Baustein 50 „Trennen“

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

Versionshistorie	gültig seit	gültig bis
SDM-V2.0_Trennen_V1.0	06.10.2020	

1. Bezug zu den Anforderungen der DS-GVO und den Gewährleistungszielen

Dieser Baustein dient vorrangig der Umsetzung folgender DS-GVO-Anforderungen (vgl. SDM-V2-Methodik-Handbuch, Teil B):

Anforderungen der DS-GVO	Gewährleistungsziele
Zweckbindung (Art. 5 Abs. 1 lit. b DS-GVO)	Nichtverkettung
Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO)	Datenminimierung
Vertraulichkeit (Art. 5 Abs. 1 lit. f DS-GVO)	Vertraulichkeit
Löschbarkeit von Daten (Art. 17 Abs. 1 DS-GVO)	Intervenierbarkeit

2. Beschreibung

Für jede Verarbeitung personenbezogener Daten muss zunächst geklärt werden, welchen Zwecken sie dienen soll. Dazu muss eine *Zweckbeschreibung* der Verarbeitungstätigkeit erfolgen, die zu dokumentieren ist. Die Zweckbeschreibung muss den Zweck so eng fassen, dass die Grenzen der Verarbeitungstätigkeit mit den für den Prozess der Verarbeitung notwendigen und erforderlichen Daten im dafür angemessenen Umfang technisch und datenschutzrechtlich bestimmbar sind. Zusätzlich sollte eine explizite Abgrenzung der Zwecke (*Zwecktrennung)* von anderen, insbesondere von thematisch „benachbarten“ Verarbeitungstätigkeiten, Verarbeitungen oder auch Befugnissen bei Zugriffen auf Datenbestände erfolgen. Wenn Verarbeitungstätigkeiten voneinander logisch bzw. funktional getrennt sind, muss eine *Zweckbindung* jeder beabsichtigten Verarbeitungstätigkeit und der dafür eingesetzten Daten, Prozesse und Systeme sowie Dienste insbesondere durch Trennungsmaßnahmen durchgesetzt werden (M50.D01).

Diese aus der Zweckbeschreibung heraus begründeten Trennungsanforderungen werden typischerweise auf der logischen Verarbeitungsebene formuliert und dann organisatorisch durch Bildung von Arbeitsgruppen, Referaten, Abteilungen, Filialen und Bereichen durchgesetzt. Diese Anforderungen nach Zwecktrennung und Zweckbindung dürfen nicht von der Informationstechnik (IT), die für eine Datenverarbeitung genutzt wird, unterlaufen werden. Die Informationstechnik muss vielmehr diese Trennungsgebote unterstützen. Die für die Verarbeitung personenbezogener Daten eingesetzte Informationstechnik muss am Zweck der Verarbeitungstätigkeit orientiert eingerichtet sein, zweckgesteuert betrieben und auf Dauer vorgehalten werden.

Als Beispiel: Ein Krankenhaus muss Patienten mit ihren Daten verwalten. Es ist deshalb generell befugt, Patientendaten in Form einer Patientenakte zu führen. Krankenhäuser eines Klinikverbunds können dafür Informationstechnik gemeinsam zur Verarbeitung von Patientenakten nutzen. Dabei ist zu beachten, dass die einzelnen Kliniken diese Informationstechnik für Verarbeitungstätigkeiten nutzen, die in ihrer Verantwortlichkeit liegen und von den Verarbeitungstätigkeiten der anderen Kliniken zu trennen sind. Das heißt, dass die Patientendaten der verschiedenen Krankenhäuser in Abhängigkeit des Risikos für die Rechte und Freiheiten der Patienten logisch oder physikalisch getrennt verarbeitet werden müssen. Gleiches gilt für unterschiedliche Verarbeitungstätigkeiten innerhalb der einzelnen Krankenhäuser, die sich beispielsweise auf bestimmte Fachabteilungen beschränken.

Zusammenfassend gilt: Unterschiedliche Zwecke von Verarbeitungstätigkeiten erzeugen unterschiedliche Befugnisse zur Verarbeitung von Daten, die unterschiedliche Trennungsmaßnahmen erfordern.

2.1 Abgrenzung zu anderen Bausteinen

Dieser Baustein listet Prüfschritte und Maßnahmen auf, mit denen Trennungsanforderungen an Daten, Systeme und Dienste sowie Prozesse sowohl innerhalb einer Organisation als auch von miteinander zusammenarbeitenden Organisationen umgesetzt werden können. Eine Trennung ist eine Voraussetzung dafür, rechtlich zulässige Verbindungen zwischen verschiedenen Organisationen und Organisationseinheiten (Arbeitsgruppen, Referaten, Abteilungen, Filialen, Bereichen) mit deren Daten, Systemen und Diensten sowie Prozessen unter organisatorischen und technischen Bedingungen herstellen zu können.

Nicht Gegenstand dieses Bausteins ist die Trennung von unterschiedlichen Rollen und Berechtigungen sowie die Abtrennung der Personendaten von Inhalts- und Kommunikationsdaten durch Pseudonymisierung oder Anonymisierung; für diese Maßnahmen sind eigene Bausteine vorgesehen.

2.2 Maßnahmen zur Durchsetzung der Trennung

Ein abgeschlossener Datenhaltungs- und Verarbeitungskontext eines Verantwortlichen – hier in der Regel für eine Verarbeitungstätigkeit – wird nachfolgend als „Mandant“ bezeichnet, die getrennte Verarbeitung im Rahmen von verschiedenen Verarbeitungstätigkeiten als „Mandantentrennung“. Die zur Datenverarbeitung eingesetzte Informationstechnik mit ihren einzelnen IT-Komponenten gilt dann als „mandantenfähig“, wenn sie in der Lage ist, zwischen verschiedenen Mandanten eine notwendige und erforderliche Trennung umzusetzen.

