Datenschutz ab Inkrafttreten der Datenschutz-Grundverordnung

Handreichung für Bibliotheken

Überblick:

A. Einleitung - Armin Talke, Staatsbibliothek zu Berlin-PK, 7.3.2018

Durch das Inkrafttreten der Datenschutz-Grundverordnung und der konkretisierenden nationalen Gesetze ändert sich nicht alles, aber vieles. Da wir aber nicht davon ausgehen können, dass die Leserinnen und Leser dieser Handreichung mit der alten Rechtslage gut vertraut waren, sprechen wir hier nicht von den Änderungen, sondern von den Regelungen insgesamt. Die Handreichung ist allerdings keinesfalls abschließend oder ausreichend, um die Datenschutzbelange der Bibliotheken zu beschreiben, geschweige denn zu lösen. Es ist immer zu bedenken, dass bei allen datenschutzrechtlich relevanten Verfahren die behördlichen Datenschutzbeauftragten zu informieren sind. Sie sind diejenigen, die die Bibliotheken beraten und unterstützen oder ihnen ihre Bedenken mitteilen müssen.

I. Was ist Datenschutz ?

Im Datenschutz(recht) geht es um die rechtlichen Voraussetzungen für die Verarbeitung personenbezogener Daten.

Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht. Gemäß Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta“) sowie Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten[1].

Das Recht auf Schutz der personenbezogenen Daten ist nicht unbeschränkt, denn es muss im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden[2]. Außerdem sind personenbezogene Daten im Bereich der Datenschutzgesetzgebung nur bis zum Tod[3] der betroffenen Person zu berücksichtigen. Nach dem Tod handelt es sich also nicht mehr um „personenbezogene Daten“, so dass die Datenschutznormen nicht mehr angewandt werden müssen. Das heißt aber nicht automatisch, dass solche Informationen oder Inhalte völlig frei verbreitet werden dürfen, denn es kann sein, dass nach spezifischen Normen wie z.B. den Archivgesetzen noch ein längerer Schutz besteht (in Landes- und Bundesarchivgesetzen gilt der Schutz i.d.R. bis 10 Jahre nach dem Tod, in Einzelfällen auch länger). Das Urheberrecht gilt, wo einschlägig, bis 70 Jahre nach dem Tod des Urhebers.

II. Normen im Datenschutzrecht

Mit dem Inkrafttreten der EU-Datenschutz-Grundverordnung (DSGVO) am 25.5.2018 ändert sich das Normgefüge EU-weit. Während die bisherigen EU-Regel, die Datenschutz-Richtlinie[4] den Mitgliedstaaten einen weiten Spielraum für ihre nationale Gesetzgebung ließen, hat die DSGVO überwiegend unmittelbare Wirkung und bedarf weitgehend gar keines nationalen Gesetzes mehr.

---

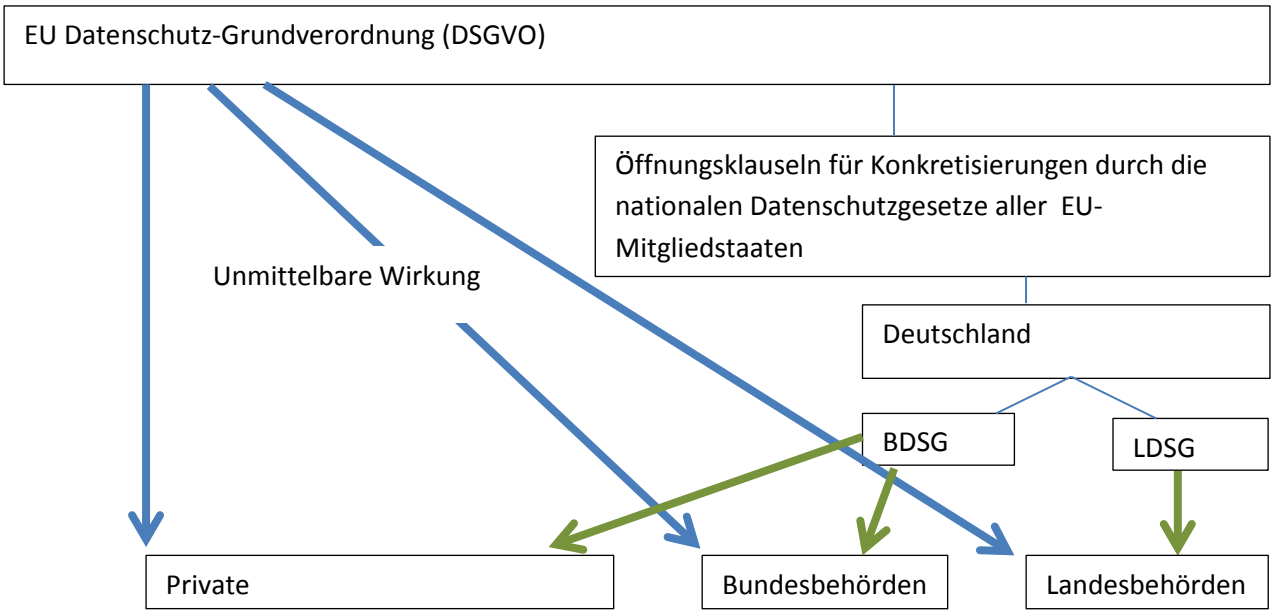
[1] Erwägungsgrund 1 der DSGVO: http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE ; übersichtliche Webseite mit dem Verordnungs-Text: https://dsgvo-gesetz.de/

[2] Erwägungsgrund 4 der DSGVO

[3] Erwägungsgrund 27 der DSGVO

[4] Richtlinie 95/46/EG: http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:31995L0046

Die bis zum 24.5.2018 geltenden Datenschutzgesetze[5] regelten im Zusammenspiel mit bereichsspezifischen Normen (z.B. Landeskrankenhausgesetze, Sozialgesetzbuch, Telemediengesetz) in Deutschland den Datenschutz mehr oder weniger abschließend.
Die DSGVO regelt aber nicht *alles* allein. Sie überlässt vielmehr an vielen Stellen den nationalen Gesetzgebern durch Öffnungsklauseln die Konkretisierung.
Wegen der Bundes- und Landeszuständigkeiten für die Gesetzgebung gibt es jetzt also neue und ganz andere Bundes[6]- und Landesdatenschutzgesetze, die ebenfalls am 25.5.2018 in Kraft treten. Sie füllen die Öffnungsklauseln der DSGVO nach der gleichen Aufteilung wie früher, also nach Bundes-, Landes und privaten Stellen.



III. Woraus ergeben sich die Möglichkeiten der verantwortlichen Stellen ?

Die Stellen – bei den Bibliotheken handelt es sich ja regelmäßig um öffentliche Stellen des Bundes oder der Länder – dürfen überhaupt nur personenbezogene Daten verarbeiten, wenn es dafür entweder eine gesetzliche Grundlage gibt oder aber eine Einwilligung der Betroffenen vorliegt, vgl. Art 2 Abs.1 und 6 Abs.1 DSGVO . Gesetzliche Grundlagen für öffentliche Einrichtungen sind z.B. ganz allgemein in Art.6 Abs.1 e) DSGVO, Art.89 DSGVO (Archiv, Wissenschaft, Forschung), konkretisierend z.B. in § 23 Abs.1 Nr.7 BDSG-2018 (etwa für Organisationsuntersuchungen), § 4 BDSG-2018 (Videoüberwachung). Die Voraussetzungen für die Einwilligung sind in Art. 7 und 8 DSGVO geregelt. Näheres zu den o.g. Normen wird weiter unten behandelt.

[5] Bundesdatenschutzgesetz für die öffentlichen Stellen des Bundes und Private / Landesdatenschutzgesetze für öffentliche Stellen der Länder
[6] BGBl.1, 2017, 44, S.2097 Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU)

IV. Was ist die „Verarbeitung“ „personenbezogener Daten“ ?

Der Begriff der **personenbezogenen Daten** ist in Art. 4 Nr.1 DSGVO definiert:

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

Der Begriff ist also denkbar weit, z.B. fällt darunter:

- Die Information, dass eine bestimmte Person registrierte/r BenutzerIn der Bibliothek ist;
- ob bzw. wann eine Person den Lesesaal betreten hat;

Unter den Begriff der „Kennung“ fällt z.B. auch die Benutzernummer, mit mittelbar (über das Benutzungssystem) ja die Identifikation der Person möglich ist. Unter online-Kennung fällt schon eine IP-Adresse, die in den Logfiles von Webseitenbetreibern auftaucht, denn auch hier könnte mit Hilfe des Serviceproviders des Webseitenbesuchers der Anschlussinhaber identifiziert werden.

Der Begriff der **„Verarbeitung“** ist in Art.4 Nr.2 DSGVO definiert:

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

Man kann also fast sagen: Alles, was mit personenbezogenen Daten in der Bibliothek passiert, fällt darunter.

V. In <u>allen Fällen</u> geltende Bedingungen für die rechtmäßige Datenverarbeitung

Ganz unabhängig davon, ob die Daten aufgrund einer Einwilligung oder auf Basis einer gesetzlichen Grundlage verarbeitet werden, müssen bestimmte Prinzipien berücksichtigt werden: Nach Art.5 DSGVO gehören zur Datenverarbeitung (grob beschrieben) folgende Gebote:

- „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“ (wird u.a. durch die Informations- und Auskunftspflichten konkretisiert, s.u.)
- „Zweckbindung“ (Datenerhebung und-verarbeitung nur für festgelegte, eindeutige und legitime Zwecke)
- „Datenminimierung“ (dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt)

- „Richtigkeit“ (auf dem neuesten Stand)
- „Speicherbegrenzung“ (heißt: Anonymisierung so früh wie möglich;)
- „Integrität und Vertraulichkeit“ (Sicherheit durch technische und organisatorische Schutzmaßnahmen
- „Rechenschaftspflicht“ (…gegenüber Datenschutzbeauftragten und Aufsichtsbehörden)

Nach Art.25 DSGVO hat die datenverarbeitende („verantwortliche“) Stelle den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sicherzustellen. Neben geeigneter technischer und organisatorischer Maßnahmen kann dazu u.a. die Pseudonymisierung gehören, die, auch wenn sie den Personenbezug nicht aufhebt, trotzdem die Identifizierung der betroffenen Person durch eine Verschlüsselung erschwert.

