Technische und organisatorische Anforderungen
an die Trennung von automatisierten Verfahren
bei der Benutzung einer gemeinsamen IT-Infrastruktur

- Orientierungshilfe Mandantenfähigkeit -

des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder

- Version 1.0 vom 11.10.2012 -

Inhalt

Einleitung

Zur Zentralisierung und Konsolidierung verteilter Datenverarbeitung sowie aus Kostengründen greifen Daten verarbeitende Stellen zunehmend auf kooperative Betriebsmodelle zurück, die die gemeinsame Nutzung von Systemen und Programmen zur automatisierten Verarbeitung personenbezogener Daten vorsehen.

Die gemeinsame Nutzung einer solchen Infrastruktur unterliegt erhöhten Anforderungen an die Trennung der personenbezogenen Daten, um die aus der gemeinsamen Nutzung entstehenden Risiken für die informationelle Gewaltenteilung, die Zweckbindung und Vertraulichkeit hinreichend zu reduzieren.

In diesem Dokument werden eine **Begriffsdefinition**, die aus Datenschutzsicht **notwendigen Schritte zur Prüfung** einer ausreichenden Trennung von automatisierten Verfahren bei der Nutzung einer gemeinsamen IT-Infrastruktur (Mandantenfähigkeit) und notwendige **Ergänzungen bestehender Datenschutz- und Informationssicherheitsmanagementsysteme** (DSMS/ISMS) dargestellt.

Begriffsdefinition

Der Begriff „Mandant“ oder „Mandantenfähigkeit“ wird häufig verwendet, wenn es Unternehmen, Behörden oder Organisationen ermöglicht werden soll, Daten in einer Datenbank logisch zu trennen und zu verwalten. Mit Hilfe der Mandantenfähigkeit können z. B. Daten verschiedener Abteilungen einer Organisation / eines Unternehmens oder verschiedener Kunden eines IT-Services / Rechenzentrums getrennt vorgehalten werden.

Die Datenschutzgesetze der Länder und des Bundes fordern jedoch, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben worden sind, getrennt voneinander verarbeitet werden. Die getrennte Verarbeitung betrifft sowohl die Speicherung als auch die Verarbeitungsfunktionen wie etwa Datenbanktransaktionen oder Datensatzbuchungen.

Aus wirtschaftlichen oder praktikablen Gründen kann es aber sinnvoll sein, dass Ressourcen wie Hard- und Software, also IT-Infrastrukturen für verschiedene, voneinander zu trennende Datenbestände gemeinsam genutzt werden. In begründeten Fällen kann daher auch eine gemeinsame Speicherung mit mandantenbezogener Kennzeichnung der Daten zulässig sein. Voraussetzung hierfür ist, dass die Daten mandantenbezogen geführt und Verarbeitungsfunktionen, Zugriffsberechtigungen und Konfigurationseinstellungen je Mandant eigenständig festgelegt werden können. Die Datenverarbeitung muss dabei zwingend durch technische Maßnahmen getrennt voneinander erfolgen. Insbesondere gilt das auch dann, wenn für die jeweiligen Daten unterschiedliche Stellen verantwortlich sind oder es sich bei den personenbezogenen Daten um besondere Arten personenbezogener Daten handelt.

Der abgeschlossene Datenhaltungs- und Verarbeitungskontext einer im datenschutzrechtlichen Sinne verantwortlichen Stelle wird in diesem Papier nachfolgend als „**Mandant**“ bezeichnet, die getrennte Speicherung und Verarbeitung als „**Mandantentrennung**“. Ein Verfahren ist „**mandantenfähig**“, wenn es eine Mandantentrennung umsetzt.

Weitere Definitionen:

- **Gemeinsame 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.
- **Gemeinsame Verfahren** im Sinne dieser Orientierungshilfe sind automatisierte Verfahren, die mehreren Daten verarbeitenden Stellen die Verarbeitung personenbezogener Daten in oder aus einem Datenbestand ermöglichen. Gemeinsame Verfahren sind auch Verfahren, die die Übermittlung von Daten einer Stelle durch Abruf einer oder mehrerer anderer Stellen ermöglichen.
- 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.

Anwendungsbereich

Die folgenden Betrachtungen gelten für Verfahren zur Verarbeitung personenbezogener Daten, bei denen im Sinne der Datenschutzgesetze mehrere Daten verarbeitende Stellen eine Datenverarbeitung auf einer gemeinsamen IT-Infrastruktur ausführen, die Datenverarbeitung aus Rechtsgründen aber voneinander zu trennen ist.

