Bundesministerium
des Innern, für Bau
und Heimat

Eine datenschutzrechtliche Einordnung von Portallösungen und Fachanwendungen in der OZG-Umsetzung

Berlin, den 15.01.2021

AG DV 1
DV1-17000/29#5

A. Vorbemerkungen

Zum Charakter und zur Entstehung des Papiers:

Dieses Papier ist ursprünglich als Handreichung für OZG-Projekte konzipiert worden und sollte eine Hilfestellung bei den durch die Projekte zu berücksichtigenden datenschutzrechtlichen Fragestellungen sowie insbesondere bei der Erarbeitung von Datenschutzkonzepten liefern[1]. Das Papier sollte sodann in einzelnen Umsetzungsprojekten erprobt und auf der Grundlage dieser Praxistests fortgeschrieben werden. Dabei sollten insbesondere auch die im Rahmen des Projektes BaföG digital gewonnenen Erfahrungen bei der rechtlichen Bewertung fixiert und für weitere Projekte nutzbar gemacht werden.

Durch folgende Festlegung der Datenschutzkonferenz vom XX.XX.2020 hat das Papier eine zusätzliche Stoßrichtung erhalten.

> *TOP 12 – Begleitung der Umsetzung des Onlinezugangsgesetzes durch die DSK*
>
> *1. Der AK Verwaltung berichtet mindestens zu den Hauptkonferenzen der DSK über wesentliche neue Entwicklungen der OZG-Umsetzung. Der Bericht kann schriftlich erfolgen.*
>
> *2. Der AK Verwaltung erarbeitet bis zum 1. Quartal 2021 ein Arbeitspapier, welches die Anforderungen an eine datenschutzrechtliche Dokumentation für eine vereinfachte Nachnutzbarkeit der Anwendungen aus dem OZG-Leistungskatalog darstellt. Der AK Verwaltung wird beauftragt, das Arbeitspapier nach Zustimmung durch die DSK den zuständigen Themenfeldinhabern zu übergeben.*
>
> *3. Der AK Verwaltung richtet eine UAG zur datenschutzrechtlichen Bewertung der OZG-Umsetzung von Portalen und auch Fachanwendungen ein, die die möglichen Konstellationen von Betreibermodellen in Bezug auf deren datenschutzrechtliche Verantwortlichkeit und Umsetzung prüft. Hierzu erfolgt auch ein stetiger Austausch mit der FITKO und dem BMI.*

Das vorliegende Papier ist vor diesem Hintergrund kurzfristig ergänzt worden, um für den vorgesehenen Austausch mit der FITKO und dem BMI einen geeigneten Rahmen vorzuschlagen.

---

[1] Die Erarbeitung wurde unterstützt durch die Rechtsanwaltskanzlei Redeker, Sellner, Dahs.

Diese Historie des Dokuments führt jedoch zugleich zu einer gewissen Hybridhaftigkeit der Darstellung, die in der weiteren Bearbeitung aber sicher geglättet werden kann.

Zur OZG-Umsetzung:

Auf Grundlage des Gesetzes zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (OZG) und des Digitalisierungsprogramms des IT-Planungsrates (IT-PR) haben sämtliche Behörden auf Bundes-, Landes- und kommunaler Ebene bis 2022 ihre Verwaltungsleistungen zu digitalisieren. Die unterschiedlichen Portallösungen und weiteren Angebote sind untereinander – unter der Überschrift der „Interoperabilität" – miteinander zu vernetzen.

Hierbei wird eine Vielzahl von personenbezogenen Daten verarbeitet. Für eine rechtskonforme Verarbeitung dieser Daten haben die jeweils Beteiligten frühzeitig den rechtmäßigen Umgang mit personenbezogenen Daten unter der Geltung der Datenschutzgrundverordnung[2], des BDSG, der Landesdatenschutzgesetze und etwaiger weiterer Fachgesetze zu prüfen.

Solche Prüfungen und Konzeptionen mögen bei bundes- und landeseigenen Projekten noch überschaubar sein. Komplex wird die Prüfung im föderalen Kontext bei der Beteiligung einer Vielzahl von Bundesländern – teilweise noch gemeinsam mit dem Bund: Insbesondere das Nachnutzungsmodell „Einer für Alle" (EfA), das die Umsetzung bzw. Nachnutzung der digitalen Lösung über die eigenen Ländergrenzen hinaus fördert, birgt daher besondere Herausforderungen, die länderübergreifende Herangehensweisen erfordern.

Mit der Zusammenarbeit zweier oder mehrerer Bundesländer müssen daher auch rechtliche Rahmenbedingungen, Verantwortlichkeiten sowie Aufgaben in Zusammenhang mit dem Thema Datenschutz beachtet werden, um den gesetzlichen Anforderungen zu entsprechen.

Die Digitalisierung von Verwaltungsleistungen bringt zudem in der Regel einen aufwändigen IT-Betrieb sowie eine langwierige Weiterentwicklung mit sich. Aufgrund der notwendigen IT-Dienstleistungen durch neue Technologien sowie Komplexität und Umfang der IT-Systeme werden immer häufiger externe Betreiber an der Digitalisierung beteiligt. Auch in diesem Kontext gilt es einen angemessenen Datenschutz für die zu digitalisierende Verwaltungsleistung zu gewährleisten. Es entspricht dem Grundsatz der DSGVO (Art. 25 DSGVO „Privacy by design

---

[2] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. L 119 vom 4. Mai 2016, S. 1 ff.

/ Privacy by default“), ganz am Anfang eines Projektes, wenn bestimmte technische und fachliche Fragen noch nicht final definiert sind, das Thema Datenschutz mitzudenken.

Für die Projekte gilt insoweit:

- einen eigenen projektbezogenen „Arbeitsstrang“ zu starten, der in den Digitalisierungsprojekten die datenschutzrechtlichen Zusammenhänge und das Thema Daten- und IT-Sicherheit von Anfang an mitdenkt und begleitet,

- den datenschutzbezogenen Sachverhalt frühzeitig zu eruieren, konkret also: Welche personenbezogenen Daten sind für das jeweilige Verwaltungsverfahren aus Fachsicht notwendig?

- die verschiedenen Verarbeitungsschritte zu definieren, also: Wann und zu welchem Zweck werden die personenbezogenen Daten der Antragsteller oder Dritter erhoben, gespeichert, abgefragt und verwendet, an Dritte (durch Übermittlung) offengelegt und gelöscht?

- die Beteiligten zu benennen, also: Wer kommt mit den Daten zu welchem Zeitpunkt und zu welchem Zweck in Berührung (Verantwortliche/Dienstleister/Dritte)?

Diese Handreichung liefert den verantwortlichen Mitarbeiterinnen und Mitarbeitern in den Behörden und den Projektbeteiligten einen kompakten und praxisnahen Überblick über die erforderlichen Datenschutzmaßnahmen, die speziell im Rahmen der länderübergreifenden Digitalisierung von Verwaltungsleistungen von Beginn an zu berücksichtigen sind. Die Handreichung soll zudem hinsichtlich der Umsetzung von technisch-organisatorischen Maßnahmen einen ersten Überblick und groben Leitfaden zur Durchführung beispielsweise der Schutzbedarfsfeststellung und Risikobewertung von Datenverarbeitungsvorgängen liefern. Das Standard-Datenschutzmodell (im Folgenden: SDM)[3] bietet darüber hinaus im Detail geeignete Mechanismen, um abstrakten rechtlichen Sicherheitsanforderungen der DSGVO konkret in technische und organisatorische Maßnahmen zu überführen.[4] Das Standard-Datenschutzmodell kann also vom

---

[3] Standard-Datenschutzmodell (SDM) der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) in der Version 2.0b, die am 17. April 2020 verabschiedet wurde.

[4] Vgl. SDM, Version 2.0b, S. 5f.

Verantwortlichen in einem zweiten Schritt ergänzend zu dieser Handreichung zwecks Konzeption und Umsetzung der technisch-organisatorischen Maßnahmen herangezogen werden.

Für die praktische Umsetzung stellen einige Datenschutzaufsichtsbehörden den Beteiligten zudem datenschutzrechtliche Mustervorlagen zur Verfügung, die indes nicht zwingend verwendet werden müssen (siehe zu einzelnen Vorlagen Abschnitt F.).[5] Ggf. bestehen landesrechtliche Besonderheiten. Dennoch mögen die Vorlagen dabei helfen, die erforderlichen Maßnahmen zu erläutern und passende Dokumente zu erstellen.

Alle Ausführungen erheben keinen Anspruch auf Vollständigkeit. Es bedarf in jedem Verwaltungsdigitalisierungsprojekt einer passgenauen Einzelfallprüfung. Die Ausführungen entstanden aus der Erfahrung in diversen Einzelfallprojekten und stehen noch unter dem Vorbehalt der Abstimmung mit der Datenschutzkonferenz bzw. weiteren Aufsichtsbehörden.

---

[5] Für die Bundesverwaltung ist zu beachten, dass eine Verpflichtung zur Verwendung der Mustervorlage des BfDI besteht: https://www.bfdi.bund.de/DE/Datenschutz/DatenschutzGVO/Aktuelles/Aktuelles_Artikel/Muster_Auftragsverarbeitung.html. Auf Landesebene stellt bspw. das LDA Bayern eine entsprechende Mustervorlage zur Verfügung: https://www.lda.bayern.de/media/muster_adv.pdf.

B. Abgrenzung und Einordnung von Grundbegriffen

Prüft man datenschutzrechtliche Zusammenhänge im Kontext der OZG-Umsetzung, kommt es auf die Verarbeitung personenbezogener Daten an. Diese beschränken sich grundsätzlich auf Informationen, die einen Bezug zu einer natürlichen Person haben können (Art. 4 Nr. 1 DSGVO). Nicht davon umfasst sind Betriebs- und Geschäftsgeheimnisse, sofern der Bezug auf eine solche natürliche Person ausgeschlossen ist.

Betriebs- und Geschäftsgeheimnisse sind eigens durch das Geschäftsgeheimnisgesetz[6] geschützt. Kommt es in digitalisierten Verwaltungsverfahren beispielsweise zu einer Offenlegung von Daten an eine breitere Öffentlichkeit, kann dieser Umstand zu einer Gefährdung von Geschäftsgeheimnissen führen. Durch eine Offenlegung steigt die Gefahr, dass diese Informationen in der Folge als „allgemein bekannt oder ohne Weiteres zugänglich" einzustufen und damit von vornherein nicht mehr als „Geschäftsgeheimnis" iSd GeschGehG einzuordnen sind. Es sollte also stets ein unkontrollierter Zugriff auf digitale Inhalte, die potentiell Geschäftsgeheimnisse enthalten, verhindert werden, damit die Daten nicht als allgemein zugänglich gelten.

Ferner sind im OZG-Kontext die technischen und organisatorischen Anforderungen der Datensicherheit zu erfüllen. Die Datensicherheit umfasst die Integrität, Vertraulichkeit und Verfügbarkeit von Daten allgemein (also auch von nicht-personenbezogenen Daten). Soweit es um die Sicherheit personenbezogener Daten geht, besteht eine Schnittmenge zum Datenschutz. Vorgaben zur Datensicherheit (insbesondere nach Art. 32 DSGVO) – sogenannte technische und organisatorische Maßnahmen oder „TOMs" - sind daher immer ein Teilaspekt einer datenschutzrechtlichen Planung, Umsetzungsbegleitung und Bewertung, der vor allem auch technische Expertise erfordert. Einzubinden in alle datenschutzbezogenen Projektphasen ist insoweit grundsätzlich auch immer technischer Sachverstand.

Spezielle Vorschriften zur Datensicherheit können sich (unabhängig vom Personenbezug der Daten) aus Gesetzen, beispielsweise aus dem BSI-Gesetz oder aus entsprechendem Landesrecht wie etwa dem Niedersächsischen Gesetz über Digitalisierung und Informationssicherheit in der Verwaltung ergeben.

Datenschutz und Datensicherheit überschneiden sich demnach, sind aber nicht deckungsgleich. So können sich aus datenschutzrechtlichen Erwägungen heraus Bedarfe nach besonderen

---

[6] Gesetz zum Schutz von Geschäftsgeheimnissen vom 18. April 2019 (BGBl. I S. 466).

Schutzmaßnahmen ergeben, die über die Schutzmaßnahmen, die die Informationssicherheit ermittelt hat, hinausgehen. Praktisch müssen daher von Beginn eines Projektes an regelmäßige Austausche zwischen dem Datenschutz- und dem IT-Sicherheitsteam erfolgen. Sicherheits- und Datenschutzkonzepte sind aufeinander abzustimmen.

Schließlich ist zu berücksichtigen, dass im Datenschutzrecht das Behördenprinzip gilt. (vgl. Art. 4 Nr. 7 3. Alt. DSGVO). Datenschutzrechtlich verantwortlich ist also nicht etwa die Bundesrepublik Deutschland, ein Bundesland oder ein Landkreis, sondern stets diejenige Behörde oder diejenigen Behörden, die über die Mittel und Zwecke der Datenverarbeitung entscheiden (hierzu sogleich noch ausführlich[7]).

Schließlich ist zu konstatieren, dass es bisher im OZG-Kontext keine einheitliche Terminologie zu den hier betrachteten Portallösungen gibt. Im Rahmen dieses Papiers soll daher zunächst ein Vorschlag zur Strukturierung dieser Diskussion gemacht werden. Dieser Vorschlag kann aber nur der Auftakt zu einer Abstimmung mit dem Ressortkreis und den Ländern sein, um zu einem tatsächlich einheitlichen Verständnis zu gelangen.

Aus Sicht des Bundesministeriums des Innern, für Bau und Heimat sind die folgenden Portalkonstellationen zu betrachten, wobei hier die relevante Datenverarbeitung erheblich variieren kann:

1. Fachunabhängige Portale eines Bundes oder Landes (z.B. Bundesportal, Serviceportal BW)

2. Fachspezifische Portale eines Bundes oder Landes (z.B. Elterngeld digital des BMFSFJ oder Rentenübersicht des BMAS)

3. Fachspezifische Portale unter Beteiligung mehrerer Länder (z.B. BaföG digital)

4. Fachspezifische Portale unter Beteiligung des Bundes und mindestens eines Landes (z.B. IfSG-Portal zur Geltendmachung von Schadensersatzansprüchen nach dem IfSG)

Wenn nachfolgend „übergreifende Portallösungen“ näher in den Blick genommen werden, sind damit fachspezifische Portale unter Beteiligung mehrerer Länder (siehe oben Ziffer 3) oder unter der zusätzlichen Beteiligung des Bundes (siehe oben Ziffer 4) gemeint. Das Zusammenspiel

---

[7] Siehe unter C. II.

der einzelnen Bundes- und Länderportale führt zum sogenannten Portalverbund. Je nach Konstellation ergeben sich unterschiedliche Konsequenzen für die Kompetenz- und Zuständigkeitsverteilung sowie für die datenschutzrechtliche Verantwortlichkeit.

C. Inhalte eines Datenschutzkonzepts

I. Anwendbare Rechtsvorschriften

Mit der Ermittlung der Beteiligten, die für die Frage nach der datenschutzrechtlichen Verantwortlichkeit von Bedeutung ist, ergibt sich der Anwendungsbereich der Datenschutzvorschriften. Bei einer automatisierten Verarbeitung personenbezogener Daten, die in einem Dateisystem verarbeitet sind oder verarbeitet werden sollen, ist die DSGVO nach Art. 2 Abs. 1 DSGVO sachlich anwendbar. Der räumliche Anwendungsbereich des Art. 3 Abs. 1 DSGVO ist bei öffentlichen Stellen des Bundes und der Länder als Verantwortliche für die Datenverarbeitung ebenfalls erfüllt. Ergänzend finden – als mitgliedstaatliche Ausgestaltung – das BDSG und die Landesdatenschutzgesetze Anwendung, was sich aus § 1 Abs. 1 Nr. 1, 2 BDSG ergibt. Danach findet das BDSG Anwendung bei der Verarbeitung personenbezogener Daten durch öffentliche Stellen des Bundes (Nr. 1) sowie für öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist (Nr. 2). Die Länder haben von ihrem diesbezüglichen Recht Gebrauch gemacht und Landesdatenschutzgesetze erlassen. Das heißt also: Bei EfA-Projekten und OZG-Umsetzungsprojekten auf Landesebene sind stets die jeweiligen Landesdatenschutzgesetze zu beachten.

Neben diesen allgemeinen Bestimmungen kann der bereichsspezifische Datenschutz relevant sein. Für den Sektor Telekommunikation enthält das Telekommunikationsgesetz (TKG) bereichsspezifische Datenschutzvorschriften. Solche sind auch im Telemediengesetz (TMG) enthalten.[8] In den verschiedenen Sozialgesetzbüchern[9] finden sich ebenfalls unterschiedliche datenschutzrechtliche Vorgaben.

