerrufen werden können. Neu ist, dass die DSGVO nun explizit verlangt, dass der Zustimmende auch vorab über die Existenz dieser **Widerrufsmöglichkeit** in Kenntnis gesetzt wird. Der leichten Administration wegen hat sich die Einführung einer Zustimmungs-/Widerrufsdatenbank bewährt, um einen Überblick zu erhalten, von welchen Bürgern, Mitarbeitern oder

11) Entwurf zu einer Verordnung der EP und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der RL 2002/58/EG.

Kunden aktuell eine aufrechte Zustimmung vorhanden ist.

Beispiele

Anwendungsbeispiele in der Gemeindepraxis sind etwa die Zustimmung, Lichtbilder auf der Homepage oder in der Gemeindezeitung zu verwenden oder Informationsmaterial zu erhalten.

Praxistipp

Mit 25. 5. 2018 sind jedoch nicht alle Zustimmungserklärungen neu einzuholen. Wurden bereits Formulierungen und Vorgehensweisen gewählt, die den Anforderungen der DSGVO entsprechen, wirkt diese Zustimmung fort. Bei allen anderen ist nachzujustieren.

3. Datenschutzrechtliche Grundsätze – Accountability

Bei den datenschutzrechtlichen Grundsätzen sticht als nennenswerte Neuerung die Rechenschaftspflicht *(„accountability")* hervor. Diese legt den Verantwortlichen die Pflicht auf, einerseits Maßnahmen zur Einhaltung der – oben genannten – Grundsätze zu implementieren und andererseits diese Einhaltung auch nachweisen zu können. Mit Letzterem wird daher ein erhöhter Dokumentationsaufwand entstehen, um der Datenschutzbehörde im Anlassfall belegen zu können, welche Maßnahmen gesetzt wurden (zB interne Datenschutzrichtlinien).

4. Ausgewählte Neuerungen

a) Der Datenschutzbeauftragte

Bisher nur freiwillig möglich, normiert die DSGVO nun unter gewissen Voraussetzungen die Pflicht, Datenschutzbeauftragte zu bestellen. Während dies im privaten Bereich an die Art und Intensität der Unternehmenstätigkeit („Kernleistungen") geknüpft ist, gilt für den öffentlichen Bereich uneingeschränkt: **Behörden und öffentliche Stellen haben einen Datenschutzbeauftragten zu bestellen.**[12)]

Betreffend die öffentlichen Unternehmen ist zu erweitern: ausschreibungspflichtig = Befreiung von Geldbußen = Pflicht zur Bestellung eines Datenschutzbeauftragten.

Die DSGVO sieht allerdings die Möglichkeit vor, dass **ein** Datenschutzbeauftragter **für mehrere** Behörden bzw öffentliche Stellen bestellt werden kann.[13)] Va auf Gemeindeebene wird dies zur Erleichterung führen, zumal nicht jede Gemeinde einen eigenen Datenschutzbeauftragten bestellen müssen wird. Eine exakte Anzahl an Gemeinden, die ein gemeinsamer Datenschutzbeauftragter betreuen darf/kann, kennt die DSGVO nicht. Je nach Größe und Organisationsstruktur der Gemeinden variiert dies. Als Anhaltspunkt können Größenordnungen aus anderen Gemeindeverbänden, die etwa ein gemeinsames Abwassermanagement erlauben, dienen.

Zu den **Aufgaben** eines Datenschutzbeauftragten zählen ua:

- Unterrichtung und laufende Beratung in datenschutzrechtlichen Angelegenheiten;
- Schulung der Mitarbeiter;
- Erstellung von Zustimmungserklärungen, Abschluss von Verträgen mit IT-Dienstleistern;
- allgemeine Vertragsgestaltung: Überbinden der datenschutzrechtlichen Verpflichtungen;
- Unterstützung bei der Erstellung und dem Führen des Verzeichnisses der Datenverarbeitungen;
- Überwachung der Einhaltung der DSGVO;
- Zusammenarbeit mit der Datenschutzbehörde.

Die DSGVO stellt keine formalen **Anforderungen** an die **Person des Datenschutzbeauftragten** (keine bestimmte Ausbildung oder Studium, keine bestimmte Berufstätigkeit). Die Voraussetzungen sind vielmehr **inhaltlicher Natur:** Die Person muss geeignet sein, die Aufgaben zu erfüllen. Dazu sind sowohl rechtliche (DSGVO, DSG 2018, uU Arbeitsrecht, Telekommunikationsrecht) als auch technische Kenntnisse (Datensicherheitsmaßnahmen, technische Standards [ISO], IT-Architektur) notwendig.

