Baustein 41 „Planung und Spezifikation“

Version: V1.0
Bezugsquelle: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

Hinweis: Dieser Baustein wurde von den Aufsichtsbehörden aus Hessen, Mecklenburg-Vorpommern, Sachsen, Schleswig-Holstein und der Evangelischen Kirche Deutschlands zur Erprobung der SDM-Methode erarbeitet und veröffentlicht. Dieser Baustein ist keine Publikation der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder.

1. Bezug zu Gewährleistungszielen

Transparenz

2. Beschreibung

Der Zweck einer Planungsphase besteht darin, alle normativen und funktionalen Aspekte zusammenzustellen, um die operative Gestaltung einer Verarbeitung und die erforderlichen technischen und organisatorischen Maßnahmen datenschutzrechtlich geführt zu bestimmen. Es sind Maßnahmen zu planen, die die operativen Anforderungen der DS-GVO sowie die Grundsätze aus Art. 5 erfüllen sollen. Darüber hinaus sind Maßnahmen zu planen, mit denen die Wirksamkeit der implementierten Maßnahmen nachgewiesen werden kann (Art. 32 Abs. 1 lit d). Um die Rechtskonformität einer Verarbeitung nachweisen zu können, muss sie u. a. kontrollierbar und prüfbar sein. Deshalb müssen in der Planungsphase einerseits alle relevanten Komponenten einer Verarbeitung zusammengestellt werden. Andererseits müssen Methoden zur Erstellung von Soll-Ist-Vergleichen für die technischen und organisatorischen Komponenten der Verarbeitung konzipiert werden. Die daraus resultierenden Prüfergebnisse müssen datenschutzrechtlich beurteilt werden können.

Die Mittel zur Gewährleistung von Kontrollierbarkeit und Prüfbarkeit sind

- die Spezifikation aus der Planungsphase,
- die Dokumentation der Daten, Komponenten und Prozesse der Verarbeitung sowie
- die Protokollierung des laufenden Betriebs.

Die Spezifikation einer Verarbeitung kann in einem Lastenheft und einem Pflichtenheft dokumentiert werden (M41.03). In einem Lastenheft formuliert der Auftraggeber (typischerweise: der Verantwortliche) seine Anforderungen. In einem Pflichtenheft legt der Auftragnehmer (bspw. ein Projektleiter oder ein externer Hersteller einer Fachapplikation) dar, wie er den Auftrag verstanden hat und welche der datenschutzbezogenen Anforderungen aus dem Lastenheft er in welchem Umfang, in welcher Qualität und Zeit umzusetzen beabsichtigt. Zeigen sich bei der Erstellung des Pflichtenheftes Unzulänglichkeiten, kann das dazu führen, dass der Auftraggeber das Lastenheft nachbessern und ggf. detaillierter formulieren muss.

Die Planung und Spezifikation einer Verarbeitung (Festlegung der Mittel i. S. d. Art. 4 Satz 1 Nr. 7 DS-GVO) ist ein wesentlicher Vorgang, um weitere Anforderungen der DS-GVO umsetzen zu können. So fordert die DS-GVO einerseits in Art. 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen („Data protection by design and by default“). Diese Forderungen lassen sich nur durch sorgfältige Planung und detaillierte Spezifikation einer Verarbeitung sachgerecht umsetzen.

Die DS-GVO fordert weiterhin bei besonders risikobehafteter Verarbeitung eine Datenschutz-Folgenabschätzung und in diesem Zusammenhang u. a. eine „systematische Beschreibung der geplanten Verarbeitungsvorgänge“ (Art. 35 DS-GVO Abs. 7). In die Planungsphase fällt sinnvollerweise auch die Durchführung zumindest des Teils einer Datenschutz-Folgeabschätzung (DSFA), in der das Risiko für Betroffene zu bestimmen ist (M41.01). Für die Durchführung von DSFA gibt es bereits einige Standard-Abläufe, die sich grundsätzlich an den Anforderungen des Artikels 35 DS-GVO orientieren. Diese Standard-Abläufe sind sehr gut geeignet, auch die Planung einer Verarbeitung zu organisieren und zu strukturieren. Insofern kann man die Planung einer Verarbeitung und die Durchführung einer Datenschutz-Folgenabschätzung in der Praxis in der Regel weitgehend zusammen durchführen. Das bedeutet nicht, dass für Verarbeitungen ohne hohes Risiko eine vollständige DSFA durchzuführen ist. Es soll vielmehr bedeuten, dass bei einer Verarbeitung mit geringem oder normalem Risiko die gleichen Fragen wie bei einer DSFA zu stellen und in der Planungsphase zu beantworten sind. Wird kein Standard-Konzept zur Planung einer Verarbeitung herangezogen, muss dieses vom Verantwortlichen selbst erarbeitet werden (M41.02).