Ferner hat besondere Relevanz, ob sensible schutzwürdige Daten Gegenstand der Verarbeitung sind, da für diese Kategorie besondere Vorschriften gelten (Art. 9 DSGVO). Schließlich ist zu fragen, aus welchen Kategorien von Betroffenen personenbezogene Daten verarbeitet werden: Sind beispielsweise Daten von Kindern oder anderen Dritten relevant? Werden ferner Daten

---

[8] Bestimmungen des TKG und des TMG, die auf die E-Privacy-Richtlinie zurückgehen, gelten neben der Datenschutz-Grundverordnung, vgl. Art. 95 DSGVO. Der „Entwurf einer Verordnung über Privatsphäre und elektronische Kommunikation“, E-Privacy-Verordnung, wird gegenwärtig noch beraten; die erforderlichen Trilog-Verhandlungen haben noch nicht begonnen. Mit Inkrafttreten der E-Privacy-Verordnung werden auf nationaler Ebene diejenigen Regelungen obsolet, die auf die E-Privacy-Richtlinie zurückgehen. Parallel gibt es seit dem 14.07.2020 einen Referentenentwurf des Bundeswirtschaftsministeriums für ein „Gesetz über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien“. Die Verarbeitung personenbezogener Daten in elektronischen Kommunikationsnetzen und bei der Nutzung von Telemedien ist daher mit besonderer Aufmerksamkeit zu prüfen.

[9] Vgl. bspw. zweites Kapitel des zehnten Sozialgesetzbuches, „Schutz der Sozialdaten“, §§ 67 ff. SGB X.

von Betroffenen verarbeitet, die nicht unmittelbar bei diesen erhoben wurden? Neben Auswirkungen auf die konkrete Rechtsgrundlage zur Verarbeitung dieser Daten sowie zu ausreichenden Informationen gegenüber den Betroffenen, haben diese Hintergründe besondere Auswirkung auf die Gewährleistung der Datensicherheit (Risikoanalyse, Schutzbedarfsfeststellung, Datenschutz-Folgenabschätzung).

II. Datenschutzrechtliche Verantwortlichkeit

Eine der zentralen datenschutzrechtlichen Fragen bei der OZG-Umsetzung ist die Prüfung der datenschutzrechtlichen Verantwortlichkeit der jeweiligen Behörde gemäß Art. 4 Nr. 7 DSGVO.[10] Verantwortlicher im datenschutzrechtlichen Sinne ist gemäß Art. 4 Nr. 7 DSGVO jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die über Mittel und Zwecke der Verarbeitung personenbezogener Daten bestimmt. Dabei sieht Art. 4 Nr. 7 DSGVO sowohl die alleinige als auch die gemeinsame Verantwortlichkeit mehrerer Stellen im Sinne eines *„zusammen mit“* als mögliche Konstellationen vor.

Bei EfA-Lösungen sind eine Vielzahl von landes- und kommunalen Behörden beteiligt, die über die Mittel und Zwecke der Datenverarbeitung entscheiden. Zwar kann auch hier die datenschutzrechtliche Verantwortlichkeit für eine Portallösung bei einer Stelle konzentriert sein; manches spricht aber auch für gemeinsame Verantwortlichkeiten gemäß Art. 26 DSGVO.

In jedem Fall sollte Klarheit über die Verteilung der datenschutzrechtlichen Verantwortlichkeit bestehen. An diese knüpft die DSGVO eine Reihe von Rechte und Pflichten. Auch die Zuständigkeit der Datenschutzaufsichtsbehörde hängt hiervon ab. Die Klärung ist mithin ein zentraler Schritt für die Umsetzung einer Portallösung.

Wer für eine Datenverarbeitung verantwortlich ist, lässt sich nach Art. 4 Nr. 7 DSGVO auf zwei Arten bestimmen: Nach dem ersten Halbsatz kommt es darauf an, wer praktisch und tatsächlich über die Mittel und Zwecke (allein oder gemeinsam) entscheidet (nachfolgend Abschnitt 1. und 2.). Über die gesetzlich vorgegebene Bestimmungsmöglichkeit hinaus kann in abzugrenzenden Fällen die Frage der Verantwortlichkeit auch individuell bestimmt werden. Dies erfolgt entweder explizit oder durch Festlegung abstrakter Kriterien. Auch dies kann zu einer deutlichen Vereinfachung in Projekten der Verwaltungsdigitalisierung führen (nachfolgend Abschnitt 3.).

---

[10] Die datenschutzrechtliche Verantwortlichkeit folgt bei staatlichen Stellen nicht dem Rechtsträger-, sondern dem Behördenprinzip.

1. Mittel und Zwecke der Verarbeitung (Art. 4 Nr. 7 1. HS DSGVO)

Die Beurteilung, wer über die Mittel und Zwecke der Datenverarbeitung bestimmt, orientiert sich stets an der tatsächlichen Verarbeitung. Konkret müssen also das geplante Mittel und die beabsichtigten Zwecke für die jeweiligen Akteure extrahiert werden, um auf diese Weise festzustellen, wer für welchen Verfahrensabschnitt über Mittel und Zwecke der Datenverarbeitung bestimmt. Der Zweck der Verarbeitung wird als „erwartetes Ergebnis, das beabsichtigt ist oder die geplanten Aktionen leitet" und das Mittel als die „Art und Weise, wie ein Ergebnis oder Ziel erreicht wird"[11] definiert. Mittel der Datenverarbeitung können dabei das zu konzipierende Antragsportal oder beispielsweise Fachverfahrensanwendungen auf nachgeordneter Behördenebene sein. Zwecke der Datenverarbeitung können verschiedenster Natur sein: Im Idealfall ergibt sich dieser aus konkreten gesetzlichen Anforderungen, wie es häufig auf Fachbehördenebene der Fall ist; für übergreifende Portallösungen kommt als Zweck aber auch die Schaffung einer möglichst sicheren, effizienten und benutzerfreundlichen Lösung in Betracht.

2. Gemeinsame Verantwortlichkeit

a) Abgrenzung zur alleinigen Verantwortlichkeit

Ergibt sich aus dem jeweiligen Projekt, dass über Mittel und Zwecke der Datenverarbeitung mehrere Akteure nebeneinander entscheiden, kommt eine gemeinsame Verantwortlichkeit in Betracht.

Die Beteiligung an den Entscheidungen einer gemeinsamen Datenverarbeitung kann verschiedene Formen aufweisen: Sie muss weder im Sinne einer gleichrangigen Verantwortlichkeit gleichmäßig verteilt, noch muss jeder Beteiligte mit gleichen Kontroll- und Zugangsrechten ausgestattet sein.[12] Voraussetzung ist jedoch stets, dass die Entscheidung über die Mittel und Zwecke der Datenverarbeitung *gemeinsam* getroffen wird und jeder Beteiligte einen bestimmenden Einfluss auf die Datenverarbeitung hat.[13] Ob dies in den OZG-Umsetzungsprojekten tatsächlich der Fall ist, hängt vom Einzelfall ab.

Abzugrenzen ist der Fall einer gemeinsamen Verantwortlichkeit von den – auch bei E-Government-Projekten durchaus relevanten – Konstellationen, dass eine verantwortliche Stelle die von ihr erhobenen Daten lediglich an eine weitere Stelle durch Übermittlung

---

[11] Art. 29 Datenschutzgruppe, WP 169, S. 16.
[12] *Böllhoff/Rataj*, WRP 2019, 1536, 1537; Kurzpapier DSK, S. 2ff.
[13] Kurzpapier DSK, S. 2ff.

offenlegt (Stichwort „Verarbeitungskette“). In diesem Fall ist hinsichtlich der weiteren Datenverarbeitung bei der empfangenden Stelle eine sequentielle abgestufte Verantwortlichkeit[14] gegeben, die keine gemeinsame Verantwortlichkeit begründet, sofern die einzelnen Datenverarbeitungsschritte klar voneinander zu trennen sind. Die Festlegung der Verantwortlichkeit ist aber eine Frage des Einzelfalls; insofern ist es denkbar, dass einzelne Datenverarbeitungsschritte einer gemeinsamen Verantwortlichkeit unterfallen. Bei einer sogenannten Verarbeitungskette trifft die Verantwortlichkeit jeweils nur denjenigen, der den jeweiligen Verarbeitungsschritt auch tatsächlich verantwortet. Bei den jeweiligen Verarbeitungsschritten handelt es sich somit um vor- und nachgelagerte Vorgänge.[15] Für eine solche nacheinander geschaltete Verantwortlichkeit kann auch die fachliche Zuständigkeit sprechen, die sich nach den jeweils zugrundeliegenden verwaltungsverfahrensrechtlichen Rechtsgrundlagen richtet. Zweck der Datenverarbeitung des jeweiligen Akteurs ist dann ausschließlich, die in seiner Zuständigkeit liegenden Aufgaben zu erfüllen. Hierzu kann auch die reine „Durchleitung“ eines Antrags an die zuständige Stelle gehören. Ein Beispiel einer solchen Kettenverantwortlichkeit ist die Umsetzung von BAföG-Digital: In diesem Digitalisierungsprojekt ist ein federführendes Ministerium allein für den Onlineantragsassistenten verantwortlich; ab der Übermittlung der Antragsdaten an die zuständigen BAföG-Ämter der Bundesländer sind diese in der Verarbeitungskette für die Bearbeitung des Antrags datenschutzrechtliche Verantwortliche. Vorrangiger Bewertungsmaßstab bleibt in diesem Zusammenhang aber stets Art. 4 Nr. 7 DSGVO, der auf die tatsächlichen Verhältnisse bei der Datenverarbeitung abstellt.

Kommt der datenschutzrechtlich Verantwortliche zu dem Ergebnis, dass eine getrennte Verantwortung im Sinne einer Verarbeitungskette vorliegt, sind diese getrennten Verantwortungsbereiche im Datenschutzkonzept darzulegen. Kommt man zu einer gemeinsamen Verantwortlichkeit, so müssen die jeweiligen Einflussmöglichkeiten aller beteiligten Stellen auf die Zwecke und Mittel der Verarbeitung in einer Vereinbarung nach Art. 26 Abs. 1 DSGVO festgelegt werden.

b) Verantwortlichkeit bei gemeinsamer Nutzung von Hard- und Software[16]

Ein besonderes Augenmerk verdient die Situation, in der bei Kettenverantwortlichkeiten beide Verantwortliche für ihren jeweiligen Teil der Datenverarbeitung dieselben Systeme

---

[14] *Böllhoff/Rataj*, WRP 2019, 1536, 1537.
[15] *Böllhoff/Rataj*, WRP 2019, 1536, 1537.
[16] Es ist hierzu weiterführend auf den Baustein „Trennen“ des Standard-Datenschutzmodells zu verwiesen: https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Trennen_V1.0.pdf.

– oftmals eines einheitlichen IT-Dienstleiters – nutzen möchten. Relevant wird hierbei insoweit die Mandantentrennung, also die IT-basierte Trennung der Datenverarbeitungen je nach eigenständig Verantwortlichem. „Mandant“ meint den abgeschlossenen Datenhaltungs- und Verarbeitungskontext einer im datenschutzrechtlichen Sinne verantwortlichen Stelle.

Die Prüfung einer ausreichenden Trennung erfordert die Betrachtung der „Abgeschlossenheit“ der Datenverarbeitung innerhalb eines Mandanten – oftmals also innerhalb einer zuständigen Behörde, die die Datenverarbeitungen für sich alleine verantwortet. Eine ausreichende Trennung der Datenverarbeitung verhindert, dass Datenschutzprobleme oder -vorfälle eines Mandanten zu einer Gefährdung anderer Mandanten führen (sog. sicherheitstechnische Isolation). Weiter setzt eine ausreichende Mandantentrennung voraus, dass die Zugriffsberechtigungen die Verarbeitungsfunktionen und die Konfigurationseinstellungen je Mandant eigenständig festgelegt werden können. Deshalb ist je nach Verantwortlichkeit mindestens Folgendes vorzusehen:

- Getrenntes, mandantenspezifisches System zur Berechtigungsvergabe
- Konfigurationsmöglichkeiten für die Nutzungsprotokollierung
- Administrative, nach einzelnen Mandanten aufgeschlüsselte Protokollierung

Bei mandantenübergreifenden Funktionen zur Verwaltung der Mandanten und der gemeinsam genutzten Infrastruktur dürfen diese grundsätzlich *nicht* die Verarbeitung personenbezogener Daten innerhalb eines Mandanten ermöglichen.

Zudem müssen mandantenübergreifende Funktionen einem Management unterliegen. Dies bedeutet konkret:

- Definition eines differenzierten Administrationskonzepts
- Revisionssichere Protokollierung der administrativen Tätigkeiten
- Festlegung eines Protokollierungskonzepts
- Definition eines mandantenspezifischen und mandantenübergreifenden Berichtswesens
- Definition von Revisionen über das Gesamtsystem

c) Besonderheit bei EfA-Projekten

Gerade bei EfA-Projekten, in denen ein Bundesland – unter zentraler Nutzung und Beauftragung eines IT-Dienstleisters – ein digitalisiertes Verwaltungsverfahren für eine Vielzahl anderer Bundesländer und Kommunen konzipiert, könnte das Zusammenwirken des federführenden Bundeslandes bzw. der federführenden Landesbehörde mit den zuständigen Stellen der nachnutzenden Bundesländer für eine gemeinsame Verantwortlichkeit sprechen. Auch hier ist indes strikt zu prüfen, ob die Vielzahl dieser Stellen wirklich gemeinsam über die Mittel und Zwecke der Datenverarbeitung entscheiden.

Als solcher gemeinsamer übergeordneter Zweck – und ein solcher abstrakter gemeinsamer Zweck des gegenseitigen Förderns ist nach der EuGH-Rechtsprechung im Sinne des Art. 4 Nr. 7 DSGVO ausreichend – kommt die im Interesse aller Bundesländer liegende Digitalisierung der Verwaltungsleistungen zur Erfüllung der Verpflichtung nach § 1 OZG in Betracht.

Allerdings muss auch bei der Betrachtung dieser Konstellation das datenschutzrechtliche Behördenprinzip strikt beachtet werden. In jedem Einzelprojekt muss also geprüft werden, inwiefern einzelne Landesbehörden Systeme nutzen, die von anderen Landesbehörden getrennt verantwortet werden. Es ist in diesem Fall nicht immer und nicht grundsätzlich von einer gemeinsamen Verantwortlichkeit auszugehen; auch Kettenverantwortlichkeiten kommen in Betracht.

d) Praktische Konsequenzen

Kommt man zu einer getrennten Verantwortlichkeit im Sinne einer Verarbeitungskette, bei dem sämtliche Verarbeitungsschritte klar voneinander getrennt sind und die zuständigen Stellen stets nacheinander tätig werden, ist jede Weiterleitung personenbezogener Daten an den jeweiligen Verantwortlichen als Offenlegung durch Übermittlung zu klassifizieren. Diese Datenverarbeitungsvorgänge müssen jeweils auf eine eigene Rechtsgrundlage gestützt werden. Sofern über ein Portal auch eine elektronische Bescheidbekanntgabe geplant ist, müssen verwaltungsrechtliche Fragen zur Bekanntgabe von Verwaltungsakten auf elektronischem Wege mitbedacht werden.

Geht man von einer gemeinsamen Verantwortlichkeit aus, müssen aufgrund des datenschutzrechtlichen Behördenprinzips Vereinbarungen im Sinne von Art. 26 Abs. 1 DSGVO jeweils zwischen den datenschutzrechtlich gemeinsam verantwortlichen Behör-

den (i.d.R. die an einem Verwaltungsverfahren beteiligten Fachbehörden) getroffen werden. In der Konsequenz wäre dann auch eine Vielzahl von Landesdatenschutzbeauftragten für die Kontrolle und Aufsicht zuständig.

In praktischer Hinsicht führen solche Konstellationen zu erheblichen Umsetzungsaufwänden, da die Integration aller Landes- und Bundesportale zu einer weitläufigen Verzahnung und in der Folge weitreichenden Haftungsfragen führt und die gemeinsame Verantwortlichkeit eine gesamtschuldnerische Haftung mehrerer hundert Stellen in unterschiedlichen Bundesländern begründen würde. Die Prüfung, ob eine gemeinsamen Verantwortlichkeit plausibel abgelehnt werden kann, ist aus Praktikabilitätsgründen also lohnenswert. Entscheidend sind jedoch jeweils die tatsächlichen Verhältnisse. Teilweise wird man die Annahme einer gemeinsamen Verantwortlichkeit nicht vermeiden können.

Festlegung der Verantwortlichkeit nach Art. 4 Nr. 7 2. HS DSGVO

Möglich ist auch, dass die Beteiligten auf Bundes-, Landes und kommunaler Ebene die Frage der datenschutzrechtlichen Verantwortlichkeit eigens festlegen. Gemäß Art. 4 Nr. 7 2. HS DSGVO kann, sofern bereits Mittel und Zwecke der Datenverarbeitung im Recht der Mitgliedsstaaten festgelegt wurden, der Verantwortliche für diese Datenverarbeitung individuell festgelegt werden. Dabei legt Art. 4 Nr. 7 1. HS DSGVO die Grenzen des rechtlich Zulässigen fest: Eine Stellung als Verantwortlicher darf nicht entgegen der tatsächlichen Einflussnahmemöglichkeiten begründet werden.[17]

Konkret kann dies für Verwaltungsdigitalisierungsprojekte durch (formelles) Gesetz oder Verordnung (Gesetz im materiellen, aber nicht im formellen Sinn) erfolgen. Ein Beispiel für eine Festlegung der Verantwortlichkeit durch formelles Gesetz im Sinne von Art. 4 Nr. 7 2. HS DSGVO findet sich in etwa in § 6 Abs. 1 Datenschutz-Grundverordnungs-Ausfüllungsgesetz Sachsen-Anhalt (DSAG LSA). Die Norm legt abstrakte Kriterien fest, welche Stelle für Übermittlungen von Daten verantwortlich ist.