In diesem Baustein verwendete Begriffe werden wie folgt definiert:

- **Gemeinsam genutzte Informationstechnik** umfasst alle technischen Mittel zur Verarbeitung personenbezogener Daten, die nicht physisch voneinander getrennt

sind und die von verschiedenen Mandanten genutzt werden. Hierzu gehören beispielsweise die gemeinsam genutzte Infrastruktur (Gebäude, Räume, Energieversorgung, Klimatisierung und die Verkabelung), die Anwendungssysteme für mehrere Mandanten sowie gemeinsame Datenbank-Managementsysteme und Datenbanken, Netzwerkkomponenten, Speicher- und Managed-Storage-Systeme sowie Backup-Systeme in konventionellen und in virtualisierten Umgebungen. Betreiber gemeinsam genutzter Informationstechnik kann einer der nutzenden Verantwortlichen selbst oder ein Auftragsverarbeiter sein. Ebenso kann die Informationstechnik gemeinsam von mehreren Verantwortlichen im Sinne des Art. 26 DS-GVO betrieben werden. Zwischen den an der gemeinsam genutzten Informationstechnik Beteiligten (Betreiber, nutzende Verantwortliche) MÜSSEN entsprechende Vereinbarungen im Sinne des Art. 26 DS-GVO getroffen werden (M50.P15). Zwischen Verantwortlichen und Auftragsverarbeitern MÜSSEN Verträge gemäß Art. 28 abgeschlossen werden (M50.P16).

- Ein **Datenzugriff** ist die Ausführung einer (möglicherweise komplexen) Funktion eines Komponenten-übergreifenden Systems oder Dienstes, mit dem personenbezogene Daten verarbeitet werden; ein Datenzugriff kann insbesondere die Ausführung einer Folge von einzelnen Verarbeitungsschritten bewirken.
- **Transaktionen** sind unteilbare, konsistente und gegeneinander isolierte logische Einheiten in beliebig komplexer Informationstechnik, insbesondere von Programmschritten eines Systems.

Die Qualität einer Trennung lässt sich nicht als Eigenschaft eines Datums, eines Systems bzw. Dienstes oder eines Prozesses erkennen, sondern nur als Beobachtung eines Zusammenhangs. Deshalb ist es sinnvoll, Prüf-Schritte zu formulieren, mit denen bei der Planung einer Verarbeitung eine ausreichende Trennung etwa bei der gemeinsam genutzten Informationstechnik festgelegt bzw. das Maß einer Trennung beurteilt werden kann.

Wird die gemeinsam genutzte Informationstechnik zur getrennten Verarbeitung personenbezogener Daten genutzt, so MUSS der Betreiber dieser Technik ein mandantenübergreifendes Datenschutzmanagement zur „regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technisch-organisatorischen Maßnahmen“ (Art. 32 Abs. 1 lit. d) DSGVO) treffen (M50.P07). Die Prüfergebnisse MÜSSEN allen für die Mandanten Verantwortlichen zur Verfügung stehen. Das betrifft insbesondere solche, aus denen sich mandantenübergreifende Auswirkungen ergeben können. Dabei MUSS eine Beteiligung aller für die Mandanten Verantwortlichen bei der Bearbeitung der Datenschutz- und Sicherheitsvorfälle vorgesehen sein (M50.P13).

Ein gemeinsames, mandantenübergreifendes Datenschutz- und IT-Sicherheitsmanagement der Informationstechnik MUSS in die betrieblichen Prozesse des Betreibers eingebunden sein (M50.P06). Insbesondere MUSS die Planung und Umsetzung von datenschutz- und sicherheitsrelevanten Änderungen an der gemeinsam genutzten Informationstechnik, unter

Beteiligung der Datenschutz- und Sicherheitsmanagements aller für die Mandanten Verantwortlichen, erfolgen.

2.2.1 Fünf Prüfschritte zur Beurteilung ausreichender Trennung der Verarbeitungen

Prüfschritt 1: Rechtliche Grundlagen

Die Festlegung, welche technischen und organisatorischen Maßnahmen erforderlich sind, um eine ausreichende Trennung von Verarbeitungen entsprechend unterschiedlicher Zwecke zu erreichen, setzt eine rechtliche Beurteilung voraus. Dazu sind sowohl die für die jeweilige Verarbeitungstätigkeit anzuwendenden spezialgesetzlichen Bestimmungen als auch die allgemeinen, datenschutzrechtlichen Bestimmungen heranzuziehen. Die Anwendbarkeit dieser rechtlichen Bestimmungen MUSS bereits im Vorfeld der Anwendung des SDM beurteilt worden sein.

Die Datenverarbeitung und die technischen und organisatorischen Maßnahmen müssen die rechtlichen Vorgaben erfüllen. Für den Aspekt der Trennung sind die folgenden Fragen zu stellen und anhand der jeweils gegebenen Antworten zu beurteilen:

- Welche Rechtsgrundlage, Zweckbeschreibung und Zweckbindung liegen der jeweiligen Verarbeitungstätigkeit zugrunde?
- Welche Verantwortlichen sollen welche Verarbeitungstätigkeiten auf einer gemeinsam genutzten Informationstechnik nutzen?
- Welche Verantwortlichen sind für welche Verarbeitungen gemeinsam verantwortlich?

