Datenschutz in der Kommunalverwaltung

Recht – Technik – Organisation

Herausgegeben von

Dr. Martin Zilkens

Dr. Lutz Gollan

Bearbeitet von

Dr. Jens Ambrock
Christiane Bongartz
Andreas Drubba
Dr. Lutz Gollan
Leif-Erik Holtz
Katja Horlbeck
Dr. Cornelia Jäger
Eric Janzen
Victoria-Sophie Krull
Cornelia Löbhard-Mann
Thomas Müthlein
Michael Schaust
Anke Schröder
Thomas Schultz
Michael Smolle
Prof. Dr. Ulrike Verch
Jan Wittig
Dr. Martin Zilkens

6., völlig neu bearbeitete Auflage

ERICH SCHMIDT VERLAG

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar.

Weitere Informationen zu diesem Titel finden Sie im Internet unter
https://ESV.info/978-3-503-21270-5

Zitiervorschlag:
Zilkens/Gollan (Hrsg.), Datenschutz in der Kommunalverwaltung, 6. Auflage 2023

1. Auflage 1991
…
4. Auflage 2014
5. Auflage 2019
6. Auflage 2023

Die 1. Auflage erschien unter
„Lübking, Datenschutz in der Kommunalverwaltung"
Die 2. Auflage erschien unter
„Lübking/Zilkens, Datenschutz in der Kommunalverwaltung"
Die 3. und 4. Auflage erschienen unter
„Zilkens, Datenschutz in der Kommunalverwaltung"

ISBN 978-3-503-21270-5 (gedrucktes Werk)
ISBN 978-3-503-21271-2 (eBook)

Druck: Hubert & Co., Göttingen

XV. Datenschutz in kommunalen Bibliotheken

Ulrike Verch

Inhaltsübersicht

Verwendete Literatur: *Brehm/Knaf/Talke,* Datenschutz ab Inkrafttreten der Datenschutz-Grundverordnung – Handreichung für Bibliotheken. Technische Informationsbibliothek Hannover, 2018. *https://oa.tib.eu/renate/handle/123456789/3659* (abgerufen am 10. 10. 2022); *Gantert,* Bibliothekarisches Grundwissen, 9. Aufl., 2016; *Grages/Plath,* Black Box statt Big Brother: Datenschutzkonforme Videoüberwachung unter BDSG und DSGVO, CR 2017, 791 ff.; *Heldt,* Gesichtserkennung: Schlüssel oder Spitzel? Einsatz intelligenter Gesichtserfassungssystem im öffentlichen Raum, Zeitschrift für IT-Recht und Recht der Digitalisierung, 2019, 285 ff.; *Jochum,* Kleine Bibliotheksgeschichte, 3. Aufl., 2007; *Katzenberger/Talke*: Die Privatsphäre der Nutzer fördern: Das müssen Bibliotheken beim Datenschutz beachten. BuB (2015) 11, 684 ff.; *Lüdtke,* Spuren des „USA PATRIOT Act" in amerikanischen Bibliotheken. Vortrag, gehalten auf dem BID-Kongress, Leipzig, 20. 03. 2007. *https://opus4.kobv.de/opus4-bib-info/frontdoor/index/index/docId/334* (abgerufen am 10. 10. 2022); *Neuer,* Open Library: Mehr Bibliothek für die Bürger, Treffpunkt Kommune, 2020. *https://www.treffpunkt-kommune.de/open-library-mehr-bibliothek-fuer-die-buerger/* (abgerufen am 10. 10. 2022); *Nikolaizig,* Tatort, Täter und Motive – Buchdiebstahl in der Bibliothek. Fachzeitschrift für Archiv, Bibliothek und Dokumentation 2017/2. *https://arbido.ch/de/ausgaben-artikel/2017/tatorte/tatort-täter-und-motive-buchdiebstahl-in-der-bibliothek* (abgerufen am 10. 10. 2022); *Schwenke,* Zulässigkeit der Nutzung von Smartcams und biometrischen Daten nach der DS-GVO, NJW 2018, 823 ff.; *Veigel/Engelbrecht:* Videoüberwachung durch bayerische öffentliche Stellen: Erläuterungen zu Art. 24 Bayerisches Datenschutzgesetz. Der Bayerische Landesbeauftragte für den Datenschutz 2020 (hg.). *https://www.datenschutz-bayern.de/3/oh_video.pdf* (abgerufen am 10. 10. 2022).

1. Einleitung

Personenbezogene Daten werden in Bibliotheken seit jeher im großen Umfang 953
erhoben. Allein die Sammlung bibliografischer Daten, die im Rahmen der Katalogisierung verarbeitet und gespeichert wird, ist enorm. So enthält die kooperativ von Bibliotheken geführte Gemeinsame Normdatei (GND), in die die frühere deutsch-österreichische Personennormdatei (PND) vor wenigen Jahren aufgegangen ist, knapp sechs Millionen individualisierte Personendatensätze. Jede veröffentlichende Person erhält dort eine eindeutige Identifikationsnummer, zudem werden akademische Grade, Geburtsjahr, beruflicher Lebenslauf, Wir-

kungsort und Arbeitsstätte festgehalten. Die Daten sind frei im Netz einsehbar und stehen unter der freien Creative Commons Lizenz CC0 1.0 und können so beliebig genutzt werden, u. a. von kommunalen Bibliotheken zur Katalogisierung, um Autorinnen und Autoren eindeutig identifizieren und zuordnen zu können.[1] Schon die antike Bibliothek in Alexandria hat im berühmten Katalogverzeichnis der *Pinakes,* die der griechische Gelehrte *Kallimachos von Kyrene* im dritten Jahrhundert v. Chr. anfertigte, nicht nur Titeldaten, sondern jeweils auch kurze Lebensläufe der Verfasser auf den Schriftrollen festgehalten.[2]

954 Heutzutage verfügen die meisten Bibliotheken über sogenannte integrierte Bibliothekssysteme oder auch Bibliotheksmanagementsysteme. Dies sind Softwareprodukte, die verschiedene Arbeitsprozesse wie Erwerbung, Erschließung, Ausleihe und Recherche in einem System vereinen und damit sowohl Titel- als auch Nutzungsdaten speichern, verarbeiten und verknüpfen.[3] Im hinteren Buchdeckel angebrachte Buchkarten, auf denen neben den Leihfristen auch die Namen der Vorentleiher stehen, gehören der analogen Vergangenheit an, auch wenn die Buchkarten in kleineren Gemeindebüchereien und Schulbibliotheken ohne EDV-Verbuchung noch vorkommen mögen. In diesem Fall sollten die Namen der Entleiherinnen und Entleiher nach Rückgabe des Buches geschwärzt oder ganz auf die Buchkarten verzichtet werden, da die öffentliche Einsichtnahme in das Leseverhalten anderer Bibliotheksnutzerinnen und Bibliotheksnutzer mangels einer Rechtsgrundlage nicht zulässig ist.

955 Die Möglichkeit, anhand von Ausleihdaten Rückschlüsse auf die Leseinteressen der Bibliothekskunden zu ziehen, hat insbesondere in den *USA* nach den Terroranschlägen vom 11. 09. 2001 und dem Inkrafttreten des USA Patriot Acts[4] zu hitzigen Diskussionen geführt. Der USA Patriot Act erlaubt dem *Federal Bureau of Investigation* (*FBI),* im Rahmen von Ermittlungen Daten zur Internet- und Bibliotheksnutzung zu verwenden. Die Bibliotheken in den USA wurden verpflichtet, bei entsprechenden Durchsuchungsanordnungen die angeforderten Daten herauszugeben und Stillschweigen über diesen Vorgang zu wahren.[5] Dies führte neben massiven Protesten dazu, dass US-amerikanische Bibliotheken Nutzerdaten im großen Umfang löschten und Schilder mit der Inschrift aufstellten „*The FBI has not been here – watch very closely for removal of this sign*". Die *American Library Association,* die US-amerikanische Bibliotheksvereinigung, verabschiedete 2003 eine Resolution gegen die staatliche Überwachung von Bibliotheken, in der es u. a. heißt: „*Privacy is essential to the exercise of free speech, free thought, and free association; and, in a library, the subject of users' interests*

1 Mehr Informationen zur Gemeinsamen Normdatei finden sich u. a. auf der Website der *Deutschen Nationalbibliothek,* verfügbar unter *https://www.dnb.de/DE/Professionell/Standardisierung/GND/gnd_node.html*, abgerufen am 10. 10. 2022.

2 *Jochum,* Kleine Bibliotheksgeschichte, S. 29.

3 *Gantert,* Bibliothekarisches Grundwissen, S. 297.

4 Der genaue Titel des Gesetzes heißt: *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001,* 115 STAT. 272 PUBLIC LAW 107-56 v. 26. 10. 2001.

5 *Lüdtke,* Spuren des „USA PATRIOT Act" in amerikanischen Bibliotheken, S. 3 ff.

should not be examined or scrutinized by others".[6] Eine vergleichbare Stellungnahme oder Positionierung des *Deutschen Bibliotheksverbands* zum Schutz der Daten von Bibliotheksbesucherinnen und -besuchern ist nicht bekannt.