Fehlt ein solch formelles Gesetz und erscheint es gleichwohl geboten, aufgrund hohem Zeitdruck und für eine zeitlich überschaubare Übergangszeit eine Regelung zur datenschutzrechtlichen Verantwortlichkeit zu treffen, so kommt ausnahmsweise im Einzelfall auch der Erlass einer Verwaltungsvorschrift in Betracht. Zwar fallen unter den Begriff „Recht der Mitgliedstaaten“ i.S. des Art. 4 Nr. 7 2. HS DSGVO in erster Linie Gesetze

[17] *Petri*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 7 Rn. 26.

im formellen oder zumindest materiellen Sinn[18] und kein reines Innenrecht (wie etwa derartige Verwaltungsvorschriften). Jedoch könnte der Rückgriff auf eine Verwaltungsvorschrift für eine Übergangszeit ausnahmsweise unter dem Gesichtspunkt hingenommen werden, dass Verwaltungsvorschriften zumindest innerhalb der öffentlichen Verwaltung rechtlich bindend sind und somit für die entsprechende Stelle verpflichtend.[19] Zudem folgt auch aus datenschutzrechtlicher Perspektive kein Minus im Betroffenenschutz, da für die betroffene Person nicht die Rechtsnatur des Festlegungsaktes von Bedeutung ist, sondern die effektive Wahrnehmung ihrer Rechte. Dafür ist aber eine klare Verantwortungszuteilung grundsätzlich eher von Vor- als von Nachteil.

Voraussetzung für den Erlass einer solchen Verwaltungsvorschrift wäre, dass der datenverarbeitenden Stelle vom nationalen Gesetzgeber bzw. dem Verordnungsgeber eine derartige Befugnis mittels Gesetz oder RVO zugewiesen werden könnte.[20] In der betreffenden Verantwortlichkeitsregelung (per Gesetz oder Rechtsverordnung oder ausnahmsweise übergangsweise auch per Verwaltungsvorschrift) müssen dann zunächst Zwecke und Mittel des Datenverarbeitungsvorgangs festgelegt werden.[21] Ist dies geschehen, kann darüber hinaus entweder der Verantwortliche konkret und explizit bezeichnet werden oder aber weitere (abstrakte) Kriterien benannt werden, die den Verantwortlichen näher bestimmen. Eine solche abstrakte Festlegung kann etwa darin bestehen, zu bestimmen, dass die stets nach Fachrecht zuständige Behörde Verantwortlicher im datenschutzrechtlichen Sinne sein soll.[22]

3. Verantwortlichkeit und verfassungsrechtliche Anforderungen

Sollen Verwaltungsleistungen bundesweit digital angeboten werden, so findet sich in Portalprojekten häufig die Konstellation, dass über ein zentrales (Bundes-)Portal die Antragstellung durch *einen* Antragsassistenten ermöglicht werden soll, der die Anträge dann an die entsprechenden Fachstellen in den Bundesländern in ein Fachverfahren weiterleitet. Rechtsgrundlagen für diese Datenverarbeitung durch unterschiedliche öffentliche Stellen finden sich in den Fachgesetzen meistens *nur* für die konkrete Datenverarbeitung in den fachspezifischen Verfahren.

---

[18] *Taeger*, in: Gabel/Taeger, 3. Aufl. 2019, DSGVO Art. 6 Rn. 66; Beispiel für Regelungen im Sinne des Art. 4 Nr. 7 2. HS DSGVO finden sich in den Datenschutzgesetzen der Bundesländer, so z.B. § 8 Abs. 1 DSG NRW oder § 7 Abs. 4 DSG Sachsen-Anhalt.

[19] Vgl. dazu *Reimer*, in: Sydow, Europäische Datenschutzgrundverordnung, DSGVO Art. 6, Rn. 24; *Hartung*, in: Kühling/Buchner, 2. Aufl. 2018, DSGVO Art. 4 Nr. 7 Rn. 14.

[20] *Hartung*, in: Kühling/Buchner, 2. Aufl. 2018, DSGVO Art. 4 Nr. 7 Rn. 14.

[21] *Sydow,* Europäische Datenschutzgrundverordnung, DSGVO Art. 4 Rn. 138.

[22] *Sydow*, Europäische Datenschutzgrundverordnung, DSGVO Art. 4 Rn. 141; inhaltlich genauso *Dalby*, in: Spindler/Schuster/Spindler, 4. Aufl. 2019, DSGVO Art. 4 Rn. 18.

Die Datenverarbeitung, die im Rahmen der Antragsassistenz eines bundeslandübergreifenden Antragsportals stattfindet, kann sich häufig nicht auf eine spezifische Rechtsgrundlage stützen, da es sich dabei um eine *zusätzliche* Datenverarbeitung handelt, die über die eigentlich erforderliche Datenverarbeitung für das Fachverfahren zur Abwicklung der Verwaltungsleistung hinausgeht. Es bedarf dafür einer eigenen Rechtsgrundlage. Um den – insbesondere vom BVerfG entwickelten recht hohen Anforderungen – an eine wirksame Datenverarbeitungsnorm zu genügen, bedarf es daher grundsätzlich der Schaffung einer (spezialgesetzlichen) Verarbeitungsnorm in dem jeweiligen Fachgesetz. Als Öffnungsklausel für eine solche mitgliedstaatliche Norm kommt dabei insbesondere Art. 6 Abs. 1 lit. e DSGVO in Betracht. Um dem verfassungsrechtlichen Bestimmtheits- und Verhältnismäßigkeitsgrundsatz zu genügen, können Datenverarbeitungen nur ganz ausnahmsweise auf Art. 6 Abs. 1 lit. e DSGVO i.V.m. den – als Auffangnormen konzipierten und naturgemäß sehr allgemein gehaltenen – Generalklauseln des BDSG (§ 3 bzw. § 22 BDSG) bzw. der Landesdatenschutzgesetze gestützt werden. Denkbar ist dies insbesondere dann, wenn eine besondere Eilbedürftigkeit besteht und insbesondere für pilothafte Anwendungen nur eine kurze, zeitlich sehr überschaubare Übergangszeit bis zum Inkrafttreten der spezialgesetzlichen Verarbeitungsnorm überbrückt werden soll und zudem die Datenverarbeitung wenig grundrechtsintensiv erscheint, also nur eine sehr geringe Eingriffsintensität aufweist.

III. Auftragsverarbeitung

Eng im Zusammenhang mit der Festlegung der Verantwortlichkeit und der Verteilung der Rollen in Verwaltungsdigitalisierungsprojekten steht die Frage der Auftragsverarbeitung.

1. Grundkonstellation nach Art. 28 Abs. 3 DSGVO

Die DSGVO verpflichtet den Verantwortlichen nicht, die gesamte Datenverarbeitung auch praktisch selbst zu bewerkstelligen. Vielmehr erlaubt sie explizit, dass der Verantwortliche Auftragsverarbeiter einsetzt, die personenbezogene Daten in seinem Auftrag und streng weisungsgebunden *für* den Verantwortlichen verarbeiten. Dabei wird es sich häufig um IT-Dienstleister handeln, die etwa Server zur Verfügung stellen und die konkrete technische Umsetzung eines größeren Digitalisierungsprojekts übernehmen. Da es sich bei dem Auftragsverarbeiter nicht um einen weiteren Verantwortlichen handelt, sondern um einen weisungsgebundenen Auftragnehmer, der im Interesse des Verantwortlichen tätig wird, bedarf es für eine Offenlegung personenbezogener Daten durch den Verantwortlichen an den Auftragsverarbeiter keiner eigenen Rechtsgrundlage mehr.

Um einen Auftragsverarbeiter einzusetzen, müssen gemäß Art. 28 Abs. 3 DSGVO eine Reihe von Anforderungen vertraglich oder durch ein „anderes Rechtsinstrument“ festgelegt werden.

Im Einzelnen fallen unter diese Anforderungen die Bindung des Auftragsverarbeiters an den Verantwortlichen, die Festlegung von Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der Pflichten und Rechte des Verantwortlichen sowie auch das Tätigwerden des Auftragsverarbeiters ausschließlich auf dokumentierte Weisung des Verantwortlichen hin.

Der Vertrag oder das andere Rechtsinstrument unterliegen wie auch die Datenverarbeitung durch den Verantwortlichen selbst der Kontrolle durch die Aufsichtsbehörde (Art. 57 Abs. 1 lit. a, 58 Abs. 1 lit. a DSGVO).

2. Einsatz von Unterauftragnehmern

Auch der Auftragsverarbeiter hat seinerseits das Recht – mit vorheriger Genehmigung des Verantwortlichen – einen weiteren Unterauftragsverarbeiter einzusetzen. Das Verhältnis zwischen Auftragsverarbeiter und Unterauftragnehmer muss ebenfalls durch einen Vertrag oder ein anderes Rechtsinstrument näher festgelegt werden. Insbesondere müssen dem Unterauftragsverarbeiter in diesem Rechtsinstrument oder Vertrag dieselben Datenschutzpflichten auferlegt werden, die in dem Vertrag zwischen Verantwortlichem und Auftragsverarbeiter bereits festgelegt wurden. Der Auftragsverarbeiter haftet für Fehler des Unterauftragnehmers gegenüber dem Verantwortlichen.

3. Regelung und Inhalt einer Auftragsverarbeitungsvereinbarung durch Vertrag

Die geläufigste Variante der Auftragsverarbeitung erfolgt durch schriftlichen Vertrag zwischen dem Auftragsverarbeiter und dem Verantwortlichen, meist als Anhang zu einem Hauptvertrag, der eine konkrete Leistungsbeschreibung enthält. Zwingend ist ein solches „Bezugsdokument“ jedoch nicht. Gibt es keinen Hauptvertrag zwischen Verantwortlichem und Auftragsverarbeiter, sind Bezugnahmen im Auftragsverarbeitungsvertrag nicht möglich. Die Regelungen sind dann entsprechend umfangreicher zu gestalten.

In diesem Vertrag müssen die Anforderungen des Art. 28 Abs. 3 DSGVO beachtet werden. Es bietet sich an, in dem Vertrag nur abstrakte Hauptpflichten festzulegen und beispielsweise die Kategorien betroffener Personen sowie Art und Zweck der Verarbeitung in Anlagen zu diesem Vertrag festzulegen. So besteht die Möglichkeit, flexibler auf Anpassungen der Datenverarbeitung durch den Verantwortlichen und in der Folge auch durch den Auftragsverarbeiter zu reagieren. Bei einer Vielzahl an Projektbeteiligten kann eine solche Anpassung schnell zu einem großen organisatorischen Aufwand führen, da unter Umständen eine große Menge an Auftragsverarbeitungsverträgen geändert und erneut unterschrieben werden müssten.

4. Auftragsverarbeitung bei EfA-Projekten

Bei EfA-Projekten nutzen, wie bereits dargestellt[23], weitere Bundesländer und/oder Kommunen eine durch ein Bundesland entwickelte und bereitgestellte Digitalisierungslösung nach.

a) Vielzahl von AV-Vereinbarungen bei EfA-Projekten?

Damit die Auftragsverarbeitungssituation nicht dazu führt, dass die an sich ressourcenschonende EfA-Strategie in ihr Gegenteil verkehrt wird, werden im Folgenden mit Blick auf die zweite Variante des Art. 28 Abs. 3 S. 1 DSGVO – die- Regelung der Auftragsverarbeitung durch ein anderes Rechtsinstrument – verschiedene Lösungswege aufgezeigt.

aa) Vertretungsweise AV-Vereinbarung

Grundsätzlich ist es möglich, Auftragsverarbeitungsvereinbarungen „in Vertretung“ abzuschließen. Dies entspricht der in unionsrechtlichen Zusammenhängen bei der Einschaltung von Auftragsverarbeitungen oftmals relevanten Übung, Standardvertragsklauseln der Europäischen Kommission „on behalf of“ zu unterzeichnen. Es kommt dann nur zu einem einmaligen Vertragsschluss, der für eine Vielzahl von Beteiligten gilt.

Dies wird auch – je nach landesrechtlichen Besonderheiten – in den Fällen zulässig sein, in denen etwa ein Landesministerium in Vertretung für eine Vielzahl von im Land relevanten datenschutzrechtlich verantwortlichen Stellen eine Auftragsverarbeitungsvereinbarung mit einem IT-Dienstleister abschließt. Dieser Lösungsweg sollte jedenfalls dann geprüft werden, wenn es sich bei dem IT-Dienstleister um ein privatwirtschaftliches Unternehmen handelt. In den Fällen, in denen IT-Betriebe eingesetzt werden, die unter den Geltungsbereich eines Erlasses oder einer Rechtsverordnung fallen können, sind die nachstehenden Lösungsmöglichkeiten relevant.

bb) Regelung durch Rechtsverordnung

Nach Art. 28 Abs. 3 DSGVO kann die Verarbeitung von Daten durch einen Auftragsverarbeiter auch auf der Grundlage eines anderen Rechtsinstruments nach dem

[23] Siehe bei C. II. 2. c).

Recht der Mitgliedstaaten erfolgen. Damit eröffnet die DSGVO den verantwortlichen Stellen in den Mitgliedstaaten einen Spielraum hinsichtlich des instrumentellen „Wie“, d.h. der konkreten Wahl des Rechtsinstruments, nicht jedoch hinsichtlich des inhaltlichen „Ob“ der Auftragsverarbeitung.[24]

Da unter den Betriff „Recht der Mitgliedstaaten“ vor allem Gesetze im formellen oder zumindest im materiellen Sinn fallen (s.o.), kann eine solche Auftragsverarbeitung durch (formelles) Gesetz sowie im Einzelfall auch durch Rechtsverordnung – sofern eine Verordnungsermächtigung nach den Anforderungen das Art. 80 Abs. 1 GG gesetzlich vorgesehen ist – geregelt werden. Ausnahmsweise und für eine bloße Übergangszeit (s.o.) könnte eine Auftragsverarbeitung auch durch Verwaltungsvorschrift geregelt werden. Handelt es sich nicht um ein zeitlich besonders eiliges Digitalisierungsprojekt, so besteht ggf. die Möglichkeit, zunächst eine entsprechende Verordnungsermächtigung zu schaffen. So oder so muss in inhaltlicher Hinsicht die zu erlassende Rechtsverordnung die gleichen Voraussetzungen im Sinne des Art. 28 Abs. 3 DSGVO erfüllen wie eine vertragliche Regelung. Dazu zählen insbesondere folgende Einzelheiten:[25]

- Das Rechtsinstrument muss gegenüber dem Auftragsverarbeiter und der verantwortlichen Stelle verbindlich sein.[26] Der Auftragsverarbeiter muss dabei konkret benannt werden, damit er nach der gesetzlichen Vorgabe an den Verantwortlichen gebunden wird.

- Für die Benennung des Verantwortlichen ist es ausreichend, dass die „bestimmten Kriterien seiner Benennung“ nach dem Recht der Mitgliedstaaten vorgesehen werden, vgl. Art. 4 Nr. 7 2. HS DSGVO.

- Weiterhin müssen die Rechte und Pflichten des Verantwortlichen festgelegt werden.

---

[24] Kühling/Martini et al., Die DSGVO und das nationale Recht, 2016, S. 80.

[25] *Spiecker gen. Döhmann*, in: Simitis/Hornung, Datenschutzrecht, DSGVO Art. 28 Rn. 48; *Hartung*, in: Kühling/Buchner, 2. Aufl. 2018, DSGVO Art. 28 Rn. 63.

[26] *Klug,* in: Gola DSGVO/, 2. Aufl. 2018 Rn. 7, DSGVO Art. 28 Rn. 7.

- Schließlich muss die Auftragsverarbeitung verbindlich angeordnet werden,[27] da die Parteien nach der DSGVO zwar zwischen der Form eines Vertrags oder eines anderen Rechtsinstruments wählen können, nicht jedoch frei sind, die Rechtsbeziehung zu einem Auftragsverarbeiter *gar nicht* zu regeln.[28]

Beispiele einer Regelung der Auftragsverarbeitung durch Rechtsverordnung gibt es, soweit ersichtlich, bisher nicht. Sehr wohl hat der Gesetzgeber vereinzelt die Auftragsverarbeitung und das Weisungsrecht verbindlich im Gesetz geregelt, vgl. § 2 Abs. 5 BKAG und § 1 Abs. 1 S. 2 AZR-Gesetz. Indes fehlen in diesen Normen die weiteren Voraussetzungen des Art. 28 Abs. 3 DSGVO, sodass in diesen Fällen für eine wirksame Auftragsverarbeitung weitere Vereinbarungen zwischen den beteiligten Stellen geschlossen werden müssen.[29]

cc) Regelung durch Verwaltungsvorschrift

Auch eine Regelung durch Verwaltungsvorschrift ist unter den obigen Voraussetzungen grundsätzlich möglich. Das gilt insbesondere für die nähere Ausgestaltung der – gesetzlich vorgesehenen – Auftragsdatenverarbeitung durch Vereinbarung. Der Abschluss einer Auftragsverarbeitung unterfällt nicht dem Vorbehalt des Gesetzes, da das Rechtsverhältnis Verantwortlicher-Auftragsverarbeiter für sich noch keine Grundrechtsbeeinträchtigung darstellt, sondern allein der internen Funktionszuweisung dient. Der Verantwortliche bleibt den Rechten der betroffenen Personen uneingeschränkt verpflichtet, sodass sich eine Auftragsverarbeitung nicht nachteilhaft für sie auswirkt.

