Gesellschaft für Datenschutz und Datensicherheit e.V.

BvD e.V. Die Datenschützer

Standard "Anforderungen an Auftragnehmer nach § 11 BDSG"

- DATENSCHUTZSTANDARD DS-BVD-GDD-01 -

GESELLSCHAFT FÜR DATENSCHUTZ UND DATENSICHERHEIT (GDD) E.V. /

BERUFSVERBAND DER DATENSCHUTZBEAUFTRAGTEN DEUTSCHLANDS (BVD) E.V.

Standard "Anforderungen an Auftragnehmer nach § 11 BDSG"
- DATENSCHUTZSTANDARD DS-BVD-GDD-01 -

Version 1.0 vom 25.09.2013

1. Auflage, 2013

Herausgeber:

Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) befürwortet den zugrunde liegenden Standard.

Link: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Wirtschaft/Inhalt/Modellvorhaben_Datenschutzsiegel/Modellvorhaben_Datenschutzsiegel.php

INHALTSVERZEICHNIS

STANDARD "ANFORDERUNGEN AN AUFTRAGNEHMER NACH § 11 BDSG" - DATENSCHUTZSTANDARD DS-BVD-GDD-01 -

ABBILDUNGSVERZEICHNIS

1 Scope

Um einen Mehrwert durch ein Audit für Dienstleistungen im Rahmen der Auftragsdatenverarbeitung nach § 11 BDSG zu kreieren, stellen die Kontrollpflichten der Auftraggeber vor und während der Verarbeitung einen Ansatz dar:

- Die Auftraggeber sind in der Praxis häufig mit der Umsetzung dieser Verpflichtung überfordert.
- Die Auftragnehmer fürchten eine übermäßige Inanspruchnahme und Bindung von Kapazitäten durch Prüfungen durch Auftraggeber.

Aus dieser Interessenlage leitet sich die Frage ab, wie und in welchem Umfang die Kontrollverpflichtung in ihrer operativen Umsetzung auf Dritte übertragen und durch Zertifikate bestätigt werden kann[1]. Dem Auftraggeber wird es dabei nicht immer möglich sein, eine Vor-Ort-Prüfung durchzuführen. Allerdings darf er sich nicht auf bloße Zusicherungen des Auftragnehmers verlassen, sondern er muss eigene Recherchen betreiben, um sich Gewissheit darüber zu verschaffen, dass gesetzlich normierte oder vertraglich vereinbarte Sicherheitsstandards eingehalten werden. Die Lösung kann darin bestehen, dass der Auftragnehmer sich einem Zertifizierungs- bzw. Gütesiegelverfahren zu Fragen des Datenschutzes und der Datensicherheit bei einer unabhängigen und kompetenten Prüfstelle unterwirft.[2]

Unterwirft man die Auftragsdatenverarbeitung nach § 11 BDSG einem allgemeinen Audit beim Auftragnehmer und durch ihn initiiert, kann das nur auf der Grundlage einer Prüfung gegen einen transparenten Anforderungskatalog (Standard) erfolgen. Denn die unterschiedlichen Positionen der beteiligten Parteien (Abwehr eines Haftungsrisikos aufgrund des individuellen Prüfauftrags an den Auftraggeber ./. Interesse an der allgemeinen Bestätigung des korrekten Dienstleistungsangebots des Auftragnehmers) erfordern, dass auf der (allgemeinen) Zertifizierung einer Dienstleistung die individuelle Prüfung des Auftraggebers aufsetzen kann.

Ein solcher Standard soll hier vorgestellt werden:

---

[1] Zur Zulässigkeit der Beauftragung Dritter zur Kontrolle im Rahmen der Auftragsdatenverarbeitung s. Gesetzesbegründung zu § 11 BDSG (2009) – BT-Drs. 16/13657 v. 01.07.2009, S. 29 –: „…Abgesehen wird davon, dass sich der Auftraggeber unmittelbar beim Auftragnehmer vor Ort oder selbst in Person überzeugt. Dies wäre regelmäßig nicht angemessen und mit einem Verlust an Flexibilität verbunden, z. B. wenn der Auftraggeber ein Testat eines Sachverständigen einholen möchte oder wenn eine schriftliche Auskunft des Auftragnehmers ausreicht. …“

[2] Siehe Orientierungshilfe Cloud Computing (Version 1.0, Stand 26.09.2011), URL: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Cloud_Computing/oh_cloud.pdf, S. 9.

Betrachtet man § 11 Abs. 1-3 BDSG aus Sicht des Normadressaten, des Auftraggebers, näher, stellt sich der Gesetzgeber einen Prozess vor, in dem sehr früh „Kontrollpflichten" entstehen. Im Rahmen des hier vorgestellten Standards ist der Auftragnehmer gehalten, diesen „Kontrollpflichten" adäquate „Kontrollziele" entgegenzustellen, deren Umsetzung durch eine neutrale Stelle auditiert und zertifiziert werden kann.

Mit anderen Worten:

Im Rahmen des Standards sind die Anforderungen an den Auftraggeber auf das Angebot des Auftragnehmers zu spiegeln (vgl. Abbildung 1: Übertragung der Anforderungen an den Auftraggeber in Erwartungen an den Auftragnehmer).

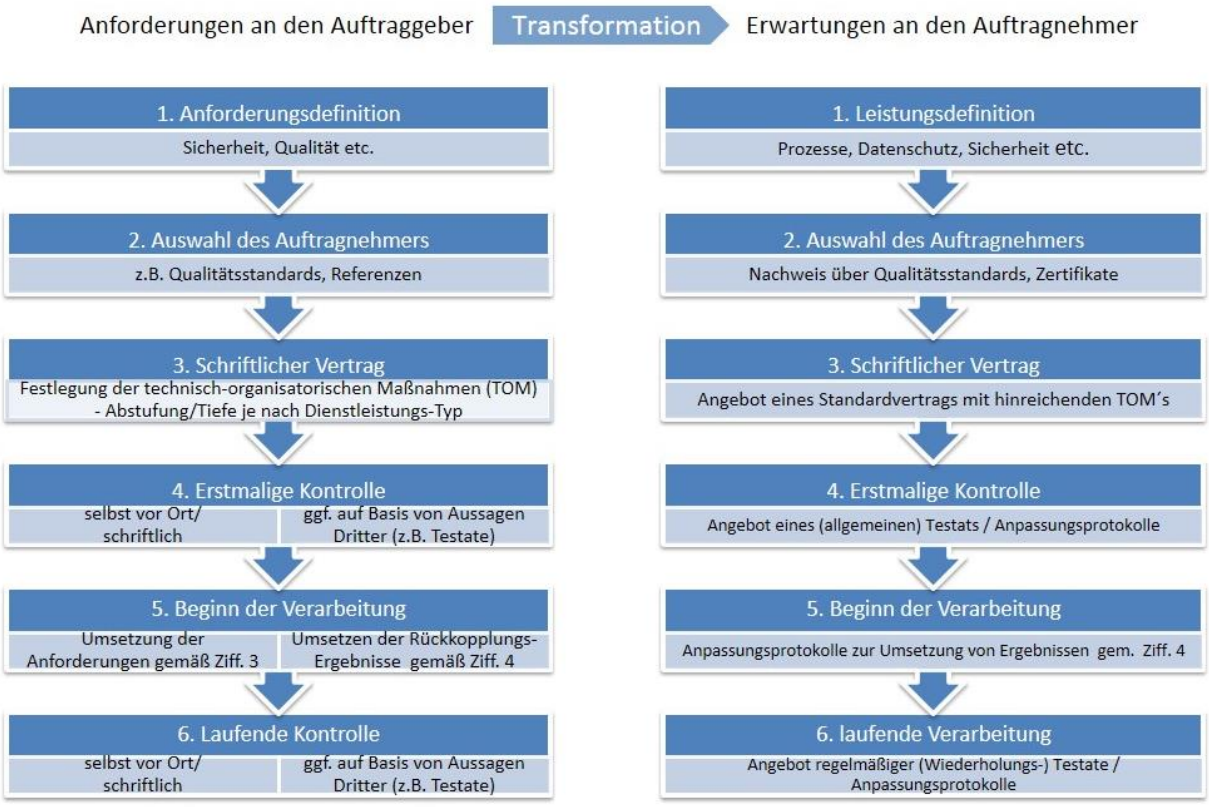

Abbildung 1: Übertragung der Anforderungen an den Auftraggeber in Erwartungen an den Auftragnehmer