2. Forschungsdaten

Neben den klassischen Katalogdaten, personenbezogenen Kunden- und Nutzungsdaten verzeichnen seit wenigen Jahren auch *Forschungsdaten* in Bibliotheken eine wachsende Bedeutung. Im Rahmen der Open Science-Bewegung, die vom *Deutschen Bibliotheksverband* große Unterstützung erfährt,[7] werden von zahlreichen Bibliotheken digitale Datenrepositorien aufgebaut und verantwortet, in denen Wissenschaftlerinnen und Wissenschaftler ihre Forschungsdaten veröffentlichen und archivieren können.[8] Und obgleich viele Forschungsdaten keine datenschutzrechtliche Relevanz haben, wenn beispielsweise technische Labor- und Messwerte publiziert werden, können sie durchaus auch Personenbezug aufweisen. Gerade in der medizinischen und sozialwissenschaftlichen Forschung betreffen die erhobenen Daten oftmals auch Persönlichkeitsrechte oder können sensible Informationen beinhalten.[9] Darüber hinaus betreiben einzelne Bibliotheken Forschungsinformationssysteme, die zum Teil einen sehr genauen Einblick in die Forschungsinteressen und Forschungsstärke einzelner Wissenschaftler und Wissenschaftlerinnen ermöglichen. 956

In diesem Zusammenhang führte 2021 ein 13-seitiges Informationspapier der *Deutschen Forschungsgemeinschaft* (DFG) mit dem Titel „Datentracking in der Wissenschaft: Aggregation und Verwendung bzw. Verkauf von Nutzungsdaten durch Wissenschaftsverlage" zu kontroversen Diskussionen. Hierin wird beschrieben, wie große Wissenschaftsverlage personenbezogene Daten im großen Umfang sammeln, aggregieren, auswerten und daraus personalisierte Profile erstellen und an Dritte weiter verkaufen, indem sie u. a. das genaue Nutzungsverhalten auf ihren Online-Plattformen und Datenbanken meist ohne Wissen 957

6 Eigene Übersetzung: „Der Schutz der Privatheit ist essentiell für die Ausübung der Meinungs-, Gedanken- und Vereinigungsfreiheit; und in einer Bibliothek sollten die Interessen der Benutzer nicht von anderen untersucht oder hinterfragt werden", siehe *Resolution on the USA PATRIOT Act and related measures that infringe on the rights of library users* der American Library Association von 2003, verfügbar unter *https://www.ala.org/ala/washoff/WOissues/civilliberties/theusapatriotact/alaresolution.htm*, abgerufen am 10. 10. 2022.

7 Verfügbar unter *https://www.bibliotheksverband.de/wissenschaft-und-bibliotheken*, abgerufen am 10. 10. 2022.

8 Ein Beispiel für eine bibliothekarisches Datenrepositorium bietet die *Hochschule der Technischen Universität Hamburg* mit der Datenbank TORE, verfügbar unter *https://tore.tuhh.de/handle/11420/2023*, abgerufen am 10. 10. 2022.

9 Ein Beispiel hierzu ist das durch das *BMBF* geförderte Projekt Gruß & Kuss, bei dem als Forschungsdaten Liebesbriefe von Bürgerinnen und Bürger erschlossen und archiviert werden, verfügbar unter *https://liebesbriefarchiv.de/liebesbriefarchiv/archivierung-liebesbriefe*, abgerufen am 10. 10. 2022.

der betroffenen Personen nachverfolgen und speichern.[10] Auch wenn das Wissenschaftstracking überwiegend Bibliotheken in einem Forschungsumfeld betrifft, so bieten auch zahlreiche Stadtbibliotheken Zugang zu wissenschaftlichen Verlagsdatenbanken, sodass deren Gäste damit ebenfalls Gefahr laufen, dass ihr Nutzungsverhalten ausspioniert werden könnte. Insbesondere die digitalen Angebote und das Verhalten des Verlags *Elsevier* haben diesbezüglich Kritik auf sich gezogen.[11]

Da die Erhebung von Forschungsdaten aber überwiegend die Bibliotheken von Hochschulen und Forschungseinrichtungen betrifft und im kommunalen Bereich nur wenige Bibliotheken wissenschaftlich ausgerichtet sind,[12] werden die Themen Open Data und Datentracking durch Wissenschaftsverlage hier nicht näher beleuchtet,[13] auch wenn Datenpublikationen u. a durch Kooperationen mit sog. Citizen-Science-Projekten schon vereinzelt den Weg in die kommunalen öffentlichen Bibliotheken finden.[14]

3. Rechtsgrundlagen der Datenverarbeitung

958 Neben den einschlägigen Vorschriften der DSGVO verfügen einzelne, aber nicht alle Bundesländer über spezielle bibliotheksgesetzliche Normen, die zum Teil bereichsspezifische Datenschutzregelungen umfassen. So heißt es beispielsweise in § 8 Abs. 1 Satz 1 des Gesetzes für Bibliotheken in *Schleswig-Holstein*[15] sowie in § 8 Abs. 1 Satz 1 des Landesbibliotheksgesetzes in *Rheinland-Pfalz*[16] wortgleich: „Bibliotheken dürfen zur Erschließung und Verzeichnung ihrer Bestände personenbezogene Daten verarbeiten und über öffentliche Netze zur

10 Aggregation und Verwendung bzw. Verkauf von Nutzungsdaten durch Wissenschaftsverlage: Ein Informationspapier des *Ausschusses für Wissenschaftliche Bibliotheken und Informationssysteme der Deutschen Forschungsgemeinschaft* (DFG) v. 28. 10. 2021, verfügbar unter *https://www.dfg.de/download/pdf/foerderung/programme/lis/datentracking_papier_de.pdf*, abgerufen am 10. 10. 2022.

11 So wird im *DFG*-Papier insbesondere das kommerzielle Forschungsinformationssystem PURE genannt, das vom Verlag *Elsevier* betrieben wird, verfügbar unter *https://www.elsevier.com/de-de/solutions/pure*, abgerufen am 10. 10. 2022.

12 Beispielsweise die Bibliotheken der Städte *Mainz* und *Trier*.

13 Weiterführende Informationen zum Thema Datenschutz von Forschungsdaten bietet die Informationsplattform *forschungsdaten.info*, verfügbar unter *https://forschungsdaten.info/themen/rechte-und-pflichten/datenschutzrecht*, abgerufen am 10. 10. 2022.

14 So hat zum Beispiel aktuell die *Stadtbibliothek Charlottenburg-Wilmersdorf* in Berlin ein Pilotprojekt für Bürgerwissenschaften eingerichtet, u. a. sollen Messgeräte angeschafft und ausgeliehen werden, mit denen die Gäste der Bibliothek Umweltdaten in ihrem Stadtteil sammeln können, verfügbar unter *https://www.wir-bieten-vielfalt-einen-ort.de/2021/10/12/pilotprojekt-citizen-science-interview-mit-dr-konstantin-kaminskij/*, abgerufen am 10. 10. 2022.

15 Gesetz für die Bibliotheken in Schleswig-Holstein (Bibliotheksgesetz – BiblG) v. 30. 08. 2016 (GVOBl. 2016, S. 791), zuletzt geändert am 13. 12. 2019.

16 Landesbibliotheksgesetz Rheinland-Pfalz v. 03. 12. 2014 (GVOBl. 2014, S. 245).

Verfügung stellen."[17] Im Kulturgesetzbuch *Nordrhein-Westfalen* wird bereichsspezifisch hervorgehoben, dass die Aufgaben, die den Kultureinrichtungen des Landes obliegen, Aufgaben des öffentlichen Interesses im Sinne von § 3 Abs. 1 DSG NRW darstellen.[18] Damit ist die Erhebung personenbezogener Daten durch kommunale Bibliotheken zulässig, sofern diese zur Erfüllung ihrer Aufgaben erforderlich ist. Obgleich in anderen Bundesländern vergleichbare bereichsspezifische Regelungen fehlen, erlauben entsprechende Generalklauseln in den Landesdatenschutzgesetzen ebenfalls eine Datenerhebung durch öffentliche Stellen, sofern diese zur Wahrnehmung im öffentlichen Interesse liegender Aufgaben notwendig ist.[19] Dies entspricht der europaweiten Regelung der DSGVO nach Art. 6 Abs. 1 Satz 1 lit. e) DSGVO.

Darüber hinaus enthalten zahlreiche *Bibliotheksbenutzungsordnungen* detail- 959
lierte Angaben, welche Daten zu welchen Zwecken erhoben werden. Die *Stadtbibliothek Stuttgart* führt in ihrer Satzung aus, dass als personenbezogene Daten der Familienname, die Vornamen, das Geburtsdatum, das Geschlecht, die Anschrift und bei Minderjährigen auch die Anschrift des/der Sorgeberechtigten sowie Daten zu den ausgeliehenen Medien und Geräten erhoben werden.[20] In der *Stadtbibliothek Freiburg im Breisgau* werden darüber hinaus bei der digitalen Selbstregistrierung noch die E-Mail-Adresse sowie die Bankverbindung der Benutzerinnen und Benutzer gespeichert.[21] In den *Stadtbüchereien Düsseldorf* sind die Datenschutzbestimmungen in der Benutzungsordnung noch ausführlicher und umfassen auch Angaben zu Medienausleihen, Löschfristen, RFID-Verbuchung und statischer Auswertung.[22] Im Gegensatz zu diesen Beispielen gibt es andere Bibliotheksordnungen, die gar keine Angaben zum Datenschutz enthalten, so etwa bei der *Stadtbücherei Regensburg*[23] oder bei der Stadtbibliothek *Nürnberg,* die stattdessen eine ausführliche Datenschutzerklärung ins Netz ge-

17 In den Bibliotheksgesetzen der Bundesländer *Hessen, Thüringen* und *Sachsen-Anhalt* findet der Datenschutz hingegen keine Erwähnung.