Ob verschiedene Verarbeitungstätigkeiten auf einer gemeinsam genutzten Informationstechnik betrieben werden dürfen, hängt von dem daraus resultierenden Risiko für die Rechte und Freiheiten der Betroffenen ab. Resultiert allein aus der gemeinsamen Nutzung einer Informationstechnik ein hohes Risiko, wird eine solche gemeinsame Nutzung nicht zulässig sein. Ein weiteres Ausschlusskriterium für eine gemeinsame Nutzung von Informationstechnik kann aus Rechtsnormen resultieren, die die gemeinsame Nutzung verbieten, weil damit eine unzulässige Offenbarung verbunden sein kann. In diesen Fällen ist Trennung verschiedener Verarbeitungstätigkeiten bzw. ein Betrieb durch verschiedene Verantwortliche, die nicht nur durch softwaretechnische Maßnahmen realisiert wird, geboten.

Bevor die Anforderungen für die Übermittlung personenbezogener Daten zwischen verschiedenen Mandanten festgelegt werden, muss geklärt werden, in welcher Form die Informationstechnik für eine Verarbeitung betrieben werden soll. Die Spannbreite reicht von einem vollständigen Betrieb der Informationstechnik für eine Verarbeitungstätigkeit in organisationseigenen Räumen durch den Verantwortlichen selbst bis zu einem vollständigen Betrieb der Informationstechnik durch Auftragsverarbeiter (bspw. Rechenzentren). In der Praxis finden sich zahlreiche Mischformen zwischen der Datenverarbeitung allein durch den Verantwortlichen selbst und der vollständig externen Auftragsverarbeitung vor.

a) Besteht ein verfassungsrechtlich begründetes Trennungsgebot?

Es gibt im Kontext insbesondere der öffentlichen Verwaltung verfassungsrechtlich begründete strukturelle Anforderungen an eine Trennung von Verarbeitungstätigkeiten oder einzelnen Verarbeitungen und deren dafür verwendeten Komponenten, die aus datenschutzrechtlicher Sicht von den Verantwortlichen zu beachten sind. Im öffentlichen Bereich sind Organisationen gemäß den drei horizontalen Gewalten (Legislative, Exekutive, Judikative) und diesen drei vertikalen Gewalten (Bund, der Länder und Gemeinden) institutionalisiert. Das Bundesverfassungsgericht hat im Volkszählungsurteil den datenschutzrechtlichen Grundsatz der informationellen Gewaltenteilung (Abschottungsgebot) entwickelt, welcher staatliche Behörden dazu verpflichtet, personenbezogene Daten auch gegenüber anderen staatlichen Behörden abzuschotten. Rechtsgründe für die Trennung von Verarbeitungen sind gesetzliche Vorgaben, insbesondere unterschiedliche Zweckbeschreibungen der Datenverarbeitung, und die Tatsache, dass für verschiedene Teilsysteme unterschiedliche Verantwortliche existieren. Die Verantwortlichen der Verwaltungen müssen diese strukturell wichtigen Trennungsgebote daher schon bei der Wahl geeigneter IT-Dienstleister (Auftragsverarbeiter) berücksichtigen (M50.P03).

Rechenzentren arbeiten üblicherweise als IT-Dienstleister für eine Vielzahl von Verantwortlichen. Datenschutzrechtlich problematisch wird es, wenn etwa ein Landesrechenzentrum für mehrere der oben genannten Gewalten Daten verarbeitet und die verfassungsrechtlich gebotene informationelle Gewaltenteilung gefährdet; dies kann zu einem erhöhten Risiko für die wirksame Wahrung der Grundrechte betroffener Personen führen. Es ist ebenfalls ein Problem, wenn Verantwortliche in wenigen oligopolartig strukturierten Rechenzentren („Clouds“) Daten verarbeiten lassen, bei denen generell weder die technischen und organisatorischen Maßnahmen geprüft werden können, noch die Zugriffe auf die Daten transparent sind oder keine wirksamen Mechanismen ausgewiesen sind, mit denen der Verantwortliche beim Auftragsverarbeiter Trennungsanforderungen durchsetzt. Jeder für einen Mandanten Verantwortliche MUSS die Wirksamkeit von Trennungsmaßnahmen in seiner Hoheit nachweisen und die Anforderungen an Spezifikation, Dokumentation und Protokollierung sowie die Kontrolle und die Überprüfung des laufenden Betriebs umsetzen (M50.S01).

b) Besteht ein Trennungsgebot innerhalb von Organisationen?

Innerhalb von Organisationen, gleichgültig ob es sich dabei bspw. um Verwaltungen, Unternehmen oder Forschungsinstitute handelt, bildet eine Verarbeitungstätigkeit („Fachverfahren“) den Ausgangspunkt zur Bewertung und Beurteilung der Durchsetzung datenschutzrechtlicher Anforderungen bzw. von Trennungen.

Die Datenbestände unterschiedlicher Verarbeitungstätigkeiten sind aufgrund unterschiedlicher Zwecke grundsätzlich zu trennen. Eine Voraussetzung für eine wirksame Trennung ist die eindeutige Zuordnung der zu verarbeitenden Daten zu den jeweiligen Verarbeitungstätigkeiten. Auf der Ebene der Systeme bilden die Fachapplikationen die

Ausgangspunkte zur jeweiligen Trennung der IT-Komponenten, die mit der Fachapplikation verbunden sind (z. B. Netzwerksegmente, CPU-Cluster, Speichersysteme).

Rechtlich gebotene Grenzen des Zugriffs auf Daten, Systeme und Dienste sowie Prozesse dürfen weder durch hierarchisch übergeordnete Rollen willkürlich aufgehoben werden noch durch die verwendete Informationstechnik bzw. von den eingebundenen IT-Dienstleistern unterlaufen werden können.