Zur Durchführung einer DSFA empfiehlt sich die Verwendung des „Privacy-Frameworks“ des Forums Privatheit ab Version V3.0[1]. Die oben aufgelisteten Aspekte einer Planung werden von diesem Framework vollständig berücksichtigt. Daher ist das Framework auch zur Strukturierung der gesamten Planungsphase geeignet.

Die folgenden Aspekte einer Verarbeitung sind zu planen:

- **Beschreibung der Datenverarbeitung** („Verarbeitung“, „Verarbeitungstätigkeit“) unter funktionalen und organisatorischen Aspekten inkl. der Festlegung der Verantwortlichkeit (M41.04). Beschrieben werden müssen die zu verarbeitenden Daten, die dabei zum Einsatz kommenden IT-Systeme und Prozesse sowie der geplante Verarbeitungskontext zur Durchführung. Die Prüfung der rechtlichen Aspekte einer Verarbeitung ist zwar nicht Gegenstand des SDM sondern dem SDM vorgelagert. Sollte dort der Zweck der geplanten Verarbeitung jedoch noch nicht ausreichend beschrieben worden sein und noch nicht geklärt sein, dass er sowohl die rechtlichen Anforderungen erfüllen als auch den Weg zur funktionalen Umsetzung zeigen muss, ist dies hier im Rahmen der Beschreibung der Datenverarbeitung nachzuholen. Dabei ist es hilfreich, wenn auch die Grenzen der Verarbeitung beschrieben werden. Dazu sollte erläutert werden, welche anderen, denkbaren Zwecke explizit nicht verfolgt bzw. erfüllt werden.

- Identifikation und Dokumentation der an der Verarbeitung beteiligten **Organisationen/Akteure und der betroffenen Personen** (M41.05). Anhand der beteiligten Organisationen und Personen müssen sämtliche Rechtsbeziehungen mit ihren gesetzlichen Grundlagen sowie Erfordernisse für vertragliche Gestaltungen und das Einholen von Einwilligungen identifiziert werden.
- Identifikation und Dokumentation der für die Verarbeitung notwendigen **Rechtsgrundlagen** (M41.06). In der Regel müssen Verträge, Texte zur Einwilligung und Datenschutzerklärungen erstellt werden. Die Rechtsgrundlagen können Detailregelungen enthalten (bspw. Lösch- und Mindestaufbewahrungsfristen, Übermittlungsbefugnisse), die die allgemeinen Anforderungen aus der DS-GVO im Rahmen der Verarbeitung konkretisieren.
- Erarbeitung von Usecases, um daraus ein **Angreifermodell** für die Verarbeitung bilden zu können, in denen beteiligte Akteure befugt und unbefugt (als Angreifer) auf Daten zugreifen könnten (M41.07). Anhand der Usecases und Akteure können alle relevanten Komponenten erkannt werden, deren Funktionieren datenschutzrechtlich überprüft werden muss, um zum Schluss dann die Risiken der Betroffenen durch den geplanten Betrieb der Verarbeitung rechtlich beurteilen zu können.
- Bestimmung des **Risikos für die Rechte und Freiheiten Betroffener** durch die Verarbeitung zunächst für den Fall, dass die Daten zum vorgesehen Zweck verarbeitet werden und noch keine zusätzlichen technischen und organisatorischen Maßnahmen getroffen werden (M41.08). *Dieses Risiko entspricht dann dem Schutzbedarf der Betroffenen.* Werden die in der Planungsphase geforderten technischen und organisatorischen Maßnahmen vollständig umgesetzt, kann das Risiko der Verarbeitung im laufenden Betrieb auf ein rechtlich verantwortbares Maß verringert werden. Die Bestimmung des dann noch vorhandenen Risikos bildet die Grundlage für den Verantwortlichen zu entscheiden, ob vor der Inbetriebnahme eine DSFA durchzuführen ist.
- Die Erarbeitung einer angemessen Form der Dokumentation sowie der Dokumentation der **funktionalen Anforderungen** an die Verarbeitung und die technischen und organisatorischen Maßnahmen ist zu planen (M41.09). Das SDM soll dabei unterstützen, anhand der Gewährleistungsziele rechtlich erforderliche und geeignete technischen und organisatorischen Maßnahmen auszuwählen, die mit Blick auf das jeweilige Angreifermodell spezifiziert sein müssen.
- Erstellung und Dokumentation eines **Migrationskonzeptes** (M41.10) für den Fall, dass ein Altdatenbestand in eine neue Applikation übernommen werden muss.
- **Bestimmung und Dokumentation der technischen und organisatorischen Maßnahmen** als wesentlicher Teil des Pflichtenhefts. Dazu gehört auch das Festlegen der Konfigurationen und der Mittel, mit denen die Prüfbarkeit im laufenden Betrieb sichergestellt werden kann. Hierbei kann insbesondere der SDM-Maßnahmenkatalog herangezogen werden, um die funktionalen Anforderungen zu erkennen (M41.11).
- Erstellung eines **Berichtes aus den vorgenannten Dokumenten**. Dieser dient dann dem Verantwortlichen als Grundlage, um das Risiko zu beurteilen und über die