Die DSGVO lässt sowohl die Benennung eines **internen** als auch eines **externen** Datenschutzbeauftragten zu. Zentral ist lediglich, dass der Datenschutzbeauftragte bei der Erfüllung seiner Pflichten in **keinen Interessenskonflikt** gerät. Das ist zu beachten, wenn – wie in der Praxis gerne – daran gedacht wird, den eigenen IT-Administrator oder den Leiter der Personalabteilung zum Datenschutzbeauftragten zu bestellen.

Unabhängig der Frage, ob extern/intern bestellt wird, ist eine relativ prominente **Eingliederung in die Organisationsstruktur** vorzusehen. So genießt der Datenschutzbeauftragte

- **Weisungsfreiheit** betreffend die Erfüllung seiner Aufgaben;
- eine direkte **Berichtslinie zur höchsten Managementebene** (bei Gemeinden der Bürgermeister);
- eine **frühzeitige Einbindung** in alle datenschutzrelevanten Fragen sowie
- den Zugang zu allen personenbezogenen Daten und Verarbeitungsvorgängen.

Im Gegenzug ist der Datenschutzbeauftragte, der im Übrigen auch von den betroffenen Personen (also zB Bürgern und Mitarbeitern) kontaktiert werden kann, zur Verschwiegenheit verpflichtet.

b) Das Verzeichnis der Datenverarbeitungen

Die **gute Nachricht:** Die Meldepflicht entfällt. Die Verantwortlichen, so auch die Gemeinden, brauchen ab Mai 2018 keine Datenverarbeitungen mehr an das Datenverarbeitungsregister (DVR) melden. Das DVR wird von der Datenschutzbehörde bis zum 31. 12. 2019 lediglich zu Archivzwecken fortgeführt, dabei werden jedoch keine Eintragungen und Änderungen mehr vorgenommen.

Die **schlechte Nachricht:** Die Pflicht zur Führung eines Verzeichnisse wandert – wenn man so will – zu den einzelnen Verantwortlichen. Anstatt des zentralen DVR hat nun jeder Verantwortliche selbst ein Verzeichnis über sämtliche von ihm durchgeführte Verar-

12) Art 37 Abs 1 lit a DSGVO.
13) Art 37 Abs 3 DSGVO.

beitungstätigkeiten zu führen, um der Datenschutzbehörde rasch einen Überblick über die Datenverarbeitungen liefern zu können. Diese Pflicht verbleibt beim Verantwortlichen, auch wenn ein Datenschutzbeauftragter bestellt wurde. Letzterer ist bei der Erstellung und Führung lediglich beratend beizuziehen.

Von dieser Pflicht existiert eine **Ausnahme.** Nicht zuletzt aufgrund des zu erwartenden Aufwands hat sich diese rasch verbreitet. Vorsicht bei der Euphorie: Die Annahme, auf ein Verzeichnis könne verzichtet werden, wenn weniger als 250 Mitarbeiter beschäftigt werden, ist dabei irreführend und als solche unrichtig. Dieses Kriterium allein ist zu wenig. **Zusätzlich** müssen drei weitere Voraussetzungen erfüllt sein, um unter die Ausnahme zu fallen:

- Es dürfen keine Daten besonderer Kategorien (früher „*sensible*" Daten) verarbeitet werden.
- Die Verarbeitung darf „*nicht nur gelegentlich*" stattfinden.
- Die Verarbeitung darf kein Risiko für die Rechte und Freiheiten der betroffenen Personen beinhalten.

Diese Bedingungen sind ebenso schwammig formuliert wie kaum einzuhalten.

Beispiel

Wird etwa für jeden Gemeindebediensteten ein Lichtbild angefertigt und auf die Homepage gestellt, geschieht dies bei jedem Bediensteten wahrscheinlich ein einziges Mal, also „gelegentlich". Aus Sicht der Gemeinde ist jedoch die Datenverarbeitung „Anfertigung eines Lichtbildes der Bediensteten zum Zwecke der Steigerung des Bürgerservice durch Anbringung auf der Homepage" keineswegs eine bloß gelegentliche, sondern in Wahrheit eine geradezu ständige. Weiters ist kaum eine Datenverarbeitung denkbar, die kein Risiko für die Rechte und Freiheiten beinhaltet – immerhin stellt jede Datenverarbeitung einen Eingriff in das Grundrecht auf Datenschutz dar.

