Arbeitshilfe

Datenschutz in Museen

Thomas Schwabenbauer

Überblick über die Inhalte der Datenschutzgrundverordnung (DSGVO) und der nationalen Datenschutzgesetze

Die Datenschutzgrundverordnung (DSGVO) ist spätestens seit Beginn ihrer Geltung zum 25. Mai 2018 aus der Medienberichterstattung nicht mehr wegzudenken. Behörden, Unternehmen, Vereine und Privatpersonen sehen sich mit realen wie auch teils fiktionalen Anforderungen konfrontiert, um den neuen Datenschutzregelungen gerecht zu werden. Die Angst vor ruinösen Bußgeldbescheiden ist ebenso verbreitet wie die Sorge, durch anwaltliche Abmahnungen »geschröpft« zu werden. Der vorliegende Beitrag gibt daher einen ersten Überblick über wichtige Inhalte der DSGVO und der einschlägigen nationalen Gesetze. Sein Ziel ist es, insbesondere staatlichen, kommunalen und privaten Museen Impulse für eine Analyse ihrer alltäglichen Datenverarbeitungen und für eine Identifizierung des bei jedem Museum mutmaßlich bestehenden Handlungsbedarfs zu geben.

Basiswissen zum Datenschutzrecht 2018

Die EU-Datenschutzreform 2018

Der Datenschutz hat seine rechtlichen Wurzeln sowohl im Grundgesetz als auch in der Europäischen Grundrechtecharta. Er soll dem einzelnen Menschen eine Kontrolle über seine persönlichen Daten gewähren. Jeder soll grundsätzlich wissen können, wer was von ihm weiß und den Fluss seiner Daten auch einigermaßen steuern können. Dieser Anspruch ist unter den Bedingungen der Informationsgesellschaft, die auch immer weniger nationale Grenzen kennt, schwer zu erfüllen. Aus diesem Grund hat sich die EU des Themas angenommen und die Datenschutzreform 2018 initiiert. Kernstück dieser Reform ist die DSGVO.

Die DSGVO versucht einerseits, das Ideal eines informationellen »Herrschaftsrechts« der Betroffenen über seine Daten trotz allgegenwärtiger und vielfach unübersehbarer Datenverarbeitungen nicht aufzugeben und durch bestimmte Mechanismen zu schützen, andererseits Datenverarbeitungen zu ermöglichen, damit sowohl der Staat seine Aufgaben erfüllen kann, aber auch Unternehmen das wirtschaftliche Potenzial, das in der »Arbeit« mit fremden Daten gesehen wird, heben können.

Was ist eine (Grund-)Verordnung?

Das Unionsrecht kennt insbesondere zwei Formen der Rechtssetzung: die Richtlinie und die Verordnung. Eine Richtlinie richtet sich vorrangig an die jeweiligen Mitgliedsstaaten; diese sind verpflichtet, den Inhalt einer Richtlinie nach den Vorgaben ihres innerstaatlichen Rechts umzusetzen.

Anders ist dies bei einer Verordnung. Eine Verordnung hat allgemeine Geltung. Sie ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedsstaat. Sie gibt also ohne nationalen Umsetzungsakt direkt den Betroffenen Rechte und erlegt ihnen Pflichten auf. Die Datenschutzgrund-Verordnung ist demnach von allen, für die sie gilt, zu beachten, d. h. von Behörden, Unternehmen, Vereinen und Privatpersonen. Allerdings hält die DSGVO eine Besonderheit bereit: Sie erlaubt im beachtlichen Umfang den Mitgliedsstaaten – v. a. im öffentlichen (Verwaltungs-)Bereich – die Verordnung nicht nur zu konkretisieren, sondern teilweise auch von ihr abzuweichen. Aus diesem Grund ist die Bedeutung des nationalen Datenschutzrechts (also des Bundesdatenschutzgesetzes BDSG und des Bayerischen Daten-

Dr. Thomas Schwabenbauer ist Richter am Verwaltungsgericht München und war bis Anfang 2018 Referent beim Bayer. Landesbeauftragten für den Datenschutz.

schutzgesetzes BayDSG) für nicht öffentliche, aber v. a. für öffentliche Stellen größer als man bei einer Datenschutzgrund-Verordnung erwarten würde.