In akuten Notfällen können diese Trennungsgebote aufgehoben werden. Eine derartige Aufhebung darf keinesfalls leichtfertig erfolgen. Sie muss rechtlich begründet und zeitlich befristet sein. Es muss zumindest im Nachhinein beurteilt werden, ob tatsächlich ein unabweisbarer Notfall oder ob ein Organisationsversagen vorlag. Der Zweck einer solchen nachträglichen Beurteilung ist es zu erkennen, ob eine Rechtsgrundlage vorlag und ob die Standardprozesse zur Bearbeitung von Störungen und Angriffen sowie der Identifikation von Notfällen verbessert werden müssen. Eine wichtige Maßnahme ist deshalb die Erstellung eines Notfall-Konzepts. Verantwortliche SOLLTEN in einem Notfall-Konzept anhand von Beispielen zeigen, in welchen Fällen kein Notfall vorliegt und wie die gestufte Aufhebung von Trennungen erfolgt (M50.P09).

Verantwortliche MÜSSEN durch die Einrichtung und Wahrung zweckgerichteter Einheiten (Abteilungen, Referate, Arbeitsgruppen) sicherstellen, dass die zweckgemäßen Verarbeitungen personenbezogener Daten auf der Ebene der Sachbearbeitung einer Organisation durch entsprechende organisatorische Einteilungen ordnungsgemäß umgesetzt werden können. Dazu gehört auch, dass Datenflüsse zwischen Bereichen mit unterschiedlichen Zwecken grundsätzlich unterbunden sind und nur unter definierten Bedingungen gesichert eingerichtet und dann kontrolliert, prüf- und beurteilbar über dokumentierte und prüfbare Schnittstellen erfolgen können.

In Bezug auf die oftmals heterogene Informationstechnik MÜSSEN Verarbeitungen, Prozesse und Datenflüsse entsprechend der Dienste identifiziert und getrennt werden. Netzzugänge, Server- und Speicherkomponenten sind ggf. getrennt von anderen Netzen, Servern und Speichermedien zu betreiben. Eine Trennbarkeit von IT-Komponenten ist Voraussetzung für die Zuordnung von Zuständigkeiten für Datenbestände, Systeme und Dienste sowie Prozesse der Datenverarbeitung (M50.P11). Dadurch sind Weisungshierarchien organisatorisch implementierbar.

Es lassen sich **physikalische Trennungen** von Organisationen (konventionell durch Gebäude) sowie innerhalb von Organisationen (Räume, IT-Komponenten, Netzwerke, Speichersysteme) von **logischen Trennungen** innerhalb von Organisationen unterscheiden (Abteilungen, Abteilungen übergreifende und eigenständige Projektgruppen, Revisoren und Auditoren; Sicherheitszonen, virtualisierte -Systeme, virtuelle Local-Networks, virtualisierte Speichersysteme, Betriebssysteme, Middleware, Anwendungsprogramme).

Es MUSS sichergestellt werden, dass die Trennungsgebote, die für gemeinsam genutzte IT-Komponenten gelten, auch in allen darüber liegenden Schichten der gemeinsam genutzten Informationstechnik gewahrt bleiben: Bspw. darf es keine Softwarekomponente geben, die Daten verschiedener Mandanten aggregiert, für die ein Trennungsgebot vorliegt (M50.S17).

Prüfschritt 2: Ausgestaltung revisionsfester Übermittlungen zwischen Mandanten

Aus den bislang genannten Gründen stellt bei einer getrennten Verarbeitung in einer gemeinsam genutzten Informationstechnik die Verarbeitung von Daten eines Mandanten bzw. einer Verarbeitungstätigkeit in einem anderen Mandanten rechtlich eine Datenübermittlung dar. Die rechtlichen Grundlagen und Anforderungen an die Zulässigkeit einer Übermittlung und die Form ihrer Durchführung sind vorab zu prüfen. So können abhängig vom anwendbaren Recht besondere Anforderungen an den automatisierten Abruf von Daten oder die Übernahme von Daten aus einem gemeinsam verantworteten Datenbestand bestehen (M50.P08).

Die Auswahl der zu übermittelnden Daten darf in jedem Fall nur an Identitätsdaten (Name, Vorname, etc.) und an solche Attribute oder Eigenschaften der betroffenen Person anknüpfen, für deren Übermittlung eine Rechtsgrundlage besteht (M50.D02). Zulässige Suchkriterien sind in der Regel vorher vertraglich festzulegen oder durch andere Rechtsgrundlagen geregelt (M50.D03). Die Einschränkung auf diese Suchkriterien MUSS technisch durchgesetzt werden. Übermittelte Daten MÜSSEN dem empfangenden Mandanten zugeordnet werden, um die neu entstandene rechtliche Verantwortung zu kennzeichnen. Die Übermittlung MUSS protokolliert werden (M50.D04). Zur Isolierung der Übermittlung von Verarbeitungsschritten (Transaktionen) innerhalb eines Mandanten darf auf übermittelte Daten erst nach Abschluss der Übermittlung zum empfangenden Mandanten und ihrer Protokollierung zugegriffen werden. Die Übermittlung darf nicht durch Zugriffe eines Mandanten auf die Datenbasis eines anderen Mandanten ermöglicht werden.

Sofern Daten zwischen Mandanten übermittelt werden, MUSS insbesondere die (Daten-)Integrität sichergestellt werden. Es MÜSSEN beim datenschutzrechtlich notwendigen Trennen Prüfungen hinsichtlich der Konsistenz der Datenbestände innerhalb der gemeinsam genutzten IT-Komponenten sowie in allen darüber liegenden Schichten der gemeinsam genutzten Informationstechnik vorgenommen werden. Solche Konsistenzprüfungen SOLLTEN automatisiert durchgeführt werden und MÜSSEN regelmäßig wiederholt werden (M50.P17).