Aufgrund der Unterschiedlichkeit der angebotenen Dienstleistungen und des gesetzlichen Mixes an Anforderungen, die teils als konkrete Maßnahmen teils als Prozesse abgebildet werden müssen, beschreibt der vorliegende Standard Maßnahmen und Prozesse, die ein Auftragnehmer zu treffen hat, um eine datenschutzkonforme Auftragsdatenverarbeitung nach § 11 BDSG anbieten zu können.

Der Standard richtet sich damit in erster Linie an Auftragnehmer und folgt insbesondere folgenden Prämissen:

- Maßstab ist die Auftragsdatenverarbeitung im Sinne des § 11 BDSG.
- Gegenstand ist die durch den Auftragnehmer angebotene und entsprechend im Sinne des § 11 BDSG zu konkretisierende Dienstleistung.
- Der Standard spiegelt die Pflichten von Auftraggebern im Rahmen einer Auftragsdatenverarbeitung auf die Anforderungen an den anbietenden Auftragnehmer.
- Der Standard ist modular zu verstehen und entsprechend der betrachteten Leistung des Auftragnehmers anzupassen.
- Die Umsetzung von „Kernmodulen“ ist obligatorisch.
- Die Umsetzung erfolgt durch dokumentierte technische und / oder organisatorische Maßnahmen oder Prozesse. Die Dokumentation umfasst insbesondere auch die Verantwortlichkeiten.
- Der Standard betrifft nur Dienstleistungen, die ausschließlich im Bereich der EU / des EWR erbracht werden.

„Kernmodule“ sind in jedem Fall umzusetzen. Branchenspezifische Vorgaben werden durch die Entwicklung weiterer leistungsabhängiger Module gewährleistet.

2 Begriffsdefinitionen

Auftraggeber: Unternehmen oder natürliche Person, die einen Auftrag gemäß § 11 BDSG erteilt hat oder erteilen will (s. a. § 3 Abs. 7 BDSG).

Auftragnehmer: Unternehmen oder natürliche Person, die einen Auftrag gemäß § 11 BDSG angenommen hat oder annehmen will (s. a. § 3 Abs. 8 BDSG).

Auftragsdaten: Personenbezogene Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

Datenschutzkonzept: Das Datenschutzkonzept beschreibt die angemessenen und erforderlichen Datenschutzvorgaben bei der Leistungserbringung. Die Prozesse und Maßnahmen sind konkret zu beschreiben.

Personenbezogene Daten: „Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“ (§ 3 Abs. 1 BDSG).

Besondere personenbezogene Daten: Personenbezogene Daten, die der Gesetzgeber als besonders sensibel eingestuft hat (§ 3 Abs. 9 BDSG):

- Angaben über die rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder philosophische Überzeugungen,
- Gewerkschaftszugehörigkeit,
- Gesundheit oder Sexualleben.

Betroffener: Bestimmte oder bestimmbare natürliche Person, deren personenbezogene Daten verarbeitet werden.

Verarbeiten: Abweichend von den Legaldefinitionen des BDSG werden, um die Lesbarkeit zu erhöhen, alle Phasen des Umgangs mit Daten (erheben, speichern, verändern, übermitteln, löschen, sperren, nutzen) unter dem Begriff „verarbeiten“ zusammengefasst.

Auftrag: Der Auftrag umfasst die Weisungen des verantwortlichen Auftraggebers, seine Daten durch den Auftragnehmer zu verarbeiten.

Risikoanalyse: Eine Risikoanalyse stellt den Wert der zu schützenden Daten den im BSI-Grundschutz[3] definierten Gefahren gegenüber. Anhand der getroffenen Maßnahmen werden Eintrittswahrscheinlichkeit und Schadenshöhe bestimmt, die zusammen Auskunft über das Risiko geben.

[3] Bundesamt für Sicherheit in der Informationstechnik (2011): IT-Grundschutz-Kataloge, 12. Ergänzungslieferung - September 2011. URL: www.bsi.bund.de/grundschutz.

3 Lesehilfe

„Kernmodule“ sind – sofern sie für die betrachtete Leistung einschlägig sind – zu erfüllen. „Module in Abhängigkeit des Leistungsumfangs“ sind verbindlich, wenn sie der Dienstleistung immanent oder Zusatzleistung des Auftragnehmers sind (z. B. Mustervertrag).

Ein Modul hat folgenden Aufbau:

- **Schutzziele:** Die Schutzziele beschreiben den Schutzauftrag des Moduls. Sie erläutern, welche Schutzziele durch die Vorgaben und Anforderungen des Moduls erfüllt werden sollen.
- **Vorgaben:** Vorgaben sind verbindliche Maßnahmen, die erfüllt sein müssen, um den Standard zu erfüllen.
- **Anforderungen:** Anforderungen stellen Ziele dar. Wie diese Ziele umgesetzt werden, um den Standard zu erfüllen, bleibt im Ermessen des Anwenders.
- **Best Practice Beispiele:** Anregung zur Umsetzung der Vorgaben und Anforderungen sollen die Best Practice Beispiele geben. Sie sind nicht Teil des Standards, d.h. sie müssen nicht 1:1 umgesetzt werden, um den Standard zu erfüllen.

4 Kernmodule

4.1 Leistungsbeschreibung

4.1.1 Beschreibung der Leistung

4.1.1.1 Schutzziele

Die Leistungsbeschreibung dient der Definition des zu betrachtenden Gegenstandes der Auftragsdatenverarbeitung im Sinne des § 11 BDSG sowie anderer Dienstleistungen des Auftragnehmers sowie zur Abgrenzung zur eigengenutzten internen (IT-)Infrastruktur des Dienstleisters (Was soll geleistet werden?). Die Leistungsbeschreibung bildet eine verbindliche Grundlage für die Gestaltung der Vertragsbeziehung zwischen Auftraggeber und Auftragnehmer und sorgt für die erforderliche Transparenz der Datenverarbeitung.

Hierzu sind folgende Grundsätze zu berücksichtigen:

- Die Auftragsdatenverarbeitung im Sinne des § 11 BDSG muss einen IT-gestützten Prozess des Auftraggebers (zumindest) unterstützen.
- Um die Dienstleistung an sich können – mehr oder weniger ausgeprägte – „Umgebungs-Schichten“ gezogen werden[4]. Die Anforderungen hieran können abstrakt definiert werden.