18 Datenschutzgesetz Nordrhein-Westfalen v. 17. 05. 2018 (GV NRW, S. 244), zuletzt geändert am 01. 10. 2022.

19 Beispielsweise § 3 des Niedersächsischen Datenschutzgesetzes v. 16. 05. 2018 (GVBl. S. 66) oder § 16 Abs. 1 des Thüringer Datenschutzgesetzes v. 15. 06. 2018 (GVBl. 2018, S. 229).

20 Siehe § 4 der Benutzungsordnung für die Stadtbibliothek der *Landeshauptstadt Stuttgart,* verfügbar unter *https://stadtbibliothek-stuttgart.de/content/download/Benutzungs-Gebuehrenordnung-Stadtbibliothek-Stuttgart.pdf*, abgerufen am 29. 10. 2022. Hier stellt sich die Frage, wozu die Angabe des Geschlechts erforderlich ist.

21 Siehe § 4 der Satzung über die Benutzung der *Stadtbibliothek Freiburg i. Br.,* verfügbar unter *https://www.stadtbibliothek.freiburg.de/geschaeftsbedingungen,* abgerufen am 29. 10. 2022.

22 Siehe § 4 der Nutzungs- und Entgeltordnung der *Stadtbibliothek Bremen,* verfügbar unter *https://stabi-hb.de/sites/default/files/2017-12/Nutzungs_und_Entgeltordnung.pdf*, abgerufen am 29. 10. 2022.

23 Siehe Benutzungsordnung und Entgeltregelung für die *Stadtbücherei Regensburg,* verfügbar unter *https://www.regensburg.de/sixcms/media.php/464/Benutzungsordnung_Deutsch_2015_Logo.pdf*, abgerufen am 29. 10. 2022.

stellt hat.[24] Andere Einrichtungen wiederum nutzen Einverständnisformulare, mit denen sie sich wie in der *Stadtbibliothek Ludwigshafen* bei der Neuanmeldung die Einwilligung in die Datenverarbeitung durch eine persönliche Unterschrift bestätigen lassen.[25] Aus rechtsdogmatischer Sicht ist eine solche Unterschrift indes nicht geboten und eine Einwilligung nur dann erforderlich, wenn weitere als die für die Bibliotheksnutzung erforderlichen Daten verarbeitet werden sollen. Die Nutzung der Einrichtung als solche darf bei öffentlichen Bibliotheken nicht von einer Einwilligung abhängig gemacht werden.[26] Eine aktuelle und umfassende Datenschutzerklärung der Bibliothek, die den Neukunden bei der Anmeldung ausgehändigt sowie auf der Website hinterlegt wird, ist jedoch nach Art. 13 DSGVO unerlässlich.

a) Verantwortung für die Datenverarbeitung

960 Wer in kommunalen Bibliotheken die Verantwortung für die Datenverarbeitung trägt, bestimmt sich nach Art. 4 Nr. 7 DSGVO. Danach ist die natürliche oder juristische Person verantwortlich, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Im Einzelfall hängt dies von der Organisations- und Rechtsform der jeweiligen Einrichtung ab. Die meisten kommunalen Bibliotheken sind unselbstständige Anstalten des öffentlichen Rechts,[27] denen als organisatorisch verselbstständigte Verwaltungseinheiten grundsätzlich Entscheidungshoheit über die Art und Weise der Datenverarbeitung zukommt, sodass sie als Verantwortliche für die Datenverarbeitung einzustufen sind.[28] Die Einhaltung datenschutzrechtlicher Regelungen ist durch die Bibliotheksleitung sicherzustellen.[29]

961 Sie muss auch der Pflicht nachkommen, einen behördlichen Datenschutzbeauftragten zu bestellen und nach Art. 37 Abs. 7 DSGVO dessen Kontaktdaten veröffentlichen sowie die Aufsichtsbehörde entsprechend zu informieren. Der Daten-

24 Siehe Benutzungs- und Gebührensatzung der *Stadtbibliothek Nürnberg,* verfügbar unter *https://www.nuernberg.de/imperia/md/stadtbibliothek/dokumente/satzungen/benutzungs_und_gebuehrensatzung_2022.pdf*, abgerufen am 29. 10. 2022.

25 Verfügbar unter *https://www.ludwigshafen.de/fileadmin/Websites/Stadt_Ludwigshafen/Veranstaltungen/Stadtbibliothek/Benutzungsordnungen/Einwilligung_zur_Datenverarbeitung_Zur_Abgabe_in_der_Bibliothek.pdf*, abgerufen am 29. 10. 2022.

26 Wenn die Bibliothek privatrechtlich organisiert ist, bedarf es eines Nutzungsvertrags mit den betroffenen Personen, der nach Art. 6 Abs. 1 Satz 1 lit. b) DSGVO Zulässigkeitsgrundlage für die Datenverarbeitung ist.

27 Siehe die Hinweise im Bibliotheksportal des *Kompetenznetzwerks für Bibliotheken (knb),* verfügbar unter *https://bibliotheksportal.de/ressourcen/recht/bibliotheksrecht-allgemein/*, abgerufen am 29. 10. 2022.

28 *EDSA,* Leitlinien 07/2020 zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO, Version 2.0, Stand Juli 2021, S. 11 ff., verfügbar unter *https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_de.pdf*, abgerufen am 29. 10. 2022.

29 *BfDI,* Die Datenschutzbeauftragten in Behörden und Betrieben, S. 17, Stand Dez. 2020, verfügbar unter *https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Broschueren/INFO4.pdf?__blob=publicationFile&v=12*, abgerufen am 29. 10. 2022.

schutzbeauftragte kann entweder aus dem Bibliothekspersonal stammen oder es wird eine externe Person benannt. Es ist nicht zwingend erforderlich, dass der Datenschutzbeauftragte selbst im öffentlichen Dienst tätig ist, auch private Personen mit entsprechender Fachexpertise können mit dieser Aufgabe vertraglich betraut werden.[30] Art. 37 Abs. 2 DSGVO räumt zudem die Möglichkeit ein, dass ein Datenschutzbeauftragter für mehrere Bereiche und Behörden zuständig ist. Sollte die Bibliothek privatrechtlich organisiert sein, wie beispielsweise die *Bücherhalle Hamburg* als Stiftung privaten Rechts[31] oder die *Stadtbibliothek Gütersloh* als GmbH,[32] gelten sie als nichtöffentliche Stellen und bestellen dementsprechend einen betrieblichen, nicht einen behördlichen Datenschutzbeauftragten. Diese begriffliche Unterscheidung hat jedoch inhaltlich keine Relevanz, abgesehen von der nur für öffentliche Einrichtungen stets zwingenden Bestellungspflicht. Privatrechtlich organisierte Bibliotheken müssen nach § 38 Abs. 1 Satz 1 BDSG dann zwingend einen Datenschutzbeauftragten benennen, wenn sie in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.[33]

Im Gegensatz zu den Bibliotheken, die unselbstständige Anstalten des öffentlichen Rechts sind, verfügen privatrechtlich organisierten Einrichtungen über eine Rechtspersönlichkeit und können deshalb Verträge im eigenen Namen schließen. Dies ist im Bereich des Datenschutzes insbesondere für die *Auftragsverarbeitung* relevant, da Bibliotheken ihre Daten oftmals nicht auf eigenen Servern speichern, sondern dazu externe Dienstleister wie zum Beispiel OCLC[34] nutzen.[35] In diesem Fall, wenn die personenbezogenen Daten nicht mehr unmittelbar und ständig dem Hoheitsbereich der verantwortlichen Stelle unterliegen, ist es notwendig, einen Vertrag zur Auftragsverarbeitung nach Art. 28 Abs. 3 DSGVO zu schließen, damit die Datenverarbeitung auch weiterhin durch die Bibliotheksleitung gesteuert und kontrolliert werden kann; die Entscheidungs- und Weisungsbefugnis über die Datenverarbeitung verbleibt stets bei der verantwortlichen Stelle.[36] 962

30 *BfDI,* Die Datenschutzbeauftragten in Behörden und Betrieben, S. 13, Stand Dez. 2020, verfügbar unter *https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Broschueren/INFO4.pdf?__blob=publicationFile&v=12*, abgerufen am 29. 10. 2022.

31 Siehe *https://www.buecherhallen.de/ueber-uns.html*, abgerufen am 29. 10. 2022.

32 Siehe *https://www.stadtbibliothek-guetersloh.de/impressum/*, abgerufen am 29. 10. 2022.

33 Zudem ist die Bestellung nach Art. 37 Abs. 1 lit c) DSGVO als zwingend erforderlich anzusehen, wenn die privaten Bibliotheken in großem Umfang besondere Kategorien von personenbezogenen Daten nach Art. 9 DSGVO verarbeiten.

34 OCLC = *Online Computer Library Center,* eine auch in Deutschland tätige Non-Profit-Organisation nach US-amerikanischen Recht, die insbesondere wegen dem WorldCat, der weltweit größten bibliographischen Datenbank, bekannt ist.

35 *Katzenberger/Talke,* BuB 2015, 686.