Daraus folgt: Nicht öffentliche wie öffentliche Stellen, d. h. Behörden, Unternehmen, Vereine und Privatpersonen müssen, soweit sie von der DSGVO betroffen sind, diese nicht nur verstehen und anwenden, sondern haben dabei auch das nationale Datenschutzrecht einzubeziehen. Das ist manchmal kompliziert, aber nichts grundlegend Neues. Schon bislang mussten Vorschriften aus verschiedenen Ebenen (EU, Bund, Land) in ihrem Zusammenspiel betrachtet werden und sind den Museen etwa aus dem Vergaberecht bekannt.

Aufbau der DSGVO

Die DSGVO ist ein Gesetzestext, der in 99 Artikeln regelt, wann und vor allem mit welchen technischen und organisatorischen Folgen personenbezogene Daten verarbeitet werden dürfen. Der Verordnung sind 173 sogenannte Erwägungsgründe (EG) vorangestellt. Diese sind leider nicht sehr leserfreundlich gestaltet, aber dennoch hilfreich. Sie zeigen auf, welche Überlegungen zum Erlass der Verordnung und ihrer Artikel geführt haben. Aus den Erwägungsgründen können keine unmittelbaren Rechte und Pflichten abgeleitet werden, dennoch bilden sie eine wichtige Auslegungshilfe für die 99 Artikel und werden demnach bei rechtlichen Streitfragen als Argumentationshilfe herangezogen.

Verbietet der Datenschutz alles?

Zunächst gilt es, mit einem Vorurteil aufzuräumen: Nur, weil ein bestimmter Vorgang oder Sachverhalt datenschutzrechtlich relevant ist – es also »irgendwie« um personenbezogene Daten geht –, heißt das nicht, dass er von vornherein verboten ist. Häufig sind Vorgänge und Sachverhalte, die datenschutzrechtlich relevant sind, erlaubt oder es ist »nur« notwendig, bestimmte Anforderungen (etwa an die Sicherheit oder an die Zugriffsmodalitäten) zu beachten. Entsprechend geht es bei Verstößen in der Praxis häufig nicht darum, dass eine Datenverarbeitung überhaupt unzulässig ist, sondern dass sie allzu gedanken- und grenzenlos betrieben wird.

Personenbezogene Daten und deren Verarbeitung

Zentralbegriff der DSGVO ist der Begriff der personenbezogenen Daten. Geht es bei einem Sachverhalt nicht um personenbezogene Daten einer natürlichen (und noch lebenden) Person, dann ist das Datenschutzrecht der EU und der Mitgliedsstaaten gar nicht erst anwendbar.

a. Personenbezogene Daten

Der Zweck der DSGVO ist der Schutz der Grundrechte natürlicher (lebender) Personen bei der Verarbeitung der ihnen »gehörenden« Daten. Entsprechend ist die Definition der personenbezogenen Daten in Art. 4 Nr. 1 DSGVO sehr weit gefasst. Eine Information ist nicht erst dann als personenbezogen anzusehen, wenn der Verantwortliche selbst eine Identifizierung der hinter den Daten »steckenden« Person durchführen kann; vielmehr genügt es, dass irgendein Dritter nach allgemeinem Ermessen diese wahrscheinlich durchführen kann (vgl. EG 26).

b. Datenverarbeitung

Die Regelungen der DSGVO knüpfen regelmäßig an die »Verarbeitung« personenbezogener Daten an. Der Verarbeitungsbegriff wird in Art. 4 Nr. 2 DSGVO definiert und ist ebenfalls sehr weit gefasst, nämlich als Oberbegriff für alle Vorgänge, die sich auf personenbezogene Daten beziehen. Somit ist alles, was mit personenbezogenen Daten geschieht, als Verarbeitung anzusehen: das Erheben, das Speichern, das Auswerten, das Übermitteln an Dritte, das interne Nutzen, aber auch das Löschen – unabhängig davon, ob die Verarbeitung mit oder ohne automatisierte Verfahren durchgeführt wird. Digitale und manuelle Verarbeitung (etwa mittels klassischer Karteikarte oder als Papierakte) werden gleich behandelt.