Auch der Begriff der „Pseudonymisierung“ ist im Gesetz (Art.4 Nr.5 DSGVO) definiert:

„Pseudonymisierung“ [ist] die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;

Wenn statt des Namens z.B. bei der Zugangskontrolle die Benutzernummer erhoben und gespeichert wird, fällt das i.d.R also noch nicht unter „Pseudonymisierung“, weil die Benutzernummer wohl durch alle MitarbeiterInnen, die Zugriff auf das Benutzungssystem haben, mit dem Namen und den übrigen im Ausleihsystem enthaltenen Daten in Verbindung gebracht werden kann. Die Benutzernummer müsste für eine Pseudonymisierung also zusätzlich verschlüsselt und der Verschlüsselungs-Algorithmus an sicherer Stelle verschlossen werden. Wenn die Daten ohnehin nicht mehr zu datenschutzrechtlich anerkannten Zwecken gebraucht werden, müssen sie gleich ganz gelöscht oder anonymisiert werden (s. dazu auch unten).

B. Informierte Einwilligung nach DSGVO (Art. 7-8 und 13-15 DSGVO) - Elke Brehm, Datenschutzbeauftragte der TIB, Stand 9.2.2018

Es gilt nach wie vor, dass eine Verarbeitung von Daten nur auf der Grundlage einer Rechtsvorschrift oder mit Einwilligung des Betroffenen erfolgen darf. Es muss daher bei der Verarbeitung personenbezogener Daten weiterhin überprüft werden, ob für die Verarbeitung der Daten eine entsprechende Rechtsgrundlage existiert.

- Privater Nutzungsvertrag siehe Art. 6 Abs. 1 b) DSGVO
- Andere Rechtsgrundlage nach Art. 6 Abs. 1 c) DSGVO

Sofern keine andere Rechtsgrundlage eingreift, kann die Datenverarbeitung durch eine Einwilligung gerechtfertigt sein (Art. 6 Abs. 1 a DSGVO). Sofern Bibliotheken öffentlich-rechtlich organisiert sind, ist die Benutzungsordnung Rechtsgrundlage für alle im Aufgabenbereich der Bibliothek liegenden

Verarbeitungen von Nutzerdaten. Wenn die Bibliothek Dienstleistungen anbietet, die über die regulären Aufgaben einer Bibliothek hinausgehen oder in einer anderen Rechtsform Dienstleistungen anbietet, ist gegebenenfalls eine Einwilligung für die Verarbeitung der Daten erforderlich. Das muss im Einzelfall geprüft werden. Mit Einführung der DSGVO werden die Wirksamkeitsvoraussetzungen der Einwilligung Betroffener vereinheitlicht. Die Vorgaben der DSGVO sind unmittelbar in allen Ländern anwendbar. Die Regelungen der DSGVO ersetzen die bisher geltenden Regelungen der nationalen Gesetzgeber. Eine anderweitige Regelung in nationalen Gesetzen ist nun nicht mehr zulässig.

1. Voraussetzungen der wirksamen Einwilligung

a) Allgemeines

Eine „Einwilligung" der betroffenen Person wird nach Art. 4 Nr. 11 DSGVO definiert als „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist".

Voraussetzungen für eine wirksame Einwilligung sind danach[7]:

- freiwillig
- für bestimmten Zweck
- in informierter Weise
- unmissverständlich in Form einer Erklärung oder sonstigen eindeutigen bestätigenden Handlung abgegebene Willensbekundung
- über das Einverständnis mit einer konkreten Verarbeitung von personenbezogenen Daten des Betroffenen.

Untätigkeit und Stillschweigen können nicht als Einwilligung gewertet werden, eine konkludente (durch eindeutige Handlung) abgegebene Einwilligung ist aber möglich (Erwägungsgrund 32 der DSGVO). Im **Forschungskontext** gilt der sogenannte „broad consent": Während normalerweise eine Einwilligung nur bezogen auf einen konkreten Zweck gegeben werden kann, kann im Forschungskontext eine Einwilligung pauschal für einen oder mehrere bestimmte Bereiche wissenschaftlicher Forschung oder Projekte erteilt werden (Erwägungsgrund 33 DSGVO).

An die **Freiwilligkeit** der Einwilligung werden deutlich höhere Anforderungen gestellt. Es gilt das **„Koppelungsverbot"**: Die Erteilung der Einwilligung darf nicht an die Erbringung einer Leistung gekoppelt werden, die nicht im Zusammenhang mit der Nutzung der Daten steht. Die Unfreiwilligkeit ist dann stets indiziert. Auf welche Fälle dies anwendbar ist, ist aber im Einzelfall noch zu klären. Für unterschiedliche Verarbeitungsvorgänge muss gesonderte Erteilung der Einwilligung möglich sein (horizontales Koppelungsverbot)[8].

[7] Schulz in: Gola, DS-GVO, Art. 4 Rn. 67 ff;
[8] Schulz in: Gola, DS-GVO, Art. 4 Rn. 68;

Sonstige Anforderungen für Wirksamkeit sind, dass das **Ersuchen um Einwilligung** in klarer und einfacher Sprache, von der Form her verständlich und leicht zugänglich und dem jeweiligen Sachverhalt leicht zuordenbar ist. Ansonsten ist die Einwilligung nicht verbindlich.

Die Einwilligung ist **jederzeit widerruflich.** Wird die Einwilligung widerrufen, bleibt die Verarbeitung der personenbezogenen Daten bis zum Zeitpunkt des Widerrufs zulässig. Der Betroffene muss vor Erteilung der Einwilligung über die Widerruflichkeit hingewiesen werden. Der Widerruf muss so einfach erfolgen können wie die Erteilung der Einwilligung.

b) Beschäftigtendatenschutz:

Die DSGVO macht keine besonderen Vorgaben für die Erteilung von Einwilligungen im Beschäftigungsverhältnis, dies ist durch die Bundes- bzw. Landesdatenschutzgesetze zu regeln. Gleichwohl ist das Vorliegen der Freiwilligkeit bei Erteilung der Einwilligung besonders zu prüfen, da ein Abhängigkeitsverhältnis besteht. In der Regel spielt die Einwilligung nur dann eine Rolle, wenn Verarbeitungen vorgenommen werden, die nicht unter Art. 6 Abs. 1 b (Erfüllung eines Vertrags mit Betroffenem) und f (Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten nach Abwägung mit Betroffeneninteressen) fallen. Zu berücksichtigen ist hier die Legitimierung von Verarbeitungen von Mitarbeiterdaten durch Betriebsvereinbarungen, die nicht umgangen werden dürfen, die aber auch die Betroffenenrechte nicht unzulässig beschränken dürfen (§ 26 Abs. 4 BDSG und die Landesrechte)[9]. Für die Freiwilligkeit und damit Wirksamkeit der Einwilligung eines Beschäftigten spricht, wenn der Beschäftigte „einen materiellen oder rechtlichen Vorteil erlangt oder Arbeitgeber und Mitarbeiter gleichgelagerte Interessen verfolgen“ (26 Abs. 2 BDSG). In der Regel bedarf die Einwilligung der Schriftform, es sei denn es liegen besondere Umstände vor. Es kann auch in die Bearbeitung der in Art. 9 Abs. 1 DSGVO genannten besonders sensiblen Personendaten eingewilligt werden. Die Einwilligung muss sich dann besonders darauf beziehen.

c) Einwilligung Minderjähriger

Einwilligung Minderjähriger für ihnen direkt angebotene Dienste (Art. 8 DSGVO): Zulässig ist die Einwilligung durch ein Kind, das das 16. Lebensjahr vollendet hat. Zwischen 13 und 16 können Mitgliedsstaaten in bestimmten Fällen eine Einwilligung des Minderjährigen genügen lassen, im Übrigen muss aber die Zustimmung des Trägers der elterlichen Verantwortung vorliegen.

d) Nachweispflichten[10]:

Der Verantwortliche muss die Erteilung der Einwilligung jederzeit nachweisen können (Art. 7 Abs. 1 DSGVO). Zwar sind neben schriftlichen, auch mündliche und elektronische Einwilligungserklärungen wirksam möglich. Der Verantwortliche muss jedoch auch später den Nachweis erbringen können, dass eine wirksame Einwilligung erteilt wurde. Insofern empfiehlt sich auch bei elektronischen Einwilligungen, z. B. durch Mitprotokollierung der Zustimmung auf der Website, dass ein Verfahren vorgesehen wird, bei dem sich der Einwilligende zuverlässig authentifizieren muss und bei dem die Einwilligung zuverlässig protokolliert, sicher gespeichert wird und auch später noch zugänglich bleibt.

e) Folgen einer fehlerhaften Einwilligung

[9] Schulz in: Gola, DS-GVO, Art. 7 Rn. 46 ff.;
[10] Hierzu ausführlicher: Schulz in: Gola, DS-GVO, Art. 4 Rn. 38 ff.;

Verstöße gegen einwilligungsspezifische Vorgaben der DSGVO führen zur umfassenden Ungültigkeit der betroffenen Teile der Einwilligung. Wie weit die Unwirksamkeit reicht, muss durch Auslegung ermittelt werden. Alle darauf beruhenden Verarbeitungen von personenbezogenen Daten sind ohne Rechtsgrundlage erfolgt. Ist die Einwilligung vollumfänglich unwirksam, sind die erhobenen Daten zu löschen[11].

2. Informationspflichten des Verantwortlichen[12]:

Mit Einführung der DSGVO gelten erhöhte Anforderungen an die **Informationspflichten des Verantwortlichen gegenüber dem Betroffenen.**

Grundsätzlich muss der Betroffene vor Erhebung der Daten und Erteilung der Einwilligung **umfassend informiert** werden. Worüber genau zu informieren ist, **ergibt sich aus Art. 13 Abs. 1 und 2 DSGVO**.

Sofern **die Daten bei Dritten erhoben** werden (z. B. anderen Institutionen oder Behörden) muss der Betroffene eine „angemessene Frist nach Erlangung der Daten, längstens jedoch innerhalb eines Monats“ über die Erhebung der Daten bei dem Dritten informiert werden. Bei der Frist handelt es sich um eine Maximaldauer, die eher den Ausnahmefall darstellen sollte[13]. Sofern es aber rechtlich oder tatsächlich unmöglich ist den Betroffenen zu informieren, oder die Erteilung mit einem unverhältnismäßigen Aufwand verbunden ist, kann auf die Information des Betroffenen verzichtet werden. Dies ist unter anderem eine Privilegierung für im öffentlichen Interesse liegende Archiv- und Forschungszwecke. Diese Ausnahmen sind allerdings eng auszulegen und bedürfen einer eingehenden Prüfung. Worüber zu informieren ist, ergibt sich aus Art. 14 DSGVO.