36 *EDSA,* Leitlinien 07/2020 zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO, Version 2.0, Stand Juli 2021, S. 4, verfügbar unter *https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_de.pdf*, abgerufen am 29. 10. 2022.

Bei öffentlichen Bibliotheken *ohne eigene Rechtspersönlichkeit* werden die Auftragsverarbeitungsverträge in der Regel im Namen des Bibliotheksträgers und damit im Namen der kommunalen Gebietskörperschaft geschlossen. Auf dem Wege der Delegation ist es jedoch möglich, dass die Bibliotheksleitungen ebenfalls befugt sind, entsprechend vertragsrechtlich zu handeln.

b) Arten der Datenverarbeitungen und Datenkategorien

963 Neben der Speicherung von Beschäftigtendaten und der Nutzung von bibliografischen Daten im Rahmen der Katalogisierung werden in kommunalen Bibliotheken insbesondere die Daten von Leserinnen und Lesern verarbeitet, die auf die Dienstleistungen der Einrichtung zurückgreifen. Zunächst werden bei der Anmeldung zur Bibliotheksnutzung die *Stammdaten* der Nutzerinnen und Nutzer erhoben, in der Regel Vorname, Nachname, Geburtsdatum, Anschrift, Anmeldedatum. Auch E-Mail-Adressen, Telefonnummern, Bankverbindungen und Geschlecht werden vielfach gespeichert sowie persönliche PIN-Nummern bzw. Geheimnummern, um an der Selbstverbuchung teilnehmen zu können. Grundsätzlich sollten nur Angaben erfasst werden, die für das Benutzungsverhältnis notwendig sind. Informationen zum Geschlecht zählen nicht dazu. Telefonnummern und E-Mail-Adressen sollten allenfalls aufgrund einer Einwilligung für die zusätzlichen Service-Dienste der Bibliothek, wie zum Beispiel die Kunden über das Eintreffen von vorgemerkten Medien schnell informieren zu können, angegeben werden müssen. Für die allgemeine Bibliotheksbenutzung selbst sind sie nicht erforderlich, allenfalls für Online-Dienste. Im Sinne der Datensparsamkeit sollte sich die Bibliothek grundsätzlich auf einen Kommunikationsweg beschränken.

964 Die Stammdaten werden in den meisten Einrichtungen im integrierten Bibliothekssystem erfasst, über das auch Ausleihen, Verlängerungen, Vormerkungen und Säumnisgebühren bei Leihfristüberschreitungen verwaltet werden. Auf dem Bibliotheksausweis sollten aus Sicherheitsgründen, falls dieser verloren geht, so wenig Angaben wie möglich gespeichert werden. Dabei ist zwischen den sichtbaren und den nur elektronisch auslesbaren Daten zu unterscheiden, die auf einem Chip gespeichert sind. Während auf dem Kartenaufdruck meistens die Kundennamen als Klarnamen genannt werden, reicht im digitalen Format die pseudonymisierte Karteneigentümer-ID neben der Kartenseriennummer und dem Gültigkeitszeitraum aus.

965 Während die Stammdaten der Leserinnen und Leser in keine besondere Datenkategorie fallen, ist es fraglich, ob die erhobenen Daten zu den ausgeliehenen Medien *(Nutzungsdaten)* gegebenenfalls als sensibel im Sinne von Art. 9 Abs. 1 DSGVO anzusehen sind. Daten zum Leseverhalten von Bibliothekskunden und -kundinnen können insofern sensibel sein, als dass aus ihnen politische Meinungen, religiöse oder weltanschauliche Überzeugungen hervorgehen könnten. Wenn sich jemand beispielsweise ausschließlich Medien zu bestimmten Themengebieten wie der aktuellen LGBT-Bewegung oder über den Islam ausleiht, lassen sich gegebenenfalls Rückschlüsse auf religiöse Einstellungen, sexuelle

Ausrichtung oder politische Interessen ziehen. Auch Ausleihdaten zu Gesundheitsratgebern sollten strengen Anforderungen unterliegen.

Dies würde bedeuten, dass bei der Verarbeitung der Nutzungsdaten besonders strikte datenschutzrechtliche Maßstäbe anzulegen sind. Nach Art. 35 DSGVO müssten die Bibliotheken in diesem Fall für die Ausleihe sensibler Medien eine *Datenschutz-Folgenabschätzung* vornehmen und sich als Rechtsgrundlage für die Datenverarbeitung nach Art. 9 Abs. 2 lit. g) DSGVO auf ein erhebliches öffentliches Interesse berufen können, das gesetzlich so verankert ist, dass der Wesensgehalt des Rechts auf Datenschutz gewahrt wird. Hier wäre zur Rechtsklarheit und zur Sicherheit für die Bibliotheken jeweils eine landesgesetzliche Regelung sinnvoll und wünschenswert, die auch angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen bestimmt.[37] Ansonsten wäre die Verbuchung sensibler Medien zu Einzelpersonen nach Art. 9 Abs. 2 lit. a) DSGVO nur mit ausdrücklicher Einwilligung der Leserinnen und Leser zulässig.

In *US-amerikanischen Bibliotheken* wird angesichts neuer gesetzlicher Regelungen in einzelnen Bundesstaaten kontrovers diskutiert, ob und wie Medien mit Informationen zu Schwangerschaftsabbrüchen aufgrund der im Jahr 2022 in vielen US-Staaten verschärften Rechtslage zu Abtreibungen noch ausgeliehen oder im Bibliothekskatalog angezeigt werden sollten.[38] Auch deutsche kommunale Einrichtungen dürfen nicht unterschätzen, wie sensibel die Daten zum Leseverhalten ihrer Kunden sein können und sollten daher bei der Verarbeitung besonders hohe Datenschutzanforderungen gewährleisten, insbesondere durch Pseudonymisierung, eine sichere Verschlüsselung, eine möglichst kurze Speicherdauer, regelmäßigen Löschroutinen, eine strenge Zugangskontrolle und eine Datenschutz-Folgenabschätzung.[39]

4. Betroffenenrechte

Als Bibliotheken noch Zettelkataloge nutzten, war die Recherche nach bibliografischen Daten mühselig und zeitaufwendig. Heutzutage sind die Bestände der kommunalen Bibliotheken über die Online-Kataloge weltweit nur mit wenigen Mausklicks digital durchsuchbar. Damit kommen Bibliotheken ihrer Kernaufgabe nach, Informationen nicht nur zu bewahren, sondern auch öffent- 966

37 Für diese Gesetzesanpassung würden sich insbesondere die Bibliotheksgesetze der Länder anbieten.

38 Vgl. *American Library Assocation,* American Library Assocation Condemns Proposed State Legislation Limiting Access to Information on Reproductive Health, verfügbar unter *https://www.ala.org/news/press-releases/2022/08/american-library-association-ala-condemns-proposed-state-legislation-limiting*, abgerufen am 19. 10. 2022.

39 Mehr Informationen zu Datenschutz-Folgenabschätzungen in Bibliotheken siehe: *Brehm/Knaf/Talke,* Datenschutz ab Inkrafttreten der Datenschutz-Grundverordnung, S. 9 ff.

lich zugänglich zu machen.[40] Doch nicht alle Autorinnen und Autoren möchten auf unbefristete Zeit mit ihren Werken in Verbindung gebracht werden, zumal wenn der Eintrag im Bibliothekskatalog nicht nur die reinen Titeldaten enthält, sondern um weitere Informationen wie Klappentexte, Abstracts, Inhaltsverzeichnisse oder Volltexte angereichert wurde.[41] Hier sind die Betroffenenrechten von Bedeutung. Sind Bibliotheken in diesem Fall ähnlich wie Suchmaschinen dazu verpflichtet, personenbezogenen Informationen aus ihren Indizes zu löschen, wenn betroffene Personen dies verlangen?

967 Art. 17 Abs. 2 DSGVO umfasst neben dem Anspruch auf Datenlöschung noch die zusätzliche Verpflichtung des Verantwortlichen, weiterführende digitale Spuren der Veröffentlichung zu tilgen, um so ein Recht auf Vergessenwerden zu gewährleisten. Ein Anspruch der betroffenen Person, der die Bibliotheken zwingt, Bücher komplett aus dem Bestand zu nehmen, lässt sich aus dieser Norm nicht ableiten,[42] aber möglicherweise ein Anspruch auf Löschung der persönlichen Daten in den Bibliothekskatalogen, insbesondere wenn diese einen Online-Zugriff über das Internet erlauben.

Ein Anspruch der *Buchautorinnen und -autoren* auf Datenlöschung nach Art. 17 Abs. 1 DSGVO setzt im Regelfall jedoch voraus, dass entweder die Rechtsgrundlage oder die Notwendigkeit zur Verarbeitung wegen Zweckerreichung entfallen ist. Bei bibliografischen Daten zum Bibliotheksbestand ist dieser Fall jedoch nur schwer vorstellbar, insbesondere da Art. 17 Abs. 3 DSGVO zahlreiche Ausnahmen von der Löschpflicht benennt, die für Bibliotheken relevant und einschlägig sind, namentlich die Datenverarbeitung zur Ausübung des Rechts auf freie Information und Meinungsäußerung, zur Wahrnehmung einer Aufgabe im öffentlichen Interesse, zur Erfüllung einer rechtlichen Verpflichtung, für öffentliche Archivzwecke, für historische oder wissenschaftliche Forschungszwecke. Wenn Löschansprüche geltend gemacht werden, verlangt der *Bundesgerichtshof* in jedem Einzelfall eine umfassende Grundrechtsabwägung auf der Grundlage aller relevanten Umstände und unter Berücksichtigung der Schwere des Eingriffs sowohl in die Grundrechte der betroffenen Person als auch der datenpublizierenden Einrichtungen als auch der Interessen von Nutzern und der Öffentlichkeit.[43] In einer Stellungnahme zum Recht auf Vergessenwerden fordert die *International Federation of Library Associations and Institutions* u. a., dass For-

40 Im Ethikkodex der *IFLA,* der *International Federation of Library Associations and Institutions,* wird der Zugang zu Informationen als erste Kernaufgabe von Bibliotheken genannt, siehe *IFLA,* Ethik-Kodex für Bibliotheks- und andere Informationsfachleute, verfügbar unter *https://www.ifla.org/de/publications/ifla-ethik-kodex-fur-bibliotheks-und-andere-informationsfachleute-kurzfassung/*, abgerufen am 19. 10. 2022.