Voraussetzung ist allerdings, dass die Verwaltungsvorschrift sowohl den Auftragsverarbeiter als auch den Verantwortlichen bindet. Das führt dazu, dass eine solche Verwaltungsvorschrift nur die Stellen binden kann, die innerhalb der öffentlichen Verwaltung stehen, also keine Privaten sind. Diese Regelung funktioniert also nur bei IT-Dienstleistern als Landesbetriebe.

---

[27] Zu der im Wortlaut entsprechenden Regelung in § 62 BDSG: *Schwichtenberg*, in: Kühling/Buchner, 2. Aufl. 2018, BDSG § 62 Rn. 5, *Scheurer*, in: Gola/Heckmann/Paschke, 13. Aufl. 2019, BDSG § 62 Rn. 23; *Spoerr*, in: BeckOK DatenschutzR, 32. Ed. 1.5.2020, BDSG § 62 Rn. 37.

[28] Kühling/Martini et al., Die DSGVO und das nationale Recht, 2016, S. 80.

[29] *Martini*, in: Paal/Pauly, 2. Aufl. 2018, DSGVO Art. 28 Rn. 25, 26.

Da es sich bei Landesbetrieben um Teile der Landesverwaltung handelt, unterstehen sie der Dienst- und Fachaufsicht des zuständigen Ministeriums. Die Befugnis zum Erlass gegenüber nachgeordneten Stellen verbindlicher Verwaltungsvorschriften ergibt sich aus der Leitungs- und Weisungskompetenz der jeweils übergeordneten Verwaltungsstelle.[30] Verwaltungsvorschriften binden Landesbetriebe mithin unmittelbar.

Wie dargestellt muss durch die Verwaltungsvorschrift aber auch eine Bindungswirkung gegenüber den verantwortlichen Stellen eintreten. Verantwortliche Stellen, die privatrechtlich organisiert sind, können nicht gebunden werden. Hier bietet es sich an, weiterhin Auftragsverarbeitungsvereinbarungen als Vertrag zu schließen.

Einer gesonderten Betrachtung bedürfen ggf. Fachverfahren, die durch Kommunen durchgeführt werden.

IV. Datenverarbeitungsschritte in einer Portallösung

Stehen Verantwortlichkeiten und Auftragsverarbeitungsverhältnisse fest, sind gedanklich die verschiedenen Verarbeitungsschritte innerhalb einer Portallösung zu durchdenken. Im Folgenden sollen typische Datenverarbeitungsschritte skizziert werden, die häufig in bundeslandübergreifenden, aber auch spezifischen Portalprojekten ablaufen[31]. Eine Orientierung an diesen Schritten hilft, bei der Erstellung des Datenschutzkonzeptes und der Datenschutzinformationen für eine Webseite etwa hinreichend zu differenzieren und sich hinsichtlich des jeweiligen Datenverarbeitungsschrittes über die Rechtsgrundlage Gedanken zu machen.

Für die Zwecke dieser Darstellung sind zunächst die unmittelbar im Bundesministerium des Innern, für Bau und Heimat betreuten Portallösungen und Fachanwendungen zugrunde gelegt worden. Für die Zwecke der Erarbeitung neuer ebenenübergreifenden Rechtsgrundlagen ist eine vertiefte Analyse der unterschiedlichen Portallösungen noch nachzuholen.

1. <u>Identifizierung und Authentisierung</u>

a) <u>Abgrenzung der Begriffe/Anforderungen</u>

---

[30] *Voßkuhle/Kaufhold*, JuS 2016, 314.

[31] Angelehnt an die Umsetzung von BAföG Digital und ähnliche Portalprojekte im OZG-Kontext.

Durch die Identifizierung weist eine Person gegenüber einer anderen Stelle ihre Identität nach, die zum Beispiel Gegenstand des Registrierungsprozesses bei der erstmaligen Nutzung einer Portallösung sein kann. Sofern das Nutzerkonto Bund oder die Nutzerkonten der Länder iSd § 3 OZG an ein Portal angebunden werden sollen, liegen die für die Identifizierung und Authentifizierung erforderlichen Verarbeitungsschritte bis zur Datenübermittlung im datenschutzrechtlichen Verantwortungsbereich des jeweiligen Nutzerkonten-Verantwortlichen, danach im Verantwortungsbereich des eigentlichen Portals/Fachverfahrens. Grundsätzlich ist aber auch die Einbindung eines portalspezifischen Kontos[32] möglich. Hier fallen die Rollen des Konten- und des Portals/Fachverfahrens-Verantwortlichen häufig zusammen. Im Zuge der individuellen Erstellung eines solchen portalspezifischen Kontos durch die jeweiligen Nutzenden sind daher die Schritte der Identifizierung und Authentisierung vorübergehend von dem Portalverantwortlichen mitzudenken, weshalb dazu im Folgenden Ausführungen erfolgen:

Eine Identifizierung ist die Übermittlung von anwendungsbezogen geeigneten Identitätsattributen (einer Identität), einschließlich authentisierender Metadaten (Authentisierung), sowie die Überprüfung (Authentifizierung) dieser Identität durch die vertrauende Entität.[33] Diese Identifizierung kann beispielsweise durch die Nutzung der Online-Ausweisfunktion des Personalausweises erfolgen. Je nach gegebenenfalls auch gesetzlich vorgegebenem Vertrauensniveau zur Nutzung des Portals, des portalspezifischen Kontos oder einer digitalisierten Verwaltungsleistung variieren die Anforderungen an den Identifizierungsprozess.

Eine Authentisierung ist Teil des Identifizierungsprozesses. Mithilfe der Authentisierung weist eine Person gegenüber einer anderen Stelle eine bestimmte Eigenschaft zweifelsfrei nach. Eine solche Eigenschaft kann beispielsweise die Berechtigung zur Nutzung eines im Rahmen der Identifizierung erstellten portalspezifischen Kontos oder eines Portals sein. Die Authentisierung kann in unterschiedlicher Art und Weise erfolgen. Das Vertrauensniveau „normal“ bietet die Authentisierung mit Benutzernamen und Passwort; einen stärkeren Schutz bietet eine sogenannte Zwei-Faktor-Authentisierung, die für Onlinedienste von substanziellem bis hohem/sehr hohem Schutzbedarf eingesetzt werden

---

[32] „Portalspezifisches Konto“ wird hier als Begriff zur Abgrenzung von den offiziellen OZG-Nutzerkonten (Nutzerkonto Bund oder Land iSd § 3 Abs. 2 OZG) verwendet und bezeichnet ein Nutzerkonto, das die jeweiligen Nutzer speziell nur für die Nutzung eines Fachportals angelegt haben.

[33] Elektronische Identitäten und Vertrauensdienste im E-Government, Technische Richtlinie TR-03107-1, Version 1.1.1 vom 07.05.2019, S. 10.

sollte. Bekannte Beispiele für eine solche Authentisierung mit zwei verschiedenen Faktoren sind die Online-Ausweisfunktion des Personalausweises, die für alle Vertrauensniveaus eingesetzt werden kann, oder das ELSTER-Verfahren, welches übergangsweise auch auf dem Vertrauensniveau substantiell eingesetzt werden. Die Frage des jeweiligen Vertrauensniveaus und Schutzbedarfs der im Weiteren verarbeiteten personenbezogenen Daten ist stets eine Frage des Einzelfalls und muss individuell geprüft werden.[34] Die Authentifizierung beschreibt wiederum den Überprüfungsvorgang der Identität bzw. der Daten durch die vertrauende Stelle.[35]

b) Überblick der möglichen Anbindungen

Für die Verarbeitung personenbezogener Daten mit besonders hohem Schutzbedarf, beispielsweise solcher Daten, die Art. 9 Abs. 1 DSGVO unterfallen, ist auf die Identifizierung ein besonderes Augenmerk zu legen. Das OZG sieht als zentrale Identifizierungskomponente Nutzerkonten vor, die Bund und Länder im Portalverbund bereitstellen (§ 3 Abs. 2 OZG). Im Rahmen von OZG-Projekten bietet es sich an, die OZG-Nutzerkonten (Nutzerkonto Bund und die landesspezifischen Nutzerkonten) als Identifizierungs- und Authentifizierungskomponenten zu nutzen. Nutzerkonten sind kein Identifizierungsmittel, sondern „Identifizierungsmittel-Broker". OZG-Nutzerkonten bieten alle im Portalverbund zugelassenen Identifizierungsmittel an (also z.B. die Online-Ausweisfunktion des Personalausweises, das ELSTER-Verfahren, alle eIDAS-notifizierten Identifizierungsmittel anderer EU-Länder). Behörden, die ihre Verwaltungsverfahren digitalisieren, müssen sich an ein OZG-Nutzerkonto einmal anbinden und sind damit zugleich davon befreit, selbst alle verfügbaren Identifizierungsmittel in jedes Formular zu integrieren

Die Inanspruchnahme einer digitalen Verwaltungsleistung setzt in aller Regel die Identifizierung und Authentisierung der Nutzer voraus. Die Anbindung der OZG-Nutzerkonten bietet einmal den Vorteil, dass sich die Rechtsgrundlagen zur Verarbeitung der Anmelde- und Registrierungsdaten unmittelbar aus dem OZG ergeben. Zudem unterstützen Nutzerkonten Identifizierungsmittel auf unterschiedlichen Vertrauensniveaus, wie etwa die On-

---

[34] Vgl. zu dem ganzen Komplex ausführlich *Schläger*, in: Schläger/Thode (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, 1. Aufl. 2018, Teil I: technische und organisatorische Maßnahmen, Rn. 284. Im Rahmen des OZG-Programms wurde außerdem mit dem sog. „Praxistool Vertrauensniveau" eine Handreichung für die Bestimmung des Vertrauensniveaus von E-Government-Anwendungen entwickelt: https://vn-check.ozg-umsetzung.de/

[35] Elektronische Identitäten und Vertrauensdienste im E-Government, Technische Richtlinie TR-03107-1, Version 1.1.1 vom 07.05.2019, S. 11.

line-Ausweisfunktion des Personalausweises für das Vertrauensniveau hoch (einschließlich aller niedrigeren Vertrauensniveaus) oder – befristet – das ELSTER-Verfahren für das Vertrauensniveau substanziell. Schließlich ist es im Sinne des OZG, einen möglichst einheitlichen Zugang zu einer Vielzahl von Portalen im Portalverbund zu schaffen, sodass sich die Anbindung der OZG-Nutzerkonten gegenüber speziell für einzelne Verwaltungsleistungen geschaffenen Nutzerkonten anbietet.

c) Einzelne Datenverarbeitungsschritte

aa) Registrierung zur Authentisierung

Sofern die Registrierung und Authentisierung nicht über ein OZG-Nutzerkonto, sondern in einem portalspezifischen Konto und damit bereits als Teil der Datenverarbeitung unter der Verantwortung des Portalbetreibers abläuft, ist der Schritt Registrierung der erste logische Datenverarbeitungsschritt. Die Registrierung ist für die Durchführung von Verwaltungsleistungen mit Hilfe von Onlineportalen ein zusätzlicher Komfort für die Nutzenden. Häufig werden dabei der Name, der Vorname, die E-Mail-Adresse und gegebenenfalls weitere Stammdaten der Nutzenden verarbeitet.

bb) Anmeldung

Im Rahmen der Anmeldung beschränkt sich die Datenverarbeitung meist auf die Verarbeitung der E-Mail-Adresse und eines Benutzernamens.

cc) Antragsdateneingabe durch die Nutzenden

Sofern es sich um ein Portal handelt, das bei der Antragstellung im Hinblick auf eine bestimmte Verwaltungsleistung unterstützen und assistieren soll, ist das Kernstück der Datenverarbeitung die Eingabe der Antragsdaten, sofern diese nicht nur lokal auf dem jeweiligen Endgerät der Nutzenden verarbeitet werden. In diesem Fall bedarf es keiner Rechtsgrundlage, da der Verantwortliche keine personenbezogenen Daten der Nutzenden verarbeitet. Es ist aber auch bei einer lokalen Datenverarbeitung darauf zu achten, ob etwa die IP-Adresse der Nutzenden übermittelt werden, da es sich auch dabei um ein personenbezogenes Datum handelt. Sofern die Antragsdaten aber unmittelbar in der Webanwendung und unter der Verantwortung des Portalbetreibenden eingegeben werden, stellt sich in diesem Abschnitt eine Vielzahl von Einzelfragen. Insbesondere ist darauf zu achten, ob gegebenenfalls die Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 Abs. 1

DSGVO (beispielsweise bezogen auf die rassische und ethnische Herkunft, religiöse Überzeugungen oder die sexuelle Orientierung), von Daten Dritter oder von Kindern erforderlich ist. Diese Fragen determinieren die Suche nach der entsprechenden datenschutzrechtlichen Rechtsgrundlage.

Insbesondere bei schriftformbedürftigen Anträgen wird sich der Prozess der Antragseingabe so gestalten, dass die Stammdaten des Antrags aus dem Identifizierungsmittel ausgelesen und – für den Nutzer unveränderbar – in das Antragsdokument übertragen werden. Aus verwaltungsverfahrensrechtlicher Sicht ist es zudem erforderlich, dass die Erklärung im Rahmen einer zusammenhängenden Sitzung abgeben wird, um am Ende des Eingabeprozesses eine rechtswirksame Willenserklärung zu erzeugen (Beweiswert, Perpetuierungsfunktion).

Der Umfang und Zweck der vom Nutzer in die Anwendung einzugebenden Daten ergibt sich aus dem jeweiligen Fachrecht.

dd) Kombi-Antrag

Gegenwärtig werden unterschiedliche Möglichkeiten diskutiert und teilweise bereits erprobt, um den Prozess der Eingabe der Antragsdaten und der Nachweiserbringung für den Nutzer zu vereinfachen.

An erster Stelle der Überlegungen steht der sogenannte „Kombi-Antrag“. Damit ist gemeint, dass sich der Nutzer bereits bei der Antragsstellung dafür entscheidet, nicht nur einen Antrag zu stellen, sondern mehrere Anträge parallel (Beispiel: Familienleistungen). Wenn etwa für mehrere Leistungen die Angabe von Name und Geburtstag eines Kindes erforderlich ist, soll diese Eingabe durch den Nutzer nur einmal erfolgen, sich aber am Ende des Eingabeprozesses in mehreren unterschiedlichen Anträgen wiederfinden. Voraussetzung ist allerdings, dass alle Anträge zeitgleich, sozusagen in einer Sitzung, gestellt werden.

ee) Automatisierte Antragsdateneingabe durch Vorbefüllung und automatisiertes Abrufen erforderlicher Nachweise auf Wunsch der Nutzenden (Once-Only-Prinzip)

Darüber hinaus soll dem Nutzenden im Zuge der Registermodernisierung bei der Beantragung von Verwaltungsleistungen ermöglicht werden, Angaben und Nachweise nicht selbst beibringen zu müssen, sondern diese mittels eines automatisierten Datenabrufs aus öffentlichen Registern abrufen zu lassen, soweit die Daten darin bereits vorliegen und er sich hiermit einverstanden erklärt (Once-Only-Prinzip).

Die Registerdaten können dann zur automatisierten Vorbefüllung von Online-Anträgen bzw. zur Ergänzung von Nachweisen während des Antragsprozesses verwendet werden oder zur Erbringung erforderlicher Nachweise. Eine nutzerfreundliche Vorbefüllung von Anträgen stellt erhebliche Anforderungen an die technische Responsivität eines Registers. Das Register hat zu gewährleisten, dass die angefragten Daten echtzeitnah bereitgestellt werden. Dagegen funktioniert eine Lösung, in der der Antragsteller die für die OZG-Leistung zuständige Behörde zur Einholung der Nachweise ermächtigt, kurzfristig auch mit solchen Registern, deren Antwortzeitverhalten eine Vorbefüllung gegenwärtig noch nicht zulassen.

Die Portale können hinsichtlich ihrer Aufgabe in Bezug auf diesen automatisierten Datenabruf unterschiedlich gestaltet werden: denkbar ist, dass die Portale selbst eine zusätzliche Assistenzfunktion für die Fachverfahren übernehmen und die „fehlenden“ Antragsdaten auf automatisiertem Wege beschaffen, bevor der Antrag an das Fachverfahren weitergeleitet wird. Dieser Weg führt aber dazu, dass der Antrag beim Fachverfahren erst dann als gestellt gilt, wenn er in entsprechend vervollständigter Form beim Fachverfahren zugestellt wird. Daraus können sich für den Nutzer insbesondere dann Nachteile ergeben, wenn ein Antrag frist- oder stichtagsgebunden ist und eine Fachverfahren für die Wahrung der Frist auch einen unvollständigen Antrag ausreichen lassen würde. Vor dem Hintergrund dieser Überlegungen wurde für das Vorhaben ELFE entschieden, dass nicht der Antragsassistent, sondern das jeweilige Fachverfahren für die Datenabrufe verantwortlich ist und diese entsprechend veranlasst. Das Fachverfahren bedient sich im Falle des Vorhabens EFLE dazu allerdings desselben IT-Dienstleisters, der auch den Antragsassistenten betreibt (Mandantentrennung!).