Implementation der Funktionen der Verarbeitung sowie der technischen und organisatorischen Maßnahmen zu entscheiden (M41.12).

- Erstellung eines **Konzeptes mit den Anforderungen an die Verarbeitung** anhand der vorgenannten Dokumentationen sowie der Entscheidungen des Verantwortlichen. zu. Dies kann in Form eines Lastenhefts geschehen. Dieses Konzept bzw. Lastenheft ist vor der Umsetzung vom Verantwortlichen förmlich abzunehmen (M41.13).
- Phase der **Implementation der Verarbeitungsprozesse und der technischen und organisatorischen Maßnahmen**. Dabei sind, unter Beachtung der realen Gegebenheiten vor Ort, in der Regel Spezifikation und Dokumentation zu ergänzen (M41.14). Spätestens für diese Phase ist die Verwendung einer Projektmanagement-Methode empfehlenswert.
- Erstellung eines **Testkonzeptes**. Anhand von Tests gegenüber dem Verantwortlichen muss dokumentierbar und nachweisbar sein, ob und in welchem Maße Teil-Anforderungen erfüllt werden können (M41.15).
- Erstellung eines **Pilotierungskonzeptes**, das für eine begrenzte Zeit den Produktionsbetrieb zu Testzwecken ermöglicht. Fehler, die sich sonst erst im Produktivbetrieb zeigen, können während dieser Pilotphase behoben werden (M41.16).
- **Prozess zur Freigabe der Verarbeitung** für den laufenden Betrieb. Dabei ist festzulegen, mit welchen Mitteln die permanente Überprüfung und Beurteilung des laufenden Betriebs der Verarbeitung im Kontext eines organisationsweit operierenden **Datenschutz-Managements** sichergestellt werden kann (M41.17).

3. Die zu spezifizierenden Ebenen einer Verarbeitung

Die Spezifikation einer Verarbeitung muss die folgenden Ebenen betrachten und darstellen:

- Die Gestaltung der **Prozesse** („Fachlichkeit“) die den fachrechtlichen und datenschutzrechtlichen Anforderungen genügen müssen,
- die Nutzung einer **Fachapplikation** durch die Sachbearbeitung,
- die **Technik** der Datenverarbeitung, der Prozesse, IT-Systeme und IT-Infrastrukturen,
- die **Schnittstellen** von Prozessen und IT-Systemen sowie
- die jeweilige **Administration** der vorgenannten Ebenen.

Spezifikation der fachlichen Prozesse

Diese Spezifikation umfasst eine Beschreibung von Prozessabläufen (M41.18) zum Erreichen des beschriebenen Zwecks, der dafür notwendigen Daten (M41.19) sowie eine zunächst nur allgemeine Beschreibung von Teilprozessen der Verarbeitung.