c. Beispiele im Museumsbereich
Ein (Museums-)Verein verarbeitet in der Regel zumindest folgende personenbezogene Daten: Name und Anschrift, Beruf, Telefonnummer, E-Mail-Adresse seiner Mitglieder; das Datum des Vereinsbeitritts; eventuell Besitzverhältnisse, Provenienzen (etwa von Personen, die bestimmte museal interessante Gegenstände besitzen). Eine Verarbeitung liegt hier nicht nur in der Speicherung der Daten in der (vielleicht »selbst gestrickten«) Mitgliederdatenbank vor. Auch Zugriffe des Vereinsvorstands oder von Beschäftigten auf diese Daten und ihre Nutzung für Vereinszwecke sind datenschutzrechtlich relevant. Gleiches gilt natürlich auch für die Offenlegung der Daten durch Übermittlung an Dritte – etwa an Dachorganisationen, Ver-sicherungen, andere Vereinsmitglieder, Kooperationspartner, Sponsoren, Leihgeber etc. Denkbar ist auch, dass etwa Mitgliederdaten an eine Stelle übermittelt werden, die über Fördermittel entscheidet, für die die Größe des Vereins maßgeblich ist. Auch das Aushängen von Daten am »schwarzen Brett« (etwa zu einem Altersjubiläum, Danksagung für eine Leihgabe etc.) ist eine Offenlegung von personenbezogenen Daten. Erst recht gilt dies für Veröffentlichungen in einer Mitgliederzeitung oder im Internet (z. B. auf der eigenen Webseite). Gerade eine Veröffentlichung an einen unbestimmten (weltweiten) Adressatenkreis ist rechtlich oft zweifelhaft und jedenfalls sorgfältig zu prüfen. Es gilt insoweit v. a. die Grundsätze der Datensparsamkeit und der Erforderlichkeit (Bezug zum Vereinszweck) zu beachten.

Auch die Veröffentlichung der Namen von Funktionsträgern und Mitarbeitern im Intra- oder Internet muss datenschutzrechtlich zulässig sein. Auch eine elektronische Zeiterfassung der Mitarbeiter – und damit zumindest von deren Anwesenheits- und Pausenzeiten – ist eine personenbezogene, zudem dem Personal- oder Mitarbeiterdatenschutz unterliegende Datenerhebung und ggf. Nutzung, die einer Rechtsgrundlage bedarf.

Nicht von der DSGVO geschützt werden Angaben über Verstorbene, wie etwa in einem Nachruf für ein Vereinsmitglied im Vereinsblatt oder die Nennung auf einer Liste der Verstorbenen (vgl. EG 27 DSGVO). Es kann allerdings das postmortale Persönlichkeitsrecht betroffen sein, für das es eigene Regelungen gibt.

Anwendungsbereich der nationalen Datenschutzgesetze
a. Allgemeines
Wie bereits erwähnt, ist neben der DSGVO auch das nationale Datenschutzrecht zu beachten. Hier ist zwischen dem BDSG und – in Bayern – dem BayDSG zu unterscheiden.

Das BDSG gilt nach seinem § 1 für die Verarbeitung personenbezogener Daten durch öffentliche Stellen des Bundes – also für Bundesbehörden – und insbesondere für nicht öffentliche Stellen, also v. a. Unternehmen und Vereine.

Das BayDSG (und nicht das BDSG) findet hingegen nach Art. 1 Abs. 1 BayDSG Anwendung für Behörden und sonstige öffentliche Stellen des Freistaates Bayern, der Gemeinden, Gemeindeverbände und der sonstigen der Aufsicht des Freistaates Bayern unterstehenden juristischen Personen des öffentlichen Rechts. Öffentliche Stellen sind auch Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen eine oder mehrere der genannten juristischen Personen des öffentlichen Rechts beteiligt sind. Grundsätzlich wird man zumindest nicht ausschließen können, dass auch Museen bei entsprechender Konzeptionierung Aufgaben der öffentlichen Verwaltung wahrnehmen.

b. Museen als öffentliche oder als nicht öffentliche Stellen
Werden Daten von einer öffentlichen Stelle verarbeitet, gelten also (teilweise) andere Regelungen als bei einer nicht öffentlichen Stelle. In welche dieser beiden Kategorien ein Museum einzuordnen ist, ergibt sich aus seiner konkreten Betriebs- und Organisationsform (vgl. ausführlich Kley, Arbeitshilfe: Betriebsformen von Museen, museum heute 51, Juni 2017, S. 49 ff., abrufbar unter: *https://www.museen-in-bayern.de/fileadmin/news_import/mh51_web.pdf*).

Soweit ein Museum als (unselbstständige) öffentlich-rechtliche Einrichtung einer Gemeinde organisiert ist und etwa Gemeindemitarbeiter dort als Beschäftigte arbeiten, ist das jeweilige Museum schon kraft seiner Organisation eine öffentliche Stelle – und muss

neben der DSGVO v. a. das BayDSG beachten. Gleiches gilt, wenn das Museum von einem kommunalen Zweckverband getragen wird.