Perspektivisch ist überdies denkbar, dass eine Portallösung eine Funktionalität bereitstellt, nach der alle im Antrag benötigten Daten, die bereits in der Verwaltung vorliegen, auf Wunsch der Nutzenden aus den jeweils originär zuständigen Registern abgerufen werden können. Die entsprechenden Datenfelder können dann mittels Registerabruf vorbefüllt werden und erforderliche Nachweise, z.B. Urkunden, direkt aus den Registern abgerufen werden, in denen sie schon vorliegen. Damit verbunden sind zwei Datenverarbeitungsvorgänge: Datenabfrage und Datenübermittlung.

Die mit diesem Komplex zusammenhängenden Fragestellungen sind Gegenstand der Arbeiten im Koordinierungsprojekt Registermodernisierung.

ff) Zwischenspeichern und Antragsunterbrechung

Um eine möglichst benutzerfreundliche und serviceorientierte Digitalisierung einer Verwaltungsleistung anzubieten, ist die Möglichkeit der Zwischenspeicherung zwecks Antragsunterbrechung eine wichtige Funktion. Bei der Konzeption eines Portals ist zu bedenken, ob die Zwischenspeicherung automatisch oder nur aufgrund manueller Speicherung erfolgen soll und wie lange beispielsweise ein unbearbeiteter Antrag im Antragssystem bleibt, bis er gelöscht wird. In diesem Zusammenhang ist weiter zu berücksichtigen, ob eine Löschung automatisch oder nur nach vorheriger Ankündigung erfolgen soll.

gg) Offenlegung durch Übermittlung an Fachbehörden

Handelt es sich um ein Portal, das ausschließlich bei der Antragstellung unterstützt, werden die Antragsunterlagen, nachdem die Nutzenden sämtliche für die Antragstellung erforderlichen Daten eingegeben haben, an die entsprechenden Fachbehörden übermittelt. Vor dem Absenden der Unterlagen stellen sich Fragen, ob den Nutzenden beispielsweise die Möglichkeit der Speicherung der Antragsunterlagen als PDF bereitgestellt werden soll und ob und wie sie darüber zu informieren sind, dass Antragsunterlagen erfolgreich übermittelt wurden. Im Hinblick auf die Problematik der Mischverwaltung, die bei Portalprojekten entstehen kann, bei dem Bund und Länder mitwirken, ist zu beachten, dass eine Eingangsbestätigung der Antragsunterlagen bei der zuständigen Fachbehörde stets nur von dieser an die Nutzenden gesendet werden sollte.

hh) Langzeitspeichern nach Übermittlung

Für „wiederkehrende“ Anträge bietet es sich an, die Möglichkeit der Langzeitspeicherung der Antragsunterlagen anzubieten. Ist jedes Jahr erneut ein Antrag zu stellen, wie zum Beispiel der Antrag auf Berufsausbildungsförderung, ist es benutzerfreundlich, wenn bestimmte Angaben gespeichert und unmittelbar für die Antragstellung verwendet werden können. Da es sich dabei um eine Serviceleistung für den Antragstellenden handelt und die Speicherung für eine lange Zeit erfolgen soll, kommt – neben dem Schaffen einer spezialgesetzlichen Rechtgrundlage (siehe hierzu bereits Abschnitt II. 3.) - als Rechtsgrundlage auch das Vorliegen einer informierten und freiwilligen Einwilligung der Nutzenden in Betracht.

Der Freiwilligkeit der Einwilligung steht insbesondere nicht schon entgegen, dass sie im Verhältnis Bürger-Staat erfolgt (vgl. den Erwägungsgrund 43 S. 1 DSGVO,

der eine solche Konstellation nur unter strengere Voraussetzungen stellt). Erforderlich ist jedoch, dass der Bürger eine echte Wahlfreiheit hat. Soweit die OZG-Leistungen den Bürgern auch weiterhin in analoger Form zur Verfügung stehen und an diese analoge Beantragung auch nicht mit zusätzlichen Erschwernissen belegt wird (zB sehr hohen Kosten), kann die Freiwilligkeit bejaht werden.

Eine Einwilligungserklärung kann per Klick („Opt-in"-Verfahren) erfolgen. Zu beachten ist in diesem Zusammenhang, dass eine Einwilligung stets nur für die Daten der Antragsteller selbst möglich ist. Insofern sind etwaige Daten Dritter, die in den Antragsdaten oder in hochgeladenen Nachweisen enthalten sein können, ggf. zu schwärzen oder getrennt von den Antragsdaten der Antragsteller zu löschen.

ii) Rückkanal

Die Einrichtung eines Rückkanals, der beispielsweise dafür genutzt werden kann, einen digitalen Verwaltungsakt als verfahrensabschließende Handlung bereitzustellen, entspricht der Stufe 3 des OZG-Reifegradmodells[36]. Bei der Einrichtung des Rückkanals sind für die Sonderkonstellation einer Zusammenarbeit von Bund und Ländern die Fragen der Mischverwaltung in verfassungsrechtlicher Hinsicht im Auge zu behalten. In verwaltungsrechtlicher Hinsicht sind die Vorgaben des Verwaltungsverfahrensrechts zur Bereitstellung von digitalen Verwaltungsakten über öffentlich zugängliche Netze zu berücksichtigen. Aus den entsprechenden Vorschriften ergeben sich eine Reihe von praktisch umzusetzenden, technischen Vorkehrungen, die im Einzelnen unter D. erläutert werden.

jj) Löschung und Korrektur, Nachreichen von Daten

Schließlich stellen sich Fragen der Kontoverwaltung (Löschung und Korrektur, Nachreichen von Daten). Optional könnten die automatische oder manuelle Löschung von Nutzerkonten, eine Möglichkeit zur Korrektur von Antragsdaten, zum Nachreichen von Antragsunterlagen oder Nachweisen vorgesehen sein. Hinsichtlich der Löschung ist stets darauf zu achten, dass keine überlange Speicherdauer verwaister Nutzerkonten möglich ist: Wird ein Nutzerkonto über längere Zeit nicht genutzt, sollte dafür eine Löschfrist vorgesehen sein[37].

---

[36] Reifegradmodell für die OZG-Umsetzung: https://leitfaden.ozg-umsetzung.de/display/OZG/2.2+Digitale+Services+im+Sinne+des+OZG

[37] So etwa explizit geregelt in § 14 Abs. 5 WiPG NRW.

b) Zusätzliche Datenverarbeitung / „Sur-Plus-Verarbeitung“

Datenschutzrechtliche Erlaubnistatbestände finden sich vielfach in Fachgesetzen, die explizit auch eine elektronische Verarbeitung der Daten von Antragsteller legitimieren. Häufig bietet es sich aber zur effektiven Umsetzung einer digitalen Verwaltungsleistung an, dass eine öffentliche Stelle zentral ein Antragsportal zur Verfügung stellt, das bei der Antragstellung und Zusammenstellung der Unterlagen unterstützt[38] und die vollständigen Unterlagen an die jeweiligen Fachstellen übermittelt. Durch dieses Serviceangebot kommt es neben der fachspezifischen zu einer zusätzlichen Datenverarbeitung (hier im Folgenden plakativ als „Sur-Plus-Verarbeitung“ bezeichnet). Um welche Daten es sich hier im Einzelnen handelt, hängt von der jeweiligen Art und den Kategorien der Daten ab, die für die jeweilige Antragsstellung auf die spezifische Verwaltungsleistung erforderlich sind. Auch diese Verarbeitung unter gesonderter Verantwortlichkeit muss sich auf datenschutzrechtliche Rechtsgrundlagen stützen können (siehe dazu allgemein bereits oben unter Abschnitt C II. 3. sowie unter IV. 2. a) gg)).

Da es im OZG für die insoweit erfolgende Sur-Plus-Datenverarbeitung keine Generalklausel gibt, sind ggf. in Fachgesetzen entsprechende Verarbeitungsgrundlagen zu prüfen.

In einigen Fachgesetzen finden sich bereits Normen, die eine Sur-Plus-Datenverarbeitung in einem übergreifenden Portal rechtfertigen. So heißt es in § 5a Abs. 2 EGovG NRW:

> *„(2) Die Ministerpräsidentin oder der Ministerpräsident und die Ministerien können neben dem Serviceportal. NRW weitere elektronische, über allgemein zugängliche Netze aufrufbare Verwaltungsportale errichten und betreiben, die die landesweite, elektronische Abwicklung von Verwaltungsleistungen im Sinne des § 5, die im engen sachlichen Zusammenhang mit ihrer jeweiligen Zuständigkeit stehen, ermöglichen (Fachportale). […]“*

Mit dieser Norm hat der Landesgesetzgeber eine Rechtsgrundlage der Landesregierung für die Errichtung übergreifender Verwaltungsportale geschaffen, über die dann die Abwicklung von Verwaltungsleistungen möglich sein soll, die eigentlich in die fachliche Zuständigkeit beispielsweise der Kommunen fallen. Insoweit erweist sich die Sur-Plus-

[38] Die Unterstützungsleistung besteht darin, dass Antragsformulare, die bisher im analogen Verfahren von Hand ausgefüllt werden mussten, digital in einer Eingabemaske im Antragsportal dargestellt werden und die Antragsdaten inkl. etwaig erforderlicher Nachweise im Anschluss medienbruchfrei ohne Ausdruck und Unterschrift sowie postalischer Versendung an die zuständige Fachbehörde übermittelt werden.

Datenverarbeitung als die Erfüllung einer öffentlichen Aufgabe, was den Anwendungsbereich der landesdatenschutzrechtlichen Generalklauseln eröffnet und die Datenverarbeitung legitimiert (siehe nachfolgend).

c) Mitgliedschaftliche datenschutzrechtliche Rechtsgrundlagen

Hier ist zu prüfen, ob, um insbesondere den recht hohen Anforderungen des BVerfG an eine wirksame Datenverarbeitungsnorm zu genügen, eine (spezialgesetzlichen) Verarbeitungsnorm in dem jeweiligen Fachgesetz geschaffen werden muss. Hintergrund ist, dass grundsätzlich mit jeder Datenverarbeitung ein Eingriff in das Recht auf informationelle Selbstbestimmung verbunden ist, und nur eine den konkreten Verarbeitungsprozess abbildende Norm dem verfassungsrechtlichen Bestimmtheits- und Verhältnismäßigkeitsgrundsatz zu genügen vermag. Parallel zur technischen Entwicklung der OZG-gestützten Beantragung einer Leistung hat daher stets auch die Schaffung einer entsprechenden Rechtgrundlage zu erfolgen. Datenverarbeitungen können daher nur ganz ausnahmsweise auf Art. 6 Abs. 1 lit. e DSGVO i.V.m. den – als Auffangnormen konzipierten und naturgemäß sehr allgemein gehaltenen – Generalklauseln des BDSG (§ 3 bzw. § 22 BDSG) bzw. der Landesdatenschutzgesetze gestützt werden. Denkbar ist dies insbesondere dann, wenn eine besondere Eilbedürftigkeit besteht und nur eine kurze, zeitlich sehr überschaubare Übergangszeit bis zum Inkrafttreten der spezialgesetzlichen Verarbeitungsnorm überbrückt werden soll und zudem die Datenverarbeitung wenig grundrechtsintensiv erscheint, also nur eine sehr geringe Eingriffsintensität aufweist. Generalklauseln erlauben Datenverarbeitung einer öffentlichen Stelle, soweit sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe erforderlich sind.

aa) § 3 BDSG und landesrechtliche Entsprechungen[39]

Nach der datenschutzrechtlichen Generalklausel in § 3 BDSG ist die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist. Die entsprechenden landesrechtlichen Regelungen ähneln meist der Formulierung im Bundesdatenschutzgesetz.

bb) § 22 BDSG und besondere Kategorien personenbezogener Daten

[39] Siehe zu der Zulässigkeit der datenschutzrechtlichen Generalklausel die Ausführungen oben unter C.II.3.

Nach der datenschutzrechtlichen Generalklausel des § 22 BDSG ist die Verarbeitung besonders schutzbedürftiger Daten nach Art. 9 Abs. 1 DSGVO zulässig, wenn sie beispielsweise aus Gründen erheblichen öffentlichen Interesses (Art. 9 Abs. 2 lit. g DSGVO in Verbindung mit § 22 Abs. 1 Nr. 1 a) BDSG) oder zur Abwehr erheblicher Nachteile für das Gemeinwohl (Art. 9 Abs. 2 lit. g DSGVO in Verbindung mit § 22 Abs. 1 Nr. 2 c 1. HS BDSG) zwingend erforderlich ist. Auf Landesebene existieren meist entsprechende Normen; die folgenden Hinweise können deshalb – sofern die landesrechtliche Rechtsgrundlage der bundesrechtlichen inhaltlich entspricht – gleichermaßen genutzt werden.

Ein erhebliches öffentliches Interesse im Sinne von Art. 9 Abs. 2 lit. g DSGVO besteht dann, wenn Belange des Allgemeinwohls in besonderem Maße berührt werden. Erwägungsgrund 46 führt dafür beispielhaft die Bekämpfung von Epidemien oder die Hilfeleistung im Katastrophenfall auf. Das öffentliche Interesse ist nur erheblich, wenn es sich auf besonders schützenswerte Belange des Gemeinwohls bezieht und diese in besonderem Maße berührt werden.[40] Dabei ist wegen der besonderen Schutzbedürftigkeit sensibler Daten eine konkrete Bedrohungslage für das Gemeinwohl erforderlich, um eine Verarbeitung zu rechtfertigen.[41]

d) Datenverarbeitung öffentlicher Stellen auf Einwilligungsbasis

Grundsätzlich bietet die Einholung der informierten und freiwilligen Einwilligung der Betroffenen eine taugliche Rechtsgrundlage für die Verarbeitung personenbezogener Daten (Art. 6 Abs. 1 lit. a DSGVO). Dabei kann die Einwilligung rechtsdogmatisch auch in eine gesetzliche Rechtsgrundlage inkorporiert werden und als Tatbestandsmerkmal fungieren; eine solche Regelung in Form eines sog. Mischtatbestandes ist besonders datenschutzfreundlich. Soll auf die Einwilligung gegenüber öffentlichen Stellen als Rechtsgrundlage zurückgegriffen werden, sind aber einige Besonderheiten zu beachten.

Zum einen sollen öffentliche Stellen grundsätzlich eher subsidiär auf diese Rechtsgrundlage zurückgreifen, da sie anders als private Stellen grundsätzlich in der Lage sind, gesetzliche Grundlagen durch Nutzung der Öffnungsklauseln der DSGVO für die spezielle Datenverarbeitung zu schaffen.

---

[40] *Rose,* in: Taeger/Gabel, 3. Aufl. 2019, BDSG § 22 Rn. 35.
[41] *Rose,* in: Taeger/Gabel, 3. Aufl. 2019, BDSG § 22 Rn. 34.

Zum anderen ist besonderes Augenmerk auf die Freiwilligkeit der Einwilligung gegenüber öffentlichen Stellen zu legen (Art. 4 Nr. 11, Art. 7 Abs. 4, Erwägungsgrund 43 DSGVO). Nach Erwägungsgrund 43 der DSGVO soll die Einwilligung nämlich dann keine Rechtsgrundlage liefern, wenn zwischen dem Betroffenen und dem Verantwortlichen ein Ungleichgewicht besteht, insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt. Die von Erwägungsgrund 43 gesicherte Freiwilligkeit ist gegenüber öffentlichen Stellen in der Regel jedoch dann gewahrt, wenn Nutzenden eine echte Wahlmöglichkeit gegeben wird – beispielsweise, wenn Betroffenen neben der Inanspruchnahme der Verwaltungsleistung auf digitalem Wege diese auch analog angeboten wird.

Zudem ist allgemein zu bedenken, dass die datenschutzrechtliche Einwilligungserklärung stets widerruflich ist, Art. 7 Abs. 3 S. 1 DSGVO. Dies muss bei der technischen Umsetzung einer einwilligungsbasierten Datenverarbeitung im Rahmen eines Tools zum Einwilligungsmanagement berücksichtigt werden. Mit dem Widerruf der Einwilligung entfällt die Rechtsgrundlage für die Datenverarbeitung. Der Widerruf erfolgt für die Zukunft. Die bis dahin erfolgte Verarbeitung bleibt von dem Widerruf unberührt, sie wird also nicht etwa im Nachhinein rechtswidrig.

Die Einwilligung kann der Betroffene durch einfachen Klick (Opt-in) in einer Checkbox erklären. Da der Verantwortliche jedoch nach Art. 7 Abs. 1 DSGVO nachweisen können muss, dass eine Einwilligung erfolgt ist, sind bestimmte (Meta-)Daten zu diesem Zweck vom Verantwortlichgen zu speichern und bis zum Ende der Verjährungsfrist einer möglichen Beschwerde von Betroffenen aufzubewahren. Erforderlich ist die Speicherung von Daten, die nachweisen, dass, durch wen, wann und für welche konkrete Datenverarbeitung die Einwilligungserklärung abgegeben wurde.[42]

Eine besondere Herausforderung, auch für die technische Umsetzung, stellt die Einholung von Einwilligungserklärungen Dritter dar. Es könnte beispielsweise für eine Antragsstellung erforderlich sein, dass Antragsteller Daten Dritter (bspw. der Eltern) eingeben müssen. Soll die gesamte Datenverarbeitung auf Einwilligungserklärungen gestützt werden, so müssten in diesem Zusammenhang auch von Dritten Einwilligungserklärungen eingeholt werden. Zwar mag auch eine vertretungsweise Einwilligung zulässig sein; der Verantwortliche bleibt aber in der Pflicht, im Zweifel nachweisen zu müssen, dass eine wirksame Vertretungsmacht vorlag. Eine Einwilligung von Dritten kann technisch etwa per

[42] Vgl. dazu im Einzelnen unten D. II. 3. b).