Aus den gesetzlichen Vorgaben des § 9 BDSG und Anlage resultiert die Pflicht der datenschutzrechtlich verantwortlichen Stelle, die automatisierte Datenverarbeitung technisch und organisatorisch abzusichern. Dieselbe Pflicht trifft gemäß § 11 Abs. 4 BDSG den Auftragnehmer im Rahmen einer Auftragsdatenverarbeitung. Damit einhergehend müssen Grundbedrohungen für die Verfügbarkeit, Integrität und Vertraulichkeit der Datenbestände erkannt und mit entsprechenden präventiven Maßnahmen versehen werden. Beim Auftragnehmer bestehen daher in Bezug auf die Datenverarbeitung zugunsten des Auftraggebers als der datenschutzrechtlich verantwortlichen Stelle als

[4] •vergleichbar BSI-Standard 100-1, 9.2.2 Erstellung der Sicherheitskonzeption:
….
- Übergeordnete Aspekte der Informationssicherheit (z.B. Organisation, Personal, Notfallvorsorge),
- Sicherheit der Infrastruktur (z.B. Gebäude, Rechenzentrum),
- Sicherheit der IT-Systeme (z.B. Server, Clients, Netzkomponenten),
- Sicherheit im Netz (z.B. Netz- und Systemmanagement) und
- Sicherheit in Anwendungen (z.B. E-Mail).

Grundbasis drei Standardsicherheitsanforderungen, die als Sicherheitsschichten aufeinander aufbauen (vergl. Abbildung 2: „Schichtenmodell“ einer Dienstleistung).

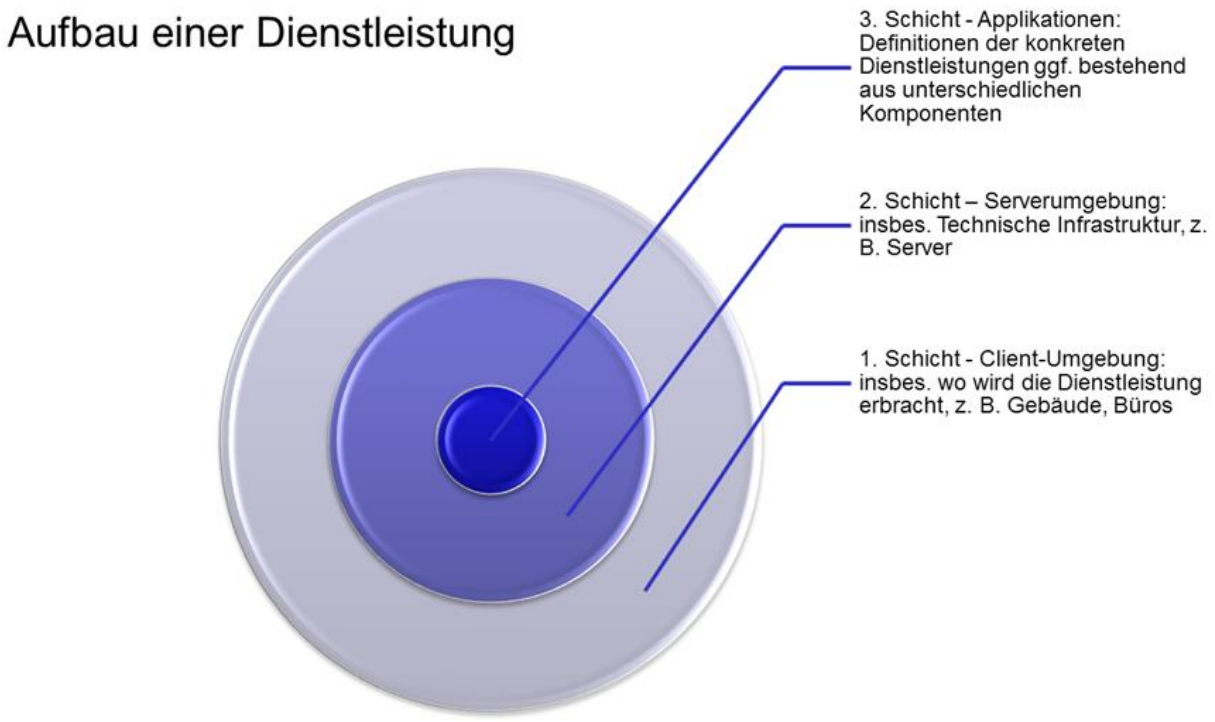

Abbildung 2: „Schichtenmodell“ einer Dienstleistung

Die äußerste Schicht bilden vor allem diejenigen Maßnahmen, die zur Abwehr eines unbefugten Zutritts bzw. Zugangs zu den im Verwaltungsbetrieb eingesetzten Datenträgern bzw. Datenträgersystemen dienen. Der Fokus ist auf die eingesetzten Datenträger gerichtet.

Eine zweite Sicherheitsschicht bildet der Rechenzentrumsbetrieb des Auftragnehmers. Aufgrund der systemischen Ausgestaltung in eine Client- (Verwaltungsgebäude) und Serverumgebung (Rechenzentrum) vollzieht sich der Schwerpunkt der Datenverarbeitung im Rechenzentrum des Auftragnehmers. Diesbezüglich müssen daher erhöhte Anforderungen an die Zutritts- und Zugangsbeschränkungen bestehen. Daneben bestehen im Rechenzentrumsbetrieb ebenfalls erhöhte Anforderung an die Verfügbarkeit und Integrität der dort gespeicherten Daten.

Werden die ersten beiden Sicherheitsschichten durch das für die Datenverarbeitung eingesetzte Personal auf legale Weise überwunden, muss im Weiteren gewährleistet werden, dass die in den zentralen Applikationen verarbeiteten personenbezogenen oder personenbeziehbaren Daten nicht unbefugt zur Kenntnis genommen oder verarbeitet werden. In diesem Zusammenhang muss bei der befugten Betreuung der Applikation darauf geachtet werden, dass Nutzeraktivitäten im Nachhinein nachvollziehbar sind.

Für die Anforderungen an die Dokumentation und die Prüfbarkeit gegen diesen Standard bedeutet das:

Bietet ein Auftraggeber alle drei Schichten als „Standard“ an, ist die Dienstleistung insgesamt überprüfbar.

Soweit jedoch in einer oder mehreren Schichten „standardmäßig“ Individualisierungen durch den Auftraggeber vorgesehen sind, ist von folgenden Prämissen auszugehen:

- Die Dienstleistung wird regelmäßig im Rahmen einer „Standard-Umgebung“ erbracht – i.d.R. Schicht 1 und 2 –, die eine Art „Basis-Sicherheit“ beschreibt und als solche prüfbar ist.
- Die Individualisierung erfolgt durch Nutzung von „Standard-Alternativen“. Auch dies bleibt prüfbar.
- Die Individualisierung erfolgt anhand der Vorgaben des Einzelfalls, die eine Einzelfallprüfung erfordern. Daher kann und muss hier ein Prozess etabliert werden, der die Umsetzung der individuellen Auftraggeberanforderungen sicherstellt.

4.1.1.2 Vorgaben

Beschreibung der zu erbringenden Leistung / Produktbeschreibung für die

- „Auswahlphase“:
  - Vereinfachte Darstellung der Leistung, insbesondere im Hinblick auf den Gegenstand und den Umfang, die Art und den Zweck der Datenverarbeitung,
  - Vereinfachte Darstellung angemessener Datenschutz- und IT-Sicherheitsmaßnahmen.
- „Vertragsphase“:
  - Muster für die konkrete Darstellung der Leistung (Standard) für SLA / ADV; s. § 11 Abs. 2 S. 2 Nr. 1 BDSG: der Gegenstand des Auftrags,
  - Muster für die konkrete Darstellung des Umfangs, der Art und des Zwecks der Datenverarbeitung, der Art der Daten und des Kreises der Betroffenen (Standard) für SLA / ADV; s. § 11 Abs. 2 S. 2 Nr. 2 BDSG: der Gegenstand des Auftrags,
  - Konkrete Darstellung für standardmäßig angebotenen Datenschutz- und IT-Sicherheitsmaßnahmen, s. § 11 Abs. 2 S. 2 Nr. 3 BDSG.