Exkurs: Datenschutz ist nicht Urheberrecht
Zur Klarstellung soll an dieser Stelle erwähnt werden, dass Datenschutzrecht und Urheberrecht voneinander zu unterscheiden sind. Das Urheberrecht versucht, das Interesse an freiem Zugang und möglichst ungehinderter Nutzung von Werken mit dem Schutz geistiger Leistungen des Schöpfers des Werks in Ausgleich zu bringen. Im Zentrum des Urheberrechts stehen das Werk und sein Schöpfer. Daher wird etwa die Frage, welche Bilder aus dem Internet einen Museumskatalog zieren dürfen, nicht durch die DSGVO oder das BDSG/BayDSG beantwortet. Diese Frage beantwortet nur das Urheberrecht. Erst wenn etwa auf einem Bild Personen erkennbar sind, kann es (auch) um die Frage gehen, ob und inwieweit eine Veröffentlichung eine Verarbeitung personenbezogener Daten darstellt und ob dies erlaubt ist.

Wann ist Datenverarbeitung erlaubt?
Die Antwort auf diese Frage ist naturgemäß abhängig vom Einzelfall. Zur groben Orientierung kann man aber Folgendes sagen:

Für öffentliche Stellen, also etwa Museen in der Form einer öffentlich-rechtlichen Einrichtung einer Gemeinde, gilt im Wesentlichen der Grundsatz, dass es – wie bislang auch – für die Datenverarbeitung einer gesetzlichen Befugnis oder einer Einwilligung bedarf. Für die gesetzliche Befugnis ist nach wie vor das nationale Recht von grundlegender Bedeutung (und weniger die DSGVO); Rechtsgrundlagen finden sich im Fachrecht (etwa dem Beamtenrecht, wenn es um Daten der Beschäftigten geht) oder im BayDSG (als Auffanggesetz). Die Einwilligung als mögliche Erlaubnis für eine Datenverarbeitung ergibt sich aus Art. 6 Abs. 1 Buchstabe a) DSGVO i. V. m. Art. 7 DSGVO und Art. 4 Nr. 11 DSGVO. Es sollte zur Vermeidung von Missverständnissen und Fehlvorstellungen allerdings unterlassen werden, Einwilligungen dort einzuholen, wo bereits aufgrund einer gesetzlichen Erlaubnis (und damit gerade ohne Einwilligung) Daten verarbeitet werden.

Für nicht öffentliche Stellen, z. B. für ein als Verein betriebenes Museum, sind hingegen neben der Einwilligung auch andere Erlaubnisse der DSGVO, aber natürlich auch des BDSG oder des Fachrechts, etwa des Arbeitsrechts, von Relevanz. Die zentrale Norm der DSGVO ist insoweit Art. 6 Abs. 1 DSGVO. Gerade für Vereine dürfte hierbei insbesondere Art. 6 Abs. 1 Buchstabe b) und f) DSGVO von Interesse sein.

Nach Art. 6 Abs. 1 Buchstabe b) DSGVO ist die Verarbeitung erlaubt für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder wenn sie zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen. Die Mitgliedschaft in einem Verein ist als Vertragsverhältnis zwischen den Mitgliedern und dem Verein anzusehen, dessen Inhalt im Wesentlichen durch die Vereinssatzung und ergänzende Regelungen (etwa eine Vereinsordnung) vorgegeben wird. Eine Vereinssatzung bestimmt insoweit die Vereinsziele, für welche die Mitgliederdaten genutzt werden können.

Nach Art. 6 Abs. 1 Buchstabe f) DSGVO ist eine Verarbeitung erlaubt, wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, 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. Auf der Basis des Art. 6 Abs. 1 Buchstabe f) DSGVO kann – je nach verfolgtem Zweck – die Datenerhebung von Nicht-Mitgliedern (Lieferanten, Besuchern und Gästen) in Betracht kommen.

Daneben ist eine Verarbeitung nach Art. 6 Abs. 1 Buchstabe a) DSGVO gestattet, wenn die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat. Für die Wirksamkeit einer Einwilligung ist v. a. Art. 4 Nr. 11 und Art. 7 DSGVO zu beachten. Eine Einwilligung ist aber nur dann erforderlich, soweit das Museum in weiter gehendem Maße personenbezogene Daten verarbeitet, als es aufgrund Art. 6 Abs. 1 Buchstabe b) und f) DSGVO befugt ist.