Prüfschritt 3: Abgeschlossenheit von Verarbeitungsschritten innerhalb eines Mandanten

Zur Prüfung auf eine ausreichende Trennung einzelner Mandanten auf von beiden Mandanten gemeinsam genutzter Informationstechnik ist die „Abgeschlossenheit“ der Datenverarbeitung innerhalb eines Mandanten zu betrachten. Die Prüfung auf Abgeschlossenheit MUSS anhand einzelner Verarbeitungsschritte erfolgen einschließlich des Nachweises, dass die Datentrennung dabei erhalten bleibt.

Ein Mandant gilt als „abgeschlossen“, wenn jeder Verarbeitungsschritt, am Beispiel von Transaktionen einer Datenbank veranschaulicht, innerhalb eines Mandanten einen gültigen Datenbestand dieses Mandanten in einen neuen gültigen Datenbestand überführt und hierbei von Daten anderer Mandanten nicht abhängt und auf diese Daten aufgrund technischer Maßnahmen weder lesend noch schreibend zugreift (M50.S02).

Diese Prüfung auf Abgeschlossenheit MUSS ganzheitlich für alle zur Verarbeitung genutzten IT-Komponenten durchgeführt werden. Die Datenhaltung MUSS jedoch stets so organisiert werden, dass für jede Repräsentation eines personenbezogenen Datums die Zuordnung zu genau einem Mandanten erfolgt. Eine ausreichende Trennung der Daten auf Ebene der Datenhaltung kann durch unterschiedliche Techniken erfolgen, z. B. in einer Datenbank durch eine abgeschlossene Einheit mit eigenen Datensätzen und einem vollständigen Satz von Tabellen. Sämtliche Zugriffe auf personenbezogene Daten MÜSSEN die vergebenen Zugriffsberechtigungen sowie diese Zuordnung berücksichtigen und durchsetzen.

Die Abgeschlossenheit eines Mandanten bedingt zwangsweise auch eine sicherheitstechnische Isolation eines Mandanten. Bei ausreichender Trennung der Datenverarbeitung SOLLEN Datenschutzprobleme oder -vorfälle eines Mandanten nicht zu Datenschutzproblemen oder -vorfällen anderer Mandanten führen (M50.S03). Wäre beispielsweise in einem System die Möglichkeit gegeben, mandantenübergreifende Zugriffe auf eigene Daten oder Daten eines anderen Mandanten zu initiieren, ohne dass die oben genannten Voraussetzungen für eine Übermittlung vorliegen, oder wird diese Möglichkeit nur durch organisatorische Maßnahmen ausgeschlossen, so läge keine Abgeschlossenheit vor und die Mandantentrennungsfähigkeit wäre nicht gegeben.

Prüfschritt 4: Unabhängigkeit der Konfigurationen unterschiedlicher Mandanten

Eine ausreichende Mandantentrennung setzt voraus, dass die Zugriffsberechtigungen, die Verarbeitungsfunktionen und die Konfigurationseinstellungen je Mandant eigenständig festgelegt werden. Zugangsberechtigungen MÜSSEN eigenständig vergeben bzw. mandantenspezifische Benutzerkennungen MÜSSEN eigenständig angelegt werden können, mit denen nur auf Daten des eigenen Mandanten zugegriffen werden kann (M50.S04). Datenschutzrechtliche Anforderungen MÜSSEN auf Mandantenebene umgesetzt und gemäß den Vorgaben der einzelnen Mandanten konfigurierbar sein.

Folgende Anforderungen MÜSSEN mandantenspezifisch zumindest vorgesehen sein:

- getrennte Systeme zur Berechtigungsvergabe (M50.S05),
- Konfigurationsmöglichkeiten für die Nutzungsprotokollierung (M50.S06) sowie
- eine administrative Protokollierung (M50.S07).

Die Berechtigungsvergabe MUSS über ein Berechtigungssystem erfolgen, das auf Ebene des einzelnen Mandanten abgeschlossen ist (M50.S11). Hierzu ist sicherzustellen, dass eine mandantenübergreifende Berechtigungsvergabe auf Anwendungsebene weder aus den einzelnen Mandanten heraus noch durch die mandantenübergreifenden Funktionen zur

Verwaltung der einzelnen Mandanten möglich ist. So SOLLTEN beispielsweise für jeden Mandanten eigene Rollen definierbar sein (M50.S12).

Die mandantenspezifische Nutzungsprotokollierung MUSS so erfolgen, dass diese sich nur auf Schritte zur Datenverarbeitung beziehen, die den jeweiligen Mandanten betreffen.

Die administrative Protokollierung MUSS sich auf die funktionalen Änderungen der Datenverarbeitung für den jeweiligen Mandanten beziehen, wenn ein Administrator bspw. eine neue Funktion einführt oder eine neue Schnittstelle erzeugt oder freigibt. Genau wie die Speicherung dieser nutzerspezifischen Protokollierung MÜSSEN auch die administrativen Protokolleinträge für jeden Mandanten getrennt gespeichert werden (M50.S13).

Es MUSS gewährleistet werden, dass die jeweiligen Verantwortlichen zusätzlich zur mandantenspezifischen administrativen Protokollierung Zugang zu den Einträgen der Protokollierung erhalten, die im Rahmen der mandantenübergreifenden Verwaltung der Verarbeitung durchgeführt wird (M50.S11).