Stilistisch gesehen muss die Information **präzise, transparent, verständlich, leicht zugänglich und in klarer und einfacher Sprache** und in der Regel unentgeltlich erfolgen. Als leicht zugänglich gelten die Informationen auch, wenn der Zugang über einen QR-Code oder Kurzlink erfolgt[14].

Die **Information kann „schriftlich oder in anderer Form, gegebenenfalls auch elektronisch“ an den Betroffenen übermittelt** werden (Art. 12 Abs. 1 und 5 DSGVO). Nach deutscher Rechtsdiktion erfasst das eine der folgenden Formen: Schriftform, Textform, elektronische Form oder vereinbarte Form (§§ 126-127 BGB) [15]. Auf Anfrage ist bei nachgewiesener Identität auch eine mündliche Erteilung möglich (Art. 12 Abs. 1 S. 3 DSGVO).

Im Interesse der die Daten nutzenden Institution sollte die Erfüllung der Informationspflichten dokumentiert werden.

Bei Verstößen gegen die Informationspflichten aus Art. 13 und 14 DSGVO drohen hohe Geldbußen (Art. 83 Abs. 5 b DSGVO). Bußgelder können gemäß § 43 Abs. 3 BDSG aber nicht gegen öffentliche Institutionen verhängt werden. Dies gilt jedoch nicht für Einrichtungen, die mit ihren

[11] Schulz in: Gola, DS-GVO, Art. 7 Rn. 52;
[12] Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) zu Informationspflichten bei Dritt- und Direkterhebung: https://www.lfd.niedersachsen.de/startseite/dsgvo/anwendung_dsgvo_kurzpapiere/ds-gvo---kurzpapiere-155196.html
[13] Franck in: Gola, DS-GVO, Art. 14 Rn. 18;
[14] Franck in: Gola, DS-GVO, Art. 12 Rn. 17 ff.;
[15] Franck in: Gola, DS-GVO, Art. 12 Rn. 23;

Dienstleistungen am Wettbewerb teilnehmen, § 43 Abs. 2 BDSG[16], das wird aber auf die meisten Bibliotheken nicht zutreffen.

3. Folgen der Änderungen

Die Anforderungen an die Wirksamkeit einer Einwilligung durch Betroffene und die neuen Informationspflichten des Verantwortlichen sind deutlich höher als vor Erlass der Datenschutzgrundverordnung. Nach dem 25.5.2018 eingeholte Einwilligungen müssen den Anforderungen der DSGVO genügen. Verfahren für die Erteilung von Einwilligungen durch Betroffene müssen daher auf Einhaltung der nun geltenden Bedingungen überprüft und entsprechend umgestaltet werden.

Es stellt sich aber die Frage, ob eine für eine abgeschlossene oder laufende Verarbeitung bereits nach den bisher geltenden Regelungen wirksam erteilte Einwilligung mit Inkrafttreten der DSGVO am 25.5.2018 weiterhin die Verarbeitung der Daten legitimieren kann, auch wenn sie die Anforderungen der DSGVO nicht erfüllt, oder ob sie unter Beachtung der mit der DSGVO eingeführten Vorgaben erneut eingeholt werden muss.

Grundsätzlich gelten bereits erteilte Einwilligungen fort, sofern sie die Anforderungen der RL 95/46/EG erfüllen und „der Art nach“ auch nach DSGVO zulässig sind, dies gilt wohl für alle nach altem Recht wirksam erteilten Einwilligungen. Der Art nach nicht den Anforderungen der DSGVO genügen wohl Einwilligungen, die durch Opt-Out-Klauseln eingeholt wurden[17]. Für laufende Verarbeitungen von Betroffenendaten sollten die Einwilligungen jedoch innerhalb von 2 Jahren angepasst, also erneut unter Einhaltung der jetzt geltenden Vorgaben eingeholt werden, dies ist aber nicht zwingend (Erwägungsgrund 171).

C. Datenschutz-Folgenabschätzung nach DSGVO (Art. 35)[18] - Elke Brehm, Datenschutzbeauftragte der TIB, Stand 9.2.2018

Die durch die DSGVO neu eingeführte Datenschutzfolgenabschätzung ersetzt die bisher nach deutschem Datenschutzrecht durchgeführte Vorabkontrolle nach § 4d Abs. 5 BDSG. Das Verfahren dient dem nach Art. 25 Abs. 1 DSGVO vorgegebenen Prinzip Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen zu gewährleisten, **indem vor Einführung eines Verfahrens Risiken bewertet und technische und organisatorische Abhilfemaßnahmen aufeinander abgestimmt werden**, um die festgestellten Risiken zu minimieren.

---

[16] Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, BT Drucksache 18/1325, S. 109;

[17] Schulz in: Gola, DS-GVO, Art. 7 Rn. 59;

[18] **Zum Thema insgesamt:** „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinnde der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt““ der Datenschutzgruppe nach Art. 29, 17/DE WP 248 Rev. 01: http://www.lfd.niedersachsen.de/startseite/dsgvo/leitlinien_art_29gruppe/ oder http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 ; Nolte/Werkmeister in: Gola, DS-GVO, Art. 35 Rn. 1 ff.;

Während die Vorabkontrolle als reine Rechtmäßigkeitsprüfung ausgestaltet war und entfiel, wenn eine Einwilligung des Betroffenen vorlag, sind mit der Datenschutz-Folgenabschätzung nun auch umfangreiche Dokumentationspflichten bzgl. der Risikobewertung und getroffenen technisch organisatorischen Abhilfemaßnahmen hinzugekommen. Eine Stellungnahme des Datenschutzbeauftragten allein genügt nicht mehr.

Eine Folgenabschätzung kann für einzelne oder mehrere ähnliche Verarbeitungsvorgänge durchgeführt werden (Erwägungsgrund 92).

1. Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung

Eine Datenschutz-Folgenabschätzung ist bei Verarbeitungen erforderlich, die „aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung **voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen**“ mit sich bringen (Art. 35 Abs. 1 DSGVO). Ein entsprechendes hohes Risiko ist bei

- Vernichtung
- Verlust
- Veränderung
- unbefugte Offenlegung oder unbefugter Zugang

der Daten gegeben (Erwägungsgrund 83).

Aufgrund des Risikos muss die Entstehung eines physischen, materiellen, immateriellen Schaden möglich sein. Dies kann z.B. im Verlust der Kontrolle über personenbezogene Daten, Einschränkungen der Rechte, Diskriminierung, Identitätsdiebstahl, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von Berufsgeheimnissen unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für betroffene Person liegen (Erwägungsgrund 85).

a) Hohes Risiko:

Ob ein **hohes Risiko** vorliegt, ergibt sich aus einer wertenden Betrachtung im Einzelfall[19]. Es liegt vor, wenn die mit Verarbeitung verbundenen Risiken über allgemein mit der Datenverarbeitung verbundene Risiken hinausgehen. Dies kann sich aus der Art, dem Umfang, der Umstände als auch der Zwecke der Verarbeitung ergeben. Zu berücksichtigen ist auch die Ursache des Risikos. Ein hohes Risiko kann insbesondere dann vorliegen, wenn eine neue Datenverarbeitungstechnologie eingeführt wird[20].

Die Verfahren müssen nach folgenden **neun Kriterien** bewertet werden[21]:

1. Liegt ein **„Bewerten und Einstufen“** insbesondere auf der Grundlage von „Aspekten, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die

[19] Nolte/Werkmeister in: Gola, DS-GVO, Art. 35 Rn. 13;
[20] Leitlinien zur Datenschutz-Folgenabschätzung der Datenschutzgruppe nach Art. 29, S 9;
[21] Leitlinien zur Datenschutz-Folgenabschätzung der Datenschutzgruppe nach Art. 29, S 9 ff.;

Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel der Person betreffen“ vor? (Erwägungsgründe 71, 91)

2. **Automatisierte Entscheidungsfindung** mit Rechtswirkung oder ähnlich bedeutsamer Wirkung (Art. 35 Abs. 3 a)
3. **Systematische Überwachung** in Form von Beobachtung, Überwachung oder Kontrolle von Betroffenen durch Erfassung von Daten über Netzwerke oder „eine systematische […] Überwachung öffentlich zugänglicher Bereiche“ (Art. 35 Abs. 3 c)
4. Vertrauliche Daten oder höchst persönliche **Daten in Sinne von Art. 9 Abs. 1 DSGVO**
5. **Datenverarbeitung „in großem Umfang“** (Erwägungsgrund 91): Zu berücksichtigen sind dabei die Zahl der Betroffenen, die verarbeitete Datenmenge, Dauer oder Dauerhaftigkeit der Datenverarbeitung, geografisches Ausmaß der Datenverarbeitung
6. **Abgleichen oder Zusammenführen von Datensätzen**
7. **Daten zu schutzbedürftigen Betroffenen**, insbesondere Kinder (Erwägungsgrund 75)
8. **Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen** (Erwägungsgrund 89, 91, Art. 35 Abs. 1 DSGVO): Wann eine Nutzung innovativ ist oder eine neue technologische oder organisatorische Lösung vorliegt bestimmt sich aus dem jeweiligen Stand der Technik. Beispiele sind das Internet der Dinge oder die Kombination aus Fingerabdruck- und Gesichtserkennung zum Zwecke der Zugangskontrolle.
9. **Hindert die Verarbeitung „die betroffene Person an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung** bzw. Durchführung eines Vertrags“? Ein Beispiel sind Anfragen zur Kreditwürdigkeit bei Kreditauskunfteien.