Auch hier gilt, dass es zur Vermeidung von Missverständnissen und Fehlvorstellungen unterlassen werden sollte, Einwilligungen für Datenverarbeitungsmaßnahmen einzuholen, die bereits aufgrund einer gesetzlichen Erlaubnis (und damit gerade ohne Einwilligung) erlaubt sind.

Für die Verarbeitung von Daten von Beschäftigten im Rahmen der Personalverwaltung sind bei nicht öffentlichen Stellen wie Vereinen Art. 88 DSGVO und § 26 BDSG, für öffentliche Stellen ggf. das Beamtenrecht zu beachten.

Schließlich gibt es noch Sondervorschriften für besondere Verarbeitungssituationen. Zu nennen ist insbesondere die Videoüberwachung. Für Museen, die als öffentliche Stelle anzusehen sind, ist hier Art. 24 BayDSG die entscheidende Norm. Für Museen, die nicht öffentliche Stellen sind, ist § 4 BDSG maßgeblich, der die Videoüberwachung öffentlich zugänglicher Räume regelt.

Soweit es nach den vorstehenden Rechtsgrundlagen zulässig ist, Daten zu verarbeiten, empfiehlt es sich, in der Satzung und in einer Vereinsordnung insbesondere das Folgende zu regeln:

- Welche Daten werden beim Vereinseintritt für die Verfolgung welcher Vereinsziele und für die Mitgliederbetreuung und -verwaltung erhoben?
- Welche Daten werden für welche anderen Zwecke bei den Mitgliedern in Erfahrung gebracht?
- Wer erhält zu welchen Daten aus welchem Grund und zu welchem Zweck Zugang?
- Welche Daten werden im Wege der Auftragsdatenverarbeitung verarbeitet (anbieten dürfte sich hier eine zusammenfassende Beschreibung der Daten in Obergruppen)?
- Welche Anlässe für Übermittlung der Daten an Dritte – etwa an Dachorganisationen, Versicherungen, andere Vereinsmitglieder, Sponsoren, Leihgeber etc. – sind vorgesehen? Auch eine Übermittlung von Mitgliederdaten zum Nachweis einer bestimmten Vereinsgröße zwecks Erhalt öffentlicher Fördermittel wird hiervon erfasst.
- Welche Daten sollen zu welchem Zweck und aus welchem Grund für welchen Zeitraum am »schwarzen Brett« ausgehängt oder in einer Mitgliederzeitung oder im Internet veröffentlicht werden?
- Wann werden welche Daten gelöscht?

Entsprechendes sollte ebenfalls bei einem Museum als öffentliche Stelle in einer Datenschutzdienstanweisung geregelt werden.

Weitere Inhalte der Datenschutzgrundverordnung

Die DSGVO enthält gar nicht so viele Vorgaben zur Frage, wann eine Datenverarbeitung erlaubt ist. Ihr Schwerpunkt liegt vielmehr in – vom Transparenzgedanken geprägten – organisatorischen und institutionellen Vorgaben, die sich entweder an eine konkrete Datenverarbeitung anschließen (Beispiel: Informationspflichten nach Art. 13, 14 DSGVO, Meldepflicht bei Datenpanne nach Art. 33 DSGVO) oder die allgemein zu beachten sind, wenn überhaupt Daten verarbeitet werden.

Adressat der DSGVO – der Verantwortliche

Die vielfältigen Pflichten der DSGVO betreffen meist den »Verantwortlichen«. Dieser Begriff wird in Art. 4 Nr. 7 DSGVO definiert. Danach ist, vereinfacht formuliert, Verantwortlicher immer die Stelle, die personenbezogene Daten verarbeitet. Also die Gemeinde, wenn das Museum dieser organisationsrechtlich zugeordnet ist, oder etwa der Verein, wenn das Museum als solcher organisiert ist.

Organisatorische und institutionelle Vorgaben der DSGVO (als Folge von Datenverarbeitung)

Ist eine Datenverarbeitung erlaubt, knüpft die DSGVO und ggf. das konkretisierende nationale Recht hieran bestimmte organisatorische Folgen. Unabhängig von einer konkreten Datenverarbeitung kennt die DSGVO weitere, vielfach eher bürokratische Vorgaben.

a. Der Datenschutzbeauftragte

Nach Art. 37 DSGVO besteht die Pflicht, einen Datenschutzbeauftragten zu benennen. Hier wirkt sich der Unterschied zwischen öffentlichen und nicht öffentlichen Stellen aus. Museen, die als öffentliche Stelle anzusehen sind, brauchen einen eigenen Datenschutzbeauftragten (wenn sie etwa als Zweckverband organisiert sind), sofern nicht für sie ohnehin der Datenschutzbeauftragte derjenigen öffentlichen Stelle zuständig ist, deren Teil das Museum ist, also etwa der Datenschutzbeauftragte der Gemeinde.