Prüfung auf ausreichende Trennung der Verfahren

Zur Prüfung, ob eine ausreichende Trennung bei der gemeinsamen Nutzung einer IT-Infrastruktur gewährleistet wird und die Datenschutz- und Datensicherheitsanforderungen angemessen und wirksam umgesetzt werden, sollten die folgenden Prüfschritte durchlaufen werden.

Prüfschritt 1: Rechtliche Grundlagen

Die Prüfung, ob durch technische und organisatorische Maßnahmen eine ausreichende Trennung der Verfahren erreicht werden kann und durch welche, setzt eine vorlaufende rechtliche Betrachtung voraus. Dazu sind heranzuziehen:

- die für das jeweilige Fachverfahren anzuwendenden spezialgesetzlichen Bestimmungen,
- die datenschutzrechtlichen Grundsätze und
- die allgemeinen datenschutzrechtlichen Bestimmungen.

Im öffentlichen Bereich ist hierbei regelmäßig der vom Bundesverfassungsgericht im Volkszählungsurteil entwickelte datenschutzrechtliche Grundsatz der informationellen Gewaltenteilung (Abschottungsgebot), welcher staatliche Behörden dazu verpflichtet, personenbezogene Daten auch gegenüber anderen staatlichen Behörden abzuschotten.

Rechtsgründe für die Trennung von Verfahren sind

- gesetzliche Vorgaben,
- insbesondere unterschiedliche Zweckbestimmungen der Datenverarbeitung,
- die Tatsache, dass für verschiedene Teilsysteme unterschiedliche verantwortliche Stellen existieren. Dies gilt auch für so genannte gemeinsame Verfahren.

Die in den nachfolgenden Abschnitten dargestellten Anforderungen und Hinweise sind nicht anwendbar auf die ausschließliche Verarbeitung von Daten, die auf landes- oder spezialgesetzlicher Grundlage unter gemeinsamer rechtlicher Verantwortung stehen, oder auf den automatisierten Abruf über die Grenzen einer gemeinsamen IT-Infrastruktur hinweg.

Die Datenverarbeitung und die technischen und organisatorischen Sicherheits- und Datenschutzmaßnahmen müssen sich an diesen rechtlichen Vorgaben orientieren.

Zu betrachten und zu bewerten sind u.a.:

- Welche Daten verarbeitenden Stellen sollen die Infrastruktur gemeinsam nutzen?
- Welche Rechtsgrundlage und welche Zweckbestimmung oder Zweckbindung liegt der jeweiligen Verarbeitung zugrunde?
- Wo liegt die gesetzgeberische Regelungskompetenz (EU/Bund/Land) für die jeweilige Verarbeitung?
- Gibt es eine Ermächtigungsbefugnis, durch welche ggf. auch eine gemeinsame Verarbeitung (gemeinsame und verbundene automatisierte Dateien) zugelassen werden dürfte – und wurde von dieser Gebrauch gemacht?
  Oder ist diese ausgeschlossen?

Die konkrete Ausprägung der gemäß Trennungsgebot notwendigen Umsetzung einer getrennten Datenverarbeitung muss sich am Schutzbedarf der Daten orientieren.

> *Beispiel: So können z.B. bei einem sehr hohen Schutzbedarf die aus der gemeinsamen Nutzung einer IT-Infrastruktur entstehenden Restrisiken nicht tragbar sein oder Rechtsnormen, die mit einer gemeinsamen Nutzung von IT-Infrastrukturen verbundenen Offenbarungen verbieten. In diesen Fällen ist dann eine physikalische Trennung bzw. ein Betrieb durch zwei unterschiedliche Stellen zwingend geboten, und die Nutzung eines von einer einzelnen Stelle betriebenen mandantenfähigen Verfahrens ist nicht zugelassen.*

Prüfschritt 2: Ausgestaltung von Übermittlungen zwischen Mandanten

Bei einer getrennten Verarbeitung auf gemeinsamer IT-Infrastruktur ist die Verarbeitung von Daten eines Mandanten in einem anderen Mandanten 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.

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. Zulässige Suchkriterien sind in der Regel vorher vertraglich festzuhalten. 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. Zur Isolierung der Übermittlung von Transaktionen innerhalb eines Mandanten darf auf übermittelte Daten erst nach Abschluss der Übermittlung und ihrer Protokollierung zugegriffen werden.

Prüfschritt 3: 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.

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 das Verfahren 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. durch eine abgeschlossene Einheit mit eigenen Datensätzen und einem vollständigen Satz von Tabellen**. Sämtliche Zugriffe auf personenbezogene Daten müssen die vergebenen Zugriffsberechtigungen (siehe Prüfschritt 4) sowie diese Zuordnung berücksichtigen und durchsetzen**.

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.

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 4:
Unabhängigkeit der Konfiguration

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.