Werden zwei dieser Kriterien erfüllt, muss in der Regel eine Datenschutz-Folgenabschätzung durchgeführt werden[22]. Sofern der für die Datenverarbeitung Verantwortliche ein nach diesen Kriterien risikoreiches Verfahren nicht als mit einem „hohen Risiko“ behaftet einschätzt, muss er den Verzicht auf die Datenschutz-Folgenabschätzung unter Einbeziehung der Position des Datenschutzbeauftragten begründen und dokumentieren[23].

b) Erforderlichkeit einer Datenschutz-Folgenabschätzung ohne Risikoprüfung:

Zwingend erforderlich ist eine Datenschutz-Folgenabschätzung nach Art. 35 Abs. 3 DSGVO insbesondere in folgenden Fällen, die per se ein hohes Risiko darstellen:

- **Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen**, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und Grundlage für Entscheidungen ist, die Rechtswirkung gegenüber natürlichen Personen entfaltet
- **Umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten** (siehe Art. 9 Abs. 1 DSGVO) oder von personenbezogenen Informationen über strafrechtliche Verurteilungen und Straftaten (Art. 10 DSGVO)
- **Systematische umfangreiche Überwachung** öffentlich zugänglicher Bereiche

[22] Weitere Beispiele siehe: Leitlinien zur Datenschutz-Folgenabschätzung der Datenschutzgruppe nach Art. 29, S. 13 f.;
[23] Weitere Beispiele siehe: Leitlinien zur Datenschutz-Folgenabschätzung der Datenschutzgruppe nach Art. 29, S. 14;

In der Bibliothekspraxis ist in der Regel nur der zweite Fall im Kontext Beschäftigtendatenschutz relevant. Dies betrifft dann aber alle Bibliotheken, da in den Personalakten oder im Betrieblichen Eingliederungsmanagement immer Gesundheitsdaten der Beschäftigten verarbeitet werden. Bei Universitätsbibliotheken kommt auch der erste Fall im Hinblick auf Forschungsinformationssysteme in Betracht, wobei je nach Ausgestaltung zu prüfen ist, wie umfassend und intensiv der Eingriff ist. Ein Beispiel für den dritten Fall ist die Einführung der Videoüberwachung in einem öffentlichen Bereich.

Zu beachten ist, dass die für Datenschutzbelange zuständige Aufsichtsbehörde der Bibliothek festlegen kann, für welche Verfahren eine Datenschutz-Folgenabschätzung durchgeführt werden muss und für welche nicht.

c) Entbehrlichkeit einer Datenschutz-Folgenabschätzung

Eine Datenschutz-Folgenabschätzung muss in folgenden Fällen nicht durchgeführt werden (Art. 35 DSGVO):

- Die Verarbeitung bringt **„wahrscheinlich [kein] hohes Risiko“** für Rechte und Freiheiten natürlicher Personen mit sich
- Wenn **bereits eine Datenschutz-Folgenabschätzung für ein Verfahren durchgeführt** wurde, dass sich von dem vorliegenden Verfahren bzgl. Art, Umfang, Umstände und Zweck der Verarbeitung nur geringfügig unterscheidet.
- Wenn **das Verfahren vor Mai 2018 durch die Aufsichtsbehörde geprüft wurde** und die Bedingungen sich nicht geändert haben (Erwägungsgrund 171)
- Bei **Schaffung einer Rechtsgrundlage wurde bereits eine Datenschutz-Folgenabschätzung durchgeführt** (Art. 6 Abs. 1 c und e, 35 Abs. 10 DSGVO)
- Konkretes Verfahren ist auf einer von der Aufsichtsbehörde erstellten optionalen **Liste von Verarbeitungsvorgängen, für die keine Folgenabschätzung erforderlich** ist[24].
- Bei **bereits laufenden und unverändert gebliebenen Verarbeitungstätigkeiten** ist eine Folgenabschätzung auch dann entbehrlich, wenn bei Einführung des Verfahrens durch den Datenschutzbeauftragten oder die Aufsichtsbehörde eine **Vorabkontrolle** nach Art. 20 der Richtlinie 95/46/EG durchgeführt wurde (Erwägungsgrund 171)

Bei bereits laufenden Verarbeitungstätigkeiten, die zwar datenschutzkonform eingeführt wurden, bei denen sich aber Änderungen ergeben haben, bei denen die Risikobewertung zur Feststellung eines hohen Risikos führen würde, muss innerhalb von zwei Jahren eine Datenschutz-Folgenabschätzung durchgeführt werden.

2. Ablauf/Durchführung der Datenschutzfolgenabschätzung[25]:

a) Vorbereitungsphase
b) Definition des Prüfungsgegenstand
c) Identifikation und Bewertung der Risiken

[24] Nolte/Werkmeister in Gola, DS-GVO, Art. 35 Rn. 28 ff.;
[25] Zur Durchführung insgesamt siehe Nolte/Werkmeister in Gola, DS-GVO, Art. 35 Rn. 37 ff., Leitlinien zur Datenschutz-Folgenabschätzung der Datenschutzgruppe nach Art. 29, S. 17 ff.;

d) Identifikation und Planung geeigneter Schutzmaßnahmen

Gegebenenfalls muss die Einbindung geeigneter Stakeholder organisiert werden. Bei hohen Restrisiken muss die Aufsichtsbehörde hinzu gezogen werden[26].

3. Inhalt der Datenschutz-Folgenabschätzung (Art. 35 Abs. 7 DSGVO)[27]:

a) **Umfassende Sachverhaltsschilderung und Definition des Prüfgegenstands**: Systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung ggfls. einschließlich der damit verfolgten berechtigten Interessen
b) **Bewertung der Notwendigkeit und Verhältnismäßigkeit** der Verarbeitungsvorgänge mit Bezug zum Zweck
c) **Bewertung der Risiken** für Rechte und Freiheiten der betroffenen Person
d) Die zur Bewältigung der Risiken geplanten **Abhilfemaßnahmen** einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz der Daten sichergestellt und Nachweis erbracht wird, dass diese Verordnung eingehalten wird

Sofern die Aufsichtsbehörde hinzugezogen werden muss, sind darüber hinaus noch die in Art. 36 Abs. 3 DSGVO genannten Informationen der Aufsichtsbehörde zur Verfügung zu stellen.

Veröffentlichung: Eine Pflicht zur Veröffentlichung der Datenschutz-Folgenabschätzung besteht nicht[28].

In besonderen Fällen kann eine Pflicht zur Konsultation der Aufsichtsbehörde bestehen (Art. 36 DSGVO).

4. Rechtsfolgen von Verstößen[29]:

Durchführung der Folgenabschätzung ist keine Voraussetzung für die Rechtmäßigkeit der konkreten Verarbeitung. Unterlassen der Durchführung kann aber einen Verstoß gegen Art. 25 Abs. 1 begründen.

Verstöße gegen Art. 35 sind bußgeldbewehrt (Art. 83 Abs. 4 a), begründen aber keine Schadensersatzpflicht gegenüber der betroffenen Person.

Bußgelder können gemäß § 43 Abs. 3 BDSG nicht gegen öffentliche Institutionen verhängt werden. Dies gilt jedoch nicht für Einrichtungen, die mit ihren Dienstleistungen am Wettbewerb teilnehmen, § 43 Abs. 2 BDSG[30], das wird aber auf die meisten Bibliotheken nicht zutreffen.

[26] Leitlinien zur Datenschutz-Folgenabschätzung der Datenschutzgruppe nach Art. 29, S. 23;
[27] Nolte/Werkmeister in Gola, DS-GVO, Art. 35 Rn. 62;
[28] Nolte/Werkmeister in Gola, DS-GVO, Art. 35 Rn. 65;
[29] Nolte/Werkmeister in Gola, DS-GVO, Art. 35 Rn. 73 ff.;
[30] Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, BT Drucksache 18/1325, S. 109;

D. Befugnisse öffentlicher Stellen[31] zur Nutzung personenbezogener Daten ohne Einwilligung der Betroffenen

Armin Talke, Staatsbibliothek zu Berlin-PK, 7.3.2018

Dieser Abschnitt widmet sich den Grundsätzen der Datenverarbeitung in öffentlichen Einrichtungen. Dabei geht es vor allem um die Frage, inwieweit in öffentlichen Einrichtungen wie z.B. Universitäts- Landes- oder Gemeindebibliotheken ohne Einwilligung des/der Betroffenen Daten erhoben und verarbeitet werden dürfen. Detailfragen z.B. der technischen Vorkehrungen oder der Informations- und Dokumentationspflichten werden hier noch nicht behandelt.

I. Wer fällt unter die Regeln für „öffentliche Stellen“ ?

Weil im Datenschutzrecht häufig zwischen nichtöffentlichen und öffentlichen Stellen unterschieden wird, helfen Definitionen bei der Abgrenzung: Nach § 2 BDSG-neu sind „öffentliche Stellen“ (des Bundes) – grob gesagt –

- Behörden, Justiz, bundesunmittelbare Körperschaften, Anstalten und Stiftungen des Bundes
- Privatrechtliche Vereinigungen öffentlicher Stellen, soweit sie über ein Land hinaus tätig werden oder der Bund die Mehrheit der Stimmen hat

Darunter fallen natürlich

- öffentliche Bibliotheken als Teil der Gemeindeverwaltung,
- Universitätsbibliotheken als Teil der „Behörde“ Universität und
- National- und Staatsbibliotheken als Teil von öffentlich-rechtlichen Stiftungen, öffentlich rechtlichen Anstalten oder unmittelbarer Teil der Landesverwaltung.

II. Was dürfen die öffentlichen Stellen ohne Einwilligung des/der Betroffenen tun ?

Wie oben gezeigt, ist das Regelungsgeflecht im Datenschutzrecht komplizierter geworden. Fast[32] ganz oben in der Regelungshierarchie steht die DSGVO. Sowie diese obligatorische oder fakultative Öffnungsklauseln enthält, kann oder muss der nationale und in Deutschland nach den Gesetzgebungszuständigkeiten des Grundgesetzes auch der Landesgesetzgeber tätig werden. Das BDSG regelt insoweit das Datenschutzrecht für die öffentlichen Stellen des Bundes und die Landesdatenschutzgesetze das Datenschutzrecht für die öffentlichen Stellen der jeweiligen Länder.