Ist das Museum als nicht öffentliche Stelle (Privatmuseum, Verein getragenes Museum) anzusehen, so besteht die Pflicht zur Benennung eines Datenschutzbeauftragten nur, wenn – laut Art. 37 Abs. 1 Buchstabe b) DSGVO – »die Kerntätigkeit (…) in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen«.

Daneben gilt es noch § 38 Abs. 1 BDSG zu beachten. Hiernach ist zusätzlich bei nicht öffentlichen Stellen ein Datenschutzbeauftragter zu benennen, wenn entweder mindestens zehn Personen *ständig* mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind oder es sich unabhängig von der Personenzahl um eine Datenverarbeitungssituation handelt, die einer Datenschutz-Folgenabschätzung unterliegt oder der geschäftsmäßigen Verarbeitung zum Zwecke der Übermittlung, der anonymisierten Übermittlung oder der Markt- oder Meinungsforschung dient.

Ist aber ein Datenschutzbeauftragter zu benennen oder soll dies freiwillig geschehen, ist zu beachten, dass eine qualifizierte Person ausgewählt wird, die – ggf. nach einer Fortbildung – in der Lage ist, die Aufgaben nach Art. 39 DSGVO zu erfüllen.

b. Das Verarbeitungsverzeichnis

Unabhängig von einer konkreten Datenverarbeitung besteht die Pflicht, ein Verzeichnis von Verarbeitungstätigkeiten zu führen (Art. 30 DSGVO), wenn das Museum personenbezogene Daten verarbeitet (was nahezu immer der Fall sein dürfte). Das Verzeichnis dient dem Nachweis der Einhaltung der DSGVO (vgl. EG 82). Hier werden die wichtigsten Informationen zu den jeweiligen Datenverarbeitungstätigkeiten abstrakt zusammengefasst. Es muss schriftlich oder in elektronischer Form geführt werden und der Aufsichtsbehörde auf Anfrage vorgelegt werden. Das Verzeichnis muss nicht veröffentlicht werden.

Ein Museum, das als öffentliche Stelle anzusehen ist, muss stets ein solches Verzeichnis führen. Nicht öffentliche Stellen müssen hingegen nach Art. 30 Abs. 5 DSGVO das Verzeichnis nicht führen, wenn sie weniger als 250 Mitarbeiter beschäftigen. Von dieser Ausnahme gibt es allerdings drei Rückausnahmen: Ein Verzeichnis ist auch bei weniger Beschäftigten zu führen, wenn entweder die vorgenommene Verarbeitung ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt oder die Verarbeitung nicht nur gelegentlich erfolgt oder eine Verarbeitung besonders sensibler Daten stattfindet. Angesichts dieser auslegungsbedürftigen Rückausnahme ist es nicht öffentlichen Stellen zu empfehlen, sicherheitshalber ebenfalls ein solches Verzeichnis zu führen.

Das Verzeichnis bietet überdies die Möglichkeit einer Bestandsaufnahme und zwingt jedes Museum, sich über die Datenverarbeitung im eigenen Haus klar zu werden. Wer ein Verzeichnis führt, weiß und kann ggf. auch der Datenschutzaufsichtsbehörde nachweisen, welche Daten er zu welchen Zwecken verarbeitet.

Ausgehend von Sinn und Zweck des Verarbeitungsverzeichnisses – Bestandsaufnahme über die Datenverarbeitungen eines Museums und Schaffung von Transparenz für die Betroffenen – sollte das Verzeichnis alle Verarbeitungstätigkeiten hinreichend konkret, aber auch nicht zu kleinteilig abbilden. Beispiele: »Personalaktenführung«, »Urlaubsverwaltung«, »Zeiterfassung«, »Geburtstagsliste«, »Einladungsverteiler«, »Newsletter«, »E-Mail-Verwaltung«, »Videoüberwachung«, »Kundendaten« (etwa Bankdaten bei Bezahlung des Eintrittspreises mittels EC-Karte) oder »Mitgliederverwaltung«. Zu jeder dieser beispielhaft aufge-

listeten Verarbeitungstätigkeiten ist eine Beschreibung zu erstellen, welche die in Art. 30 Abs. 1 Satz 2 DSGVO genannten Angaben enthält. Ein Muster für ein solches Verzeichnis eines Vereins ist unter *www.lda.bayern.de/media/muster_1_verein_verzeichnis.pdf* abrufbar.