41 Siehe beispielsweise *Bibliotheksverbund Bayern,* verfügbar unter *https://www.bib-bvb.de/web/b3kat/kataloganreicherun*, abgerufen am 19. 10. 2022.

42 Bei Werken, die über das Pflichtexemplarrecht den Weg in die Bibliothek gefunden haben und somit dauerhaft archiviert werden müssen, wäre eine Aussonderung in keinem Fall erlaubt.

43 *BGH,* Urt. v. 27. 07. 2020, Az. VI ZR 405/18, ECLI:DE:BGH:2020:270720UVIZR405.18.0.

schende Zugang zu personenbezogenen Informationen zu biografischen, genealogischen und anderen Forschungsvorhaben erhalten, dass keine Personen des öffentlichen Lebens aus Trefferlisten entfernt werden und dass Personennamen dauerhaft indexiert werden, um die Verfügbarkeit von Inhalten für historische und andere wissenschaftliche Zwecke sicherzustellen.[44]

968 Während sich Bibliotheken in Hinblick auf die Zugänglichkeit und Archivierung bibliografischer Daten auf Art. 5 Grundgesetz stützen können, ist die Rechtslage in Bezug auf die Daten der *Bibliotheksnutzer* eine andere. Nach den Grundsätzen der Datenminimierung und Datenvermeidung müssen diese so schnell wie möglich gelöscht werden, sobald es keinen Grund mehr gibt, sie vorzuhalten. Deshalb sollten die Ausleihdaten direkt und unverzüglich nach der Buchrückgabe gelöscht werden, sofern das Medium nicht beschädigt wurde oder Säumnisgebühren entstanden sind. Davon unbenommen kann ein anonymisierter Datensatz für die Ausleihstatistik eine längerfristige Verarbeitung und Speicherung haben. Die Stammdaten der Kunden sollten ebenfalls unverzüglich nach Beendigung des Benutzungsverhältnisses gelöscht werden, sofern keine offenen Forderungen mehr bestehen. Einrichtungen, die für die Bibliotheksbenutzung Jahresgebühren erheben, lassen zuweilen das Nutzungsverhältnis für längere Zeit „ruhen", um es mit der Zahlung der neuen Gebühr wieder aufleben zu lassen, und vermeiden auf diese Weise die Ausstellung eines neuen Ausweises. So schreibt die *Stadtbibliothek Essen* beispielsweise auf ihrer Website: „Mit diesem Bibliotheksausweis können Sie 12 Monate lang in allen Einrichtungen der Stadtbibliothek alle Medien kostenlos entleihen. Danach können Sie den Ausweis verlängern oder ruhen lassen, eine Kündigung ist nicht nötig."[45] Das heißt, wenn die Bibliothekskunden den Ausweis nicht verlängern oder aktiv kündigen, werden die Daten auf unbestimmte Zeit gespeichert.[46] Bei der *Stadtbibliothek Nürnberg* werden die Stammdaten nach 36 Monaten ohne aktiven Ausleihvorgang gelöscht, sofern keine offenen Forderungen bestehen.[47]

969 Es erscheint fraglich, wie lange die Speicherung der Stammdaten bei Nichtnutzung gerechtfertigt ist. Im Sinne der Datenminimierung nach Art. 5 Abs. 1 lit. c) DSGVO wäre eine deutlich kürzere Löschfrist angemessen, zumal eine Neuregistrierung für die Bibliothekskunden jederzeit möglich ist. Noch vor Inkrafttreten der DSGVO hielt der *Berliner Beauftragte für Datenschutz und Informationsfreiheit* im Jahr 2006 eine Speicherfrist von zwei Jahren für inaktive Bibliothekskonten für verhältnismäßig, um einerseits das Recht auf informationelle Selbstbestim-

44 *IFLA,* Stellungnahme zum Recht auf Vergessenwerden vom 25. 02. 2016, verfügbar unter *https://www.ifla.org/wp-content/uploads/2019/05/assets/clm/statements/rtbf-full-statement-de.pdf*, abgerufen am 19. 10. 2022.

45 Informationen zur Ausleihe der *Stadtbibliothek Essen,* verfügbar unter *https://www.stadtbibliothek-essen.de/ausleihe_2/ausleihe.de.html*, abgerufen am 19. 10. 2022.

46 Eine genaue Speicherfrist wird in der Datenschutzerklärung der Stadtbibliothek nicht angegeben.

47 Datenschutzhinweise zur Anmeldung der *Stadtbibliothek im Bildungscampus Nürnberg,* verfügbar unter *https://www.nuernberg.de/internet/stadtbibliothek/datenschutz_anmeldung.html*, abgerufen am 19. 10. 2022.

mung zu wahren und andererseits den Wiedereinstieg in die Bibliotheksnutzung zu erleichtern.[48] In jedem Fall sollten die genauen Lösch- und Speicherfristen den Leserinnen und Lesern in den Datenschutzerklärungen der kommunalen Bibliotheken verständlich bekannt gegeben werden, um größtmögliche Transparenz zu gewährleisten.

5. Beispiele aus der Praxis

a) RFID-Verbuchung

970 Die Abkürzung RFID steht für „Radio Frequency Identification" und bedeutet Identifizierung über Funkwellen. Die Technik kommt in sehr vielen kommunalen Bibliotheken zum Einsatz, insbesondere bei der Ausleihverbuchung, Mediensortierung und als Maßnahme zur Diebstahlsicherung.[49] Dabei wird in jedem Medium ein Transponder („Tag") angebracht, der das Objekt eindeutig identifiziert, und von einem Lesegerät, das hochfrequente Radiowellen erzeugt, ausgelesen werden kann. Mittels dieser kontaktlosen Funktechnologie kann anders als die herkömmliche Verbuchung mittels Barcodescanner die stapelweise Verbuchung von Medien erfolgen, womit Bibliotheken und auch ihre Gäste, wenn sie die RFID-Selbstausleihe nutzen, sehr viel Zeit einsparen. Während in der Logistikbranche auch Transponder mit eigenen Sendern ausgestattet werden, die selbstständig funken können, sog. aktive Tags, beschränken sich Bibliotheken in der Regel auf die passiven Tags, die mit maximal 45 cm eine vergleichsweise geringe Funkreichweite aufweisen.[50]

Aus Sicht des Datenschutzes birgt die Technologie diverse Gefahren für das Recht auf informationelle Selbstbestimmung, u. a. durch das unbemerkte Ausspionieren, die Erstellung von Bewegungsprofilen oder die Verknüpfung mit Hintergrunddatenbanken, wobei den betroffenen Personen oftmals gar nicht bewusst ist, dass sie Gegenstände mit sich tragen, die Daten preisgeben können, da die Tags in vielen Fällen nahezu unsichtbar sind.[51] Umso wichtiger ist es deshalb, den Einsatz der RFID-Technologie so zu gestalten, dass zum einen möglichst wenig personenbezogene Daten erhoben werden und zum anderen ein hoher Sicherheitsstandard gewährleistet wird.

48 *BlnBDI,* Tätigkeitsbericht 2006, S. 152, verfügbar unter *https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/jahresbericht/BlnBDI-Jahresbericht-2006-Web.pdf*, abgerufen am 06. 11. 2022.

49 So haben beispielsweise im Jahr 2015 die *Öffentlichen Bibliotheken in Berlin* an allen 75 Standorten die RFID-Verbuchung eingeführt, weitere Informationen verfügbar unter *https://bibliotheksportal.de/ressourcen/digitale-services/rfid-fuer-berlins-oeffentliche-bibliotheken/*, abgerufen am 29. 10. 2022.

50 Weiterführende Informationen zum RFID-Einsatz in Bibliotheken sind auf dem *Bibliotheksportal*, dem Informationsportal des *Kompetenznetzwerks für Bibliotheken (knb)* erhältlich, verfügbar unter *https://bibliotheksportal.de/ressourcen/digitale-services/rfid/*, abgerufen am 29. 10. 2022.

51 *BfDI,* RFID – Funkchips für jede Gelegenheit?, S. 5 und S. 12, Stand August 2020, verfügbar unter *https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Flyer/RFIDFunkchipsFuerJedeGelegenheit.pdf?__blob=publicationFile&v=5*, abgerufen am 29. 10. 2022.