Für die Verarbeitung in Bund und Ländern gilt Art.6 DSGVO, der entweder

- eine Einwilligung des Betroffenen in die Datenverarbeitung (Abs.1 a))
- oder bestimmte Zwecke für die Datenverarbeitung (Abs.1 b) bis f))

erfordert. Für die Datenverarbeitung in öffentlichen Bibliotheken kommt als Rechtsgrundlage vor allem Abs.1 e) DSGVO in Betracht: „die Verarbeitung ist für die Wahrnehmung einer Aufgabe

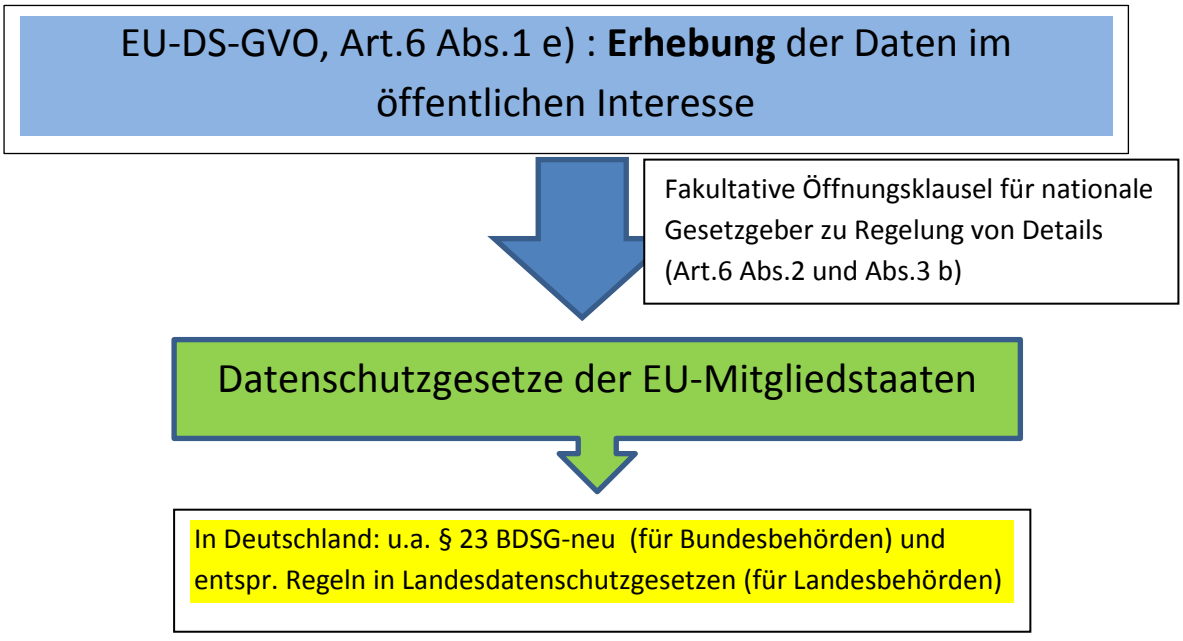
[31] Nicht behandelt sind in diesem Kapitel u.a.: Datenübermittlung (§25 BDSG-2018)Beschäftigten-Datenschutz (Art. 9 Abs.2 b DSGVO; § 26 BDSG-2018)

[32] Darüber steht noch das EU-Primärrecht wie z.B. der Vertrag über die Europäische Union und der Vertrag über die Arbeitsweise der Europäischen Union

erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde“

Näheres dazu kann der nationale Gesetzgeber (per „Fakultativer Öffnungsklausel“) regeln[33]. Dem entsprechend sind im in Deutschland verabschiedeten BDSG-neu in § 23 Details zur Verarbeitung „zu anderen Zwecken“ durch öffentliche Stellen geregelt. Subsidiär, d.h., wenn in Spezialregeln wie dem § 23 zu einem Bereich nichts geregelt ist, gilt § 3 BDSG, nach dem die Datenverarbeitung zulässig ist, „wenn sie zur Erfüllung der“ […] „Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist.“ Das heißt aber nicht, dass hier erleichterte Bedingungen herrschen, denn die allgemeinen Grundsätze des Datenschutzes[34] sind auch hier immer zu berücksichtigen.

Auf Spezialgesetze zu besonderen Arten von Daten (z.B. der Umgang mit Sozialdaten ist im SGB X geregelt) kann hier nicht eingegangen werden.



Die Vorschrift schafft für öffentliche Stellen im Rahmen der jeweiligen Aufgabenerfüllung eine nationale Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch denselben Verarbeiter zu einem anderen Zweck als zu demjenigen, zu dem er sie ursprünglich erhoben hat (Weiterverarbeitung). Soweit eine der tatbestandlichen Voraussetzungen nach Absatz 1 erfüllt ist,

[33] DSGVO, Art.6 Abs.3b)
[34] S.o

kann die Weiterverarbeitung personenbezogener Daten durch öffentliche Stellen auf diese Vorschrift gestützt werden[35].

Der Einfachheit halber wird man in der Praxis für den Alltag davon ausgehen können, dass für die Verarbeitung durch öffentliche Stellen in Deutschland nur die Regeln des BDSG-neu bzw. der Landesdatenschutzgesetze gelten, so dass eine Prüfung der Voraussetzungen des Art. 6 DSGVO nicht mehr notwendig ist.

1. Spezialnorm für öffentliche Einrichtungen des Bundes: § 23 Abs.1 Nr.3 und Nr.7:

(1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch öffentliche Stellen im Rahmen ihrer Aufgabenerfüllung ist zulässig, wenn…
3. die Daten allgemein zugänglich sind oder der Verantwortliche sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Weiterverarbeitung offensichtlich überwiegt,
…
oder
7. sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen des Verantwortlichen dient; dies gilt auch für die Verarbeitung zu Ausbildungs- und Prüfungszwecken durch den Verantwortlichen, soweit schutzwürdige Interessen der betroffenen Person dem nicht entgegenstehen.

Was „allgemein zugängliche Daten“ in § 23 Abs.1 Nr.3 sind (den Begriff gab es im alten BDSG), hat das BVerfG in einem Urteil beschrieben:

„Allgemein zugänglich sind Daten, die sich sowohl ihrer Zielsetzung als auch ihrer Publikationsform nach dazu eignen, einem individuell nicht bestimmbaren Personenkreis Informationen zu vermitteln“[36]. Dazu gehören Angaben in Massenmedien, wie Zeitungen, Rundfunk und Fernsehen, Daten auf Internetseiten n, Lexika, Adress- und Telefonverzeichnissen, Dokumentationen, Ausstellungskatalogen und wissenschaftliche Monographien und Flugblättern[37].

Soweit aber z.B. Rundschreiben, Register o.ä. nur an einen bestimmten Personenkreis gerichtet sind, gehört deren Inhalt nicht zu den „allgemein zugänglichen Daten“.

Beispiel: Daten aus Teilnehmerverzeichnissen werden mit Zustimmung der TeilnerInnen i.d.R nur den anderen VeranstaltungsteilnehmerInnen überlassen, aber nicht der Allgemeinheit. Informationen darüber, wer dort dabei war, dürfen Bibliotheken daher z.B. nicht anderweitig für ihre Zwecke, z.B. in einem öffentlichen Veranstaltungsbericht, der ins Internet gestellt wird, verbreiten.

[35] Regierungsentwurf, S. 95 : http://dip21.bundestag.de/dip21/btd/18/113/1811325.pdf
[36] z.B. BVerfGE 103, 44 (60).
37 u.a. Gola/Schomerus, BDSG, 12. Aufl., 2015, § 28 Rdnr. 32

§ 23 Abs.1 Nr.7 gab es im Wortlaut fast gleich im alten BDSG, §14 Abs.3. In Bibliotheken dürfte von den dort geregelten zulässigen Zwecken der Datenverarbeitung insbesondere die „Organisationsuntersuchungen“ eine Rolle spielen. Solche Untersuchungen liefern notwendige Entscheidungsgrundlagen für die Optimierung der Aufbau- und Ablauforganisation[38]. In solche Organisationsprüfungen dürfen nur personenbezogene Daten einbezogen werden, die von der verantwortlichen Stelle selbst zu ihrer sonstigen Aufgabenerfüllung gespeichert oder genutzt werden[39].

Soweit der Anonymisierungsaufwand nicht unverhältnismäßig groß ist, sind Organisationsuntersuchungen bevorzugt mit anonymisierten Daten durchzuführen. In solchen Fällen sind keine Persönlichkeitsrechte betroffen und das Datenschutzrecht nicht zu berücksichtigen. Soweit aber die (auch mittelbare) Erkennbarkeit einzelner Personen nicht ausgeschlossen werden kann, sind sie in ihren Interessen stark berührt[40]. Daher müssen die Einrichtungen durch Zugriffsbeschränkungen und Verschlüsselungen zumindest für eine deutliche Erschwerung der Identifikation sorgen, z.B. durch eine starke Pseudonymisierung mit Beschränkung der Zugriffsrechte auf das absolut Notwendige[41].

Beispiel: Nutzerforschung
Eine Bibliothek möchte untersuchen, wie viele BenutzerInnen den Lesesaal nutzen, wie viele und wie lange ihn temporär verlassen. Daraus kann sich ableiten, ob bessere Aufenthalts- und Verpflegungsmöglichkeiten im Lesesaal oder auf dem Bibliotheksgelände geschaffen werden sollten. Da dabei untersucht werden muss, ob dieselben BenutzerInnen den Lesesaal verlassen, die auch hineingegangen sind, müssen die Benutzernummern der ein- und ausgehenden Personen, die per RFID am Ein- und Ausgang ausgelesen werden, abgeglichen werden. Diese Nummer ist eindeutig einer Person zugewiesen und kann im Benutzungssystem mit der Person in Verbindung gebracht werden. Die Identifizierbarkeit muss durch Verschlüsselung/Pseudonymisierung erschwert werden, so dass der Aufwand für die Rückrechnung der verschlüsselten Daten in die Benutzernummer mit hohem Aufwand verbunden ist.

4. Datenverarbeitung für Forschung und Archivzwecke, Art. 89 DSGVO

Unter Berücksichtigung der Grundsätze des Art.89 DSGVO dürfen personenbezogene Daten für „im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken…“ verwendet werden. Nach Art.89 DSGVO müssen personenbezogene Daten überall, wo dies möglich ist, anonymisiert werden. Solange dies im Interesse der Archiv- , Wissenschafts- und Forschungszwecke nicht machbar ist, muss dem Datenschutz durch andere Sicherungen Rechnung getragen werden, z.B. durch technische und organisatorische Maßnahmen oder Pseudonymisierung.