4.1.1.3 Anforderungen

- Für die „Angebotsphase“
  - Der Gegenstand der Leistungen, in dessen Rahmen personenbezogene Daten verarbeitet werden sollen, ist beschrieben.
  - Die hierfür eingesetzten Produkte und Technologien sind angemessen beschrieben.
  - Vereinfachte Beschreibung des Datenschutzstandards für Angebotsauswahl und Vertragsphase.
- Für die Vertragsphase
  - Maßnahmen für einen wirkungsvollen Datenschutz und Datensicherheit (Datenschutzkonzept, Sicherheitskonzept) sind beschrieben.
  - Musterklauseln und / oder Verträge für die Leistungserbringung sowie für die Auftragsdatenverarbeitung gemäß § 11 BDSG liegen vor.
  - Eingebundene Unterauftragnehmer sind offengelegt.
  - Die Vorgehensweise bei der Leistungserbringung während und nach Vertragsabschluss kann erläutert werden.
  - Die notwendigen Informationen werden dem Auftraggeber für sein Verfahrensverzeichnis bereitgestellt.
  - Der Auftraggeber ist über Prüfungen durch Datenschutzaufsichtsbehörden zu informieren.

4.1.1.4 Best Practice Beispiele

- Neben allgemeinen Beschreibungen der Leistungserbringung werden kundenspezifische Dokumente gefertigt.
- Die DIN SPEC 1041 (DIN Spezifikation für Outsourcingprojekte bei technologieorientierten wissensintensiven Dienstleistungen) hilft kleinen und mittleren Unternehmen bei der Durchführung von Outsourcingprojekten. Das Strukturelement „Service Provider Auswahl“ der DIN SPEC 1041 sollte hinreichende Vorgehensmodelle und Maßnahmen beinhalten, um auf Auftragnehmerseite eine umfassende Beschreibung der Dienstleistung sicherzustellen.

4.1.2 Beschreibung der Herstellung

4.1.2.1 Schutzziele

Die operative Durchführung der Dienstleistung ist detailliert zu beschreiben.

4.1.2.2 Vorgaben

Die Dokumentation ist hinreichend vollständig, einheitlich und in sich schlüssig für den Standardprozess vorzulegen.

4.1.2.3 Anforderungen

- Vollständige Prozessbeschreibung der zu erbringenden Leistung (z.B. durch Flussdiagramme) und aller Schnittstellen.
- Beschreibung, wann und unter welchen Umständen der Einflussbereich vom Auftraggeber auf den Auftragnehmer oder umgekehrt übergeht (z.B. Gefahrenübergang bei Datenübergabe).
- Aufstellung aller Unterauftragnehmer und Dienstleister und ihrer Funktion mit Bezug für die Auftragsbearbeitung. IT-Dienstleister mit Zugriff auf Auftragsdaten gehören dazu.
- Die Aktualisierung der Liste aller Unterauftragnehmer und Dienstleister mit Zugriff auf Auftragsdaten ist sicherzustellen.
- Es gibt Qualitätssicherungsprozesse.

4.1.2.4 Best Practice Beispiele

Ein übergeordnetes Dokument mit Verweis auf Prozessbeschreibungen und Arbeitsanweisungen erleichtert das Verständnis, wie die Leistung erbracht wird. Die Zulieferungen von Unterauftragnehmern sollte angemessen dargestellt werden.

4.2 Input-Management

Datenweitergaben vom Auftraggeber zum Auftragnehmer in großem Umfang oder / und in hoher Regelmäßigkeit als Teil der Leistungserbringung sind umfassend zu dokumentieren.

4.2.1 Schutzziele

- Beschreibung der Schutzmaßnahmen und Abläufe der Datenübertragung vom Auftraggeber inkl. Kontrolle und Annahmedokumentation.
- Auflistung von Datenquellen neben dem Auftraggeber mit Rechtsgrundlage.

4.2.2 Vorgaben

- Sämtliche Datenübertragungsvorgänge sind dokumentiert.
- Die Dokumentation umfasst u.a. Zeitpunkt, Absender, Art und Umfang der entgegengenommenen Daten. Die angebotene Dienstleistung bestimmt den Umfang der Dokumentation.
- Falls relevant: Nennung der Rechtsgrundlage bei Verwendung externer Datenquellen.

4.2.3 Anforderungen

Prozessdokumentation der Datenweitergabe vom Auftraggeber zum Auftragnehmer.

4.3 Auftragsmanagement

Sind regelmäßig mehrere Unternehmen in eine Leistungserbringung eingebunden oder sind innerhalb des Auftragnehmers viele Stellen mit der Verarbeitung der Daten des Auftraggebers befasst, kommt dem Auftragsmanagement eine besondere Bedeutung zu. Ein Nachweis über funktionierende Schnittstellen zwischen den beteiligten Stellen und Unternehmen und die vollständige Kontrolle über den jeweiligen Status eines Auftrags stehen hierbei im Vordergrund.

4.3.1 Schutzziele

Es soll geprüft und nachgewiesen werden, dass ein revisionssicheres Auftragsmanagement implementiert ist. Verbindlichkeit, Handlungssicherheit und aktueller Status für jeden Auftrag müssen bei allen Beteiligten jederzeit sichergestellt sein.

4.3.2 Vorgaben

- Beschreibung der Maßnahmen und Abläufe zur Auftragsbearbeitung inkl. Tätigkeiten von Unterauftragnehmern und Dienstleistern mit Bezug zur Auftragsbearbeitung.

- Beschreibung der Rollen und Schnittstellen zwischen Auftragnehmer und Auftraggeber und ihrer Aufgaben und Weisungsbefugnisse.
- Beschreibung der Änderungsprotokollierung während der Auftragsbearbeitung.

4.3.3 Anforderungen

Dokumentation des Auftragsmanagements inkl. Schnittstellenbeschreibungen und Steuerungs- u. Kontrollfunktionen.

4.4 Output-Management

Werden Datenweitergaben vom Auftragnehmer zum Auftraggeber als Teil der Leistungserbringung definiert, kann durch dieses Modul die Datenschutzkonformität der entsprechenden Prozesse geprüft werden.

4.4.1 Schutzziele

Eine Weitergabe von Daten vom Auftragnehmer zum Auftraggeber oder die Weitergabe an eine dritte Stelle muss sicher hinsichtlich Vertraulichkeit und Integrität sein und darf ausschließlich von hierfür autorisierten Personen durchgeführt werden.

4.4.2 Vorgaben

- Beschreibung der Maßnahmen und Abläufe der Datenübertragung zum Auftraggeber oder anderen Empfängern.
- Ein Berechtigungskonzept, welcher Mitarbeiter welche Daten weitergeben darf, liegt vor.
- Die Datenübertragung wird protokolliert.
- Insbesondere IT-Anwendungen, in denen massenhaft personenbezogene Daten gespeichert werden, weisen durch die Möglichkeit zum Export besondere Risiken für eine unbefugte Weitergabe auf. Diesen besonderen Risiken ist durch geeignete Maßnahmen wirksam zu begegnen.

