Baustein 50 „Trennung“

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

Nichtverkettung, Datenminimierung, Integrität, Vertraulichkeit

2. Beschreibung

Voraussetzung für eine rechtskonforme Datenverarbeitung ist eine grundrechtskonforme Zwecksetzung (vgl. Art. 6 DS-GVO). Eine sich daran anschließende Zweckdefinition ist wiederum die Voraussetzung dafür, die erforderlichen Daten und die Angemessenheit der Prozesse einer Verarbeitung bestimmen zu können. Der ausgewiesene Zweck einer Verarbeitung erlaubt eine logische und praktische Abgrenzung bzw. Trennung einer Verarbeitung von anderen Verarbeitungen. Die Abgrenzung von Verarbeitungen, einzelnen Verarbeitungstätigkeiten und Zugriffen auf bestimmte Datenbestände ist wiederum eine wesentliche Voraussetzung dafür, um eine befugte Verarbeitung von speziellen Befugnissen z. B. für externe Organisationen und unbefugten Verarbeitungen unterscheiden zu können.

Als Beispiel: Ein Krankenhaus ist generell befugt, Patientendaten in Form einer Patientenakte zu führen. Diese generelle Befugnis bedeutet jedoch nicht, dass innerhalb eines Krankenhauses sämtliche Mitarbeiter/-innen, unabhängig vom definierten Zweck ihrer einzelnen Verarbeitungstätigkeiten, auf sämtliche Daten einer Patientenakte Zugriff nehmen dürfen. Von den intern Beschäftigten unterschiedlicher Abteilungen und Tätigkeiten sind wiederum externe Dienstleister des Krankenhauses zu unterscheiden, die nur auf eng begrenzte Bereiche der vom Krankenhaus betriebenen IT und deren Datenbestände zugreifen dürfen.

Sehr knapp formuliert gilt die Regel: Unterschiedliche Zwecke der Tätigkeiten erzeugen unterschiedliche Befugnisse zur Verarbeitung, die unterschiedliche Trennungsmaßnahmen erfordern. Diese zweckdefinierten Trennungsanforderungen, die typischerweise auf der organisatorischen Ebene formuliert werden, dürfen dann nicht von der Technik, die als Infrastruktur für die Datenverarbeitung genutzt wird, unterlaufen werden. Die Technik muss vielmehr diese Trennungsgebote unterstützen. Die für die Datenverarbeitung verwendete Technik muss am Zweck der Verarbeitung orientiert eingerichtet sein und betrieben werden.

Dieser Baustein listet Prüfschritte und Maßnahmen auf, mit denen sich Daten, IT-Systeme und Prozesse sowohl innerhalb einer Organisation als auch von anderen Organisationen trennen lassen. Die Trennung ist eine Voraussetzung dafür, um anschließend rechtlich zulässige Verbindungen zwischen verschiedenen Organisationen und Organisationseinheiten (Abteilungen, Filialen) mit deren Daten und Systemen unter organisatorische und technische Bedingungen herstellen zu können. Nicht Gegenstand dieses Bausteins ist die Trennung von unterschiedlichen Rollen und Berechtigungen oder die Abtrennung der Personendaten von Inhalts- und Kommunikationsdaten durch Pseudonymisierung oder Anonymisierung.

3. Umsetzung der Nichtverkettung

Der abgeschlossene Datenhaltungs- und Verarbeitungskontext eines Verantwortlichen wird nachfolgend als „Mandant“ bezeichnet, die getrennte Speicherung von Daten und deren Verarbeitung als „Mandantentrennung“. Eine Verarbeitung gilt als „mandantenfähig“, wenn sie in der Lage ist, eine Mandantentrennung umzusetzen.

In diesem Baustein verwendete Begriffe werden wie folgt definiert:

- **Gemeinsam genutzte IT-Infrastrukturen** umfassen alle informationstechnischen Ressourcen, die nicht physisch voneinander getrennt sind. Hierzu gehören beispielsweise Anwendungssysteme für mehrere Mandanten sowie gemeinsame Datenbank-Managementsysteme und Datenbanken, Speicher- und Managed Storage-Systeme sowie Backup-Systeme in konventionellen und virtualisierten Umgebungen.
- Ein **Datenzugriff** ist die Ausführung einer (möglicherweise komplexen) Funktion eines Anwendungssystems, mit dem personenbezogene Daten genutzt oder anderweitig verarbeitet werden, und kann insbesondere die Ausführung einer Folge von Transaktionen bewirken.
- **Transaktionen** sind unteilbare, konsistente und gegeneinander isolierte logische Einheiten von Programmschritten eines Anwendungssystems.