[38] Simitis, BDSG, 8.Aufl., 2014, § 23 Rn.99
[39] Gola / Schomerus, BDSG, 12. Aufl., 2015, § 14 Rn.25, in Bezug auf das alte BDSG
[40] Simitis, § 23 Rn.100
[41] S.o.; Vgl. Simitis, BDSG, § 3 Rn.217a; das Gebot der Pseudonymisierung folgt direkt aus Art.6 Abs.4 e) DSGVO

5. Videoüberwachung öffentlicher zugänglicher Räume, § 4 BDSG-2018

Unter Anderem zur Wahrnehmung ihres Hausrechts ist unter Berücksichtigung der Verhältnismäßigkeit die Videoüberwachung erlaubt. Die Speicherung der Bilddaten ist nur erlaubt, wenn das für den Zweck unter Berücksichtigung der Schutzwürdigen Belange erforderlich ist. Die Erforderlichkeit setzt voraus, dass die Maßnahme geeignet ist, d. h. das Überwachungsziel tatsächlich erreicht wird, und dass dafür kein anderes, gleich wirksames, zumutbares, aber den Betroffenen weniger in seinen Rechten beeinträchtigende Mittel zur Verfügung steht. Insofern ist eine Beobachtung mit Aufzeichnung nicht erforderlich, wenn der Einrichtung auch die bloße Beobachtung möglich und zumutbar ist[42]. Es gelten auch hier wieder die allgemeinen Grundsätze der Datenminimierung, der technisch-organisatorischen Maßnahmen etc.

Bei der Videoüberwachung ist den Betroffenen durch geeignete Maßnahmen bekanntzumachen:

- Der Umstand, dass beobachtet wird. Dafür reicht es aus, dass die Kamera für jedermann sichtbar ist[43]. In Zweifelsfällen ist sicher ein gut sichtbarer Hinweis erforderlich

- der Name und die Kontaktdaten des Verantwortlichen

Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

6. Verschärfte Bedingungen bei besonderen Kategorien von Daten, u.a. Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung

Die Verarbeitung besonders sensibler („besonderer Kategorien“) personenbezogener Daten ist nach Art.9 Abs.1 der DSGVO prinzipiell untersagt. Ausnahmen von diesem Verbot sind in Art.9 Abs.2 geregelt, z.B.

- Daten, „die die betroffene Person offensichtlich öffentlich gemacht hat“ (Abs.2 e)
- Verarbeitung erlaubt, soweit sie „für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke“ […] „erforderlich“ ist (Abs.2 j) ist“. Die EU-Mitgliedstaaten dürfen hierzu (weitere) eigene Gesetze erlassen. Das wurde in Deutschland in § 27 BDSG-neu für die Wissenschaft und in § 28 BDSG-neu für die Forschung getan. Danach gelten hierfür sehr verschärfte Bedingungen. Die Veröffentlichung ohne Einwilligung der Betroffenen Person ist immer unzulässig.

Beispiele:

- In Nachlässen finden sich häufig Brief-Korrespondenzen mit anderen Personen, in denen sensible Daten zu finden sind. Auch Katalogdaten, z.B. die Angabe der

[42] Gola/Klug/Körffer in: Gola/Schomerus, Bundesdatenschutzgesetz 12. Auflage 2015, § 6b, Rn. 18a / b

[43] Gola/Klug/Körffer in: Gola/Schomerus, Bundesdatenschutzgesetz 12. Auflage 2015, § 6b, Rn.23

KorrespondenzpartnerInnen oder Inhaltsangaben, können solche sensiblen Daten sein.
- Ausleihdaten: Aus diesen kann sich z.B. auf politische Überzeugungen, sexuelle Vorlieben oder gesundheitliche Belange schließen lassen

III. Informationspflichten, Art. 13-15 DSGVO, §§ 32-34 BDSG-neu

Auch in Situationen, in denen für die Erhebung und Verarbeitung personenbezogener Daten keine Einwilligung erforderlich ist (z.B. nach Art.6 DSGVO und § 23 BDSG-neu), sind die datenverarbeitenden Einrichtungen regelmäßig dazu verpflichtet, die Betroffenen über die Verarbeitung der auf ihre Person bezogenen Daten zu informieren. Die Gegenstände dieser Informationspflicht sind vor allem in Art.14 DSGVO geregelt.

Was ist den Personen mitzuteilen ?

Nach Art.14 DSGVO sind den Betroffenen u.a. folgende Informationen zu geben:

Informationen zu Adressaten.:

- den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters sowie die Kontaktdaten des Datenschutzbeauftragten;
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
- Bei Auftragsdatenverarbeitung durch ein Unternehmen oder auf einem Server, der in einem Staats außerhalb der EU gelegen ist: Die Absicht des Verantwortlichen, die personenbezogenen Daten an einen Empfänger in einem Drittland oder einer internationalen Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines von der EU-Kommission anerkannten Verfahrens oder Garantien

Außerdem:

- die Dauer, für die die personenbezogenen Daten gespeichert werden
- das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung und eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- aus welcher Quelle die personenbezogenen Daten stammen …

Zeitpunkt der Mitteilung:

- … innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats

Bei beabsichtigter Änderung des Zwecks der Daten-Nutzung:

Wenn die Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erlangt wurden, so stellt er der betroffenen Person vor dieser

Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Art.14 Absatz 2 (s. oben: „Außerdem“) zur Verfügung.

Keine der o.g. Informationen ist erforderlich, wenn die betroffene Person bereits über die Informationen verfügt

E. Auskunftsrecht der betroffenen Person, Art.15 DSGVO - Armin Talke, Staatsbibliothek zu Berlin-PK, 7.3.2018

Die betroffene Person, z.B. eine Bibliotheksbenutzerin, hat nach Art.15 DSGVO (Ergänzend: § 34 BDSG-2018 bzw. entsprechende Landesgesetze) das Recht, Auskunft darüber zu verlangen, ob die Einrichtung Daten über sie verarbeitet und ggf. welche das sind.

Das ist u.a. deswegen sehr relevant für die Einrichtungen, weil sie selbst a) einen Überblick über die von ihr verarbeiteten personenbezogenen Daten haben müssen, b) diese zügig und möglichst ohne großen Aufwand zusammenführen können müssen und c) sie innerhalb einer Frist von 1 Monat dem Antragsteller zur Verfügung stellen müssen, Art. 12 Abs.3 DSGVO. Diese Frist kann in komplexen Fällen um zwei Monate verlängert werden. Über Fristverlängerungen ist die betroffene Person unter Angabe der für die Verzögerung verantwortlichen Gründe innerhalb eines Monats nach Eingang ihres Antrags zu informieren.

Gemäß der Art. 12 Abs. 1 und Art. 5 Abs. 2 DSGVO haben Verantwortliche bereits vorbereitend geeignete organisatorische Maßnahmen zu treffen, um betroffenen Personen beantragte Auskünfte fristgerecht und in einer geeigneten Form zur Verfügung zu stellen.

Die wesentlichen Gesichtspunkte des Auskunftsrechts in Listenform:

- Der Antrag auf Auskunft: Keine bestimmte Form vorgeschrieben
- Die Form der Auskunft: Die Einrichtung muss eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung stellen. Wenn der Antrag elektronisch gestellt wird, müssen die Informationen in einem gängigen elektronischen Format zur Verfügung gestellt werden, soweit der/die AntragstellerIn dies wünscht. Nach Erwägungsgrund 63 zur DSGVO heißt es diesbezüglich, dass der Verantwortliche nach Möglichkeit den Fernzugang zu einem sicheren System bereitstellen können sollte, der der betroffenen Person direkten Zugang zu ihren personenbezogenen Daten ermöglichen würde. In jedem Fall ist bei der Auskunftserteilung darauf zu achten, dass angemessene Sicherheitsanforderungen eingehalten werden.
- Wesentlicher Inhalt der Auskunft (u.a.) nach Art. 15 DSGVO (hier nicht abschließend !):
    - die Verarbeitungszwecke
    - die Kategorien personenbezogener Daten, die verarbeitet werden (durchaus relevant, weil von Ausleihdaten besondere Kategorien i.S.d. Art.9 Abs.1 DSGVO (z.B. politische Meinungen, religiöse oder weltanschauliche Überzeugungen) berührt sein können

  - falls möglich, die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer
  - das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung
  - das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
  - wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten
- Werden personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die geeigneten Garantien gemäß Artikel 46 im Zusammenhang mit der Übermittlung unterrichtet zu werden. (s.u. zur Auftragsdatenverarbeitung im Ausland)
- Keine Beeinträchtigung der Datenschutzrechte Dritter, indem z.B. Informationen auch über diese auf den Kopien mitgeliefert werden
- Konsequenzen bei Nichterteilung der Auskunft: Der/die Betroffene kann verlangen, dass die Information der Datenschutz-Aufsichtsbehörde erteilt wird, § 34 Abs.3 BDSG-neu

Ausnahmen von der Auskunftspflicht:

- Forschung/ Archive: Keine Auskunft geboten, wenn
  - die Auskunft bestimmte Forschungszwecke unmöglich machen oder unverhältnismäßig behindern würde, § 27 Abs.2 BDSG-neu (gestützt auf Art. 89 DSGVO)
  - Archivmaterial nicht durch den Namen der Person erschlossen ist oder das Archivgut auch anderweitig nicht mit vertretbarem Aufwand auffindbar ist

Nach § 34 Abs.2 BDSG-neu sind die Gründe der Auskunftsverweigerung zu dokumentieren. Die Ablehnung der Auskunftserteilung ist gegenüber der betroffenen Person zu begründen, soweit nicht durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde.

- Keine automatische Verarbeitung

Über Daten, die die Stelle weder automatisiert verarbeitet noch nicht automatisiert verarbeitet und in einem Dateisystem gespeichert hat, muss nur Auskunft erteilt werden, soweit die betroffene Person Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem von der Betroffenen Person geltend gemachten Informationsinteresse steht.

F. Recht auf Berichtigung und Löschung („Recht auf Vergessenwerden“) - Armin Talke, Staatsbibliothek zu Berlin-PK, 7.3.2018

Vorläufig machen wir Sie an dieser Stelle nur auf die einschlägigen Gesetzestexte aufmerksam:

Artikel 16 DSGVO

Recht auf Berichtigung

Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten — auch mittels einer ergänzenden Erklärung — zu verlangen.