c. Auftragsverarbeitung und Auftragsverarbeitungsvertrag
Beauftragt ein Museum eine andere Stelle mit der Verarbeitung personenbezogener Daten, liegt eine sogenannte Auftragsverarbeitung vor. Diese ist (nur) unter bestimmten Voraussetzungen rechtlich erlaubt. Die Auftragsverarbeitung erleichtert die Arbeitsteilung und die Einbindung von Personal und Kompetenz, über die ein Museum möglicherweise selbst nicht verfügt. Anwendungsbeispiele gibt es viele: Nutzung von Clouddiensten, Finanzbuchhaltung durch Rechenzentren, Fernwartung der eigenen IT-Systeme (soweit damit, wie fast immer, auch personenbezogene Daten verarbeitet werden), Nutzung von Leasing-Kopiergeräten (die häufig die kopierten Dokumente in einem Zwischenspeicher speichern), Werbeadressenverarbeitung in einem Lettershop, Auslagerung der Backup-Sicherheitsspeicherung und anderer Archivierungen oder Beauftragung eines Sicherheitsdiensts, der an der Pforte Besucher- und Anlieferdaten erhebt.

Eine Auftragsverarbeitung ist dann zulässig, wenn Art. 28 DSGVO beachtet wird. Dies setzt voraus, dass es überhaupt einen schriftlichen Vertrag mit dem Dienstleister gibt und der Vertrag die Inhalte hat, die Art. 28 DSGVO verlangt. Als Auftragsverarbeiter darf nur ein Dienstleister ausgewählt werden, der kompetent und zuverlässig ist. Bei der Überprüfung und Anpassung der bisherigen Verträge (es gibt keinen Bestandsschutz für Altverträge!) und der Kontrolle, ob der ausgewählte Dienstleister zuverlässig ist, dürfte in der Praxis oft Handlungsbedarf bestehen.

d. Unterrichtung und Verpflichtung der Beschäftigten
Nach Art. 29 DSGVO dürfen Beschäftigte personenbezogene Daten grundsätzlich nur auf Weisung des Verantwortlichen erarbeiten. Ergänzend dazu regelt Art. 32 Abs. 4 DSGVO, dass der Verantwortliche Schritte unternehmen muss, um sicherzustellen, dass ihm unterstellte Personen, die Zugang zu personenbezogenen Daten haben (insbesondere Beschäftigte), diese nur auf seine Anweisung verarbeiten. Es ist daher geboten, alle Beschäftigten (auch ehrenamtliche Mitarbeiter) auf die Einhaltung der Vorgaben der DSGVO zu verpflichten. Ein entsprechendes Muster ist abrufbar unter
www.lda.bayern.de/media/info_verpflichtung_beschaeftigte_dsgvo.pdf

Informationspflichten
Erhebt ein Museum personenbezogene Daten direkt bei der betroffenen Person, so hat es als Verantwortlicher nach Art. 13 Abs. 1 und Abs. 2 DSGVO zum Zeitpunkt der Datenerhebung eine entsprechende datenschutzrechtliche Unterrichtung vorzunehmen. Teilt der Verantwortliche die vorgesehenen Informationen nicht, nicht vollständig oder inhaltlich unrichtig mit, so verletzt er seine Informationspflichten.

Werden hingegen personenbezogene Daten nicht bei der betroffenen Person erhoben, sondern auf andere Art und Weise, so ergeben sich Informationspflichten aus Art. 14 Abs. 1 und Abs. 2 DSGVO. Die meisten dieser Informationspflichten haben denselben Inhalt wie Art. 13 Abs. 1 und Abs. 2 DSGVO. Der Verein muss diese Informationen innerhalb einer angemessenen Frist, spätestens jedoch innerhalb eines Monats nach der Erhebung erteilen (Art. 14 Abs. 3 Buchstabe a) DSGVO). Zur Orientierung über die Information kann folgendes Kurzpapier dienen: *www.lda.bayern.de/media/dsk_kpnr_10_informationspflichten.pdf*

Meldepflicht bei Datenpannen
Die DSGVO regelt in den Art. 33 und 34 den Umgang bei Datenpannen. Dabei ist eine abgestufte Meldepflicht vorgesehen: Eine Meldung an die Datenschutzaufsichtsbehörde hat zu erfolgen, es sei denn, dass die Datenpanne »voraussichtlich nicht zu einem Risiko« für den

Betroffenen führt. Diese Ausnahme von der Meldepflicht darf nicht zu weit ausgelegt werden, allerdings ist auch zu vermeiden, dass die Aufsichtsbehörde mit »Lappalien« behelligt wird. Kriterium für die Frage, ob ein Risiko besteht, ist daher v. a. die Art der Daten (ist es besonders sensibel?) und ob die Daten vieler Personen von der Panne betroffen sind.