4.4.3 Anforderungen

- Dokumentation der Prozesse und Schnittstellen bei der Weitergabe von Daten.
- Dokumentation der Berechtigungen und Protokollierungen.

4.5 Datenschutzkonzept

Eine umfassende Beschreibung der Erfüllung der datenschutzrechtlichen Vorgaben.

4.5.1 Eingabekontrolle

4.5.1.1 Schutzziele

Alle Veränderungen an den Daten des Auftraggebers sind nachvollziehbar und revisionssicher protokolliert. Die Ordnungsmäßigkeit einer Verarbeitung personenbezogener Daten bzw. ein Verstoß gegen die Ordnungsmäßigkeit der Datenverarbeitung ist damit jederzeit nachweisbar.

4.5.1.2 Vorgaben

Art und Umfang der Protokollierung muss dem Schutzziel Eingabekontrolle angemessen sein.

4.5.1.3 Anforderungen

- Veränderungen, die an den Auftragsdaten vorgenommen werden, sind angemessen zu protokollieren.
- Ein Protokollierungskonzept liegt vor.
- Die Änderungsprotokolle werden regelmäßig stichprobenartig kontrolliert, um zu prüfen, ob Änderungen ausschließlich von berechtigten Personen durchgeführt worden sind.
- Die Prüfung darf nicht von Personen durchgeführt werden, die mit der Eingabekontrolle überwacht werden.
- Es existiert eine technische und organisatorische Beschreibung der Verfahren und Prozesse zur Protokollierung.

4.5.2 Trennungsgebot

4.5.2.1 Schutzziele

Die Gewährleistung des Trennungsgebots ermöglicht, dass verschiedene Auftraggeber datenschutzkonforme Datenverarbeitungen von demselben Auftragnehmer durchführen (lassen) können. Die Mandantentrennung kann auch ganz oder teilweise auf logischer Ebene stattfinden.

4.5.2.2 Vorgaben

Es ist zu gewährleisten, dass personenbezogene Daten verschiedener Auftraggeber und verschiedener Aufträge eines Auftraggebers getrennt verarbeitet werden können.

4.5.2.3 Anforderungen

- Ein Berechtigungskonzept existiert, das die Mandantentrennung umsetzt.
- Es besteht eine Funktionstrennung zwischen Produktiv-, Entwicklungs-, Schulungs- und Testsystemen. Echtdaten von Produktivsystemen dürfen nur nach ausdrücklicher Weisung / Zustimmung des Auftraggebers in einem Entwicklungs-, Schulungs- oder Testsystem verwendet werden, und nur wenn die Sicherheit des Entwicklungs-, Schulungs- oder Testsystems vergleichbar mit der des Produktivsystems ist.[5]
- Tests führen nicht zur Verringerung des Schutzniveaus von Vertraulichkeit, Integrität oder Verfügbarkeit personenbezogener Daten.

4.5.2.4 Best Practice Beispiele

- Die Trennung von Produktiv- und Testumgebung ist durch geeignete und wirksame Maßnahmen (Proxies, Firewalls, VLANs und DMZ, Terminal Server etc.) gewährleistet.
- Auftraggeberspezifische Verschlüsselung von Datensätzen zur Durchsetzung der Zweckbindung und Vertraulichkeitssicherung gegenüber den Administratoren.
- Vergabe von Zugriffsrechten einzeln pro Verfahren/Auftraggeber.

[5] Für die Legitimierung gegenüber den Betroffenen ist der Auftraggeber verantwortlich, z. B. durch Einwillligung der Betroffenen.

- Der Datenverkehr zwischen verschiedenen Verfahren/Auftraggebern ist auf den geregelten Verfahrensablauf begrenzt.
- Weitere Anregungen und Erläuterungen finden sich in der „Orientierungshilfe Mandantenfähigkeit“ der Aufsichtsbehörden.[6]

4.5.3 Auftragskontrolle

4.5.3.1 Schutzziele

Gewährleistung einer weisungsgebundenen Datenverarbeitung.

4.5.3.2 Vorgaben

- Es ist sicherzustellen, dass der Auftrag gemäß der vereinbarten Leistung und den vereinbarten technischen und organisatorischen Maßnahmen erfüllt wird.
- Es ist sicherzustellen, dass Weisungen des Auftraggebers erfüllt werden.
- Auftraggeber und Auftragnehmer vereinbaren, auf welchem Wege (z.B. schriftlich, Fax, E-Mail) Weisungen verbindlich entgegengenommen werden.
- Weisungen werden angemessen dokumentiert.
- Es ist verbindlich festzulegen, wer auf Seiten des Auftraggebers Weisungen erteilen und wer auf Seiten des Auftragnehmers Weisungen entgegennehmen darf.
- Es existiert ein Prozess („Auftragskontrolle“), der die Bearbeitung des Auftrags gemäß Leistungsvereinbarung mit dem Auftraggeber und von Auftraggeberweisungen bis auf die unterste Ebene der Leistungserbringung, d.h. inkl. aller beteiligten Dienstleister, sicherstellt.
- Die Weisungen des Auftraggebers werden nach einem definierten Prozess entgegengenommen, auf Datenschutzkonformität geprüft, ggf. umgesetzt und archiviert (Change Management).

6 Technische und organisatorische Anforderungen an die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen IT-Infrastruktur, Orientierungshilfe Mandantenfähigkeit, Version 1.0 vom 11.10.2012, URL: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Gemeinsame_IT-Infrastruktur__Technische_und_organisatorische_Anforderungen__Trennungsgebot_und_Mandantenf__higkeit_/Gemeinsame_IT-Infrastruktur__Technische_und_organisatorische_Anforderungen__Trennungsgebot_und_Mandantenf__higkeit_.php

4.5.3.3 Anforderungen

- Die Bearbeitung von Aufträgen und Weisungen beim Auftragnehmer nach Entgegennahme der Auftraggeberweisung erfolgt nur nach Maßgabe der verantwortlichen Weisungsempfänger des Auftragnehmers.
- Es wird regelmäßig überprüft, ob die durchgeführte Datenverarbeitung auftrags- und weisungsgemäß erfolgte.
- Im Prozess Auftragskontrolle ist eine Prüfung der Datenschutzkonformität der Weisung implementiert.

4.5.4 Prozessbeschreibung Auskunft

4.5.4.1 Schutzziele

Schutzziele des Auskunftsanspruchs aus § 34 BDSG sind die Gewährleistung des Transparenzgebots (*Die Betroffenen sollen „wissen können, wer was wann und bei welcher Gelegenheit über sie weiß“*) und der Rechtsdurchsetzung zu Gunsten des Betroffenen (Intervenierbarkeit).

4.5.4.2 Vorgaben

- Existenz eines Datenschutzprozesses beim Auftragnehmer, der an den entsprechenden Prozess des Auftraggebers angebunden werden kann.
- Existenz eines Prozesses, um auftragsbezogene Auskunftsbegehren geordnet entgegenzunehmen und unverzüglich an den zuständigen Auftraggeber weiterzuleiten.
- Der Auftragnehmer stellt sicher, dass er alle im Rahmen eines berechtigten Auskunftsbegehrens geforderten Daten zeitnah und vollständig zur Verfügung stellen kann (technische Umsetzung). Dabei ist sicherzustellen, dass die Daten anderer Personen, Mitarbeiter oder Auftraggeber nicht mitbeauskunftet werden.

4.5.4.3 Anforderungen

- Rollen, Tätigkeiten und Verantwortlichkeiten im Hinblick auf den Auskunftsprozess auf Auftragnehmerseite und die Schnittstelle zum Auftraggeber sind umfassend beschrieben.
- Eine Qualitätskontrolle hinsichtlich der zu beauskunftenden Daten ist wirksam etabliert.