Ob eine ausreichende Trennung bei der gemeinsamen Nutzung einer IT-Infrastruktur gewährleistet wird und ob die Datenschutzanforderungen angemessen und wirksam umgesetzt werden, lässt sich anhand folgender Prüfschritte prüfen:

3.1 Sieben Prüfschritte zur Beurteilung ausreichender Trennung der Verarbeitungen

Prüfschritt 1: Rechtliche Grundlagen

Die Beurteilung, ob durch technische und organisatorische Maßnahmen eine ausreichende Trennung von Verarbeitungen erreicht werden kann und durch welche, setzt eine vorlaufende rechtliche Prüfung voraus. Dazu sind erneut die für die jeweiligen Verarbeitungen anzuwendenden spezialgesetzlichen Bestimmungen, die datenschutzrechtlichen Grundsätze und die allgemeinen datenschutzrechtlichen

Bestimmungen heranzuziehen (M50.34). Diese müssen bereits im Vorfeld der Anwendung des SDM bewertet worden sein.

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

- Für den öffentlichen Bereich: Wo liegt die gesetzgeberische Regelungskompetenz (EU/Bund/Land) für die jeweilige Verarbeitung?
- Welche Rechtsgrundlage, welche Zweckbestimmung oder Zweckbindung liegt der jeweiligen Verarbeitung zugrunde?
- Welche Verantwortlichen sollen welche Verarbeitungen auf einer gemeinsamen IT Infrastruktur nutzen?

Ob verschiedene Verarbeitungen auf einer gemeinsamen IT-Infrastruktur betrieben werden dürfen, hängt auch von dem daraus resultierenden Risiko für die Rechte und Freiheiten der Betroffenen ab. Resultiert allein aus der gemeinsamen Nutzung einer IT-Infrastruktur ein hohes Risiko, wird eine solche gemeinsame Nutzung nicht zulässig sein. Ein weiteres Ausschlusskriterium für eine gemeinsame Nutzung von IT-Infrastrukturen kann aus Rechtsnormen resultieren, die die gemeinsame Nutzung verbieten, weil damit eine unzulässige Offenbarung verbunden sein kann. In diesen Fällen ist eine physikalische Trennung bzw. ein Betrieb durch verschiedene Verantwortliche zwingend geboten.

Prüfschritt 2: Besteht ein verfassungsrechtlich begründetes Trennungsgebot?

Bevor die Anforderungen für die Übermittlung personenbezogener Daten zwischen verschiedenen Mandanten festgelegt werden sollen, muss geklärt werden, in welcher Form die IT für eine Verarbeitung betrieben werden soll. Die Spannbreite reicht von einem vollständigen Eigenbetrieb der IT in organisationseigenen Räumen bis zu einem vollständigen Betrieb der IT durch Auftragsverarbeiter (bspw. Rechenzentren). In der Praxis findet man zahlreiche Mischformen zwischen Eigenbetrieb und Auftragsverarbeitung vor.

Es gibt verfassungsrechtlich begründete strukturelle Anforderungen an eine Trennung von 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) mit ihren Organisationen (Parlamente, Ministerien und Verwaltungen, Gerichte) und die drei vertikalen Gewalten des Bundes, 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 Zweckbestimmungen der Datenverarbeitung, und die Tatsache, dass für verschiedene Teilsysteme unterschiedliche Verantwortliche existieren.

Verwaltungen müssen diese strukturell wichtigen Trennungsgebote daher schon bei der Wahl geeigneter IT-Dienstleister und Rechenzentren berücksichtigen (M50.05).

Rechenzentren arbeiten üblicher Weise für eine Vielzahl von Verantwortlichen. Datenschutzrechtlich problematisch wird es dann, wenn etwa ein Landesrechenzentrum für mehrere der Gewalten Daten verarbeitet und die verfassungsrechtlich gebotene informationelle Gewaltenteilung gefährdet, da dies zu einem erhöhten Risiko für die wirksame Wahrung der Grundrechte Betroffener führen kann. Es ist ebenfalls ein Problem, wenn Verantwortliche in wenigen oligopolartig strukturierten Rechenzentren („Clouds“) rechnen lassen, bei denen 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 Auftraggeber den Auftragnehmer steuert. Organisationen, Organisationsverbünde (Parlamente, Gerichte, Bundes- und Landesverwaltungen, Konzerne, Forschungsverbünde, Berufsgeheimnisträger) und Rechenzentren sind deshalb gehalten, die Wirksamkeit von Trennungsmaßnahmen in ihrer Hoheit nachzuweisen sowie auf die Dokumentation und die Überprüfung des laufenden Betriebs hinzuwirken (M50.06).