E-Mail („Double-opt-in"-Verfahren) oder per Erklärung des Betroffenen eingeholt werden, die bestätigt, dass ihm eine solche Einwilligung der Dritten vorliegt.

Meistens lassen sich für eine verantwortliche öffentliche Stelle gesetzliche Rechtsgrundlagen finden, die die Datenverarbeitung rechtfertigen. Sinnvoll kann die Einholung einer Einwilligungserklärung aber beispielsweise für die langfristige Speicherung von Antragsdaten oder für reine Service-Zusatzleistungen sein[43], die für die Durchführung der digitalen Verwaltungsleistung an sich nicht erforderlich sind, aber eine besonders anwenderfreundliche Nutzung des Onlinedienstes ermöglichen.

Konkret könnte eine Checkbox folgendermaßen formuliert sein, auch wenn die genaue Formulierung stets eine Frage des Einzelfalls ist:

> *Ja, ich habe die Nutzungsbedingungen (verlinken) und die Datenschutzerklärung (verlinken) zur Kenntnis genommen und willige in die Erhebung und Verarbeitung meiner für [*Zweck ergänzen*] erforderlichen personenbezogenen Daten ein. Die Einwilligung kann jederzeit widerrufen werden; die Rechtmäßigkeit der bis zum Zeitpunkt des Widerrufs verarbeiteten personenbezogenen Daten bleibt davon unberührt.*

V. Technische Aspekte der Datenverarbeitung

Für den umfangreichen Pflichtenkatalog der DSGVO, der den Verantwortlichen adressiert, sind die Risiken für die Rechte und Freiheiten der betroffenen Personen zu berücksichtigen. Vor der Aufnahme oder Durchführung einer Verarbeitung personenbezogener Daten sind „Eintrittswahrscheinlichkeit und Schwere der Risiken" zu berücksichtigen. Ob eine Datenschutz-Folgenabschätzung durchzuführen ist, beurteilt sich nach der gemäß Art. 24 Abs. 1 Satz 1 DSGVO vorzunehmenden Risikobewertung (siehe dazu Ziffer VI.).

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten,

---

[43] Wie beispielsweise die nochmalige Zusammenfassung der Daten in einem Extra-PDF am Ende der Antragstellung.

Art. 32 Abs. 1 S. 1 DSGVO. Durch diese Bestandsaufnahme werden vor Beginn einer Verarbeitung mögliche Risiken[44] identifiziert, bewertet und Maßnahmen benannt, mit denen diese Ereignisse auf ein akzeptables Maß gesenkt werden können. Die Revision der Risikoanalyse, -bewertung und -behandlung erfolgt regelmäßig. Eine weitverbreitete Möglichkeit der Revision ist die Dokumentation und Pflege im Rahmen der Aktualisierung des Datenschutzkonzepts. Dafür sind Analyse-, Bewertungs- und Entscheidungsprozesse zu dokumentieren. Während einer datenschutzrechtlichen Revision oder Prüfung muss nachvollziehbar sein, welche technischen und organisatorischen Maßnahmen in Bezug auf welche Verarbeitungstätigkeiten ergriffen worden sind.

Die von Art. 32 DSGVO vorgegebenen Bewertungskriterien betreffen neben der Risikobewertung auch den Schutzbedarf. Die Schutzbedarfsfeststellung erfolgt anhand der festgelegten Gewährleistungsziele „Vertraulichkeit", „Integrität", Verfügbarkeit", „Belastbarkeit" und definierter Schutzbedarfsskalen, die die Grundlage für die Ausarbeitung der Maßnahmenliste und deren Bewertung darstellen.[45]

Um die Anforderungen, die insbesondere Art. 32 DSGVO aus technischer Perspektive an die Datenverarbeitung stellt, zu verwirklichen, empfiehlt es sich, die folgenden Schritte[46] durchzuführen: Schutzbedarf feststellen (1.), Risiko bewerten (2.), Maßnahmen treffen und Nachweise erbringen (3.).

1. Durchführung einer Schutzbedarfsermittlung

Zur Ermittlung des angemessenen Schutzniveaus nach Art. 32 DSGVO muss für den Verantwortlichen klar sein, welchen Schutzbedarf die relevanten personenbezogenen Daten besitzen. In der Praxis gibt es dafür verschiedene Ansätze, die regelmäßig auf das Schadenspotential abzielen. Vereinfacht wird man in Kategorien des Schutzbedarfs „kein/gering", „normal" und „hoch" sprechen und handeln können. Die Schutzbedarfsfeststellung ist als ein erster Schritt

---

[44] Vgl. zur Begriffsdefinition „Risiko", die innerhalb der DSGVO nicht erfolgt, das Kurzpapier Nr. 18 der Datenschutzkonferenz, S. 2: „*Ein Risiko im Sinne der DSGVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann."*; *Alt*, DS 2020, 169; Nach Erwägungsgrund 75 sind mögliche Schäden für die Rechte und Freiheiten natürlicher Personen physische, materielle und immaterielle Schäden zu fassen.

[45] Vgl. dazu im Einzelnen SDM, Version 2.0b, S. 9 ff.

[46] Vgl. dazu den Abschnitt „D3 Risiken und Schutzbedarf" des SDM, Version 2.0b, S. 42 ff; sowie das Papier des BayLDA zur „Sicherheit der Verarbeitung – Art. 32 DSGVO".

essentiell, wenn es darum geht, geeignete technische und organisatorische Maßnahmen auszuwählen.[47] Das Risiko, das eine Verarbeitungstätigkeit ohne implementierte Schutzmaßnahmen erzeugt, definiert den notwendigen Schutzbedarf. Eine Dokumentation der Risikoanalyse und der Schutzbedarfsfeststellung kann auch gemeinsam erstellt werden, um den Schutzbedarf inklusive möglicher auftretender Schadensszenarien sowie der Risiken zu ermitteln. Unterschiedliche Modelle und Konzepte[48] bieten dazu Leitfäden und Verfahrensvorschläge.

2. Risikoanalyse

Die Risikoanalyse kann sich methodisch an einem vereinfachten Gefährdungsmodell bzw. Schutzstufenmodell orientieren. Die Höhe des Risikos hängt sowohl von der Eintrittswahrscheinlichkeit (Eintrittseinschätzung) der Gefährdung als auch von der Höhe des möglichen Schadens ab. Der Risikoanteil „*Höhe des Schadens*“ kann nur von der Behörde selbst auf Grundlage von Erfahrungswerten bewertet werden. Beim Eintritt einer Gefährdung müssen die Art des Schadens und mögliche Folgeschäden eingeschätzt werden. Eine mögliche Berücksichtigung schließt ein, ob und wie ein Schaden zu beheben und welche Zeit zur Schadensbehebung zu berücksichtigen ist. Die Eintrittshäufigkeit muss durch geeignetes Fachpersonal – unterstützt durch Statistiken und Erfahrungen – beurteilt werden.

a) Durchführung einer Schwellwertanalyse

Eine Schwellwertanalyse stellt die *Höhe des Risikos* fest und gibt Antwort darauf, ob ein „normales“ oder „hohes“ Risiko für eine Verarbeitungstätigkeit vorliegt. Wenn eines der Regelbeispiele nach Art. 35 Abs. 3 DSGVO vorliegt, wird das Risiko mit „hoch“ bewertet und die Durchführung einer Schwellwertanalyse ist nicht mehr notwendig, die Datenschutz-Folgenabschätzung ist deshalb zwingend vorzunehmen (s.u.). Es bestehen keine Vorgaben zur Durchführung von Schwellwertanalysen, sodass die Bewertung anhand der Methodik des Verfahrenseigentümers vorgenommen werden. Die Schwellwertanalyse sollte anhand von festgelegten Kriterien erfolgen und sich in den Datenschutzmaßnahmen

---

[47] Vgl. SDM, Version 2.0b, S. 47f.; siehe auch das Papier des BayLDA zur „Sicherheit der Verarbeitung – Art. 32 DSGVO“.

[48] Vgl. zum Beispiel das „Schutzstufenkonzept“ der LDI Niedersachsen, den „BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS)“ sowie das Standard-Datenschutz-Modell des Arbeitskreises Technik der DSK. Letzteres ist eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele. Als Orientierungshilfe bietet es standardisierte Empfehlungen der Aufsichtsbehörden sowie eine vordefinierte Umsetzungssystematik.

wiederspiegeln. Aus Art. 5 Abs. 1 DSGVO lassen sich sieben „Grundsätze“ bzw. „Gewährleistungsziele“ entnehmen, anhand derer eine Schwellwertanalyse durchgeführt werden kann:

- Transparenz,
- Nichtverkettung,
- Datenminimierung,
- Intervenierbarkeit,
- Verfügbarkeit,
- Integrität und
- Vertraulichkeit.[49]

Eine Methodik könnte daher sein, die Erfüllung der Gewährleistungsziele für jede Verarbeitungstätigkeit zu prüfen.

b) Durchführung einer Risikobewertung

Nachdem mittels der Schwellwertanalyse die Liste der möglichen Risiken identifiziert wurde, erfolgt im nächsten Schritt die Risikobewertung zur Identifizierung der *Höhe des Schadens* sowie der *Eintrittswahrscheinlichkeit*. Für jedes ermittelte Risiko werden somit drei Faktoren bewertet:

- Schwere des Schadens
- Eintrittswahrscheinlichkeit
- Umfang des Risikos

Wenn die verantwortliche Stelle noch keine festgelegte Methodik zur Durchführung der Schwellwertanalyse bzw. der Risikobewertung aufgesetzt und etabliert hat, kann Anlage Nr. 3 „Vorlage: Risikoanalyse und Datenschutzfolgenabschätzung“ als Vorlage inkl. relevanter Fragen und Ausfüllhinweise verwendet werden.

3. Maßnahmen und Nachweise

Auf Basis der Risikoanalyse und -bewertung denkbarer Schäden sowie der Schutzbedarfsfeststellung werden die notwendigen technischen oder organisatorischen Maßnahmen ermittelt, die diese Risiken minimieren und die zum Schutz der Rechte der Betroffenen erforderlich sind. Die

[49] Vgl. auch SDM, Version 2.0b, S. 10.

konzipierten technischen und organisatorischen Maßnahmen werden hinsichtlich der Kosten und der vorliegenden Rahmenbedingungen optimiert; d.h. sie stellen die minimale Basis einer Konformität mit bestehenden gesetzlichen Anforderungen dar. Die Maßnahmen sind zu priorisieren, sodass die Ressourcen zur Umsetzung sinnvoll geplant werden können.[50]

Diese Maßnahmen sind zu Nachweiszwecken zu dokumentieren. Das Datenschutzmanagementsystem, kurz DMS, stellt alle dokumentierten und implementierten Regelungen, Prozesse und Maßnahmen dar, mit denen der datenschutzkonforme Umgang mit personenbezogenen Daten in der Behörde systematisch gesteuert und kontrolliert wird. Das oben beschriebene Datenschutzkonzept setzt auf dem DMS der verantwortlichen Stelle auf. Dieses verfahrensspezifische Datenschutzkonzept unterscheidet sich von einem behördenweiten Informationssicherheitsrahmenkonzept[51]. Dieses letztgenannte Konzept dient als Grundlage zur Erfüllung der gesetzlichen Anforderungen an den Datenschutz einer Behörde. Es beschreibt alle erforderlichen Maßnahmen zur Aufrechterhaltung des Datenschutzes sowie alle IT-Systeme, die personenbezogene Daten verarbeiten. Das verfahrensspezifische Datenschutzkonzept hingegen bewertet die Verarbeitung personenbezogener Daten im speziellen durch das betreffende Verfahren und prüft die eigens für spezielle Verfahren erforderliche technische und organisatorische Maßnahmen.

Das verfahrensspezifische Datenschutzkonzept gliedert sich in das DMS des Verantwortlichen nach der DSGVO ein. In Abbildung 1 ist der Bezug eines typischen verfahrensspezifischen Datenschutzkonzeptes zu den angrenzenden Fachgesetzen, zur DSGVO, zum SDM und zum behördenspezifischen Datenschutzmanagement zu erkennen.

---

[50] Der AK Technik der DSK veröffentlich im Rahmen eines Maßnahmenkatalogs sukzessive sogenannten „Bausteine“, die einzeln zur Anwendung freigegeben werden, siehe hier den Hinweis auf die Bausteine „Dokumentation“, „Protokollieren“ und „Löschen“ vom 30.06.2020.

[51] Vgl. dazu die „Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DSGVO“ der DSK, S. 2.

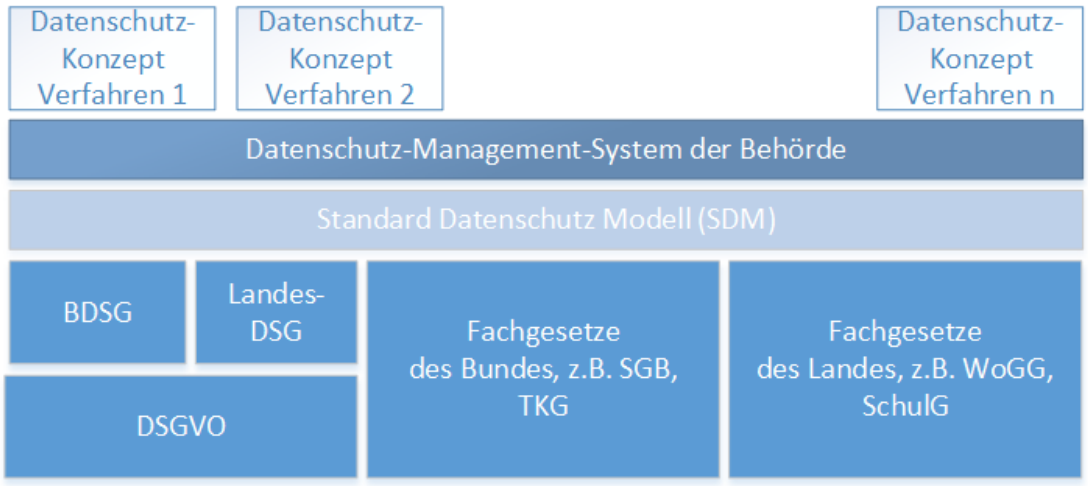

Abbildung 1: Einordnung eines verfahrensspezifischen Datenschutzkonzepts

Schließlich ist zu definieren, in welchen Abständen die Inhalte des Datenschutzkonzepts und die notwendigen Maßnahmen überprüft und ggf. überarbeitet werden müssen, damit die darin und in den Anlagen enthaltenen Angaben stets aktuell sind. Dies ist in DSGVO der „Rechenschaftspflicht“ des Verantwortlichen gemäß Art. 5 Abs. 2 DSGVO begründet. Aus den Erfahrungen der Praxis empfiehlt sich eine jährliche Fortschreibung bzw. Aktualisierung des Datenschutzkonzeptes. Bei neuen technischen Gegebenheiten oder veränderten Anforderungen muss ggf. eine Neubewertung des Risikos sowie des Schutzbedarfes durchgeführt werden, was wiederum die Etablierung neuer Datenschutzmaßnahmen und die Aktualisierung des Datenschutzkonzeptes, des Maßnahmenkatalogs und des Verzeichnisses von Verarbeitungstätigkeiten nach sich ziehen kann.

VI. Datenschutz-Folgenabschätzung

1. Notwendigkeit der Durchführung nach Art. 35 DSGVO

Der Verantwortliche muss vor Beginn der Datenverarbeitung eine datenschutzrechtliche Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchführen, wenn entweder eine Pflicht für die konkrete Verarbeitungstätigkeit nach Art. 35 Abs. 4 DSGVO (sog. Black List) vorliegt, ein Regelbeispiel nach Art. 35 Abs. 3 DSGVO erfüllt ist oder grundsätzlich aufgrund von Art, Umfang, Umständen und Zweck der Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen anzunehmen ist, Art. 35 Abs. 1 DSGVO.

Aus Sicht des Europäischen Datenschutzausschusses (EDSA) ist keine Datenschutz-Folgenabschätzung erforderlich, „falls ein Verarbeitungsvorgang gemäß Art. 6 Abs. 1 lit. c, e auf einer

Rechtsgrundlage im Unionsrecht oder im Recht der Mitgliedstaaten beruht und diese Rechtsvorschrift den konkreten Verarbeitungsvorgang regelt und falls bereits im Rahmen der Schaffung dieser Rechtsgrundlage eine DS-FA erfolgte (Art. 35 Abs. 10 DSGVO), es sei denn, ein Mitgliedstaat erklärt, dass es notwendig ist, vor den fraglichen Verarbeitungstätigkeiten eine DS-FA durchzuführen."[52] Eine DS-FA kann auch von Nutzen sein, wenn die Auswirkungen eines Technologieprodukts auf den Datenschutz untersucht werden sollen, was z. B. der Fall sein kann, wenn ein Hardware- oder Softwareprodukt aller Wahrscheinlichkeit nach von mehreren für die Datenverarbeitung Verantwortlichen für verschiedene Verarbeitungsvorgänge eingesetzt wird.[53]

2. Positiv- und Negativliste

Eine Datenschutz-Folgenabschätzung ist entbehrlich, wenn die Verarbeitungstätigkeit auf einer sog. White List nach Art. 35 Abs. 5 DSGVO aufgeführt wird. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), zuständig für die öffentlichen Stellen des Bundes, § 9 BDSG, hat bislang noch keine White List i.S.d. Art. 35 Abs. 5 DSGVO veröffentlicht. Auch die Landesdatenschutzbehörden, die zuständig für die Datenverarbeitung durch Landesbehörden sind, haben noch keine entsprechende Liste veröffentlicht.