Daneben kann es sein, dass nicht nur die Aufsichtsbehörde, sondern auch die betroffene Person über eine Panne informiert werden muss. Dies aber nur dann, wenn ein hohes Risiko für deren Rechte und Freiheiten besteht. Auch hier gibt es aber Ausnahmen in Art. 34 DSGVO. Bei Museen dürfte eher nicht damit zu rechnen, dass dort derart sensible Datenverarbeitungen stattfinden.

Bußgeld und Haftung

Nach Art. 83 DSGVO kann die Datenschutzaufsichtsbehörde für genau festgelegte Verstöße Geldbußen verhängen. Während damit zumindest grundsätzlich die Gefahr besteht, dass v. a. Vereine für Verstöße gegen Datenschutzvorschriften mit Geldbußen belegt werden, sind öffentliche Stellen privilegiert. Soweit diese nicht am Wettbewerb teilnehmen – bei Museen dürfte das zumeist zu verneinen sein –, können gegen sie nach Art. 22 BayDSG keine Bußgelder verhängt werden.

Neben der Sanktion Bußgeld besteht nach Art. 82 DSGVO zudem die Möglichkeit, dass materielle oder immaterielle Schäden von Betroffenen durch den Verantwortlichen, der einen Datenschutzverstoß begangen hat, zu ersetzen sind.

Aufsichtsbehörde und Ansprechpartner

Die DSGVO sieht sogenannte Aufsichtsbehörden vor. Gemeint ist damit nicht eine Fachaufsicht – etwa das Wissenschaftsministerium als für Museumsfragen (teilweise) zuständiges Ressort –, sondern eine Datenschutzaufsicht. Die Aufgabe dieser Behörden ist es, die Verantwortlichen zu beraten, aber auch zu kontrollieren und bei Verstößen einzuschreiten, indem sie etwa eine Datenverarbeitung untersagen oder ein Bußgeld verhängen.

In Bayern gibt es seit jeher zwei Aufsichtsbehörden. Die Aufsichtsbehörde für öffentliche Stellen (und damit für die als solche organisierten Museen) ist der Bayerische Landesbeauftragte für den Datenschutz mit Sitz in München. Seine Geschäftsstelle ist im Internet erreichbar unter *www.datenschutz-bayern.de*. Für die nicht öffentlichen Stellen (also v. a. für Vereine) ist das Bayerische Landesamt für Datenschutzaufsicht mit Sitz in Ansbach zuständig. Das Landesamt ist im Internet erreichbar unter *www.lda.bayern.de*.

Literaturhinweise

- Text der DSGVO (einschließlich der Erwägungsgründe) und Text des BDSG abrufbar etwa unter *https://dsgvo-gesetz.de*
- Informationen zum BayDSG unter *www.gesetze-bayern.de*
- »Schritt für Schritt zum neuen Datenschutz. Hilfen für Vereine, kleine Unternehmen und Selbständige in Bayern«, zugänglich unter *www.dsgvo-verstehen-bayern.de*
- Der Bayerische Landesbeauftragte für den Datenschutz, Datenschutzreform 2018, abrufbar unter *www.datenschutz-bayern.de/datenschutzreform2018*
- Bayerisches Landesamt für Datenschutz, Handreichungen für kleine Unternehmen und Vereine, abrufbar unter *www.lda.bayern.de/de/kleine-unternehmen.html*
- Der Baden-Württembergische Landesbeauftragte für den Datenschutz, Datenschutz im Verein nach der Datenschutzgrundverordnung (DSGVO). Informationen über die datenschutzrechtlichen Rahmenbedingungen beim Umgang mit personenbezogenen Daten in der Vereinsarbeit, abrufbar unter *www.baden-wuerttemberg.datenschutz.de/datenschutz-im-verein*
- Bayerisches Landesamt für Datenschutz (Hrsg.): Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine. Das Sofortmaßnahmen-Paket, München 2017