Prüfschritt 3: Besteht ein organisationsbezogenes Trennungsgebot?

Innerhalb von Organisationen bildet eine Verarbeitung (ehemals: „Fachverfahren“) den Ausgangspunkt zur Durchsetzung, Bewertung und Beurteilung der Durchsetzung datenschutzrechtlicher Anforderungen bzw. von Trennungen. Auf der Ebene der IT bildet die Fachapplikation den Ausgangspunkt zur Isolierung der IT-Komponenten, die mit der Fachapplikation verbunden sind (Netzwerksegmente, CPU-Cluster, Speichersysteme).

Rechtlich gebotene Grenzen des Zugriffs auf Daten, IT-Systeme und Prozesse dürfen grundsätzlich weder durch hierarchisch übergeordnete Rollen willkürlich aufgehoben werden noch auf der Ebene der verwendeten Informations- und Kommunikationstechniken bzw. von den eingebundenen IT-Dienstleistern unterlaufen werden. Wenn Trennungsgebote in Notfällen aufgehoben werden, dann muss zumindest im Nachhinein eine Beurteilung durchgeführt werden, ob tatsächlich ein Notfall oder ob ein Organisationsversagen vorlag. Ziel einer solchen Beurteilung ist es, Standardprozesse zur Bearbeitung von Störungen und Angriffen sowie der Identifikation von Notfällen zu verbessern. Eine wichtige Maßnahme ist deshalb die Erstellung eines Notfall-Konzepts mit gestufter Freigabe von Trennungen (M50.37).

Organisationen 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 unterbunden sind und nur unter definierten Bedingungen gesichert eingerichtet und dann kontrolliert, prüf- und beurteilbar über wohldefinierte und prüfbare Schnittstellen erfolgen können.

In Bezug auf die oftmals heterogenen IT Infrastrukturen sind Verarbeitungen, Prozesse und Datenflüsse entsprechend der Dienste zu identifizieren und zu separieren, d.h. Netzzugänge, Server- und Speicherinfrastrukturen separiert von anderen Netzen, Servern und Speichermedien zu betreiben. Durch eine Isolierung von IT-Komponenten ist eine Zuordnung von Zuständigkeiten für Datenbestände, IT-Systeme sowie Prozesse der Datenverarbeitung, bzw. sind Weisungshierarchien organisatorisch implementierbar (M50.39).

Es lassen sich **physikalische Trennungen** von Organisationen (konventionell durch Gebäude) sowie innerhalb von Organisationen (Räume, IT-Gerätschaften, Netzwerke, Speichersysteme) von **logischen Trennungen** innerhalb von Organisationen unterscheiden (Abteilungen, Abteilungen übergreifende und eigenständige Projektgruppen, Revisoren und Auditoren; Sicherheitszonen, virtualisierte IT-Systeme, virtuelle Local-Networks, virtualisierte Speichersysteme, Betriebssysteme, Middleware, Anwendungsprogramme). Verschiedene Aufgaben benötigen Zugang gemäß Geschäftsverteilungsplan, um eine Aufgabe in der zugewiesenen Zuständigkeit erfüllen zu können. An diesen Stellen gilt es, Schutzmaßnahmen der Zutrittskontrolle zu Räumen (M50.19), der Zugangskontrolle zu IT-Systemen (M50.20) und der Zugriffskontrolle auf Programme und Daten (M50.21), im Rahmen eines Identitätenmanagements und der Authentifizierung und Autorisierung zu treffen.

Prüfschritt 4: Ausgestaltung revisionsfester Übermittlungen zwischen Mandanten

Aus den in Prüfschritt 2 genannten Gründen ist bei einer getrennten Verarbeitung auf gemeinsamer IT-Infrastruktur die Verarbeitung von Daten eines Mandanten in einem anderen Mandanten rechtlich als Datenübermittlung auszugestalten. Die rechtlichen Grundlagen und Anforderungen an die Zulässigkeit der 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 (M50.35).