Die technische Umsetzung einer getrennten Datenverarbeitung mithilfe relationaler Datenbanken SOLLTE durch unterschiedliche Maßnahmen erfolgen, die hier beispielhaft mit zunehmendem Grad der Trennung dargestellt sind (M50.S08):

- Alle Mandanten nutzen dieselben Tabellen in einer einzigen, gemeinsamen Datenbank eines Datenbanksystems. Jeder Datensatz wird um ein Attribut für den jeweils zutreffenden Mandanten ergänzt. Lediglich die Applikation realisiert die Trennung, indem sie dieses Attribut auswertet.
- Jeder Mandant arbeitet auf seinen eigenen Tabellen innerhalb derselben (d. h. einer einzigen) Datenbank. Die Tabellennamen enthalten jeweils ein mandantenspezifisches Präfix.
- Jeder Mandant erhält seine eigene Datenbank mit eigenen Tabellen.
- Arbeiten Mandanten auf eigenen Tabellen oder eigenen Datenbanken, lässt sich die Mandantentrennung in Abhängigkeit von den Konfigurationsmöglichkeiten des verwendeten Datenbankmanagementsystems durch eine Abbildung auf verschiedene physische Speicherstrukturen (wie Datendateien, dedizierte Speicherorte (Tablespaces, Raw Devices) innerhalb der gemeinsam genutzten Informationstechnik verstärken.
- Jeder Mandant wird durch einen eigenen Prozess des Datenbankmanagementsystems (DBMS) bedient. Jeder dieser DBMS-Prozesse legt die mandantenspezifischen Daten in separaten Datenbanken in derselben oder in unterschiedlichen physischen Strukturen ab.
- Jeder Mandant arbeitet innerhalb eines (virtuellen) Systems mit eigenem (virtuellen) Speicher für das Datenbanksystem.

Prüfschritt 5: Beschränkung der mandantenübergreifenden Verwaltung der Datenverarbeitung

Mandantenübergreifende Funktionen zur Verwaltung der Mandanten und der gemeinsam genutzten Informationstechnik dürfen grundsätzlich keine Verarbeitung personenbezogener Daten eines Mandanten ermöglichen.

Ausgenommen hiervon sind Funktionsträgerdaten der einzelnen Mandanten, die dazu dienen, das mandantenspezifische Berechtigungssystem erstmalig einzurichten und dann zu verwalten. Auch das Anlegen und Löschen von Mandanten innerhalb des Systems gehört zu den Funktionen einer mandantenübergreifenden Verwaltung (M50.S09). Diese mandantenübergreifende Verwaltung MUSS gewährleisten, dass die geltenden Bestimmungen eingehalten werden können, auch wenn es sich um eine Auftragsverarbeitung handelt.

Beispiel: Bei Beendigung der Auftragsverarbeitung für einen Mandanten muss den Anforderungen nach Herausgabe und Löschung der verbliebenen Daten entsprochen werden können, ohne dass dies Auswirkungen auf die Verarbeitung anderer Mandanten hat.

Die mandantenübergreifende Verwaltung MUSS revisionssicher protokolliert werden (M50.S17). Diese Protokolle MÜSSEN auch bei einer Prüfung einzelner Mandanten genutzt werden können. Mandantenübergreifende Datenzugriffe sind nur in begründeten Ausnahmefällen zulässig und nur im für die jeweilige Aufgabenstellung erforderlichen Umfang, insbesondere für die mandantenübergreifende Verwaltung und zur Beseitigung von Notfallsituationen, wenn andere Maßnahmen mit geringeren Zugriffsrechten nicht ausreichend sind. Diese Ausnahmefälle MÜSSEN vorher definiert und jeweils mit einer Rechtsgrundlage ausgestattet sein (M50.S16). Die Vergabe der hierfür vorgehaltenen Rollen MÜSSEN restriktiv gehandhabt werden; diese Rollen dürfen nicht Nutzern auf Anwendungsebene zugeordnet werden.

Mandantenübergreifende Funktionen und Einrichtungen MÜSSEN einem Datenschutz-Management unterliegen. Dazu gehören

- ein Administrationskonzept (M50.P01),
- ein Protokollierungskonzept und eine revisionssichere Protokollierung der administrativen Tätigkeiten (M50.S14),
- sowohl ein mandantenspezifisches als auch ein mandantenübergreifendes Berichtswesen (M50.P02),
- Revisionsaktivitäten über das Gesamtsystem (M50.S15),
- Prozesse für das mandantenspezifische und mandantenübergreifende Change-Management (M50.P04),
- die Überwachung dieser Prozesse einschließlich der Korrekturmaßnahmen bei Abweichungen (M50.P05).

2.2.2 Was ist zu dokumentieren?

Der Nachweis einer wirksamen Trennung MUSS insbesondere eine Dokumentation der technischen und organisatorischen Maßnahmen und eine Protokollierung über ihre Wirksamkeit umfassen, die eine Trennung der Daten auf Ebene der Datenhaltung, Datenverarbeitung und des Datentransports sicherstellen (M50.P14).

Als Nachweis einer ausreichenden Trennung einzelner Mandanten MUSS dargestellt werden, ob bzw. wie die Daten eines Mandanten zwischen den Mandanten oder der von vielen Verarbeitungen gemeinsam genutzten Informationstechnik übertragen werden können und real übertragen werden. Im Rahmen dieses Nachweises MUSS dargestellt werden, mit welchen technischen und organisatorischen Maßnahmen die verarbeiteten personenbezogenen Daten getrennt werden. Dabei MUSS beschrieben werden, welcher Mandant im Kontext welcher Verarbeitung die gemeinsame Informationstechnik nutzt. Zum anderen MUSS dargestellt werden, wie die für den Nachweis einer ordnungsgemäßen Datenverarbeitung notwendigen Daten, z. B. die Nutzungsprotokollierung, die administrative Protokollierung und die vergebenen Berechtigungen, für einzelne Mandanten getrennt gespeichert werden.