4.5.4.4 Best Practice Beispiele

- Es sind Formulare vorhanden, die die für eine Bearbeitung eines Auskunftsersuchens notwendigen Angaben anfordern und den Auskunftsprozess anstoßen können. Hierzu gehören insbesondere „Pflichtfelder“, die eine genaue Zuordnung erlauben (Kundennummer etc.).
- Aufbau eines Kommunikationswegs, um „fehlgeleitete“ Auskunftsbegehren an die richtige Stelle weiterzuleiten.
- Zur Beantwortung eines Auskunftsbegehrens sind Mustertexte empfehlenswert, um eine vollständige Beauskunftung sicherzustellen. Checklisten helfen, alle relevante Datenquellen abzufragen.

4.5.5 Prozessbeschreibung Berichtigung

4.5.5.1 Schutzziele

Das Recht auf Berichtigung verschafft dem Betroffenen Interventionsmöglichkeiten. Dies ist umfassend sicherzustellen.

4.5.5.2 Vorgaben

- Existenz eines Datenschutzprozesses beim Auftragnehmer, der an den entsprechenden Prozess des Auftraggebers angebunden werden kann.
- Existenz eines Prozesses, um auftragsbezogene Berichtigungsbegehren geordnet entgegenzunehmen und unverzüglich an den zuständigen Auftraggeber weiterzuleiten.
- Der Auftragnehmer stellt sicher, dass er alle im Rahmen eines berechtigten Berichtigungsbegehrens geforderten Berichtigungen zeitnah und vollständig durchführen kann (technische Umsetzung). Berichtigungen in bereits archivierten Datenbeständen (Backups) sind am Verhältnismäßigkeitsgrundsatz auszurichten. Sperrvermerke als Alternative zur Berichtigung können ausreichend sein.

4.5.5.3 Anforderungen

- Rollen, Tätigkeiten und Verantwortlichkeiten im Hinblick auf den Berichtigungsprozess auf Auftragnehmerseite und die Schnittstelle zum Auftraggeber sind umfassend beschrieben.

- Eine Qualitätskontrolle hinsichtlich der zu berichtigenden Daten ist wirksam etabliert.
- Wenn personenbezogene Daten redundant vorhanden sind, muss sich die Berichtigung auf alle Datensätze beziehen.

4.5.5.4 Best Practice Beispiele

Auf Seiten des Auftragnehmers sind Zuständigkeiten für die Durchführung von Berichtigungen festgelegt. Die Festlegung der Zuständigkeiten beschränkt sich auf die technische Durchführung und nimmt die finale Entscheidung des Auftraggebers zur Durchführung nicht vorweg.

4.5.6 Prozessbeschreibung Sperrung

4.5.6.1 Schutzziele

Das Recht auf Sperrung verschafft dem Betroffenen Interventionsmöglichkeiten. Dies ist umfassend sicherzustellen.

4.5.6.2 Vorgaben

- Existenz eines Datenschutzprozesses beim Auftragnehmer, der an den entsprechenden Prozess des Auftraggebers angebunden werden kann.
- Existenz eines Prozesses, um auftragsbezogene Sperrbegehren geordnet entgegenzunehmen und unverzüglich an den zuständigen Auftraggeber weiterzuleiten.
- Der Auftragnehmer stellt sicher, dass er alle im Rahmen eines berechtigten Sperrungsbegehrens geforderten Sperrungen zeitnah und vollständig durchführen kann (technische Umsetzung).

4.5.6.3 Anforderungen

- Rollen, Tätigkeiten und Verantwortlichkeiten im Hinblick auf den Sperrungsprozess auf Auftragnehmerseite und die Schnittstelle zum Auftraggeber sind umfassend beschrieben.
- Eine Qualitätskontrolle hinsichtlich der Sperrung ist wirksam etabliert.
- Wenn personenbezogene Daten redundant vorhanden sind, muss sich die Sperrung auf alle Datensätze beziehen.

- Gesperrte Daten sind in keinem System sichtbar.
- Gesperrte Daten im datenschutzrechtlichen Sinne dürfen nicht übermittelt werden.

4.5.6.4 Best Practice Beispiele

Auf Seiten des Auftragnehmers sind Zuständigkeiten für die Durchführung von Sperrungen festgelegt. Die Festlegung der Zuständigkeiten beschränkt sich auf die technische Durchführung und nimmt die finale Entscheidung des Auftraggebers zur Durchführung nicht vorweg.

4.5.7 Prozessbeschreibung Löschung

4.5.7.1 Schutzziele

Das Recht auf Löschung verschafft dem Betroffenen Interventionsmöglichkeiten. Dies ist umfassend sicherzustellen.

4.5.7.2 Vorgaben

- Existenz eines Datenschutzprozesses beim Auftragnehmer, der an den entsprechenden Prozess des Auftraggebers angebunden werden kann.
- Existenz eines Prozesses, um auftragsbezogene Löschbegehren geordnet entgegenzunehmen und unverzüglich an den zuständigen Auftraggeber weiterzuleiten.
- Der Auftragnehmer stellt sicher, dass er alle im Rahmen eines berechtigten Löschbegehrens geforderten Löschungen zeitnah und vollständig durchführen kann (technische Umsetzung).
- Ist eine Löschung technisch nicht möglich oder stellt sie einen unverhältnismäßig hohen Aufwand dar, ist die Sperrung sicherzustellen.

4.5.7.3 Anforderungen

- Rollen, Tätigkeiten und Verantwortlichkeiten im Hinblick auf den Löschprozess auf Auftragnehmerseite und die Schnittstelle zum Auftraggeber sind umfassend beschrieben.
- Eine Qualitätskontrolle hinsichtlich der Löschung ist wirksam etabliert.

- Wenn personenbezogene Daten redundant vorhanden sind, muss sich die Löschung auf alle Datensätze beziehen.

4.5.7.4 Best Practice Beispiele

Auf Seiten des Auftragnehmers sind Zuständigkeiten für die Durchführung von Löschungen festgelegt. Die Festlegung der Zuständigkeiten beschränkt sich auf die technische Durchführung und nimmt die finale Entscheidung des Auftraggebers zur Durchführung nicht vorweg.

4.5.8 Prozessbeschreibung Sicherheitsvorfall

4.5.8.1 Schutzziele

Ziel der Vorschrift ist es, die Betroffenen bei Datenschutzverletzungen vor möglichen Beeinträchtigungen ihrer Rechte und Interessen zu schützen sowie eine effektivere Durchsetzung datenschutzrechtlicher Regelungen zu ermöglichen.

4.5.8.2 Vorgaben

- Beschreibung, wie der Datenschutzprozess des Auftragnehmers an den entsprechenden Prozess des Auftraggebers angebunden werden kann.
- Existenz eines Prozesses, um Verstöße gegen die Weisungen des Auftraggebers oder gegen die Vorschriften zum Schutz personenbezogener Daten zu erkennen und unverzüglich den Auftraggeber zu informieren. Dazu gehören auch Sachverhalte, die geeignet sind, die Interessen des Auftraggebers zu tangieren.
- Existenz eines Prozesses, um Vorfälle, die eine gesetzliche Informationspflicht auslösen, zu erkennen, den Auftraggeber unverzüglich zu informieren und Maßnahmen zur Schadensminimierung einzuleiten.
- Existenz eines Prozesses, um einen Sicherheitsvorfall zeitnah zu untersuchen und aufzuklären.