Für eine hochauflösende Planung und Spezifikation dieser Ebene ist eine Prozessmodellierung, bspw. mit den Mitteln des BPM (Business Prozess Modelling) empfehlenswert. Aus Datenschutzsicht sind hier die fachgesetzlichen und vertraglichen sowie die datenschutzrechtlichen Anforderungen zu berücksichtigen. Von dieser Ebene

ausgehend ist die Angemessenheit und Erforderlichkeit der technischen Umsetzung zu beurteilen.

Spezifikation der Fachapplikation (M41.20)

Die Spezifikation einer Verarbeitung sollte von der Ebene der Sachbearbeitung aus gestaltet werden. Entsprechend sind weitere arbeitsteilige Rollen zu definieren und Berechtigungen zu erteilen. Dabei sollten die folgenden Aspekte bzgl. der Sachbearbeitung beachtet werden:

- ausreichende Festlegung der Funktionalitäten der Fachapplikation,
- ausreichend gestaltete Anwendbarkeit der Fachapplikation (zweckgemäßes Nutzerinterface, Anwendungshandbuch),
- vollständige Dokumentation der Fachapplikation seitens des Herstellers (Systemhandbuch),
- klare Anweisungen (Dienstvereinbarungen) zur Sachbearbeitung bzw. zur Nutzung der Fachapplikation durch fachlich Vorgesetzte sowie
- Überprüfbarkeit bei Fehlhandlungen der Sachbearbeitung.

Zum Schutz von Bürgern, Kunden und Patienten ist in einem genau abgegrenzten und festgelegten Rahmen eine dem Schutzbedarf sind angemessene, datenschutzrechtliche Kontrollmöglichkeiten der Sachbearbeitung durch Vorgesetzte anhand von Protokollierungen zu planen, die jedoch nicht zur Leistungskontrolle zweckentfremdend genutzt werden dürfen.

Zur Spezifikation von Schutzvorkehrungen in der Fachapplikation empfiehlt es sich, folgende Fragen zu beantworten:

- Wie kann sichergestellt werden, dass die Fachapplikation in der vorgesehenen Zeit und an den gewünschten Orten (Telearbeit?) verfügbar ist?
- Wie lässt sich sicherstellen, dass die Richtigkeit der Daten und ggfs. der Berechnungen geprüft werden können?
- Wie kann sichergestellt werden, dass nur Befugte Zugriffe auf die Daten nehmen können?
- Wie kann der Umfang der Datenerfassung und der Berechnungen gestaltet werden, dass mit den Daten und genutzten IT-Systemen nur zweckgemäß gearbeitet werden kann?
- Wie kann sichergestellt werden, dass die Fachapplikation jederzeit geändert werden kann, so dass neue rechtliche und funktionale Anforderungen erfüllt werden können? Wie kann zugleich sichergestellt werden, dass keine nicht-autorisierten Änderungen durchgeführt werden können?
- Wie lässt sich sicherstellen, dass die Rechtmäßigkeit der Verarbeitung und der Nachweis darüber jederzeit erbracht werden kann?
- Wie lässt sich sicherstellen, dass Betroffene jederzeit darüber Auskunft erhalten können, welche Daten von ihnen verarbeitet werden?

Eine Fachapplikation muss in der Lage sein, Daten sicher zu speichern, zu verändern und zu löschen und ausgeführte Funktionalitäten im erforderlichen Umfang zu protokollieren.

Spezifikation der IT-Infrastruktur und der IT-Systeme (M41.21)

Fachapplikationen setzten auf IT-Infrastrukturen auf, die ihrerseits zur Umsetzung von Datenschutz- und IT-Sicherheitsanforderungen sorgsam zu spezifizieren und auszuwählen sind. Zu dieser Infrastruktur zählt die Hardware (PC und mobile Endgeräte, Server, Netzkomponenten wie Switche und Router, Netzwerkkabel und WLAN, Speichersysteme wie NAS oder SAN, Magnetplatten, SSDs, Bänder, optische Systeme, Drucker) sowie applikationsunabhängige Software (Betriebssysteme, virtuelle Betriebssysteme und Container, Middleware und IT-Dienste wie Mailsystem, Ticketsystem, Datenbanken, Sicherheitsgateways(Proxys, Firewalls), Drucker- bzw. MFC-Netzwerke, VPN-Zugänge).