Artikel 17 DSGVO

Recht auf Löschung („Recht auf Vergessenwerden“)

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

a) Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.

b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.

c) Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2 Widerspruch gegen die Verarbeitung ein.

d) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.

e) Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.

f) Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.

(2) Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um

für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

(3) Die Absätze 1 und 2 gelten nicht, soweit die Verarbeitung erforderlich ist

a) zur Ausübung des Rechts auf freie Meinungsäußerung und Information;

b) zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Absatz 2 Buchstaben h und i sowie Artikel 9 Absatz 3;

d) für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder

e)zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Die Erwägungsgründe 65 und 66 der DSGVO sind für die Interpretation und Anwendung der o.g. Normen wichtig:

(65)

Eine betroffene Person sollte ein Recht auf Berichtigung der sie betreffenden personenbezogenen Daten besitzen sowie ein „Recht auf Vergessenwerden“, wenn die Speicherung ihrer Daten gegen diese Verordnung oder gegen das Unionsrecht oder das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt, verstößt. Insbesondere sollten betroffene Personen Anspruch darauf haben, dass ihre personenbezogenen Daten gelöscht und nicht mehr verarbeitet werden, wenn die personenbezogenen Daten hinsichtlich der Zwecke, für die sie erhoben bzw. anderweitig verarbeitet wurden, nicht mehr benötigt werden, wenn die betroffenen Personen ihre Einwilligung in die Verarbeitung widerrufen oder Widerspruch gegen die Verarbeitung der sie betreffenden personenbezogenen Daten eingelegt haben oder wenn die Verarbeitung ihrer personenbezogenen Daten aus anderen Gründen gegen diese Verordnung verstößt. Dieses Recht ist insbesondere wichtig in Fällen, in denen die betroffene Person ihre Einwilligung noch im Kindesalter gegeben hat und insofern die mit der Verarbeitung verbundenen Gefahren nicht in vollem Umfang absehen konnte und die personenbezogenen Daten — insbesondere die im Internet gespeicherten — später löschen möchte. Die betroffene Person sollte dieses Recht auch dann ausüben können, wenn sie kein Kind mehr ist. Die weitere Speicherung der personenbezogenen Daten sollte jedoch rechtmäßig sein, wenn dies für die Ausübung des Rechts auf freie Meinungsäußerung und Information, zur Erfüllung einer rechtlichen Verpflichtung, für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse

liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

(66) Um dem „Recht auf Vergessenwerden“ im Netz mehr Geltung zu verschaffen, sollte das Recht auf Löschung ausgeweitet werden, indem ein Verantwortlicher, der die personenbezogenen Daten öffentlich gemacht hat, verpflichtet wird, den Verantwortlichen, die diese personenbezogenen Daten verarbeiten, mitzuteilen, alle Links zu diesen personenbezogenen Daten oder Kopien oder Replikationen der personenbezogenen Daten zu löschen. Dabei sollte der Verantwortliche, unter Berücksichtigung der verfügbaren Technologien und der ihm zur Verfügung stehenden Mittel, angemessene Maßnahmen — auch technischer Art — treffen, um die Verantwortlichen, die diese personenbezogenen Daten verarbeiten, über den Antrag der betroffenen Person zu informieren.

G. Der Datenschutzbeauftragte (Art. 37 bis 39 DSGVO) - Karin Knaf, Bayerische Staatsbibliothek, 22.02.2018

Die Verpflichtung zur **Benennung** eines Datenschutzbeauftragten, seine **Stellung** und seine **Aufgaben** regelt die DSGVO in den **Art. 37ff.** Im Erwägungsgrund 97 finden sich dazu ergänzende Ausführungen.

1. Benennung eines Datenschutzbeauftragten

Öffentliche Stellen haben nach Art. 37 Abs. 1 Buchst. a DSGVO jedenfalls einen Datenschutzbeauftragten zu benennen, soweit sie eine Verarbeitung von personenbezogenen Daten durchführen. Das wird in wissenschaftlichen Bibliotheken regelmäßig der Fall sein.

Neu ist, dass der Datenschutzbeauftragte einer öffentlichen Stelle nicht mehr zwingend ein Beschäftigter dieser Einrichtung sein muss (Art. 37 Abs. 6 DSGVO). Die Benennung des Datenschutzbeauftragten erfolgt auf Grundlage seiner Qualifikation und seines Fachwissens auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis sowie seiner Fähigkeit zur Erfüllung der Aufgaben nach Art. 39 DSGVO.

Wie bisher kann für mehrere Behörden und Dienststellen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe ein gemeinsamer Datenschutzbeauftragter benannt werden.

Als Neuerung sieht die DSGVO vor, dass der Verantwortliche bzw. Auftragsverarbeiter die Kontaktdaten des Datenschutzbeauftragten veröffentlichen muss und die Daten der Aufsichtsbehörde[44] mitzuteilen hat.

2. Stellung des Datenschutzbeauftragten

[44] Z.B. in Bayern für öffentliche Stellen dem Bay. Landesbeauftragten für den Datenschutz

Art. 38 DSGVO regelt die Stellung des Datenschutzbeauftragten. So ist der Datenschutzbeauftragte frühzeitig und ordnungsgemäß (Abs. 1) in alle mit der Verarbeitung der personenbezogenen Daten zusammenhängenden Fragen einzubinden. Er ist von der öffentlichen Stelle bei seinen Aufgaben zu unterstützen und es sind ihm die zur Aufgabenerfüllung erforderlichen Ressourcen (Sachmittel, Personal) zur Verfügung zu stellen.

Bei der Erfüllung seiner Aufgaben ist der Datenschutzbeauftragte grundsätzlich unabhängig von fachlichen Weisungen. Er darf auch nicht wegen der Erfüllung seiner Aufgaben abberufen oder benachteiligt werden. Dies wird in Art 38 Abs. 2 DSGVO klargestellt.

Betroffene Personen können sich zu allen im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten stehenden Fragen unmittelbar an den Datenschutzbeauftragten wenden. Dies wird in Abs. 4 klargestellt. Der Datenschutzbeauftragte selbst ist an die rechtlichen Vorgaben zur Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden (Abs. 5).

3. Aufgaben des Datenschutzbeauftragten

Art. 39 Abs. 1 DSGVO legt die gesetzlichen Mindestaufgaben des Datenschutzbeauftragten fest: Diese sind zunächst **Unterrichtung** und **Beratung** des Verantwortlichen und der Beschäftigten hinsichtlich der datenschutzrechtlichen Pflichten aber auch - jetzt neu – die **Überwachung der Einhaltung** der datenschutzrechtlichen Vorschriften. Dadurch erfährt die innerbehördliche Stellung des Datenschutzbeauftragten eine „**grundsätzliche Wesensveränderung**“[45].

Dennoch bleibt die Verantwortung für die Einhaltung des Datenschutzes weiterhin bei der Leitung der öffentlichen Stelle.

Dazu kommen noch die Beratung auf Anfrage im Zusammenhang mit der Datenschutz-Folgenabschätzung (Art. 35 DSGVO) und Überwachung der Durchführung sowie die Zusammenarbeit mit der Aufsichtsbehörde (Art. 39 Abs. 1 d) und e).

Das Führen des Verzeichnisses der Verarbeitungstätigkeiten (Art. 30 DSGVO) ist keine originäre Aufgabe des Datenschutzbeauftragten. Sie kann ihm aber nach Art. 38 Abs. 6 DSGVO übertragen werden; ein Konflikt mit den sonstigen Aufgaben ist nicht zu befürchten. [46]

Es ist davon auszugehen, dass bezüglich der behördlichen Datenschutzbeauftragten diverse **ergänzende landesrechtliche Bestimmungen** getroffen werden. Daher sind die jeweiligen an die Datenschutz-Grundverordnung angepassten Datenschutzgesetze der Länder abzuwarten und daraufhin zu prüfen. In Bayern ist eine solche Regelung zum behördlichen Datenschutzbeauftragten etwa im Art 12 BayDSG- E (Entwurfs des angepassten Bayerischen Datenschutzgesetzes) zu finden[47], wonach dem Datenschutzbeauftragten vor dem erstmaligen Einsatz oder einer wesentlichen Änderung automatisierter Verfahren Gelegenheit zur Stellungnahme zu geben ist.

---

[45] So der Bay. Landesbeauftragter für den Datenschutz https://www.datenschutz-bayern.de/datenschutzreform2018/ueberblick-4.html

[46] Wilde/Ehmann/Niese/Knoblauch, Datenschutz in Bayern, 26. AL, 10/2016, Erl. Zur DSGVO, Art. 39.

[47] LTDrs. 17/19628 vom 12.12.2017
https://www.datenschutzbayern.de/datenschutzreform2018/baydsg_neu_12_12_2017.pdf

H. Auftragsverarbeitung (Art. 28, 29 DSGVO)) - Karin Knaf, Bayerische Staatsbibliothek, 22.02.2018

Art. 28 DSGVO regelt die **Auftragsverarbeitung.** Die DSGVO hat den gewohnten Begriff „Auftragsdatenverarbeitung" damit durch den neuen Begriff „Auftragsverarbeitung" ersetzt. Dieser neue Begriff selbst führt dabei nicht zu veränderten Anforderungen.

Nach wie vor bleibt die Auftragsverarbeitung privilegiert, d.h. der Auftragsverarbeiter ist nicht „Dritter“ im Sinne des Datenschutzrechts mit der Folge, dass keine gesonderte Rechtsgrundlage für die Übermittlung von Daten an ihn erforderlich ist und keine Rechtmäßigkeitsprüfung nach Art. 6 DSGVO.

Positiv ist zu bewerten, dass es mit der Neuregelung zu einer Vereinheitlichung der Vorschriften der Auftragsverarbeitung kommt.

Die grundsätzlichen Verantwortlichkeiten zwischen Verantwortlichen und Auftragsverarbeiter sind klar geregelt: der Verantwortliche ist nach Art. 5 Abs. 2 DSGVO für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. Er ist auch Adressat der Betroffenenrechte und hat gegenüber dem Auftragsverarbeiter Weisungsbefugnis.

Zur Haftung ist festzustellen, dass grundsätzlich sowohl der Verantwortliche wie auch der Auftragsverarbeiter haften. Der Auftragsverarbeiter jedoch nur bei einem Verstoß gegen die ihm durch die DSGVO auferlegten Pflichten oder bei Nichtbeachtung einer Weisung.