Um die Übermittlungen auf das Zulässige zu beschränken, darf die Auswahl von Daten zur Übermittlung in jedem Fall nur an Identitätsdaten (Name, Vorname, etc.) und solche Attribute oder Eigenschaften der Betroffenen anknüpfen, für deren Übermittlung eine Rechtsgrundlage besteht (M50.02). Zulässige Suchkriterien sind in der Regel vorher vertraglich festzulegen (M50.03). Die Einschränkung auf diese Suchkriterien ist technisch durchzusetzen. Übermittelte Daten müssen dem empfangenden Mandanten zugeordnet werden, um die neu entstandene rechtliche Verantwortung zu kennzeichnen. Der Fakt der Übermittlung ist zu protokollieren (M50.04). Zur Isolierung der Übermittlung von Transaktionen innerhalb eines Mandanten darf auf übermittelte Daten erst nach Abschluss der Übermittlung und ihrer Protokollierung zugegriffen werden.

Prüfschritt 5: Abgeschlossenheit der Transaktionen innerhalb eines Mandanten

Zur Prüfung auf eine ausreichende Trennung der einzelnen Mandanten auf einer gemeinsamen Infrastruktur ist die „Abgeschlossenheit“ der Datenverarbeitung innerhalb eines Mandanten zu betrachten. Die Prüfung auf Abgeschlossenheit muss

transaktionsbasiert erfolgen und nachweisen, dass die Datentrennung erhalten bleibt (M50.08).

Ein Mandant gilt als „abgeschlossen“, wenn jede Transaktion in einem Mandanten einen gültigen Datenbestand eines 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.

Diese transaktionsorientierte Prüfung auf Abgeschlossenheit muss ganzheitlich für die für die Verarbeitung genutzten Komponenten zur Datenverarbeitung, Datenhaltung und Datenübertragung durchgeführt werden.

Die Datenhaltung muss jedoch stets so organisiert werden, dass für jede Instanz 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 (siehe Prüfschritt 5) sowie diese Zuordnung berücksichtigen und durchsetzen (M50.34).

Die Abgeschlossenheit muss insbesondere auch für die Risiken und Maßnahmen aus den Bereichen Datenschutz und Datensicherheit gelten. Die Abgeschlossenheit eines Mandanten bedingt zwangsweise auch eine sicherheitstechnische Isolation eines Mandanten. Bei ausreichender Trennung der Datenverarbeitung dürfen Datenschutzprobleme oder -vorfälle eines Mandanten nicht zu einer Gefährdung anderer Mandanten führen (M50.08).

Wäre beispielsweise in einem System die Möglichkeit gegeben, mandantenübergreifende Zugriffe auf eigene Daten oder Daten eines anderen Mandanten zu initiieren, ohne dass die o. g. Voraussetzungen für eine zulässige Übermittlung vorliegen, oder wird diese Möglichkeit nur durch organisatorische Maßnahmen ausgeschlossen, so läge keine Abgeschlossenheit vor und die Mandantenfähigkeit wäre nicht gegeben.

Prüfschritt 6: Unabhängigkeit der Konfigurationen unterschiedlicher Mandanten

Eine ausreichende Mandantentrennung setzt voraus, dass die Zugriffsberechtigungen die Verarbeitungsfunktionen und die Konfigurationseinstellungen je Mandant eigenständig festgelegt werden. Die eigenständige Vergabe von Zugangsberechtigungen bedingt das Anlegen von mandantenspezifischen Benutzerkennungen, mit denen nur auf Daten ihres Mandanten zugegriffen werden kann (M50.09).

Sind für die technischen Sicherheits- und Datenschutzmaßnahmen auf Basis einer Risikoanalyse oder aufgrund gesetzlicher Vorgaben mandantenspezifische Anforderungen ersichtlich, so müssen diese Anforderungen auf Mandantenebene umgesetzt und gemäß den Vorgaben der einzelnen Mandanten konfigurierbar sein.

Als Anforderungen sind hierfür mandantenspezifisch zumindest vorzusehen

- getrennte Systeme zur Berechtigungsvergabe (M50.10),
- Konfigurationsmöglichkeiten für die Nutzungsprotokollierung (M50.11) sowie
- eine administrative Protokollierung (M50.12).

Die Berechtigungsvergabe muss über ein Berechtigungssystem erfolgen, das auf Ebene des einzelnen Mandanten abgeschlossen ist (M50.22). 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 müssen beispielsweise für jeden Mandanten eigene Rollen definierbar sein(M50.23).