Konkret sind folgende *technische* und organisatorische *Maßnahmen* i. S. d. Art 32 DSGVO zu empfehlen: 971

- Verschlüsselung der Daten,
- wirksame Authentisierung der Lesegeräte,
- keine bibliografischen Angaben auf den Tags, sondern nur formale Angaben wie Mediennummern,
- keine RFID-Tags auf den Bibliotheksausweisen[52] sowie
- strenge Löschroutinen.

Entscheidend ist, dass keine personenbezogenen Daten und bibliografischen Informationen zu Ausleihvorgängen auf den RFID-Chips gespeichert werden, sodass eine Verknüpfung von Medien und Leserinnen und Lesern unmöglich ist. Des Weiteren bedarf es nach Ansicht des *BfDI* für RFID-Anwendungen einer Datenschutz-Folgenabschätzung.[53]

Um ihren datenschutzrechtlichen Transparenzpflichten nach Art. 12 DSGVO nachzukommen, sollten kommunalen Bibliotheken in jedem Fall den Einsatz der RFID-Technik deutlich kennzeichnen, da diese ansonsten für die betroffenen Personen nur schwer erkennbar ist, und umfassend über die Funktionsweise und den Verwendungszweck informieren.[54]

b) Videoüberwachung

Obgleich es zu Straftaten in Bibliotheken keine aussagekräftigen Statistiken gibt, kennen viele Einrichtungen das Problem des Bücherschwunds. Viele Medien werden unbewusst oder bewusst verstellt, manche aber auch entwendet.[55] Neben Diebstählen kommen auch mutwillige Sachbeschädigungen vor, beispielsweise wenn in alten Drucken wertvolle Stiche säuberlich mit Rasierklin- 972

52 So enthalten die Kundenkarten der *Bücherhallen Hamburg* beispielsweise keine RFID-Chips, während die *Stadtbibliothek Solingen* auf ihrer Homepage von „RFID-Bibliotheksausweisen" spricht, siehe *https://www.solingen.de/de/inhalt/rfid-technik/*, abgerufen am 31. 10. 2022. Auch wenn auf diesen keine Klarnamen, sondern nur Lesernummern gespeichert werden, lassen sich diese jedoch einer konkreten Person zuordnen und stellen mithin personenbezogene Daten dar.

53 *BfDI,* RFID – Funkchips für jede Gelegenheit?, S. 11, Stand August 2020, verfügbar unter *https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Flyer/RFIDFunkchipsFuerJedeGelegenheit.pdf?__blob=publicationFile&v=5*, abgerufen am 29. 10. 2022. Allerdings finden RFID-Anwendungen nicht in allen Listen der Datenschutz-Aufsichtsbehörden von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DSGVO, für die gemäß Art. 35 Abs. 1 DSGVO eine Datenschutz-Folgenabschätzung vom Verantwortlichen durchzuführen ist, Erwähnung.

54 Als Beispiel sei die Website der *Stadtbibliothek Solingen* genannt, auf der unter dem Reiter „Selbstverbuchung" ausführlich über die RFID-Technologie informiert wird, verfügbar unter *https://www.solingen.de/de/inhalt/rfid-technik/*, abgerufen am 29. 10. 2022.

55 *Nikolaizig,* arbido 2017/2.

gen oder Teppichmessern entfernt werden.[56] Auf diese Weise werden in Bibliotheken einzigartige Unikate zerstört. Aber nicht nur bei wertvollen Altbestände sind die Verluste schmerzhaft, sondern auch wenn anderen Leserinnen und Lesern so der Zugang zur Literatur vereitelt wird. Deshalb war es in Bibliotheken schon immer üblich, in den Lesesälen Aufsichtspersonal zu beschäftigen, das nicht nur für Ruhe sorgt und Auskünfte gibt, sondern auch die Gäste überwacht.

973 Aufgrund hoher Personalkosten und des technischen Fortschritts gehen manche Einrichtungen vermehrt dazu über, Videoüberwachung in ihren Räumlichkeiten einzusetzen. Beispielsweise lässt die *Stadtbibliothek Nürnberg* ihre Lesesäle mit Videokameras überwachen und beruft sich dabei auf Art. 24 Abs. 1 BayDSG. In ihrer Datenschutzerklärung gibt sie an, dass die Videoüberwachung „dem Schutz der Rechtsgüter Leben, Gesundheit und Eigentum von Personen, die sich in den Räumlichkeiten der Stadtbibliothek Nürnberg aufhalten, sowie dem Schutz und dem Funktionserhalt öffentlicher Einrichtungen, Dienstgebäude und Sachwerte einschließlich wertvollen Kulturguts vor Diebstahl und Vandalismus" diene. Außerdem wird als weitere Begründung die Erweiterung der Öffnungszeiten ohne anwesendes Fachpersonal genannt. Das Bildmaterial aus der Videoüberwachung wird für 14 Tage gespeichert und danach gelöscht.[57]

Ob eine umfassende Videoüberwachung von Stadtbibliotheken mit Bildaufzeichnung mit einer so weit gefassten Begründung wie in Nürnberg allgemein zulässig ist, erscheint indes fraglich. Mangels bereichsspezifischer Rechtsverordnungen für Bibliotheken oder Kultureinrichtungen sind für die Frage der Zulässigkeit der Videoüberwachung durch öffentliche Stellen neben den allgemeinen Vorschriften der DSGVO,[58] welche die Videoüberwachung nicht konkret regelt, die Landesdatenschutzgesetze der Länder maßgeblich.[59] Ähnlich wie im bayerischen Datenschutzgesetz verfügen auch andere Bundesländer über vergleichbare Regelungen zur Videoüberwachung durch öffentliche Stellen. So erlaubt beispielsweise § 20 DSG NRW die Videoüberwachung in öffentlich-zugänglichen Bereichen, zur Wahrnehmung des Hausrechts, zur Kontrolle von Zugangsberechtigungen und zum Schutz des Lebens, der Gesundheit, des Eigentums und des Besitzes.

974 Allerdings müssen die Schutzziele der Videoüberwachung hinreichend *bestimmt* sein und dürfen nicht nur von einer theoretischen abstrakten Gefährdung ausgehen. Vielmehr muss die Bibliothek im Einzelfall aufgrund *konkreter Tatsachen* die hinreichende Wahrscheinlichkeit einer Rechtsgutgefährdung fest-

56 Ein verurteilter Straftäter, der in zahlreichen Bibliotheken Werke beschädigt und gestohlen hat, versuchte mit dieser Methode beispielsweise in der *Stadtbibliothek Trier* in einem alten Druck eine historische Karte zu entfernen, siehe der Beitrag in der *taz* vom 21. 04. 2021, Dem Büchermarder auf der Spur, verfügbar unter *https://taz.de/Diebstahl-in-Bibliotheken/!5763164/*, abgerufen am 10. 10. 2022.

57 Verfügbar unter *https://www.nuernberg.de/internet/stadtbibliothek/datenschutz_videoueberwachung.html*, abgerufen am 10. 10. 2022.

58 Insbesondere Art. 6 Abs. 2 und 3 DSGVO.

59 *Veigel/Engelbrecht,* Videoüberwachung durch bayerische öffentliche Stellen, S. 10.

stellen.[60] Ansonsten bestände die Gefahr der übermäßigen flächendeckenden Videoüberwachung des öffentlichen bzw. öffentlich zugänglichen Raums, wenn die Befürchtung von abstrakten Gefahren den Zweck legitimieren würde. Entsprechend müssen die kommunalen Bibliotheken Vorfälle, die Rechtsgüter in der Vergangenheit bedroht oder geschädigt haben, dokumentieren und eine Gefährdungsprognose vornehmen, ob das Risiko eines erneuten Schadeneintritts mit hinreichender Wahrscheinlichkeit gegeben ist.[61]

Doch selbst wenn der Zweck der Datenverarbeitung ausreichend bestimmt ist, dürfen keine *schutzwürdigen Interessen* der betroffenen Personen überwiegen. Damit bedarf es für jede Installation einer Videokamera einer Güterabwägung im individuellen Einzelfall nach dem Grundsatz der Verhältnismäßigkeit.[62] Der Schutz der Privatsphäre und das informationelle Selbstbestimmungsrecht der Bibliothekskunden und -kundinnen sind mit dem angestrebten Schutz der Rechtsgüter abzuwägen. Die Videoüberwachung muss in Hinblick auf den im Vorweg festgelegten konkreten Zweck geeignet, erforderlich und angemessen sein.[63] 975

Sofern andere Schutzmaßnahmen wie z. B. Sicherungsetiketten in den Medien, ein Mitnahmeverbot von Taschen oder die Installation einer Alarmanlage einen genauso effektiven Schutz gegen Diebstahl bieten wie die Videoüberwachung, ist letztere nicht erforderlich und damit unzulässig.[64] Dabei gilt eine Maßnahme im Rahmen der *Verhältnismäßigkeitsprüfung* nur dann als vergleichbar, wenn sie einen geringeren oder ähnlichen finanziellen Aufwand verursacht. Die Beschäftigung von teurem Sicherheitspersonal als Alternative zur kostengünstigen Videoüberwachung kann dagegen nicht als Argument gegen die Erforderlichkeit der Maßnahme angeführt werden.[65]

Maßgeblich für die Ermessensentscheidung ist auch, welche *Bereiche* der Bibliothek von der Videoüberwachung erfasst werden. Grundsätzlich müssen alle Gesamtumstände der konkreten Überwachungsmaßnahme, u. a. auch das zeitliche Ausmaß, der Grad der Bildauflösung und das Vorhandensein von Aus- 976

60 *LfDI RP,* Orientierungshilfe für die Videoüberwachung in und an staatlichen Hochschulen, Stand 2022, S. 3, verfügbar unter *https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/oh_videoueberwachung_hochschulen.pdf*, abgerufen am 29. 10. 2022.