Abgesehen von der Unsicherheit der Ausnahme bietet das Erstellen des Verzeichnisses auch Vorteile: Nach dem ersten Aufwand, den Ist-Stand in eine geeignete Verzeichnisform zu gießen, dient das Verzeichnis auch intern als Überblick, der etwa im Falle von Löschungs- oder Auskunftsbegehren herangezogen werden kann.

Eine bestimmte **Form** des Verzeichnisses ist nicht vorgegeben. Es muss lediglich sichergestellt sein, dass das Verzeichnis der Datenschutzbehörde übergeben werden kann. Eine elektronische Führung, wenn ausdruckbar, wird sich daher zum Standard entwickeln.

Praxistipp

Aufgrund der leichten Adaptierbarkeit empfiehlt sich die Verwendung von Excel, Word oder vergleichbarer Software.

Betreffend den **Inhalt** gibt die DSGVO relativ klar vor, welche Angaben **für jede Verarbeitungstätigkeit** in das Verzeichnis aufzunehmen sind:

- Zweck der Verarbeitung;
- Kategorie und Art der Daten;
- welche betroffenen Personen?
- gegebenenfalls: an wen werden die Daten übermittelt?
- Speicherdauer;
- allgemeine Beschreibung der Datensicherheitsmaßnahmen;
- idealerweise Rechtfertigungsgrund;
- wenn möglich allfällige Löschfrist;
- allgemeine Angaben: Name und Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten.

c) Die Betroffenenrechte

Recht auf **Auskunft,** Recht auf **Richtigstellung,** Recht auf **Löschung** … alles Begriffe, die schon aus dem aktuellen Datenschutzrecht bekannt sind. Schon bisher konnte jeder Betroffene beantragen, der Auftraggeber möge ihm bekannt geben, welche seiner personenbezogenen Daten verarbeitet werden. Ebenso ist es möglich, die Löschung dieser Daten zu beantragen. Wenn keine Aufbewahrungspflichten oder Rechtfertigungsgründe entgegenstehen, ist diesem Antrag auch zu folgen.

Diese altbekannten Betroffenenrechte stehen natürlich auch nach der DSGVO zur Verfügung und haben in Einzelheiten kleine Verschärfungen erfahren. Bspw hat die Auskunft oder Löschung nunmehr **binnen einem Monat** zu erfolgen (bisher acht Wochen).[14] Die Fristverkürzung kann in Einzelfällen durchaus eine zeitliche und organisatorische Herausforderung darstellen.

Neu ist weiters, dass der Antrag auf Auskunft nicht mehr in Schriftform gestellt werden muss, sohin – theoretisch – auch mündlich zulässig ist. Der bisher stets verpflichtende Identitätsnachweis ist nur mehr in Zweifelsfällen vom Antragsteller zu erbringen.

Praxistipp

Dennoch empfiehlt sich weiterhin, den Antragsteller zum Nachweis seiner Identität aufzufordern; immerhin würde die Beauskunftung an die falsche Person einen gravierenden **Datenschutzverstoß** darstellen. In einem solchen Fall ist – wie bei jeder anderen Datenbeschädigung oder Datenverlust – die betroffene Person zu informieren. Dies schon nach geltender Rechtslage. Neu ist, dass hinkünftig **auch die Datenschutzbehörde zu verständigen** ist.

Bei der Frage, welche Informationen zu beauskunften sind, gesellen sich neben dem bereits bisher erforderlichen Inhalt (die personenbezogenen Daten inkl Kategorie, Verarbeitungszweck, Herkunft und Empfänger) auch der Hinweis auf die Speicherfrist sowie die Belehrung über weitere Betroffenenrechte und Beschwerdemöglichkeiten. Ebenso ist eine Kopie der Daten auszuhändigen (bei elektronischen Anträgen elektronisch; bei Anträgen auf Papier in Papierform).

14) Bei komplexen Begehren ist eine Verlängerung auf zwei Monate möglich.

Praxistipp

Dabei kann die Möglichkeit, den Betroffenen einen Fernzugang (zB Log-in auf der Homepage) einzurichten, in dem der Betroffene seine Daten sieht, eine Erleichterung darstellen.