Die mandantenspezifische Nutzungsprotokollierung darf 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. Genau wie die Speicherung dieser nutzerspezifischen Protokollierung müssen auch die administrativen Protokolleinträge für jeden Mandanten getrennt gespeichert werden (M50.24).

Es muss gewährleistet werden, dass die jeweiligen Daten verarbeitenden Stellen zusätzlich zur mandantenspezifischen administrativen Protokollierung Zugang zu den Einträgen der Protokollierung erhalten, die im Rahmen der mandantenübergreifenden Verwaltung der Verarbeitung durchgeführt wird. Zusätzlich zur mandantenspezifischen administrativen Protokollierung sind auch die Protokolleinträge zugänglich zu machen, die im Rahmen der mandantenübergreifenden Verwaltung der Verarbeitung durchgeführt wurden (M50.12).

Die technische Umsetzung einer getrennten Datenverarbeitung mithilfe relationaler Datenbanken kann durch unterschiedliche Maßnahmen erfolgen (M50.13):

- 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 gemeinsamen IT-Infrastruktur 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 bekommt seine eigene virtuelle Maschine mit eigener virtueller Festplatte für das Datenbanksystem.

Prüfschritt 7: Beschränkung der mandantenübergreifenden Verwaltung der Datenverarbeitung

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

Ausgenommen hiervon sind Funktionsträgerdaten der einzelnen Mandanten, die dazu dienen, das mandantenspezifische Berechtigungssystem erstmalig einzurichten. Auch das Anlegen und Löschen von Mandanten innerhalb des Systems gehört zu den Funktionen einer mandantenübergreifenden Verwaltung. Die Organisation der Datenspeicherung muss gewährleisten, dass für diese Verwaltungsfunktionen auch die geltenden Bestimmungen für eine Auftragsdatenverarbeitung eingehalten werden können (M50.14).

Beispiel: Bei Beendigung des Auftragsdatenverhältnisses 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 (M50.24). 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. Die Vergabe der hierfür vorgehaltenen Rollen ist sehr restriktiv zu handhaben und diese Rollen dürfen nicht Nutzern auf Anwendungsebene zugeordnet werden.

Mandantenübergreifende Funktionen und Einrichtungen müssen einem Management unterliegen. Dazu gehören

- die Definition eines Administrationskonzepts (M50.26),
- die Festlegung eines Protokollierungskonzepts und eine revisionssichere Protokollierung der administrativen Tätigkeiten (M50.27),
- die Definition sowohl eines mandantenspezifischen als auch eines mandantenübergreifenden Berichtswesens (M50.28),
- die Definition von Revisionaktivitäten über das Gesamtsystem (M50.29),

- die Definition von Prozessen für das mandantenspezifische undmandantenübergreifende Change-Management (M50.30).
- die Überwachung dieser Prozesse einschließlich der Korrekturmaßnahmen bei Abweichungen (M50.31).

3.2 Was ist zu dokumentieren?

Der Nachweis einer wirksamen Umsetzung der 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 (M50.15).

Als Nachweis einer ausreichenden Trennung einzelner Mandanten ist darzustellen, ob bzw. wie die Daten eines Mandanten zwischen der von viele Verarbeitungen gemeinsam genutzten Infrastruktur und der mandantenspezifischen Infrastruktur übertragen werden können und real übertragen werden. Im Rahmen dieses Nachweises ist zum einen darzustellen, mit welchen technischen und organisatorischen Maßnahmen die verarbeiteten personenbezogenen Daten getrennt werden. Dabei muss beschrieben werden, wer die gemeinsame Infrastruktur nutzt. Zum anderen ist darzustellen, 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 und in eine andere Infrastruktur überführt werden können.

3.3 Wie ist mit den Restrisiken bzgl. einer unzureichenden Trennung umzugehen?

Grundsätzlich bedeutet eine unzureichende Trennung, dass eine Verarbeitung nicht stattfinden darf, weil dadurch die datenschutzrechtlich gebotene Zweckbindung nicht hinreichend sichergestellt ist und damit die Datenschutzkonformität des gesamten Verarbeitungsprozesses gefährdet ist.

Risiken, die durch technische und organisatorische Maßnahmen nicht oder nur zum Teil ausreichend reduziert wurden, müssen explizit ausgewiesen werden. Risiken, die aufgrund einer unzureichenden Trennung der Mandanten bestehen, sind gesondert aufzuführen (M50.38).