61 *Veigel/Engelbracht,* Videoüberwachung durch bayerische öffentliche Stellen, S. 22.

62 *LfDI RP,* Orientierungshilfe für die Videoüberwachung in Kommunen, Stand 2022, S. 6, verfügbar unter *https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/oh_vue_kommunen.pdf*, abgerufen am 29. 10. 2022.

63 *ULD SH,* Videoüberwachung durch öffentliche Stellen nach § 14 Landesdatenschutzgesetz Schleswig-Holstein, Stand 2019, S. 2, verfügbar unter *https://www.datenschutzzentrum.de/uploads/video/Videoberwachung_LDSG-2019.pdf*, abgerufen am 29. 10. 2022.

64 Nach Ansicht des *OVG NRW* ist eine Alarmanlage in Bibliotheken jedoch weniger geeignet, Diebstähle zu verhindern, als eine Videoüberwachung, da sie nur im Fall von Diebstählen ausgelöst wird, aber keine Sachbeschädigungen verhindern kann, siehe *OVG NRW,* Urt. v. 08. 05. 2009, Az. 16 A 3375/07.

65 *Veigel/Engelbracht,* Videoüberwachung durch bayerische öffentliche Stellen, S. 26.

weichmöglichkeiten, berücksichtigt werden.[66] Wird beispielsweise nur der Rückgabekasten an der Eingangstür gefilmt, bei dem sich die Gäste nur kurz zum Einwurf der Medien aufhalten, oder werden Leseplätze von der Videokamera dauerhaft erfasst? In die Privatsphäre der Leserinnen und Leser wird insbesondere dann intensiv eingegriffen, wenn die Kamera Buchtitel oder Bildschirme abfilmt und somit festhält, welche Inhalte gerade gelesen werden. Eine solche Videoaufzeichnung wäre nur dann angemessen, wenn zuvor eine schwerwiegende Gefährdungslage festgestellt wurde oder die Videoüberwachung dem Schutz von besonders wertvollem Kulturgut dient, wie beispielsweise in der wissenschaftlichen Bibliothek der *Stadt Trier* bei der Lektüre von kostbaren Handschriften und Inkunabeln.

977 Des Weiteren ist in Hinblick auf den Schutz der Intimsphäre zu beachten, dass Videoüberwachung in bestimmten Räumlichkeit stets tabu ist.[67] Die *Stadtbibliothek Stuttgart* hatte 2014 in ihrem Neubau Videokameras in den Toilettenräumen installiert und musste diese nach Nutzerbeschwerden und einer Beanstandung des behördlichen Datenschutzbeauftragten wieder entfernen.[68] Grundsätzlich sollten Kameras räumlich so angebracht werden, dass sie nur die Bereiche der Bibliothek erfassen, in denen besondere Gefahrensituationen bestehen.[69] Neben dem Schutz der Bibliothekskunden und -kundinnen müssen dabei auch die Interessen des *Personals* beachtet werden. Deshalb sollte die Überwachung nicht auf Stellen gerichtet sein, an denen sich Beschäftigte regelmäßig aufhalten, wie zum Beispiel an Info- und Ausleihtheken. Des Weiteren darf die Videoüberwachung in den Lesesälen nicht außerhalb der Öffnungszeiten erfolgen, wenn noch Personal anwesend ist, da sie zu diesen Zeiten grundsätzlich nicht erforderlich ist. Um die Interessen der Beschäftigten hinreichend zu schützen, ist bei der Planung der Videoüberwachung in jedem Fall auch der Personalrat miteinzubeziehen.[70]

978 Sofern die Bibliothek eine Videokamera installiert, muss sie zudem ihren *Informationspflichten* nach Artt. 13 und 14 DSGVO nachkommen und gut erkennbare Hinweisschilder, dass die Bibliothek videoüberwacht wird, anbringen. Diese müssen schon dann wahrnehmbar sein, bevor die Gäste das Gebäude betre-

66 *ULD SH,* Videoüberwachung durch öffentliche Stellen nach § 14 Landesdatenschutzgesetz Schleswig-Holstein, Stand 2019, S. 2, verfügbar unter *https://www.datenschutzzentrum.de/uploads/video/Videoberwachung_LDSG-2019.pdf*, abgerufen am 29. 10. 2022.

67 *LfDI RP,* Orientierungshilfe für die Videoüberwachung in Kommunen, Stand 2022, S. 3, verfügbar unter *https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/oh_vue_kommunen.pdf*, abgerufen am 29. 10. 2022.

68 Siehe Meldung in den *Stuttgarter Nachrichten* vom 23. 01. 2014, verfügbar unter *https://www.stuttgarter-nachrichten.de/inhalt.stadtbibliothek-stuttgart-videoueberwachung-in-der-toilette.12277b06-ea7d-4d22-a112-baa9712324fc.html*, abgerufen am 29. 10. 2022.

69 *Veigel/Engelbrecht,* Videoüberwachung durch bayerische öffentliche Stellen, S. 26.

70 *TLfDI,* Leitfaden für die Videoüberwachung durch öffentliche Stellen in Thüringen, Stand 2021, S. 44, verfügbar unter *https://www.tlfdi.de/fileadmin/tlfdi/datenschutz/Kommunales/Leitfaden_OH_Video_oeffentl_Stellen.pdf*, abgerufen am 29. 10. 2022.

ten.[71] Das gilt auch, wenn die Einrichtung keine echten Kameras, sondern lediglich Attrappen aufhängt, da sie in vergleichbarer Weise in das Persönlichkeitsrecht der betroffenen Personen eingreifen, wenn diese nicht sicher sein können, ob die Kameras echt oder unecht sind.[72] Die Hinweisschilder müssen nach Artt. 12 f. DSGVO neben einem Kamerabildsymbol auch die Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten enthalten, die Rechtsgrundlage und den Zweck der Videoüberwachung benennen sowie die Speicherdauer der Daten angeben, sofern eine Aufzeichnung des Videomaterials erfolgt. Sinnvoll ist die Verknüpfung mit einem QR-Code oder einer Internetadresse, über die weiterführende Informationen abgerufen werden können.[73]

Wenn die Videoaufnahmen *aufgezeichnet* und gespeichert werden, ist im Vor- 979
weg festzulegen, wer die Legitimation zur Sichtung des Materials erhält. Dabei sollte der Personenkreis so klein wie möglich gehalten werden.[74] Eine *Weitergabe* an Dritte ist grundsätzlich verboten und nur ausnahmsweise an die zuständigen Ermittlungsbehörden zur Verfolgung vorgefallener Straftaten möglich.[75] Auch die genauen *Speicher- und Löschfristen* müssen klar definiert und den betroffenen Personen gemäß Art. 13 Abs. 2 lit. a) DSGVO bekannt gegeben werden. Sobald der Zweck, für den die Daten erhoben worden sind, erfüllt ist, müssen diese nach Art. 17 Abs. 1 lit. a) DSGVO unverzüglich gelöscht werden.[76] Da für die Datenauswertung maximal zwei bis drei Arbeitstage notwendig sind, sollte die Löschung grundsätzlich nach diesem Zeitraum erfolgen, mithin nach spätestens 72 Stunden, sofern die Daten nicht ausnahmsweise nach einem konkreten Vorkommnis zur Beweissicherung länger vorgehalten werden dürfen.[77]

Beim Einsatz von Videokameras in kommunalen Bibliotheken gibt es grund- 980
sätzlich vier Möglichkeiten der *Ausgestaltung*: Die Videobeobachtung, die Video-

71 *ULD SH,* Videoüberwachung durch öffentliche Stellen nach § 14 Landesdatenschutzgesetz Schleswig-Holstein, Stand 2019, S. 2, verfügbar unter *https://www.datenschutzzentrum.de/uploads/video/Videoberwachung_LDSG-2019.pdf*, abgerufen am 29. 10. 2022.

72 *LfDI RP,* Orientierungshilfe für die Videoüberwachung in Kommunen, Stand 2022, S. 9, verfügbar unter *https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/oh_vue_kommunen.pdf*, abgerufen am 29. 10. 2022.

73 Eine idealtypisches Vorlage ist beim *ULD SH* zu finden, verfügbar unter *https://www.datenschutzzentrum.de/uploads/video/Vorgelagertes_Hinweisschild.pdf*, abgerufen am 29. 10. 2022.

74 *LfDI RP,* Orientierungshilfe für die Videoüberwachung in Kommunen, Stand 2022, S. 8, verfügbar unter *https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/oh_vue_kommunen.pdf*, abgerufen am 29. 10. 2022.

75 *LfDI RP,* Orientierungshilfe für die Videoüberwachung in Kommunen, Stand 2022, S. 8, verfügbar unter *https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/oh_vue_kommunen.pdf*, abgerufen am 29. 10. 2022.

76 *DSK,* Videoüberwachung nach der Datenschutzgrundverordnung (Kurzpapier Nr. 15), Stand 2018, S. 3, verfügbar *https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_15.pdf*, abgerufen am 29. 10. 2022.