4.5.8.3 Anforderungen

- Der Auftragnehmer kennt die für seine Leistungserbringung relevanten Informationspflichten nach einem Sicherheitsvorfall.
- Es ist definiert, was im Kontext der Leistungserbringung unter einem „Sicherheitsvorfall“ zu verstehen ist.

4.5.8.4 Best Practice Beispiele

Eine Orientierung gibt die Praxishilfe der GDD „Praxishilfe zur BDSG-Novelle II (2009)“.

4.6 IT-Sicherheitskonzept

IT-Sicherheit lässt sich nicht durch wenige „Standardmaßnahmen“ herstellen. Das Zusammenspiel der eingesetzten Geräte, Softwareprodukte, Netzwerke und Mitarbeiter bestimmt, wie anfällig ein Unternehmen gegenüber Gefahren wie z.B. Feuer, Defekt, Spionage oder Fehlbedienung ist. Auf der anderen Seite kosten Sicherheitsmaßnahmen Geld. Deshalb dokumentiert ein IT-Sicherheitskonzept einen Kompromiss zwischen Sicherheit und Wirtschaftlichkeit. Idealerweise informiert es auch über die Entscheidungsgründe, die einen Auftraggeber befähigen zu verstehen, warum auf bestimmte Maßnahmen verzichtet wird.

Es gibt vielfältige Methoden, ein IT-Sicherheitskonzept zu erstellen. Die praktische Erfahrung zeigt, dass konkrete Vorgaben zum Vorgehen und zum Inhalt kostenträchtige Streitigkeiten zwischen Auftraggeber und Auftragnehmer vermeiden helfen. Aus diesem Grund orientiert sich dieser Standard an den BSI-Standards 100-2 und 100-3, die flexibel auf alle Branchen und Unternehmensgrößen anwendbar und praktisch erprobt sind, schließt aber die Anwendung anderer etablierter IT-Sicherheitsstandards nicht aus. Der Verzicht auf eine neue Methode erlaubt es, die Vorarbeiten z.B. für eine ISO 27001 oder andere Zertifizierung zu verwenden.

4.6.1 Schutzziele

Das IT-Sicherheitskonzept beschreibt, mit welchen technischen und organisatorischen Maßnahmen der Auftragnehmer die ihm anvertrauten Auftragsdaten schützt. Der Schutz umfasst folgende Schutzziele:

- Vertraulichkeit: Nur durch den Auftragnehmer oder Auftraggeber bevollmächtigte Personen haben Zugriff auf die Auftragsdaten.
- Integrität: Nur durch den Auftragnehmer oder Auftraggeber bevollmächtigte Personen können Auftragsdaten verändern.
- Verfügbarkeit: Die Auftragsdaten stehen dem Auftraggeber rechtzeitig und in dem mit ihm vereinbarten Umfang zur Verfügung.

Die in diesem Modul konkret beschriebenen technischen und organisatorischen Maßnahmen stellen ein Mindestmaß dar, das nicht unterschritten werden darf. Welche Maßnahmen im Einzelfall eingesetzt werden, legt ein Auftragnehmer in seinem IT-Sicherheitskonzept fest.

4.6.2 Vorgaben

Das IT-Sicherheitskonzept soll den Schutz der Auftragsdaten beschreiben. Dazu müssen alle Räume, die Infrastrukturen und IT-Geräte betrachtet werden, die die Sicherheit der Auftragsdaten beeinflussen können.

Netzwerke sind zu betrachten, soweit durch sie Auftragsdaten fließen oder Geräte, die Auftragsdaten speichern oder verarbeiten, an diesem Netzwerk angeschlossen sind.

Unterauftragnehmer sind in die Betrachtung einzubeziehen, wenn sie

- Zugriff auf Auftragsdaten erlangen können (z.B. Hard- und Softwarewartung, als Administratoren),
- für die Leistungserbringung relevant sind (z.B. Rechenzentren, Cloud Anbieter, Druckereien, Logistikunternehmen).

4.6.2.1 Erstellung und Verwendung des IT-Sicherheitskonzepts

1. Der Auftragnehmer hat ein IT-Sicherheitskonzept basierend auf der angebotenen Leistung erstellt, das die Sicherheit der Auftragsdaten zum Gegenstand hat.
2. Das IT-Sicherheitskonzept erfüllt den BSI-Standard 100-2 „IT-Grundschutz-Vorgehensweise“ oder einen anderen etablierten Standard und dokumentiert folgende Schritte:
    - IT-Strukturanalyse,
    - Risikoabschätzung hinsichtlich der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit der zu schützenden Auftragsdaten (z.B. nach BSI-Grundschutz),
    - die betrachteten Schadensszenarien in der Risikoabschätzung,
    - Ableitung der Maßnahmen für IT-Systeme, Kommunikationsverbindungen und Räume.
3. Wenn die Art der Auftragsdaten durch den Auftragnehmer nicht erkennbar ist (z.B. Hosting), beschreibt das IT-Sicherheitskonzept das angebotene Schutzniveau. Die Beschreibung muss hinsichtlich ihrer Konkretheit und Detaillierung einen Auftraggeber in die Lage versetzen zu beurteilen, ob das angebotene Schutzniveau für seinen konkreten Schutzbedarf angemessen ist.
4. Der Auftragnehmer stellt (potentiellen) Auftraggebern entweder das vollständige IT-Sicherheitskonzept zur Verfügung oder eine Zusammenfassung, die hinreichend detailliert ist, so dass ein Auftraggeber das angebotene Schutzniveau einschätzen

kann. Die betrachteten Schadensszenarien und die angenommene Schutzwürdigkeit der Auftragsdaten müssen klar erkennbar sein.

5. Wenn die Schutzziele der Auftragsdaten durch IT-Systeme oder Personal von Unterauftragnehmern beeinträchtigt werden können, sind deren IT-Sicherheitskonzepte in das IT-Sicherheitskonzept des Auftragnehmers zu integrieren.

6. Wenn Unterauftragnehmer ihrerseits Unterauftragnehmer mit Zugriff auf die Auftragsdaten einsetzen, müssen die IT-Sicherheitskonzepte der Unterauftragnehmer die Sicherheitsmaßnahmen der Unterunterauftragnehmer enthalten.

7. Das IT-Sicherheitskonzept enthält ein Schulungskonzept zur IT-Sicherheit.

8. Das IT-Sicherheitskonzept regelt die Löschung oder Zerstörung defekter oder ausgemusterter Datenträger.

4.6.2.2 Mindeststandard Gebäudesicherheit

Das Gebäude, in dem die Auftragsdaten verarbeitet werden, muss eine wirksame Außenhautsicherung aufweisen.

4.6.2.3 Mindeststandard Zutrittsschutz

- Der Zutritt ist wirksam auf berechtigte Personen technisch zu beschränken. Für Unternehmensfremde existiert eine Besucherregelung (z.B. Registrierung und Begleitung durch einen Mitarbeiter).
- Die Anzahl der berechtigten Personen ist auf ein unbedingt nötiges Minimum zu beschränken.
- Die Zutrittsberechtigung erfolgt aufgabenangemessen.
- Ausgegebene Schlüssel, Zutrittskarten u.ä. sind registriert und werden bei Ausscheiden zurückgefordert und – falls möglich – gesperrt.
- Auftraggeberunterlagen und -daten sind insbesondere bei Abwesenheit von Mitarbeitern gegen unbefugte Einsichtnahme zu schützen.
- Zu den Serverräumen, Patchräumen usw. haben nur berechtigte Personen Zutritt.