Diese Systeme sind im Hinblick auf Betrieb, funktionale Eigenschaften und technisch-organisatorische Maßnahmen anhand des ausgewiesenen Zwecks und des Nachweises der Wirksamkeit der getroffenen Maßnahmen zu spezifizieren.

Um ein Netzwerk zu planen, müssen die folgenden Aspekte spezifiziert und in Form von Netzplänen dokumentiert sein:

- Festlegung der Topologie des Netzwerks,
- Festlegung der Hosts im Netzwerk,
- Festlegung der laufenden Services auf den Hosts,
- Konfiguration aller Services und Applikationen,
- Konfiguration aller Protokolle und Logs.

Spezifikation von Schnittstellen (M41.22)

Schnittstellen für Datenflüsse zwischen Systemen mit unterschiedlichen Verantwortlichen sind grundsätzlich als Indikatoren für potenzielle Zweckänderungen zu betrachten, denen deshalb eine besondere rechtliche Aufmerksamkeit geschenkt werden muss.

Zu solchen Schnittstellen zählen Hardware-Schnittstellen (Laufwerke, USB), Monitor und Drucker), Software-Schnittstellen (Exportoptionen aus Programmen, APIs, Zugriffe auf Datenbanken) sowie insbesondere Netzwerk-Schnittstellen an Routers und Switches, an denen Datenabflüsse eingerichtet werden können. Besondere Aufmerksamkeit muss auch generalisierten Adaptern gelten wie beispielsweise einem ESB (Enterprise Service Bus) oder einer Clearingstelle bzw. einem Nachrichtenbroker, bei denen die Kommunikationen über einen gemeinsam genutzten Kommunikationsbus für eine Vielzahl von Punkt-Zu-Punkt-Verbindungen zwischen Anbietern und Nutzern von Softwarediensten geleitet werden.

Die folgenden Fragen sind zu beantworten: Wie wird sichergestellt,

- dass eine rechtlich korrekt eingerichtete Schnittstelle verfügbar ist und dass der Status geprüft werden kann,
- dass diese Schnittstelle nur von befugten Empfängern/Sendern genutzt wird,
- dass die Nutzung der Schnittstelle – oder auch eine zurückgewiesene Nutzung – transparent erfolgt,

- dass eine Schnittstelle geschlossen werden kann und
- dass Änderungen in Formaten, Protokollen oder Aufrufformen, die sich auf die Nutzung der Schnittstelle auswirken, von der Schnittstelle auch berücksichtigt werden?

Spezifikation der Administration von Programmen und Systemen (M41.23)

Der Administration ist insofern besondere Beachtung zu schenken, weil ein Administrator einerseits mit weitreichenden Befugnissen ausgestattet sein muss, um die technischen Eigenschaften zu implementieren und zu konfigurieren. Andererseits ist ein Administrator rechtlich grundsätzlich nicht befugt, auf Inhaltsdaten der Sachbearbeitungsebene zuzugreifen.

Vielfach lässt sich ein Zugriff durch Administratoren insbesondere zur Behebung von Funktionsstörungen oder Systemänderungen aber nicht vollständig vermeiden. Weil beiden Anforderungen zugleich gerecht zu werden grundsätzlich schwierig ist, ist auf eine sorgfältige Planung und Dokumentation der Administrationstätigkeiten und des revisionsfesten Nachweises darüber insbesondere durch Protokollierung zu achten.

Eine Spezifikation der Aktivitäten und deren Überwachung sind in einem gesteigerten Maße notwendig, wenn die Fachadministration nicht durch organisationseigenes Personal geschieht, sondern bspw. eine Fernwartung durch externe Hersteller durchgeführt wird. Gleiches gilt, wenn ein Fachverfahren im Rahmen einer Auftragsverarbeitung in einem Rechenzentrum extern administriert wird.

In einem genau abgegrenzten und festgelegten Rahmen ist eine datenschutzrechtliche Kontrolle einer Administration, zum Schutz der von der Sachbearbeitung verarbeiteten Daten Betroffener, anhand von fachlichen Protokollierungen notwendig, die jedoch nicht zur Leistungskontrolle genutzt werden dürfen.