77 *LfDI RP,* Orientierungshilfe für die Videoüberwachung in Kommunen, Stand 2022, S. 8, verfügbar unter *https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/oh_vue_kommunen.pdf*, abgerufen am 29. 10. 2022.

aufzeichnung, die Videobeobachtung in Kombination mit einer Videoaufzeichnung und die Videoüberwachung im sog. Black-Box-Verfahren. Im Vergleich zur Videoaufzeichnung wird die Videobeobachtung grundsätzlich als das mildere Mittel gesehen, das weniger in das Grundrecht der informationellen Selbstbestimmung eingrifft, da kein Datenbestand erzeugt wird.[78] Das *OVG NRW* hat im Jahr 2009 in Bezug auf die Regelung des früheren Bundesdatenschutzgesetzes die Ansicht vertreten und ausgeführt, dass die Benutzer und Benutzerinnen „durch den offenen Einsatz von Videotechnik im Ergebnis nicht wesentlich mehr beeinträchtigt [werden], als wenn die Bibliotheksräume von einer dort anwesenden Person beobachtet würden", und weiter: „Die Situation, in der die Beobachtung erfolgt, ist nicht durch besondere Privatheit geprägt. Im Gegenteil müssen Personen, die sich in einer öffentlichen Bibliothek aufhalten, stets damit rechnen, den Blicken der übrigen Bibliotheksbenutzer sowie der dort Beschäftigten ausgesetzt zu sein."[79] Entsprechend hat das Gericht das vorinstanzliche Urteil des *VG Münster*[80] bestätigt, das die Videobeobachtung in der Bibliothek des *Kommunalwissenschaftlichen Instituts der Universität Münster* erlaubt, aber die nicht anlassbezogene Speicherung der Filmaufnahmen verboten hatte. Denkbar wäre jedoch, dass in einem konkreten Gefahrenfall über einen Art *Notfallknopf* eine Videoaufzeichnung gestartet wird, die als anlassbezogene Speicherung dem Grundsatz der Verhältnismäßigkeit entsprechen würde.[81]

981 Als besonders eingriffsschonend sieht dagegen das *OVG Lüneburg* die Videoüberwachung im *Black-Box-Verfahren* an und hat entschieden, dass mit Hilfe dieses Verfahrens Bus- und Bahnfahrende im öffentlichen Nahverkehr zum Zweck der Prävention von schweren Straftaten flächendeckend rund um die Uhr durch Videokameras überwacht werden dürfen.[82] Die Filmaufnahmen werden auf einem nicht vernetzten Rechner, der in einem abgesonderten Raum steht, zu dem nur ein sehr kleiner Personenkreis Zugang hat, mit Verschlüsselung und Passwortschutz gespeichert und nach 24 Stunden wieder unbesehen gelöscht bzw. überschrieben, ausgenommen, wenn in dieser Zeit Straftaten festgestellt wurden. Aufgrund dieser technischen Maßnahmen, insbesondere der strikten Löschroutine, ist sichergestellt, dass der Eingriff in das Grundrecht auf informationelle Selbstbestimmung im Regelfall minimal und die Gefahr, dass das Videomaterial für andere Zwecke missbraucht wird, ausgeschlossen ist.[83]

c) Gesichtserkennung

982 Einer besonderen rechtlichen Bewertung bedarf die Videoüberwachung, wenn sie mit Gesichtserkennungssoftware arbeitet. Die automatisierte *Gesichtserken-*

78 *Veigel/Engelbrecht,* Videoüberwachung durch bayerische öffentliche Stellen, S. 27.
79 *OVG NRW,* Urt. v. 28. 05. 2009, Az. 16 A 3375/07.
80 *VG Münster,* Urt. v. 19. 10. 2007, Az. 1 K 367/06.
81 *Veigel/Engelbrecht,* Videoüberwachung durch bayerische öffentliche Stellen, S. 27.
82 *OVG Lüneburg,* Urt. v. 07. 09. 2017, Az. 11 LC 59/16, ECLI:DE:OVGNI:2017:0907.11LC59.16.00.
83 *Grages/Plath,* CR 2017, 794 ff.

nung mit Hilfe eines Algorithmus zählt wie der Iris-Scans oder der Abgleich von Fingerabdrücken zu den biometrischen Verfahren.[84] Da künstliche Intelligenz zur Identifizierung von Personen genutzt wird, gelten die so erhobenen Daten nach Art. 4 Nr. 14 DSGVO und Art. 9 Abs. 1 DSGVO als besonders sensibel und schützenswert und unterliegen deshalb einem generellen Verarbeitungsverbot, das nur wenige Ausnahmen zulässt, zum Beispiel durch eine ausdrückliche Einwilligung (Art. 9 Abs. 2 lit. a) DSGVO), zu wissenschaftlichen Forschungszwecken (Art. 9 Abs. 2 lit. j) DSGVO) oder zur Wahrnehmung bestimmter, gesetzlich festgelegter Rechte und Pflichten (Art. 9 Abs. 2 lit. b) DSGVO). Jedoch fehlen landesgesetzliche Rechtsgrundlagen für Bibliotheken zur Nutzung algorithmischer Verfahren, die biometrischen Daten verarbeiten. Deshalb wäre die Nutzung von Gesichtserkennungssoftware nur mit einer ausdrücklichen und freiwilligen Einwilligung[85] der Bibliothekskundinnen und -kunden möglich. Diese wäre allerdings praktisch nur schwer umsetzbar, da die Einwilligung im Vorweg erfolgen muss und die betroffenen Personen über Art, Zwecke, Umfang und Reichweite der Verarbeitung informiert werden müssen. Bei nicht einsichtsfähigen Kindern ist zudem die Einwilligung beider Elternteile bzw. Erziehungsberechtigten notwendig. Zudem ist für die Verarbeitung von biometrischen Daten, die automatisiert verarbeitet werden, eine Dateschutz-Folgenabschätzung nach Art. 35 DSGVO erforderlich.[86]

Bisher ist die Nutzung von biometrischen Daten in Bibliotheken eher unüblich, könnte aber zukünftig für digitale Zugangskontrollen im Rahmen des *Open-Library-Konzepts*,[87] das Bibliothekskunden und -kundinnen auch außerhalb der regulären Öffnungszeiten Zutritt zur Bibliothek gewährt, zunehmend Relevanz erhalten.[88] In einigen Stadtbüchereien indes hat die automatisierte Gesichtserkennung bereits mit humanoiden *Robotern* Einzug erhalten.[89] Neben zahlreichen Sensoren und einer intelligenten Spracherkennung sind die Geräte auch mit einer Gesichtserkennungssoftware ausgestattet, die u. a. das Alter und die aktuelle Stimmung ihrer Gesprächspartnerinnen und -partner erkennen kann, 983

84 *Heldt,* MMR 2019, 286 ff.

85 Wenn es nur eine Bibliothek vor Ort gibt und mithin für die Leserinnen und Leser keine Wahlmöglichkeit besteht, erscheint die Freiwilligkeit einer Einwilligung zweifelhaft, siehe *Schwenke,* NJW 2018, 826 ff.

86 Gemäß *BfDI,* Liste von Verarbeitungsvorgängen gemäß Art. 35 Abs. 4 DSGVO für Verarbeitungstätigkeiten öffentlicher Stellen des Bundes, verfügbar unter *https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Muster/Liste_VerarbeitungsvorgaengeArt35.pdf;jsessionid=88DF629DE0BF06EE53EA5A5F7DE5AA66.intranet242?__blob=publicationFile&v=5*, abgerufen am 29. 10. 2022.

87 *Neuer,* Open Library: Mehr Bibliothek für die Bürger, Treffpunkt Kommune, 2020.

88 So haben beispielsweise die *Leipziger Städtischen Bibliotheken* während der Corona-Pandemie ein Einlassmanagementsystem mit automatischer Gesichtserkennung der Sensape GmbH genutzt, siehe den Bericht des Unternehmen unter *https://www.sensape.com/projects/digital-access-management-library-leipzig*, abgerufen am 29. 10. 2022.

89 Beispielsweise in den kommunalen Bibliotheken der *Städte Köln, Düsseldorf, Hannover, Regensburg, Biberach* und *Frankfurt am Main.*

um individuell auf ihre Gegenüber eingehen zu können.[90] Aus Sicht des Datenschutzrechtes ist nicht ersichtlich, auf welcher Rechtsgrundlage und zu welchem Zweck die Verarbeitung dieser Bildaufnahmen zulässig ist, insbesondere wenn Kinder mit den Robotern kommunizieren.[91]

90 Diese Aussagen beziehen sich auf den humanoiden Roboter „Pepper" der Firma *CleverGuides GmbH,* nähere Informationen verfügbar unter *https://www.biteam.de/share/Events/Infotage2019/Vortraege/Partner/CleverGuides_Pepper-ein_humanoider_Roboter_in_B2B-Einsatz.pdf*, abgerufen am 29. 10. 2022.

91 Ein Datenverarbeitung auf der Grundlage einer ausdrücklichen Einwilligung nach Art. 6 Abs. 1 lit. a) DSGVO bzw. Art. 9 Abs. 2 lit. a) DSGVO wäre zwar theoretisch denkbar, aber praktisch schwer umsetzbar, da diese im Vorweg erfolgen muss und die betroffenen Personen über Art, Zwecke, Umfang und Reichweite der Verarbeitung informiert werden müssen. Bei nicht einsichtsfähigen Kindern ist zudem die Einwilligung aller Erziehungsberechtigten notwendig.