Für den Fall, dass keine Daten des Antragstellers verarbeitet werden, ist nach wie vor eine **Negativauskunft** zu erteilen. Können solche Daten lediglich intern nicht (sofort) gefunden werden, kann der Betroffene zur Mithilfe *(wo vermutest du deine Daten?)* aufgefordert werden, wenngleich diese – im DSG noch unstrittige – **Mitwirkungspflicht** nun nur mehr in den Erwägungsgründen angedeutet wird.

Die Beantwortung des Auskunftsbegehrens kann durchaus hohe Kosten auflaufen lassen. Bisher ist im DSG klar geregelt, dass eine Beauskunftung pro Jahr kostenlos zu erfolgen hat. Eine solche absolute Zahl findet sich in der DSGVO nicht mehr. Stattdessen können Verantwortliche die Beauskunftung verweigern (oder wahlweise kostenpflichtig beantworten), wenn die Antragstellung des Betroffenen offenkundig unbegründet oder exzessiv häufig stattfindet. Selbst wenn der Datenbestand nicht sehr dynamisch ist, wird aber weiterhin eine Auskunft pro Jahr kostenlos zu erteilen sein.

Beim Recht auf Richtigstellung und Löschung werden – abgesehen von der Fristverkürzung – keine in der Praxis allzu relevanten Neuerungen vorgesehen. Das DSG 2018 sieht dabei eine **Erleichterung für Daten in Back-ups** vor: Sind nämlich die Berichtigung oder Löschung von automationsunterstützt verarbeiteten Daten nicht unverzüglich, sondern nur zu bestimmten Zeitpunkten möglich, kann die Datenverarbeitung (anstatt die Daten zu löschen) eingeschränkt werden.[15] MaW: Die Speicherung der Daten ist vorerst weiter zulässig, alle anderen Verarbeitungsschritte jedoch sind untersagt. Dies entspricht dem in der DSGVO neu enthaltenen Recht auf **Einschränkung der Datenverarbeitung.**[16]

Komplettiert werden die Betroffenenrechte mit dem (bereits bekannten) Recht auf Widerspruch sowie dem (neuen) Recht auf Datenportabilität. Beide werden in der Gemeindepraxis jedoch kaum eine Rolle spielen.

d) Weitere Neuerungen

Natürlich kennt die DSGVO weitere Neuerungen, deren praktische Relevanz auf Gemeindeebene jedoch untergeordnet werden kann. Auch um die Grenzen des Beitrags nicht zu sprengen, darf lediglich in Stichwortform auf die neuen Grundsätze privacy by design, privacy by default, das Verbot des Profiling und die Datenschutz-Folgeabschätzung verwiesen werden.

15) § 3 DSG 2018.
16) Art 18 DSGVO.

➜ In Kürze

Die Frage, ob eine Datenverarbeitung zulässig ist oder nicht, wird nach Geltung der DSGVO nur in wenigen Ausnahmefällen anders zu beurteilen sein als bisher. Die wesentlichen Änderungen, die die DSGVO mit sich bringt, betreffen va das Geschehen rund um die Datenverarbeitungen, wie etwa die Pflicht zur Führung eines Verarbeitungsverzeichnisses und Bestellung eines Datenschutzbeauftragten. Trotz Ausnahme von den drastisch angehobenen Geldbußen sind die Gemeinden gut beraten, diese Anforderungen einzuhalten, um Schäden gleich welcher Art zu verhindern.

➜ Zum Thema

Über den Autor:
Mag. Martin Führer, LL. M., ist als selbständiger Rechtsanwalt spezialisiert auf Datenschutzrecht/IT-Recht und Vergaberecht. Zudem zertifizierter Datenschutzbeauftragter und Lektor an der FH St. Pölten für IT- und Medienrecht.

Kontakt: urbanek | lind | schmied | reisch Rechtsanwälte OG, Domgasse 2, 3100 St. Pölten.
Tel: + 43 (0)2742 351 550
E-Mail: fuehrer@ulsr.at
Internet: www.ulsr.at

➜ Literatur-Tipp

Datenschutz konkret (5 Mal jährlich)
Kennenlernabo: 2 Hefte € 15,– (inkl Versand im Inland)
Internet: dako.manz.at

MANZ Bestellservice:
Tel: (01) 531 61-100
Fax: (01) 531 61-455
E-Mail: bestellen@manz.at
Besuchen Sie unseren Webshop unter www.manz.at