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 der Vorgaben der einzelnen Mandanten konfigurierbar sein.

Als Anforderungen sind hierfür mandantenspezifisch zumindest vorzusehen

- ein getrenntes, mandantenspezifisches System zur Berechtigungsvergabe,
- Konfigurationsmöglichkeiten für die Nutzungsprotokollierung sowie
- eine administrative Protokollierung.

Die Berechtigungsvergabe muss über ein auf Ebene des einzelnen Mandanten abgeschlossenes Berechtigungssystem erfolgen. 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.

Die Zuordnung zu jeweils einem Mandanten ist in der folgenden Abbildung verdeutlicht:

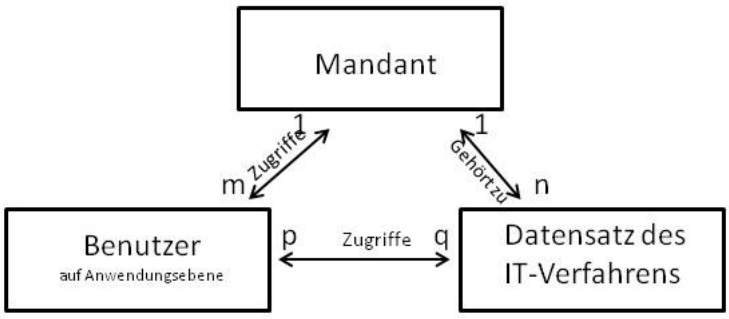

Abbildung 1: Schematische Darstellung Berechtigungsvergabe

Die mandantenspezifische Nutzungsprotokollierung darf sich nur auf Schritte zur Datenverarbeitung beziehen, die den jeweiligen Mandanten betreffen. Die Anforderungen der „Orientierungshilfe Protokollierung“[1] der Datenschutzbeauftragten des Bundes und der Länder sind hierfür mandantenspezifisch umzusetzen.

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

[1] http://www.lfd.m-v.de/dschutz/informat/protokol/oh-proto.pdf

jeden Mandanten getrennt gespeichert werden.

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 des Verfahrens durchgeführt wird. Zusätzlich zur mandantenspezifischen administrativen Protokollierung sind auch die Protokolleinträge zugänglich zu machen, die im Rahmen der mandantenübergreifenden Verwaltung des Verfahrens durchgeführt wurden.

Prüfschritt 5: 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.

> *Beispiel: So muss bspw. bei Beendigung des Auftragsdatenverhältnisses für einen Mandanten 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. 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 differenzierten Administrationskonzepts,
- eine revisionssichere Protokollierung der administrativen Tätigkeiten und Festlegung eines Protokollierungskonzepts,
- die Definition eines mandantenspezifischen und mandantenübergreifenden Berichtswesens,
- die Definition von Revisionen über das Gesamtsystem und
- die Definition von Prozessen für das mandantenspezifische und mandantenübergreifende Change-Management.

Konzeption und Umsetzung des Datenschutzmanagements

Risikoanalyse

Die Datenschutzgesetze des Bundes und der Länder fordern, vor der Entscheidung über die Einführung oder die wesentliche Änderung eines automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden sollen, eine Risikoanalyse durchzuführen. Diese Risikoanalyse dient als Nachweis, dass die Gefahren für die Rechte der Betroffenen durch angemessene technische und organisatorische Sicherheits- und Datenschutzmaßnahmen beherrscht werden können. Hierbei müssen auch die speziellen Risiken für die Vertraulichkeit, Integrität, Verfügbarkeit, Transparenz, Nicht-Verkettbarkeit und Intervenierbarkeit bei der getrennten Datenverarbeitung auf einer gemeinsamen IT-Infrastruktur betrachtet werden.

Die Risikoanalyse muss diese Risiken insbesondere mit dem Fokus auf den für die Betroffenen entstehenden Gefährdungen einer unzureichenden Datentrennung betrachten.

Wenn die IT-Grundschutz-Standards und die IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) angewendet werden, ist eine Risikoanalyse gemäß dem BSI-Standard 100-3 erforderlich, wenn ein hoher oder sehr hoher Schutzbedarf gegeben ist oder die genannten speziellen Risiken nicht von Bausteinen aus den IT-Grundschutz-Katalogen abgedeckt sind. Ergeben sich zusätzliche, noch nicht berücksichtigte Risiken, so sind diese nach dem genannten Standard zu bewerten und falls erforderlich mit weiteren Maßnahmen auf ein tragbares Maß zu vermindern.

Nachweis ausreichender Sicherheits- und Datenschutzmaßnahmen und Dokumentationspflicht

Der Nachweis einer wirksamen Umsetzung der auf Basis der Risikoanalyse erforderlichen Sicherheits- und Datenschutzmaßnahmen muss insbesondere die Maßnahmen umfassen, die eine Trennung der Daten auf Ebene der Datenhaltung, Datenverarbeitung und des Datentransports sicherstellen.