Die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung kann sich aus der Black List (Art. 35 Abs. 4 DSGVO) des BfDI[54] ergeben. Danach ist eine Datenschutz-Folgenabschätzung gem. Art. 35 Abs. 1 DSGVO erforderlich, für die mindestens zwei der dort genannten Merkmale zutreffen.

Bei Onlinediensten häufig betroffen ist das Kriterium der Datenverarbeitungen in großem Umfang (Nr. 5 der Black List). Für die Annahme einer Datenverarbeitung in großem Umfang sind verschiedene Kriterien zu beachten:[55]

---

[52] Art. 29 – Datenschutzgruppe WP 248 Rev. 01, S. 15.
[53] Art. 29 – Datenschutzgruppe WP 248 Rev. 01, S. 8.
[54] https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Liste_Verarbeitungsvorgaenge-Art35.html;jsessionid=3FA252AA76EFDB24DE9ECCEC07143862.2_cid344?nn=9937868, zuletzt aufgerufen am 29.07.2020 in der Version 1.1 vom 01.10.2019.
[55] Art. 29 – Datenschutzgruppe WP 248 Rev. 01, S. 11.

- Zahl der Betroffenen, entweder als konkrete Anzahl oder als Anteil der entsprechenden Bevölkerungsgruppe[56]

- verarbeitete Datenmenge bzw. Bandbreite der unterschiedlichen verarbeiteten Datenelemente

- Dauer oder Dauerhaftigkeit der Datenverarbeitung

- geografisches Ausmaß der Datenverarbeitung: Verarbeitung auf regionaler, nationaler oder supranationaler Ebene[57]

Im Übrigen ist stets im Einzelfall zu prüfen, ob gegebenenfalls als weiteres Kriterium die Verarbeitung vertraulicher oder höchstpersönlicher Informationen (Nr. 4 der Black List), beispielsweise von Finanzdaten (Buchstabe d) oder besonderer Kategorien personenbezogener Daten (Buchstabe a) im Raum steht. Ist kein oder nur ein Kriterium der Black List einschlägig, so ist auch die allgemeine Regel des Art. 35 Abs. 3 DSGVO zu beachten. Hierbei handelt es sich jedoch stets um eine Prüfung des Einzelfalls.

---

[56] Dazu *Baumgartner*, in: Ehmann/Selmayr, 2. Aufl. 2018, DSGVO Art. 35 Rn. 38: Der Parlamentsentwurf der DSGVO stellte in einem teilweise vergleichbaren Zusammenhang auf einen Schwellenwert von 5.000 betroffenen Personen innerhalb von zwölf aufeinanderfolgenden Monaten ab. Der Gesetzgeber hat sich jedoch gegen eine schematische Herangehensweise entschieden, so dass im Einzelfall auch bei deutlich weniger Betroffenen eine umfangreiche Verarbeitung vorliegen kann.

[57] In Anlehnung an EG 91 der DSGVO, der sich auf Art. 35 Abs. 3 lit. b DSGVO bezieht. Er bietet aber auch für die Auslegung des Begriffes innerhalb der „Black - List" einen Anhaltspunkt. Siehe auch *Schwendemann,* in: Sydow, DSGVO, Art. 35 Rn. 13, mit Hinweis auf den ursprünglichen Parlamentsentwurf und den Erwägungsgrund 75, der eine Schwelle für ein „konkretes Risiko" bei einer Verarbeitung von 5000 betroffenen natürlichen Personen innerhalb von 12 Monaten vorgesehen hat. Dieser Schwellenwert liegt nun höher, weil der Erwägungsgrund 91 von einem „wahrscheinlich hohen Risiko" spricht und keine zahlenmäßige Grenze erwähnt.

D. Prozedurale Vorkehrungen

I. Verzeichnis von Verarbeitungstätigkeiten

Nach Art. 30 Abs. 1 S. 1 DSGVO ist der Verantwortliche verpflichtet, ein Verzeichnis über alle Verarbeitungstätigkeiten[58] schriftlich – auch in elektronischer Form –- zu führen. Dem Verantwortlichen wird dadurch die Einhaltung der Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO bezüglich der Einhaltung der DSGVO erleichtert: In dem Verarbeitungsverzeichnis werden die Verarbeitungstätigkeiten dokumentiert, die in der Zuständigkeit des Verantwortlichen liegen. Deshalb sind die im Rahmen von Digitalisierungsprojekten neu hinzukommenden Verarbeitungstätigkeiten auch für die interne Verarbeitungsübersicht festzuhalten. Im Gegensatz zum früheren Verfahrensverzeichnis wird das Verarbeitungsverzeichnis regelmäßig nicht öffentlich geführt[59] und ist nur auf Anfrage der Aufsichtsbehörde zur Verfügung zu stellen, Art. 30 Abs. 4 DSGVO.

Der notwendige Inhalt des Verarbeitungsverzeichnisses eines Verantwortlichen ergibt sich aus Art. 30 Abs. 1 S. 2 lit. a bis g DSGVO, wobei eine Erweiterung oder Modifizierung erforderlicher Informationen auf Landesebene möglich ist.[60] Auch der Auftragsverarbeiter muss nach Art. 30 Abs. 2 DSGVO ein Verarbeitungsverzeichnis führen, das in Bezug auf die darin aufzunehmenden Pflichtangaben weniger umfangreich ausfällt.

Das Muster-Verarbeitungsverzeichnis im Anhang enthält noch keine landesrechtlichen Besonderheiten. Es ist für einen Verarbeitungsvorgang gedacht, der im Rahmen der Digitalisierung von Verwaltungsleistungen unter der Verantwortung einer öffentlichen Stelle oder Behörde in das Gesamtverzeichnis aufzunehmen ist.

---

[58] Vgl. dazu die grundlegenden „Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DSGVO“ der DSK, hier.

[59] In Brandenburg ist vorgesehen, dass es von Jedermann eingesehen werden kann, vgl. § 4 Abs. 3 S. 1 BbgDSG.

[60] In Art. 8 Abs. 2 BayDSG heißt es beispielsweise: *„Bei der Verarbeitung von Daten im Sinne des Art. 9 Abs. 1 DSGVO sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Personen vorzusehen. Diese Maßnahmen sind in dem Verzeichnis nach Art. 30 DSGVO darzustellen.“* In Art. 31 S. 1 BayDSG ist zudem vorgesehen, dass neben den zwecken auch die Rechtsgrundlage für die Datenverarbeitung sowie ggf. die Verwendung von Profiling mit aufzunehmen ist. Nach Art. 31 S. 2 BayDSG findet Art. 30 Abs. 5 DSGVO, wonach das Verarbeitungsverzeichnis erst ab einer bestimmten Betriebsgröße zu führen ist, keine Anwendung.

II. Umgang mit Betroffenenrechten

1. Überblick über Betroffenenrechte nach DSGVO

Die Rechte der Betroffenen ergeben sich aus Art. 12 ff. DSGVO. Die zur Gewährleistung dieser Rechte getroffenen Maßnahmen sind im Datenschutzkonzept darzustellen. Insbesondere ist dabei auf die folgenden kurz skizzierten Rechte näher einzugehen.

a) Transparente Information (Art. 13, 14 DSGVO)

Es kann ein kurzer Hinweis erfolgen, dass Nutzende im Rahmen der Datenschutzerklärung über die Verarbeitung der Daten entsprechend der Vorgaben gemäß Art. 13, 14 DSGVO informiert werden und wo diese Datenschutzerklärung zu finden ist.

b) Grundsätzliches Verfahren bei der Bearbeitung von Anfragen Betroffener / Auskunftsanspruch nach Art. 15 DSGVO

Unter diesem Stichwort können kurze Ausführungen erfolgen, wie bei elektronischen oder schriftlichen Anfragen der Betroffenen innerhalb der Organisation des Verantwortlichen verfahren und in welcher Form eine Auskunft oder Antwort erteilt wird. Weitere Unterpunkte können sich auf den Auskunftsanspruch nach Art. 15 DSGVO, das Recht auf Berichtigung nach Art. 16 DSGVO und das Recht auf Löschung und Einschränkung der Verarbeitung nach Art. 17 und 18 DSGVO beziehen.

c) Widerspruchs- und Beschwerderecht (Art. 21 Abs. 1, 77 DSGVO)

Gemäß Art. 21 DSGVO kann eine betroffene Person Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten erheben, sofern die Datenverarbeitung auf der Rechtsgrundlage des Art. 6 Abs. 1 lit. e DSGVO erfolgte. Zu diesem Thema kann der Hinweis erfolgen, dass die Betroffenen auf dieses Recht in der Datenschutzinformation hingewiesen und etwaige Beschwerden im Einzelfall geprüft werden.

d) Gewährleistung der Integrität und Vertraulichkeit

Die Datenverarbeitung ist gem. Art. 5 Abs. 1 lit. f DSGVO insgesamt in einer Weise zu gewährleisten, die durch geeignete technische und organisatorische Maßnahmen eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung. Auch dazu kann erklärungsweise ein kurzer Abschnitt in der Datenschutzkonzeption erfolgen.

2. Datenschutzinformation

Den Verantwortlichen treffen nach der DSGVO Transparenz- und Informationspflichten, Art. 12 ff DSGVO. Insbesondere ist er gesetzlich verpflichtet, je nach Konstellation eine transparente Datenschutzinformation nach Art. 13 und 14 DSGVO zu erstellen und diese den Betroffenen in transparenter und leicht zugänglicher Form zu übermitteln. Dabei reicht auch eine Abrufbarkeit der Datenschutzinformation etwa auf der Informationswebseite eines Onlineportals.

a) Abgrenzung der Information nach Art. 13 und 14 DSGVO

Werden die Daten beim Betroffenen direkt erhoben, so muss eine Datenschutzinformation unter Beachtung der Anforderungen des Art. 13 DSGVO erfolgen. Art. 14 DSGVO stellt hingegen Anforderungen für den Fall auf, dass die Daten nicht beim Betroffenen selbst, sondern etwa über eine dritte Person erhoben werden. In beiden Erklärungen muss unter anderem auf die Zwecke, die Rechtsgrundlagen und den Verantwortlichen hingewiesen werden. Die Benennung der Kategorien personenbezogener Daten ist nur nach Art. 14 DSGVO erforderlich. Beide Vorschriften sehen Ausnahmen von der Informationspflicht etwa in dem Fall vor, dass der Betroffene bereits über die Informationen verfügt. Zur Beurteilung der Frage, ob die Informationen im Verfügungsbereich des Betroffenen sind, bietet sich eine Orientierung an Sinn und Zweck der Informationspflichten an. Die Information dient in erster Linie dazu, den Betroffenen durch ausreichende Information in die Lage zu versetzen, seine Betroffenenrechte nach den Art. 12 ff. DSGVO geltend zu machen. Art. 14 DSGVO hält gegenüber Art. 13 noch eine Reihe weiterer im Einzelfall zu prüfender Ausnahmen der Informationspflicht bereit, wie etwa die Unmöglichkeit oder Unverhältnismäßigkeit der Auskunftserteilung (Art. 14 Abs. 5 DSGVO).

b) Webseitenerklärung

Eine Datenschutzinformation, die über die Verarbeitung personenbezogener Daten durch eine Informationswebseite oder einen Onlinedienst informiert, muss auf dieser Webseite ohne weiteres auf- und abrufbar sein. Nicht erforderlich ist es entgegen weitverbreiteter Praxis hingegen, dass die Betroffenen der Webseitenerklärung *zustimmen*. Es handelt sich dabei nicht um eine Einwilligungserklärung nach Art. 7 DSGVO, die der Betroffene explizit in informierter Weise erteilen muss. Hinsichtlich der Datenschutzinformation muss es dem Betroffenen lediglich möglich sein, die entsprechenden Informationen – *bevor* die Datenverarbeitung erfolgt – zur Kenntnis zu nehmen. Da der Verantwortliche jedoch nach Art. 12 Abs. 1 DSGVO gehalten ist, geeignete Maßnahmen zu treffen, die Informationen nach den Art. 13 und 14 DSGVO in möglichst transparenter und leicht zugänglicher Form

zu vermitteln, bietet es sich an, Nutzende mit einer Checkbox auf die Datenschutzerklärung hinzuweisen. Der Text dieser Checkbox sollte indes keine Zustimmung des Betroffenen, sondern lediglich seine Kenntnisnahme erfordern und einen Link auf die entsprechende Datenschutzinformation enthalten.

3. Praktische Konsequenzen

Aus der Pflicht zur Gewährung von Betroffenenrechten ergibt sich eine Reihe von praktisch und technisch umzusetzenden prozeduralen Anforderungen, die im Folgenden dargestellt werden.

a) Festlegung von Zuständigkeiten zum Umgang mit Betroffenenrechten

Der Verantwortliche muss sich im Einzelnen darüber Gedanken machen, wer bzw. welche Organisationseinheit innerhalb seiner Struktur für die konkrete Bearbeitung von Betroffenenanfragen zuständig ist. Konkret sollte also beispielsweise eine Behörde, die datenschutzrechtlich verantwortlich ist, eine Abteilung speziell benennen; die Benennung einzelner Mitarbeiter ist nicht erforderlich.

Diese Information ist zum einen im Datenschutzkonzept auszuführen und zum anderen rein organisatorisch umzusetzen. Im Einzelnen sollte für die Betroffenen mithin eine Möglichkeit der Kontaktaufnahme via Telefon oder E-Mail bzw. postalisch bestehen, die innerhalb der Arbeitsorganisation des Verantwortlichen auch betreut wird, sodass etwa sichergestellt ist, dass auf ein Auskunftsersuchen hin eine entsprechende Antwort innerhalb eines überschaubaren Zeitraumes erfolgt. Die Ausführungen im Datenschutzkonzept können insofern auch bei der Erläuterung der jeweiligen Betroffenenrechte erfolgen, indem jeweils daraufhin gewiesen wird, welche Organisationseinheit in welcher Form beispielsweise auf eine Löschanfrage reagiert.

b) Einwilligungsmanagement

Nach Art. 7 Abs. 1 DSGVO muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung eingewilligt hat. Nach Art. 7 Abs. 1 DSGVO liegt die materielle Beweislast, dass sämtliche im Antragsprozess Betroffenen eingewilligt haben, beim datenschutzrechtlich Verantwortlichen. Der Verantwortliche muss nachweisen, dass er eine wirksame Einwilligung von der betroffenen Person *erhalten* hat[61]. Zu diesem

[61] Siehe zu den Anforderungen an eine wirksame Einwilligung schon unter C. IV. 2. d).

„Erhalten“, macht die DSGVO keine genauen Angaben[62]. Kann der Verantwortliche den Nachweis im Streitfall nicht erbringen, gilt die Einwilligung mit allen daraus resultierenden Haftungsrisiken als nicht erteilt[63]. Ausreichend ist, dass nachgewiesen werden kann, dass eine eindeutige, bestätigende Handlung vorlag (z.B. durch die Nutzung einer Opt-in-Lösung).[64]

Der in der Praxis *rechtssicherste* Nachweis im Sinne des Art. 7 Abs. 1 DSGVO ist die schriftliche Einwilligung oder die Speicherung der gesamten Einwilligung in Textform.

Entsprechend dem Grundsatz der Datenminimierung soll die Nachweispflicht des Verantwortlichen allerdings nicht zu einer unnötigen Speicherung weiterer Daten des Betroffenen führen, sondern lediglich eine angemessene Dokumentation beim Verantwortlichen einführen.[65] Das bedeutet, dass die Verantwortlichen über ausreichend Daten verfügen sollten, um zu zeigen, dass eine Einwilligung erteilt wurde. Sie sollten jedoch nicht mehr Informationen erheben, als dazu erforderlich ist. Ausreichend und gleichzeitig dem Grundsatz der Datensparsamkeit entsprechend stellt deshalb *die elektronische Protokollierung der Einwilligungserteilung* eine gute Alternative dar. Der Nachweis über die elektronische Einwilligung gelingt dabei am leichtesten über ein sog. Double-Opt-in Verfahren, wobei nach einer elektronischen Einwilligungserklärung der Erklärende mit einer an die von ihm angegebenen E-Mail-Adresse aufgefordert wird, die erfolgte Einwilligung zu bestätigen.[66] Diese Variante stellt sich freilich in der Praxis als nicht sehr nutzerfreundlich dar, da zusätzliche Aktionen von den Betroffenen gefordert werden.

Nutzerfreundlicher ist deshalb die bloße Speicherung der Metadaten durch den Verantwortlichen. Dies ist ausreichend, da der Inhalt der Einwilligungserklärung nach der DSGVO nicht jederzeit durch den Betroffenen abrufbar sein muss[67]. Zum Nachweis genügt es deshalb, entsprechende Metadaten des Einwilligenden zu speichern, die protokollieren, wer, wann die Einwilligung erteilt hat.

---

62 *Taeger,* in: Taeger/Gabel, Art. 7 DSGVO, Rn. 4.

63 *Stemmer*, in: BeckOK DatenschutzR, 31. Ed. 1.2.2020, DSGVO Art. 7 Rn. 86.