Der Verantwortliche MUSS Risiken, die trotz der Gewährleistung eines angemessenen Schutzniveaus bestehen, und Risiken, die aufgrund einer unzureichenden Trennung der Mandanten bestehen, gesondert aufführen (M50.P10). Alle Verantwortlichen, die auf gemeinsam genutzter Informationstechnik arbeiten, MÜSSEN verbliebene Risiken dokumentieren (s. SDM-V2b, Kap. D.3.3) (M50.P12).

3. Differenzierung bei hohem Schutzbedarf

Vernetzte und gemeinsam genutzte Dienste und Systeme bilden grundsätzlich ein Risiko für das datenschutzrechtliche Trennungsgebot. Ein weiteres Risiko ist ein zu gering ausgebildeter Grad der Arbeitsteilung sowie die Abhängigkeit von externem Sachverstand bzw. dauerhaftem IT-Support wie durch Fernwartung, durch Bereitstellung von Hardware, das Einspielen von Hersteller-Updates und anderen Patches bei Anwendungsprogrammen, Datenbanken, Betriebssystemen oder Administrationstools der IT-Services.

Wenn hoher Schutzbedarf für die betroffenen Personen hinsichtlich der Trennung einer Verarbeitung von anderen Verarbeitungen vorhanden ist, dann MUSS der Verantwortliche prüfen, ob auf eine Vernetzung der verwendeten Systeme oder organisationsexterne IT-Dienstleistungen verzichtet werden kann.

Die folgende Auflistung ist nach zunehmender Wirksamkeit einer Trennung bei einem System und der Datenhaltung geordnet:

a) Logische Trennung ohne technische Unterstützung, die allein auf einer Organisationsanweisung beruht, welche der verfügbaren Daten nicht verarbeitet werden dürfen;

b) logische Trennung durch parallel betriebene Instanzen innerhalb einer Applikation, die aufgrund von der Sachbearbeitung zugänglichen Regeln eine Hürde für den Zugriff auf verfügbare Daten einzieht (typisch: Mandantentrennung durch Regeln innerhalb einer Datenbankinstanz);
c) logische Trennung durch parallel betriebene Instanzen innerhalb einer Applikation, die aufgrund der Administration zugänglichen Regeln eine Hürde für den Zugriff auf verfügbare Daten einzieht (typisch: Mandantentrennung durch Regeln innerhalb einer Datenbankinstanz);
d) logische Trennung von Fachapplikationen, die parallel innerhalb eines Betriebssystems betrieben werden (typisch: mehrere Datenbank-Instanzen);
e) logische Trennung von Fachapplikationen, von der jeweils eine Instanz in einem virtuellen Betriebssystem betrieben wird, wobei die virtuellen Systeme als „Gäste“ auf einem gemeinsamen Betriebssystem („Host“) aufsetzen;
f) physikalische Trennung von Fachapplikationen, bei der jede Fachapplikation in einem Betriebssystem auf einer eigenen IT-Hardware in einem gemeinsamen Rack eines Server-Raums über unterschiedliche Netze erreichbar betrieben wird;
g) physikalische Trennung von Fachapplikationen, bei der jede Fachapplikation in einem Betriebssystem auf einer eigenen IT-Hardware in unterschiedlichen Räumen eines Gebäudes über unterschiedliche Netze erreichbar betrieben werden;
h) physikalische Trennung von Fachapplikationen, bei der jede Fachapplikation in anderen Rechenzentren, die bspw. spezialisiert für bestimme Verwaltungen („Landesrechenzentrum“, „kommunales Rechenzentrum“) oder für spezielle Berufsgeheimnisträger („Apotheken-Rechenzentrum“) betrieben werden.

Es lassen sich weitere Zwischenstufen formulieren, wobei ganz wesentlich auch die Trennung von Netzen – logisch anhand von Regeln auf Routern und Switches – oder anhand physikalischer Trennung auf der Ebene der Verkabelung zu beachten ist.

Die Umsetzung eines hohen Schutzbedarfs KANN eine physikalische Trennung von Datenbeständen sowie aller Komponenten einer Verarbeitung (das entspricht in der obigen Liste ab Eintrag f)) erfordern. Das KANN auch die Trennung der Netze für die Sachbearbeitung, für die Administration sowie für besondere Services wie bspw. Drucker erfordern (M50.S10).

4. Referenzen

5. Zusammenfassung der Maßnahmen

Die einzelnen Maßnahmen können hinsichtlich des Anwendungsbereichs unterschieden werden nach Maßnahmen, welche primär auf einzelne Verarbeitungstätigkeiten angewandt werden sollten (kursive Darstellung) und solche, welche primär die gesamte Organisation betreffen und damit im Rahmen des Datenschutzmanagements gebündelt und verwaltet werden sollten. Weiterhin sind alle Maßnahmen grob den Phasen des

Datenschutzmanagement-Prozesses (siehe SDM-Methode) zugordnet. Maßnahmen, die in früheren Versionen des Bausteins enthalten waren, aber in einer nachfolgenden Version ungültig wurden, werden weiterhin aufgeführt (~~durchgestrichene Darstellung~~). Damit bleibt die Nummer einer Maßnahme bei einer neuen Version erhalten. Die Spalte „Gültigkeit“ gibt an, seit welcher Version die Maßnahme in der enthaltenen Form gültig ist. Bei ungültigen Maßnahmen enthält diese Spalte die Versionsnummer des Bausteins, in der die Maßnahme letztmalig gefordert bzw. empfohlen wurde.