Als Nachweis einer ausreichenden Trennung einzelner Mandanten ist darzustellen, ob bzw. wie die Daten eines Mandanten zwischen der gemeinsamen Infrastruktur und der mandantenspezifischen Infrastruktur übertragen werden können. Im Rahmen dieses Nachweises ist zum einen darzustellen, mit welchen technischen und organisatorischen Mitteln die im Verfahren verarbeiteten personenbezogenen Daten getrennt werden. Dabei muss berücksichtigt werden, welche Daten verarbeitende Stellen die gemeinsame Infrastruktur nutzen. 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.

Eine getrennte Datenverarbeitung ist durch technische Maßnahmen sicherzustellen. Die jeweils damit verbundenen spezifischen Vor- und Nachteile sowie deren Risiken müssen dabei betrachtet werden. Die technische Umsetzung einer getrennten Datenverarbeitung mithilfe relationaler Datenbanken kann durch unterschiedliche Maßnahmen erfolgen:

- 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.

Der Nachweis sollte die Durchführung und Ergebnisse der Prüfschritte 1 bis 5 umfassen.

Restrisikobetrachtung

Risiken, die nicht oder nur zum Teil durch die Datensicherheits- und Datenschutzmaßnahmen ausreichend reduziert wurden, müssen explizit ausgewiesen werden. Risiken, die aufgrund einer unzureichenden Trennung der Mandanten bestehen, sind gesondert aufzuführen.

Die Übernahme der Restrisiken muss schriftlich durch den Leiter der dem Mandanten zugeordneten Daten verarbeitenden Stelle erfolgen. Die Übernahme der Restrisiken muss durch alle Daten verarbeitenden Stellen erfolgen, die auf der gemeinsamen Infrastruktur eine getrennte Datenverarbeitung durchführen. Die Übernahme der Restrisiken ist wechselseitig allen an der getrennten Datenverarbeitung beteiligten Stellen zur Kenntnis zu geben.

Datenschutz- und Sicherheitsmanagement

Wird eine gemeinsame Infrastruktur zur getrennten Verarbeitung personenbezogener Daten genutzt, so ist ein mandantenübergreifendes Datenschutz- und Sicherheitsmanagement einzurichten.

Jede Daten verarbeitende Stelle hat für die mandantenbasierte Verarbeitung personenbezogener Daten einen Ansprechpartner in Fragen des Datenschutzes und der Datensicherheit zu benennen. Üblicherweise sind hierfür die betrieblichen oder behördlichen Datenschutz- und IT-Sicherheitsbeauftragten zu benennen.

Die gemeinsam genutzte Infrastruktur muss regelmäßig durch das gemeinsame, mandantenübergreifende Datenschutz- und Sicherheitsmanagement auf angemessene technische und organisatorische Datenschutz- und Sicherheitsmaßnahmen sowie eine wirksame Umsetzung insbesondere der Datentrennung geprüft werden. Die Prüfergebnisse, insbesondere solche, aus denen sich mandantenübergreifende Auswirkungen ergeben können, sind allen Mandanten zur Verfügung zu stellen.

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.

Das gemeinsame, mandantenübergreifende Datenschutz- und Sicherheitsmanagement muss in die betrieblichen Prozesse der gemeinsam genutzten Infrastruktur eingebunden sein. 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 Stellen erfolgen.

Fazit

Die ordnungsmäßige, getrennte Verarbeitung personenbezogener Daten in einer gemeinsamen IT-Infrastruktur muss, aufsetzend auf einer Betrachtung der rechtlichen Rahmenbedingungen, durch zusätzliche technische und organisatorische Sicherheitsmaßnahmen sichergestellt werden.

Zum Nachweis einer ordnungsgemäßen Verfahrenstrennung ist es zunächst erforderlich,

- die **rechtlichen Grundlagen,** auch zur Zulässigkeit der Datenübermittlungen zwischen Mandanten, wo diese vorgesehen sind, zu prüfen,
- die **Revisionsfähigkeit der Übermittlungen** zwischen den Mandanten,
- die **Abgeschlossenheit der Transaktionen innerhalb der Mandanten** und
- die **Unabhängigkeit der Konfiguration** nachzuweisen sowie
- die **Beschränkungen der mandantenübergreifenden Verwaltung der Datenverarbeitung** strikt umzusetzen.

Auf Basis dieser Vorüberlegungen ist dann das **Datenschutz- und Sicherheitsmanagement** auf diese besondere Form der Datenverarbeitung anzupassen.