Grundsätzlich soll durch die Vorschriften zur Auftragsverarbeitung gewährleistet werden, dass auch bei Einschaltung eines Auftragsverarbeiters (vgl. zum Begriff Art. 4 Nr. 8 DSGVO) der Schutz der betroffenen Personen nicht beeinträchtigt wird. Dazu werden dem Auftragsverarbeiter aber auch dem Auftraggeber verschiedene Pflichten auferlegt.

So ist etwa die sorgfältige Auswahl des Auftragsverarbeiters notwendig (Art. 28 Abs. 1 DSGVO), ebenso wie die Festlegung der gegenseitigen Rechte und Pflichten in einer Vereinbarung. Art. 28 Abs. 3 DSGVO sieht insoweit vor, dass die Verarbeitung auf der Basis eines Vertrags erfolgt, der den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festlegt. Die detailierten Regelungsgegenstände des Vertrags sowie die weiteren datenschutzrechtlichen Anforderungen sind ausführlich in Art. 28 Abs. 3 ff DSGVO und Art. 29 DSGVO vorgegeben.

In Anbetracht des Umfangs und der Komplexität der Regelungen ist jedenfalls ein schriftlicher Vertrag geboten, obgleich die Schriftform nur zur Regelung des Einsatzes eines Unter-Auftragsnehmers nach Art. 28 Abs. 2 DSGVO zwingend ist. Um die Anforderungen gesetzeskonform bewältigen zu können, ist zu empfehlen, die von den Aufsichtsbehörden zu dieser Thematik zu erwartenden Orientierungshilfen und Musterverträge zu nutzen.

Hinzuweisen ist darauf, dass für die nach altem Recht abgeschlossenen Verträge kein Bestandsschutz besteht! Das heißt, diese Verträge sind auf den Prüfstand zu stellen und den Erfordernissen des neuen Rechts anzupassen.

Für die **Auftragsverarbeitung in Drittstaaten** (d.h. Staaten außerhalb der Europäischen Union) sind unbedingt die **Art. 44-49 DSGVO** zu berücksichtigen. Eine Übermittlung von personenbezogenen Daten in ein Drittland oder eine internationale Organisation ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die für diese Datenübermittlung in der DSGVO festgelegten Bedingungen erfüllen und auch die sonstigen Bestimmungen der DSGVO eingehalten werden: das heißt, der Verantwortliche muss zunächst prüfen und sicherstellen, dass die allgemeinen Vorgaben der DSGVI eingehalten werden. Dann sind die Voraussetzungen der Art. 44 ff DSGVO zu prüfen.

Nach **Art. 45 DSGVO** ist demnach eine Übermittlung zulässig, wenn die Europäische Kommission entschieden hat, dass ein **angemessenes Schutzniveau** besteht. Liegt kein solcher **Angemessenheitsbeschluss** vor, darf der Verantwortliche oder Auftragsverarbeiter personenbezogene Daten in ein Drittland oder an eine internationale Organisation nur übermitteln, wenn die Voraussetzungen des **Art. 46 DSGVO** vorliegen, also sofern er geeignete Garantien vorgesehen hat und durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen: so etwa rechtlich bindende und durchsetzbare **Dokumente zwischen Behörden und öffentlichen Stellen** (Art. 46 Abs. 2a) DSGVO), unternehmensinterne Datenschutzvorschriften **(„Binding Corporate Rules"- BCRs** , vgl. Art. 47 DSGVO) oder **Standarddatenschutzklauseln (SCCs)**, die von der Kommission oder der Aufsichtsbehörde in einem bestimmten Verfahren angenommen werden (Art. 46 Abs. 2c) und d) DSGVO) sowie **genehmigte Verhaltensregeln (Codes of Conduct- CoC)** – Art. 46 Abs. 2e) DSGVO oder **Zertifizierungen** (Art. 46 Abs. 2f) DSGVO)

In Sonderfällen kann nach **Art. 49 DSGVO** eine Datenübermittlung erfolgen. Praxisrelevant z.B. beim Vorliegen einer **ausdrücklichen Einwilligung**, bei der die betroffene Person zuvor über die Risiken einer Datenübermittlung informiert worden sein muss (Art. 49 Abs. 1 a) DSGVO) oder wenn die Datenübermittlung zur **Erfüllung eines Vertrags** (Art. 49 Abs. 1 b) c) DSGVO) oder zur **Geltendmachung von Rechtsansprüchen** (Art. 49 Abs. 1 e) DSGVO) erforderlich ist.

Hinzuweisen ist noch auf **Art. 48 DSGVO**. Danach können Gerichtsurteile und behördliche Anordnungen von Drittstaaten, die eine Datenübermittlung in diese fordern, unbeschadet anderer Regelungen nur anerkannt und durchgesetzt werden, wenn sie auf einer internationalen Übereinkunft, wie einem Rechtshilfeabkommen, beruhen.

I. Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO)

Art 30 Abs. 1 DSGVO verpflichtet Unternehmen und Behörden zur Führung eines „Verzeichnisses von Verarbeitungstätigkeiten". Nach **Art. 30 Abs. 2 DSGVO** muss auch der Auftragsverarbeiter ein Verzeichnis führen.

Konkret ist das Verzeichnis von Verarbeitungstätigkeiten vom „Verantwortlichen" zu führen, also von der öffentlichen Stelle, die über die Verarbeitung entscheidet (Art. 4 Nr. 7 DSGVO).

Das Verzeichnis von Verarbeitungstätigkeiten ist daher nicht mehr - wie etwa bisher das Verfahrensverzeichnis nach Art. 26 Abs. 1 BayDSG – rechtlich zwingend vom behördlichen Datenschutzbeauftragten zu führen.

Der Behördenleiter kann aber die Führung dieses Verzeichnisses dem behördlichen Datenschutzbeauftragten nach Art. 38 Abs. 6 DSGVO behördenintern als besondere Aufgabe übertragen, da entgegenstehende Interessenskonflikte nicht erkennbar sind (vgl. oben).

Auch das vom Auftragsverarbeiter zu führende Verzeichnis kann so delegiert werden.

Neu ist, dass auch nicht automatisierte Verarbeitungstätigkeiten aufzunehmen sind (Art. 2 Abs. 1 DSGVO).

Das **Verzeichnis der Verarbeitungstätigkeiten** enthält nach Art. 30 Abs. 1 Satz 2 DSGVO folgende Angaben:

- den Namen und die Kontaktdaten des/der Verantwortlichen
  (Bezeichnung der Behörde/öffentlichen Stelle sowie ihre Postanschrift, E-Mail-Adresse und Telefonnummer) Sind mehrere Stellen für eine Verarbeitung verantwortlich, sind die Daten aller verantwortlichen zu nennen

- den Namen und die Kontaktdaten des Datenschutzbeauftragten
  (Familiennamen, dienstliche Postanschrift, E-Mail-Adresse und Telefonnummer)

- die Zwecke der Verarbeitung
  Regelmäßig wird der Zweck sich aus der Erfüllung der der Einrichtung zugewiesenen Aufgabe ergeben

- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten

- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen

- gegebenenfalls Angaben zu Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation. Im Falle einer Übermittlung an ein Drittland oder eine internationale Organisation nach Art. 49 Abs. 1 Unterabsatz 2 DSGVO sind die geeigneten Garantien, in Bezug auf den Schutz personenbezogener Daten festzuhalten - soweit erforderlich ist dazu auf ergänzende Dokumente zu verweisen;

- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;

- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Absatz 1 DSGVO.

Das **Verzeichnis des Auftragsverarbeiters** nach Art. 30 Abs. 2 DSGVO sieht eine neue Verpflichtung für die Auftragsverarbeiter vor. Sie müssen künftig ein „**Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung**“ mit folgenden Angaben führen:

- den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist
  Jeder Auftragsverarbeiter muss hier neben seinem eigenen Namen und seinen Kontaktdaten (s.o.) auch die Namen und Kontaktdaten aller öffentlichen Stellen und ggf. privater Unternehmen aufführen, in deren Auftrag personenbezogene Daten verarbeitet werden;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten (s.o.);
- die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden
- gegebenenfalls Angaben zu Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 DSGVO.

Die beiden Verzeichnisse können schriftlich oder elektronisch geführt werden (Art. 30 Abs. 3 DSGVO) und sind der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

Eine Veröffentlichung der Verzeichnisse ist von der DSGVO nicht mehr vorgesehen. Auch gibt es kein Recht auf Einsichtnahme in das Verzeichnis der Verarbeitungstätigkeiten (vgl Erwägungsgrund 82).

Auskunftsersuchen des Betroffenen, ob und ggf. welche Daten zu seiner Person von der Behörde oder öffentlichen Stelle verarbeitet werden, sind im Rahmen des Art. 15 DSGVO zu lösen.

Auskunftsersuchen über den Inhalt der Verzeichnisse richten sich nach den allgemeinen Informationszugangsrechten und den dort festgelegten Anspruchsgrundlagen.

Die Ausnahme von der Pflicht zur Führung der Verzeichnisse nach Art. 30 Abs. 5 DSGVO findet keine Anwendung für Behörden und öffentliche Stellen.

Hinsichtlich der Gestaltung der Verzeichnisse ist keine gesetzliche Vorgabe gegeben; es ist aber auch hier zu empfehlen die zu erwartenden Mustervorgaben der Aufsichtsbehörden zu berücksichtigen.

J. Einige Quellen:

- Überblick des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein
  https://www.datenschutzzentrum.de/dsgvo/

- Hinweise zum Verzeichnis von Verarbeitungstätigkeiten: https://www.datenschutzzentrum.de/uploads/dsgvo/Hinweise-zum-Verzeichnis-von-Verarbeitungstaetigkeiten.pdf
- Muster Verarbeitungsverzeichnis Auftragsverarbeiter: https://datenschutzzentrum.de/uploads/dsgvo/Muster-Verarbeitungsverzeichnis-Auftragsverarbeiter.pdf
- Muster Verarbeitungsverzeichnis Verantwortlicher: https://datenschutzzentrum.de/uploads/dsgvo/Muster-Verarbeitungsverzeichnis-Verantwortlicher.pdf
- Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) zu Informationspflichten bei Dritt- und Direkterhebung: https://www.lfd.niedersachsen.de/startseite/dsgvo/anwendung_dsgvo_kurzpapiere/ds-gvo--kurzpapiere-155196.html