64 *Paschke,* in: Ehmann/Selmayr/Heckmann, 2. Aufl. 2018, DSGVO Art. 7 Rn. 69.

65 *Paschke*, in: Ehmann/Selmayr/Heckmann, 2. Aufl. 2018, DSGVO Art. 7 Rn. 72, Artikel-29-Datenschutzgruppe, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, S. 24.

66 *Taeger*, in: Taeger/Gabel, 3. Aufl. 2019, DSGVO Art. 7 Rn. 41.

67 So war es bisher nach deutschen Recht vorgesehen, vgl. § 13 Abs. 2 TMG bzw. § 28 Abs. 3a BDSG aF soweit diese elektronisch eingeholt wurde, dazu *Gola*, in: Schulz, DSGVO, 2. Aufl. 2018, Art. 7 Rn. 63.

Nicht ausreichend wäre hingegen der Nachweis, dass ein Dienst technisch erst nach Ankreuzen eines Einwilligungstextes genutzt werden kann.[68] Die Datenschutzkonferenz fordert insofern einen konkreten Einwilligungsnachweis auf Einzelnutzerebene.[69] Zur Erfüllung der Verpflichtung kann sich der Verantwortliche Hilfspersonen bedienen, solange und soweit sein jederzeitiges uneingeschränktes Recht zum Zugriff auf die Dokumentation rechtlich und tatsächlich sichergestellt ist.[70]

Eine Befristung der Nachweispflicht enthält Art. 7 Abs. 1 DSGVO nicht. Zur Wahrung der Verhältnismäßigkeit wird aber aus Art. 5 Abs. 1 lit. c DSGVO abzuleiten sein, dass die Pflicht zur Vorhaltung des Nachweises endet, wenn die Verarbeitung vollständig abgeschlossen ist, die personenbezogenen Daten beim Verantwortlichen nicht mehr vorhanden sind oder der Verantwortliche kein rechtliches Interesse (etwa mit Blick auf Schadensersatzprozesse) mehr daran hat, den Nachweis noch führen zu können (ggf. mit Ablauf der Verjährungsansprüche der Betroffenenrechte).[71]

c) Löschkonzept

Das Löschen von personenbezogenen Daten dient mehreren Grundsätzen der DSGVO wie z.B. der Datenminimierung, der Speicherbegrenzung und der Zweckbindung. Nach Art. 17 DSGVO ist der Verantwortliche auf Verlangen der Betroffenen zur Löschung, d.h. zur Unkenntlichmachung, der gespeicherten personenbezogenen Daten verpflichtet. Zudem besteht eine Löschpflicht, wenn es gesetzlich vorgegebene Speicherfristen gibt, die die maximale Speicherdauer bestimmter Daten begrenzen. Aus Art. 17 Abs. 1 DSGVO i.V.m. Art. 5 Abs. 1 Buchst b und c DSGVO i.V.m. dem u.a. in Art. 6 DSGVO normierten Grundsatz der Erforderlichkeit folgt zudem eine allgemeine Löschpflicht: Die Daten sind zu löschen, sobald sie nicht mehr erforderlich sind. Aufgrund des unionsrechtlichen Normwiederholungsverbots kann eine solche *allgemeine* Löschpflicht nicht im mitgliedstaatlichen Recht geregelt werden. Jedoch können und sollten konkrete Regelun-

---

[68] *Hanloser*, ZD 2019, 287 (288); *Stemmer*, in: BeckOK DatenschutzR, 31. Ed. 1.2.2020, DSGVO Art. 7 Rn. 87, 88; Artikel-29-Datenschutzgruppe, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, S. 25.

[69] ZD 2019, 287; Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, Stand: März 2019, abrufbar unter: www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf, s. dazu auch Artikel-29-Datenschutzgruppe, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, S. 25.

[70] *Spiecker gen. Döhmann*, in: Simitis/Hornung/, Datenschutzrecht, DSGVO Art. 7 Rn. 45.

[71] *Spiecker gen. Döhmann*, in: Simitis/Hornung/, Datenschutzrecht, DSGVO Art. 7 Rn. 44.

gen, die etwa die Löschung ein bestimmtes Ereignis knüpfen oder eine maximale Löschfrist festlegen, in den betreffenden datenschutzrechtlichen Regelungen enthalten sein. Diese sind in dem Zusammenhang stets auf ihre Einschlägigkeit zu prüfen.

Im Übrigen sieht die DSGVO keine starren, im Einzelnen definierte Löschfristen vor. Erwägungsgrund 39 DSGVO ist in diesem Zusammenhang aber zu entnehmen, dass der Verantwortliche Fristen für die Löschung der Daten oder aber eine regelmäßige Überprüfung vorsehen sollte, damit diese nicht länger als nötig gespeichert bleiben. Der Verantwortliche ist also verpflichtet zu dokumentieren, wie im Einzelnen mit den Antragsdaten umgegangen wird. Dazu zählt auch die Aufstellung eines Löschkonzepts. Die Pflicht, Löschfristen zu definieren, gilt unabhängig von einem entsprechenden Verlangen der Betroffenen nach Art. 17 DSGVO.

Der Verantwortliche kann sich zur Erarbeitung eines Löschkonzepts an den Grundsätzen der Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO), der Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO) und der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) orientieren. Nach diesen Grundsätzen ist stets festzulegen, zu welchem Zweck und auf welcher Rechtsgrundlage die Daten gespeichert werden können. In einem zweiten Schritt sind die verarbeiteten Daten in Datenkategorien einzuteilen (beispielsweise Protokolldaten, Antragsdaten, Log-Files etc.). Da diese Datenkategorien meistens zu unterschiedlichen Zwecken verarbeitet werden, ist anschließend zu überlegen, unter welchen Umständen und zu welchem Zeitpunkt der ursprüngliche Zweck der Verarbeitung entfällt. Mit Wegfall der Erforderlichkeit müssen die Daten gelöscht werden. Für die Bestimmung der Löschfrist kommt es darauf an, wie lange die Verarbeitung der Daten tatsächlich erforderlichen ist, also der mit der Verarbeitung intendierte Zweck erreicht ist. Besteht der Datenverarbeitungsschritt des Verantwortlichen beispielsweise darin, Daten an einen weiteren Verantwortlichen durchzuleiten, entfällt der Verarbeitungszweck nicht notwendigerweise bereits mit der Übermittlung der Daten an die empfangsberechtigte Behörde, sondern erst dann, wenn diese Daten rechtssicher bei der empfangsberechtigten Behörde eingegangen sind. Zu beachten sind jedoch stets die Ausnahmen, die Art. 17 Abs. 3 DSGVO vorsieht. Hier ist insbesondere Art. 17 Abs. 3 lit. e DSGVO praxisrelevant: Danach ist eine Speicherung von Daten solange zulässig, wie der Verantwortliche diese zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt.

Für Onlinedienste und Antragsportale sollen die folgenden Ausführungen als Denkanstöße dienen, hinsichtlich welcher Löschfristen der Verantwortliche bei der Konzeption Überlegungen anstellen sollte:

- **Cookies und Log-Files**

Cookies sind kleine Dateien, die auf den Endgeräten der Nutzenden gespeichert werden. Sie enthalten einen sog. Identifier sowie ggf. weitere Daten und sind daher personenbeziehbar. Sie werden eingesetzt, damit ein bestimmter Nutzer durch den Server „wiedererkannt“ werden kann. Es sind verschiedene Arten von Cookies zu unterscheiden:

- Beim Aufrufen einer Webseite werden häufig sogenannte Session-Cookies auf dem Endgerät der Nutzenden gespeichert. Session-Cookies dienen dazu, die grundlegenden Funktionalitäten der Webseite zu ermöglichen (Lastverteilung auf mehrere Server; kurzzeitige Speicherung der Inhalte eines Warenkorbs o.ä.). In der Regel müssen sie nicht länger als 30 Minuten verfügbar sein und können dann verfallen.
- Von Session-Cookies zu unterscheiden sind persistente (auch: permanente) Cookies. Persistente Cookies sind nicht nur für die Dauer einer Session verfügbar, sondern können eine deutlich längere „Lebensdauer“ von Tagen oder Monaten haben. Sie werden häufig für Webtracking genutzt, da sich mit ihnen das Nutzerverhalten über längere Zeit nachverfolgen lässt.

Schließlich werden beim Besuch einer Webseite bestimmte Daten der Nutzenden auch in sogenannten Logfiles gespeichert (meist: IP-Adresse, aufgerufene Webseite, Referrer, Zeitstempel o.ä.). Logfiles dienen meist dazu, die Webseite zu warten, Fehler zu finden und Cyberattacken zu entdecken und zu verfolgen. Wie lange Logfiles gespeichert werden, hängt davon ab, zu welchen Zwecken sie konkret eingesetzt werden sollen. Für die genannten Zwecke sind meist 60 bis 90 Tage ausreichend. Sofern sich aus bestimmten Sicherheitsstandards andere Anforderungen an die Speicherdauer ergeben, kann diese Zahl auch variieren.[72]

- **Rechtlich relevante Protokolldaten**

  Wird in einem Portal beispielsweise die elektronische Bekanntgabe eines Verwaltungsakts angeboten oder von einem Betroffenen eine Einwilligungserklärung eingeholt, so sollten der Abruf des Verwaltungsakts oder der Nachweis einer erteilten Einwilligung protokolliert werden. Das Protokoll muss dazu die erforderlichen personenbezogenen Daten enthalten. Für die Löschfrist der Protokolldaten muss geprüft werden, wie lange die Daten zum Zweck der Nachweisführung aufbewahrt werden müssen.

[72] So gilt etwa nach den BSI-Mindeststandards Bund für Protokollierung und Detektion von Cyberangriffen eine Aufbewahrung von Logfiles für eine Dauer von 90 Tagen; vgl. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_Protokollierung_und_Detektion_Version_1_0.pdf

- **Unvollständige Anträge**

  Wenn die Möglichkeit bestehen soll, einen Antrag zu beginnen und ihn zu einem späteren Zeitpunkt fortzusetzen, wird dieser unvollständige Antrag zwischengespeichert. Abgesehen davon, dass festzulegen ist, ob die Zwischenspeicherung automatisch oder manuell erfolgen soll, ist es notwendig, zu definieren, wie lange ein unfertiger Antrag im Antragssystem gespeichert bleiben soll. Dem Zweck einer nutzerfreundlichen Anwendung entsprechend, dürfte hier eine vierwöchige Speicherdauer genügen. Aus Gründen der Transparenz bietet es sich an, die Betroffenen beispielsweise eine Woche vor endgültiger Löschung des unfertigen Antrags, per E-Mail auf die bevorstehende Löschung hinzuweisen.

- **Wiederkehrende Anträge**

  Je nach zu digitalisierender Verwaltungsleistung kann eine Funktionalität des Portals die langfristige Speicherung einer größeren Menge von Antragsdaten sein, wenn die Verwaltungsleistung (die konkrete Antragstellung etwa) jährlich erneut in Anspruch genommen werden soll. In solchen Fällen bietet sich eine langfristige Speicherung an. Auch hier dürfen Daten aber freilich nicht unbegrenzt gespeichert bleiben. Überlegenswert ist in solchen Fällen die Verknüpfung der Löschung der langfristig gespeicherten Antragsdaten mit der Löschung des Fachnutzerkontos. Eine angemessene Löschfrist könnte sich hier etwa aus dem Umstand ergeben, dass ein Fachnutzerkonto zwei Monate länger als die wiederkehrende Antragsfrist ungenutzt bleibt.

- **Löschung nach elektronischer Einreichung eines Antrags**

  Handelt es sich um einen einmalig einzureichenden Antrag, der über das Portal elektronisch eingereicht werden kann, sollten die Antragsdaten nach erfolgreicher Übermittlung an Behörden im Fachverfahren beispielsweise, die die Daten unter eigener datenschutzrechtlicher Verantwortlichkeit verarbeiten, nicht länger als notwendig im Antragssystem verbleiben. Um hier besonders nutzerfreundlich zu agieren, ist es ggf. zu rechtfertigen, den Antrag noch eine gewisse Zeit (beispielsweise 30 Tage) vorzuhalten und ihn dann nach vorheriger Ankündigung per Mail automatisch zu löschen. Auch hier ist es aber stets eine Frage des Einzelfalls, ob sich eine längere Speicherung des Antrags nach Einreichung etwa aus dem Umstand ergibt, dass die Daten noch zum Nachreichen weiterer Daten und Dokumente für die Nutzenden zur Verfügung stehen sollen.

- **Löschung der Nutzerkonten**

Die Registrierungsdaten der Nutzenden können zum Zweck weiterer Antragstellungen beispielsweise im Antragssystem verbleiben und müssten so nicht jedes Mal erneut eingegeben werden. Technisch ist insofern einmal die manuelle Löschmöglichkeit des Nutzerkontos zu jedem beliebigen Zeitpunkt inklusive sämtlicher dort noch zwischen- oder langzeitgespeicherter Daten vorzusehen (§ 8 Abs. 4 OZG).

Daneben ist eine automatische Löschfrist zu definieren: Wird das Nutzerkonto für eine längere Zeit nicht genutzt (sog. verwaistes Nutzerkonto), sollte eine automatische Löschung nach vorheriger Ankündigung erfolgen. Die konkrete Löschfrist kann sich – wie oben ausgeführt – daran orientieren, wann in etwa mit einer erneuten Nutzung des Kontos zu rechnen ist, etwa weil die Frist eines wiederkehrenden Antrags abläuft. Wird das Konto innerhalb dieser Frist nicht benutzt, so kann sich eine automatische Löschung nach weiteren zwei Monaten anbieten. Gibt es keine wiederkehrende Antragsfrist, erscheint in der Regel eine automatische Löschung der Konten sechs Monate nach der letzten Anmeldung angemessen.

E. Erforderlichkeit der Abstimmung mit behördlichen Datenschutzbeauftragten und zuständigen Aufsichtsbehörden

Vor der Implementierung von Digitalisierungsprojekten sind die jeweiligen behördlichen Datenschutzbeauftragten der für den Datenschutz verantwortlichen Stellen (1) und – ggf. und nicht immer zwingend – die Aufsichtsbehörden auf Bundes- und Landesebene (je nach Zuständigkeit) einzubinden (2). Das „Ob", „Wie" und „Wann" ist je nach Projekt und je nach Zuständigkeit unterschiedlich zu beurteilen. Die Erfahrung in vorangegangenen Projekten zeigt jedenfalls, dass Verantwortliche sich zu den vorstehenden Einzelaspekten aus datenschutzrechtlicher und IT-sicherheitsbezogener Sicht idealerweise schon konzeptionelle Gedanken machen sollten, bevor die Aufsichtsbehörden involviert werden. Die behördlichen Datenschutzbeauftragten sind indes von Beginn an mit einzubinden, da hier auf die behördeninterne Erfahrung beim Umgang mit datenschutzrechtlich relevanten Themen, der Einbindung der zuständigen Aufsichtsbehörde und der üblichen prozeduralen Vorkehrungen innerhalb der jeweiligen Behörde (Umgang mit Betroffenenrechten, Verarbeitungsverzeichnis etc.) aufgebaut werden kann.

Aus rechtlicher Sicht sind ferner folgende Besonderheiten zu beachten:

- Auf Bundesebene sind keine Vorschriften relevant, nach denen der BfDI von einer innerhalb seines Zuständigkeitsbereiches liegenden öffentlichen Stelle proaktiv eingebunden werden muss. Lediglich § 69 BDSG sieht eine solche Einbindungspflicht dann vor, wenn es sich um eine Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung handelt.

- Einige Landesdatenschutzgesetze sehen dagegen Besonderheiten für die Konsultation der zuständigen Aufsichtsbehörden vor. In § 27 Abs. 5 DSG NRW heißt es beispielsweise:

  > *„Die oder der Landesbeauftragte für Datenschutz und Informationsfreiheit ist frühzeitig über Planungen zur Entwicklung, zum Aufbau oder zur wesentlichen Veränderung automatisierter Datenverarbeitungs- und Informationssysteme zu unterrichten, sofern in dem jeweiligen System personenbezogene Daten verarbeitet werden sollen. Entsprechendes gilt für Entwürfe für Rechts- oder Verwaltungsvorschriften des Landes, wenn sie eine Verarbeitung personenbezogener Daten vorsehen."*

  In § 24 Abs. 3 DSAG LSA heißt es:

  > *„Der Landesbeauftragte für den Datenschutz ist rechtzeitig über grundlegende Planungen des Landes zum Aufbau und*

> *zur Änderung von automatisierten Verfahren zur Verarbeitung von personenbezogenen Daten zu unterrichten. Er ist vor dem Erlass von Rechts- und Verwaltungsvorschriften, die den Umgang mit personenbezogenen Daten betreffen, zu hören.“*

Deshalb kann es – je nach landesrechtlicher Ausgestaltung – zwingend erforderlich sein, frühzeitig den Kontakt zu den zuständigen Aufsichtsbehörden zu suchen. Auch hier sollten dennoch grundlegende Entscheidungen behördlicherseits getroffen worden sein, um den Projektfortschritt nicht zu gefährden. Die Gesetze sehen jedenfalls lediglich eine Unterrichtungs-, nicht aber eine Zustimmungspflicht vor. Ein Konsens zwischen der federführenden Landesbehörde und der zuständigen Datenschutzaufsichtsbehörde ist insoweit nicht zwingend erforderlich.