Folgende Fragen müssen in Bezug auf Administratoren in einer Planungsphase beantwortet werden: Wie ist sichergestellt, dass:

- Administratoren ausreichend verfügbar sind (Service Level etc.),
- nur solche Administratoren eingesetzt werden, die fachlich ausgebildet sind und kompetent agieren; das betrifft auch den Vertretungsfall,
- nur vertrauenswürdige und befugte Administratoren tätig werden, die nachweisbar auf Wahrung der Vertraulichkeit verpflichtet wurden,
- sämtliche relevante Administrationstätigkeiten vollständig und integer protokolliert und in angemessener Weise durch Vorgesetzte nachweislich überprüft werden,
- Administratoren keinen Rollenkonflikten unterliegen bzw. arbeitsteilig agieren und
- Administratoren an Änderungen von Verarbeitungstätigkeiten angemessen beteiligt sind?

4. Referenzen

Forum Privatheit, 2017: „Whitepaper Datenschutz-Folgenabschätzung", https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum-Privatheit-WP-DSFA-3-Auflage-2017-11-29.pdf

Rupp, Christine, 2014: Requirements-Engineering und -Management: Aus der Praxis von klassisch bis agil, Hanser-Verlag.

5. Zusammenfassung der Maßnahmen

M41.01 Entscheidung herbeiführen, ob eine DSFA gem. Art. 35 DS-GVO durchzuführen ist
M41.02 Erstellung eines Planes zur Gestaltung der Planungsphase
M41.03 Planung der Erstellung eines Lasten- und Pflichtenhefts
M41.04 Planung der Erarbeitung einer an den funktionalen und organisatorischen Notwendigkeiten eines Projekts orientierte Beschreibung der Verarbeitung
M41.05 Planung der Erarbeitung einer Dokumentation, in der Akteure, Beteiligte und Betroffene identifiziert werden, einschließlich der Rechtsbeziehungen untereinander.
M41.06 Planung der Erarbeitung einer Übersicht der vorhandenen und der zu schaffenden Rechtsgrundlagen
M41.07 Planung der Erarbeitung eines Angreifer- bzw. Vertrauensmodells für die Verarbeitung
M41.08 Planung der Bestimmung des Risikos bzw. Schutzbedarfs für Betroffene
M41.09 Planung der Erarbeitung der Dokumentation der funktionalen Anforderungen
M41.10 Ggfs. Planung der Erstellung eines Migrationskonzepts für die Übernahme des Altdatenbestands
M41.11 Planung der Bestimmung der technischen und organisatorischen Maßnahmen
M41.12 Planung des Berichts an den Verantwortlichen bzgl. der zu treffenden Entscheidungen zum weiteren Fortgang
M41.13 Planung der Erstellung des Umsetzungskonzepts entsprechend den Planungen und Entscheidungen
M41.14 Planung der Implementationsphase der Verarbeitung und der technischen und organisatorischen Maßnahmen
M41.15 Planung der Erstellung eines Test
M41.16 Planung der Erstellung eines Pilotierungskonzepts
M41.17 Planung des Übergangs vom Projekt in den Produktionsbetrieb sowie Eingängen der Überwachung der Verarbeitung in das organisationsweite Datenschutz-Management.
M41.18 Planung der Erstellung der Dokumentation der Prozessabläufe
M41.19 Planung der Erstellung der Dokumentation der zu verarbeitenden Daten
M41.20 Planung der Spezifikation der Fachapplikation
M41.21 Planung der Spezifikation der IT-Infrastruktur und IT-Systemen
M41.22 Planung der Spezifikation der Schnittstellen

M41.23 Planung der Spezifikation der Adminstrationstätigkeiten auf den verschiedenen Ebenen („Administrationskonzept“)

6. Anmerkung zur Nutzung dieses Bausteins

Dieser Baustein darf – ohne Rückfrage bei einer Aufsichtsbehörde – kommerziell und nicht kommerziell genutzt, insbesondere vervielfältigt, ausgedruckt, präsentiert, verändert, bearbeitet sowie an Dritte übermittelt oder auch mit eigenen Daten und Daten Anderer zusammengeführt und zu selbständigen neuen Datensätzen verbunden werden, wenn der folgende Quellenvermerk angebracht wird:

„Datenschutzaufsichtsaufsichtsbehörden der Bundesländer Hessen, Mecklenburg-Vorpommern, Sachsen, Schleswig-Holstein sowie der Evangelischen Kirche Deutschlands. Datenlizenz Deutschland – Namensnennung – Version 2.0 (www.govdata.de/dl-de/by-2-0).“