Soll die Verarbeitung trotz nachweislich vorhandener Risiken stattfinden, muss der für die Daten des jeweiligen Mandanten Verantwortliche die verantwortbaren Restrisiken durch eine schriftliche Erklärung formell übernehmen (M50.40). Die Übernahme der Restrisiken muss also durch alle Verantwortlichen erfolgen, die auf der gemeinsamen Infrastruktur eine getrennte Datenverarbeitung durchführen. Die Übernahme der Restrisiken ist wechselseitig allen an der getrennten Datenverarbeitung beteiligten Verantwortlichen zur Kenntnis zu geben (M50.41).

Jeder Verantwortliche hat für die mandantenbasierte Verarbeitung personenbezogener Daten einen Ansprechpartner in Fragen des Datenschutzes und der Datensicherheit zu benennen (M50.42). Üblicher Weise sind dies die betrieblichen oder behördlichen Datenschutz- und IT-Sicherheitsbeauftragten.

Wird eine gemeinsame Infrastruktur zur getrennten Verarbeitung personenbezogener Daten genutzt, so ist ein mandantenübergreifendes Datenschutzmanagement einzurichten. Die gemeinsam genutzte Infrastruktur muss regelmäßig durch das gemeinsame, mandantenübergreifende Datenschutzmanagement auf angemessene technische und organisatorische Maßnahmen sowie eine wirksame Umsetzung insbesondere der Datentrennung geprüft werden. Die Prüfergebnisse sind allen Mandanten zur Verfügung zu stellen. Das betrifft insbesondere solche, aus denen sich mandantenübergreifende Auswirkungen ergeben können (M50.16).

Im Rahmen des gemeinsamen, mandantenübergreifenden Datenschutz- und Sicherheitsmanagements ist ein gesondertes Vorgehen für mandantenübergreifende Datenschutz- und Sicherheitsvorfälle einzurichten, welches eine Beteiligung aller Mandanten in der Bearbeitung der Datenschutz- und Sicherheitsvorfälle vorsieht (M50.43).

Das gemeinsame, mandantenübergreifende Datenschutz- und Sicherheitsmanagement muss in die betrieblichen Prozesse der gemeinsam genutzten Infrastruktur eingebunden sein (M50.33). Insbesondere darf die Planung und Umsetzung von Änderungen an der gemeinsamen Infrastruktur nur unter Beteiligung des Datenschutz- und Sicherheitsmanagements aller an der getrennten Datenverarbeitung beteiligten Verantwortlichen erfolgen.

4. Differenzierung bei hohem Schutzbedarf

Vernetzte Computersysteme bilden grundsätzlich ein Risiko für das datenschutzrechtliche Trennungsgebot. Ein weiteres Risiko ist ein zu gering ausgebildeter Grad der Arbeitsteilung sowie das Angewiesensein auf externen Sachverstand bzw. mit dauerhaftem IT Support wie z. B. 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 hinsichtlich der Trennung einer Verarbeitung von anderen Verarbeitungen vorhanden ist, dann muss geprüft werden, ob auf einen Netzanschluss der verwendeten IT-Systeme oder organisationsexterne IT-Dienstleistungen verzichtet werden kann.

Die nachfolgende Auflistung ist nach zunehmender Wirksamkeit einer Trennung bei einem IT-System und der Datenhaltung sortiert:

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 durch die 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 von durch die 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 Betriebssysteme 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 Gebäude(komplexes) über unterschiedliche Netze erreichbar betrieben werden;
h) physikalische Trennung von Fachapplikationen, bei der jede Fachapplikation in anderen Rechenzentren (in unterschiedlichen Ländern), die bspw. spezialisiert für bestimme Verwaltungen („kommunales Rechenzentrum“) oder für spezielle Berufsgeheimnisträger („Apotheken-Rechenzentrum“) betrieben werden (M50.17).

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 Kabelstränge zu beachten ist.

Die Umsetzung hohen Schutzbedarfs verlangt grundsätzlich eine physikalische Trennung aller Komponenten einer Verarbeitung (das entspricht in der obigen Liste ab Eintrag f)) (M50.32). Das betrifft auch die Trennung der Netze für die Sachbearbeitung, für die Administration sowie für besondere Services wie bspw. Drucker (M50.18).