Ebene Daten

Nr.	Maßnahme	PDCA	Gültigkeit
M50.D01	*Zweckbeschreibung, Zwecktrennung und Zweckbindung durchführen und dokumentieren*	P	V1.0
M50.D02	*Prüfung der Rechtsgrundlage für jede Datenübermittlung*	P	V1.0
M50.D03	*Vertragliche Festlegung der Suchkriterien für zu übermittelnde Daten*	P	V1.0
M50.D04	*Protokollierung jeder Datenübermittlung*	P, D	V1.0

Ebene Systeme

M50.S01	Nachweis der Prüffähigkeit der von ihm betriebenen Systeme bzgl. der Wirksamkeit der Trennung zu anderen Verarbeitungen und Organisation durch den Dienstleister	C	V1.0
M50.S02	Nachweis der Abgeschlossenheit eines Mandanten	P, D, C	V1.0
M50.S03	*Sicherheitstechnische Isolation eines Mandanten*	P, D, C	V1.0
M50.S04	*Mandantenspezifische Benutzerkennungen*	P, D	V1.0
M50.S05	Getrennte Systeme zur Berechtigungsvergabe	P	V1.0
M50.S06	Konfigurierbarkeit der Nutzungsprotokollierung	P, D	V1.0
M50.S07	Protokollierung der (*mandantenspezifischen* und mandantenübergreifenden) Administrationsaktivitäten	D	V1.0
M50.S08	Mandantentrennung innerhalb einer relationalen Datenbank	P, D	V1.0

M50.S09	Festlegung von Funktionen, die verarbeitungs- oder systemübergreifend zur Verwaltung von Personen und technischen Ressourcen genutzt werden dürfen	P	V1.0
M50.S10	Trennung von Datenbeständen, IT-Komponenten oder Netzen für die Sachbearbeitung, für die Administration sowie für besondere Services wie bspw. Drucker bei hohem Schutzbedarf	P, D	V1.0
M50.S11	*Mandantenspezifisch abgeschlossene Berechtigungsvergabe*	P, D	V1.0
M50.S12	*Mandantenspezifisch abgeschlossene Rollendefinitionen*	P, D	V1.0
M50.S13	*Mandantenspezifische Protokollierung*	D	V1.0
M50.S14	Mandantenübergreifende Protokollierung der Administration	D	V1.0
M50.S15	Definition der Revisionsaktivitäten über das Gesamtsystem	P	V1.0
M50.S16	Mandantenübergreifende Datenzugriffe müssen definiert und mit Rechtsgrundlage ausgestattet sein	P	V1.0
M50.S17	Es darf keine zusätzlich eingesetzte Softwarekomponente eine bereits durchgesetzte Mandantentrennung aufheben.	P, D	V1.0

<u>Ebene Prozesse</u>

M50.P01	Mandantenübergreifendes Administrationskonzept	P	V1.0
M50.P02	*Mandantenspezifisches*- und mandantenübergreifendes Berichtswesen	P, D	V1.0
M50.P03	*Angemessene Auswahl eines zur Umsetzung von Trennungsgeboten geeigneten Auftragsverarbeiters (bspw. Rechenzentrum als Dienstleister)*	P	V1.0
M50.P04	Definition von Prozessen für das mandantenspezifische und das mandantenübergreifende Changemanagement	P	V1.0

M50.P05	Überwachung von Managementprozessen einschließlich der Korrektur bei Abweichungen	C	V1.0
M50.P06	Einbindung des gemeinsamen, mandantenübergreifenden Datenschutz- und Sicherheitsmanagement in die betrieblichen Prozesse der gemeinsam genutzten Informationstechnik	P, D, C	V1.0
M50.P07	Regelmäßige Überprüfung der mandantenübergreifend genutzten Informationstechnik durch das Datenschutzmanagement	C	V1.0
M50.P08	*P27 Prüfung der Rechtsgrundlage bei Datenübermittlung zwischen Mandanten*	P	V1.0
M50.P09	Notfall-Konzept mit gestufter Aufgabe von Trennungen	P	V1.0
M50.P10	*Dokumentation von Restrisiken*	P	V1.0
M50.P11	Getrennte Einrichtung von IT-Komponenten und Diensten	P, D	V1.0
M50.P12	Dokumentation von Restrisiken durch alle an der getrennten Datenverarbeitung beteiligten Verantwortlichen	P	V1.0
M50.P13	Mandantenübergreifendes Datenschutz- und Sicherheitsmanagement	P, D, C	V1.0
M50.P14	Dokumentation der Wirksamkeit der Trennungsmaßnahmen anhand von Protokollen	P, C	V1.0
M50.P15	Vereinbarungen zwischen Beteiligten an gemeinsam genutzter Informationstechnik gem. Art. 26 DS-GVO treffen	P	V1.0
M50.P16	Verträge zwischen Verantwortlichen und Auftragsverarbeitern gem. Art. 28 DS-GVO schließen	P	V1.0
M50.P17	Prüfen der Übermittlung zwischen Mandanten im Hinblick auf Erhalt der Integrität	P, D, C	V1.0

6. Bezug zum Datenschutzmanagement

Dieser Baustein bezieht sich auf Anforderungen der operativen Trennung von Verarbeitungstätigkeiten sowie daraus abgeleitet der Daten, Systeme, Dienste und Prozesse.

Viele Bausteine in Bezug auf Durchsetzung von getrennten Daten, Systemen und Diensten sowie Subprozessen sind aus der Sicht der gesamten Organisation zu planen, zu betreiben, zu prüfen und permanent zu verbessern.

7. 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:

„Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz). Veränderungen, Bearbeitungen, neue Gestaltungen oder sonstige Abwandlungen der bereitgestellten Daten sind mit einem Veränderungshinweis im Quellenvermerk zu versehen. Datenlizenz Deutschland – Namensnennung – Baustein Trennen (www.govdata.de/dl-de/by-2-0).“