5. Zusammenfassung der Maßnahmen

Ebene Daten

M50.01 Zuordnung jedes einzelnen Datums zu genau einem Mandanten
M50.02 Prüfung der Rechtsgrundlage für jede Datenübermittlung
M50.03 Vertragliche Festlegung der Suchkriterien für zu übermittelnde Daten
M50.04 Protokollierung jeder Datenübermittlung

Ebene Systeme

M50.05 Angemessene Auswahl eines zur Umsetzung von Trennungsgeboten geeigneten Rechenzentrums
M50.06 Nachweis der Prüffähigkeit der von ihm betriebenen Systeme bzgl. der Wirksamkeit der Trennung zu anderen Verarbeitungen und Organisation durch den Dienstleister
M50.07 Transaktionsorientierte Abgeschlossenheit eines Mandanten
M50.08 Sicherheitstechnische Isolation eines Mandanten
M50.09 Mandantenspezifische Benutzerkennungen
M50.10 Getrennte Systeme zur Berechtigungsvergabe
M50.11 Konfigurierbarkeit der Nutzungsprotokollierung
M50.12 Protokollierung der (mandantenspezifischen und mandantenübergreifenden) Administrationsaktivitäten
M50.13 Mandantentrennung innerhalb einer relationalen Datenbank
M50.14 Festlegung von Funktionen, die verarbeitungs- oder systemübergreifend zur Verwaltung von Personen und technischen Ressourcen genutzt werden dürfen
M50.15 Dokumentation der Wirksamkeit der Trennungsmaßnahmen anhand von Protokollen
M50.16 Regelmäßige Überprüfung der mandantenübergreifend genutzten Infrastruktur durch das Datenschutzmanagement
M50.17 Trennung von Fachapplikationen und deren Daten entsprechend Schutzbedarfseinstufung
M50.18 Trennung der Netze für die Sachbearbeitung, für die Administration sowie für besondere Services wie bspw. Drucker bei hohem Schutzbedarf
M50.19 Zutrittskontrolle zu Räumen
M50.20 Zugangskontrolle zu IT-Systemen
M50.21 Zugriffskontrolle auf Programme und Daten
M50.22 Mandantenspezifisch abgeschlossene Berechtigungsvergabe
M50.23 Mandantenspezifisch abgeschlossene Rollendefinitionen
M50.24 Mandantenspezifische Protokollierung
M50.25 Revisionssichere Protokollierung der mandatenübergreifenden Verwaltung
M50.26 Mandantenübergreifendes Administrationskonzept
M50.27 Mandatenübergreifende Protokollierung der Administration
M50.28 Mandantenspezifisches- und mandantenübergreifendes Berichtswesen
M50.29 Definition der Revisionsaktivitäten über das Gesamtsystem
M50.30 Definition von Prozessen für das mandantenspezifische und das mandantenübergreifende Changemanagement
M50.31 Überwachung von Managementprozessen einschließlich der Korrektur bei Abweichungen
M50.32 Physikalische Trennung von Fachapplikationen (IT-Systemen und Daten) bei hohem Schutzbedarf

M50.33 Einbindung des gemeinsamen, mandantenübergreifenden Datenschutz- und Sicherheitsmanagement in die betrieblichen Prozesse der gemeinsam genutzten Infrastruktur

Ebene Prozesse

M50.34 Rechtlich prüfen, welches Maß an Trennung eine Verarbeitung mit ihren Komponenten Daten, Systemen und Prozessen erfordert
M50.35 Prüfung der Rechtsgrundlage bei Datenübermittlung zwischen Mandanten
M50.36 Zugriffsmöglichkeiten auf mandantenspezifische und mandantenübergreifende Protokolleinträge für den Verantwortlichen
M50.37 Notfall-Konzept mit gestufter Freigabe von Trennungen
M50.38 Dokumentation von Restrisiken
M50.39 Separierte Einrichtung von IT-Verbünden und Diensten
M50.40 Formale Übernahme des Restrisikos durch schriftliche Erklärung
M50.41 Bekanntgabe der Übernahme von Restrisiken an alle an der getrennten Datenverarbeitung beteiligten Verantwortlichen
M50.42 Benennung eines Ansprechpartners für Datenschutz und IT-Sicherheit bei mandatenbasierter Verarbeitung
M50.43 Mandantenübergreifendes Datenschutz- und Sicherheitsmanagement

6. Anmerkung zur Nutzung dieses Bausteins