4.6.2.4 Mindeststandard Zugangsschutz

- Wirksame Maßnahmen zur Zugangskontrolle zu Geräten mit Zugang zu Auftragsdaten müssen eingesetzt werden (z.B. Passwörter).

- Internetdienste, wie z.B. Kundenportale, mit Zugang zu Auftragsdaten müssen einen verpflichtenden Zugangsschutz (z.B. Passwortschutz) besitzen. Der Zugangsschutz darf bei keiner Anmeldung deaktivierbar oder optional sein.
- Es existiert ein Passwortkonzept mit Bildungs- und Aufbewahrungsregeln.
- Der Schutz der gespeicherten Passwörter ist risikoangemessen (z.B. durch Hash und Salt).
- In öffentlichen Netzen werden Passwörter bei Anmeldung verschlüsselt übermittelt.
- Für jede Person muss nach Möglichkeit ein eigener persönlicher Zugang bestehen.
- Zugangsberechtigungen sind auf das für die Bearbeitung der Aufträge notwendige Minimum zu beschränken.
- Ein wirksames Identitätsmanagementsystem ist etabliert (z.B. Dokumentation der vergebenen Zugangsberechtigungen).
- Die Anzahl der Administratoren ist auf ein unbedingt nötiges Minimum zu beschränken.

4.6.2.5 Mindeststandard Zugriffsschutz

- Ein Berechtigungskonzept für alle Applikationen, mit denen Auftragsdaten verarbeitet werden, liegt vor.
- Rollen und die zugehörigen Rechte sind genau und vollständig beschrieben.
- Die Rechte sind auf ein Mindestmaß beschränkt. Administrationsrechte sind von Benutzerrechten getrennt.
- Ein Prozess zur Rechteverwaltung mit Genehmigungsschritten existiert und wird nachweisbar eingehalten.

4.6.2.6 Mindeststandard Verfügbarkeit

- Die Verfügbarkeit von aktuellen und korrekten personenbezogenen Daten kann dem Leistungsversprechen angemessen technisch sichergestellt werden.
- Mittel sind bspw. ausreichende Redundanz, Backup, Speicherkapazität und Performanz.
- Sofern eine automatisierte Datensicherung eingesetzt wird, wird automatisch geprüft, ob die Sicherung erfolgreich durchgeführt worden ist. Bei Fehlern werden Administratoren automatisch benachrichtigt.

- Die Konfigurationen der Anwendungen, die für die Auftragsabwicklung notwendig sind, sind dokumentiert.

4.6.2.7 Mindeststandard Datenübertragung

- Für Datenübertragung durch öffentliche Netzwerke an den oder vom Auftraggeber wird eine Verschlüsselungsmöglichkeit angeboten.
- Jede Datenübertragung durch öffentliche Netzwerke an oder von Stellen wie z.B. Unterauftragnehmer oder List Broker erfolgt verschlüsselt.
- Das Sicherheitsniveau der verwendeten Verschlüsselungstechnik ist für den festgestellten Schutzbedarf angemessen.

4.6.3 Anforderungen

Ein Berechtigungskonzept liegt vor, das die nutzbaren Rollen und ihre Rechte in den für die Leistungserbringung verwendeten Anwendungen beschreibt. Wenn einem Auftraggeber Rollen bereitgestellt werden, sind diese ebenfalls zu beschreiben.

4.6.4 Best Practice Beispiele

4.6.4.1 Angemessene Passwortkomplexität

Ein Passwort dient zusammen mit dem Login-Namen als Ausweis, dass man berechtigt ist. Es erfüllt die Aufgabe eines Türschlüssels. Administratorenpasswörter sind wie Generalschlüssel.

Generell lässt sich jedes Passwort durch (intelligentes) Durchprobieren aller denkbaren Zeichenkombinationen erraten („Brute Force-Angriff“). Die Passwortkomplexität ist ein wesentliches Mittel, die Zeit oder die Kosten zum Erraten so hoch zu treiben, dass sich ein Angriff wirtschaftlich nicht mehr lohnt. Für ein Administratorenpasswort, das weitreichende Zugriffsrechte einräumt, ist ein Angreifer bereit, mehr Zeit oder Geld zu investieren als für ein wenig privilegiertes Benutzerpasswort. Deshalb sollten Administratorenpasswörter auch deutlich komplexer als Benutzerpasswörter sein.

Die folgenden Faktoren bestimmen die Komplexität eines Passworts:

- Anzahl der Zeichen,
- Größe des Zeichenraums, d.h. die nutzbaren Buchstaben in Groß- und Kleinschreibung, Zahlen und Sonderzeichen,

- Zufälligkeit der Zeichen, d.h. die Zeichen bilden weder Namen, Wörter aus einem Wörterbuch, Datums- oder Zeitangaben noch andere bekannte Muster,
- Anzahl der Fehleingaben, ehe die Anwendung das Konto sperrt oder Zwangspausen zwischen den Anmeldeversuchen einführt.

Je komplexer ein Passwort ist, desto schwieriger ist es, sich dieses zu merken. Deshalb bevorzugen Benutzer einfache Passwörter mit geringer Sicherheit. Diese Tendenz wird durch einen Zwang zum regelmäßigen Passwortwechseln verstärkt.

Welche Länge angemessen ist, hängt von dem Angriffsszenario ab:[7] Passwortgeneratoren und Passwortspeicher erleichtern die technische Umsetzung.

Die Dauer, ein Passwort durch Brute Force zu erraten, hängt stark von der eingesetzten Rechenleistung ab. Diese steigt von Jahr zu Jahr an. Aus diesem Grund ist eine starre Längenempfehlung nicht möglich. Bereits 2009 konnte ein Passwort bestehend aus 10 Buchstaben (52 mögliche Zeichen) in ca. 16 Tagen erraten werden.[8]

4.7 Datenschutz-Managementsystem

Das Datenschutz-Managementsystem stellt den Datenschutz nachhaltig sicher, so wie er im Datenschutzkonzept definiert worden ist.

Ausdrücklicher Bestandteil des Datenschutz-Managementsystems sind die gesetzlichen Vorgaben zum Datenschutz (z.B. § 11 BDSG).

4.7.1 Schutzziele

Eine Auftragsdatenverarbeitung genießt eine gesetzliche Privilegierung, die den Auftraggeber von Datenschutzübermittlungsvorschriften (u.a. § 28 BDSG) befreit. Als Gegenleistung übernimmt der Auftraggeber die datenschutzrechtliche Verantwortung und Haftung für seinen Auftragnehmer. Daraus erwächst für den Auftragnehmer die Verpflichtung, seinerseits die Einhaltung von Datenschutzbestimmungen sicherzustellen. Das Datenschutz-Managementsystem ist ein Instrument, dieser Verpflichtung nachzukommen.

[7] Fox, Dirk; Schaefer, Frank (2009): Passwörter – fünf Mythen und fünf Versäumnisse, DuD 7/2009, S. 425-429.
[8] Fox, Dirk (2009): Mindestlängen von Passwörtern und kryptographischen Schlüsseln, DuD 10/2009. S. 620-623.

4.7.2 Vorgaben

- Ein Datenschutzbeauftragter ist unabhängig von der gesetzlichen Bestellpflicht nach § 4f Abs. 1 BDSG schriftlich bestellt, weil der Datenschutzbeauftragte eine unverzichtbare Kontrollaufgabe wahrnimmt.

- Die Fachkunde des Datenschutzbeauftragten erfüllt die Vorgaben des Düsseldorfer Kreises vom 24./25.11.2010 („Mindestanforderungen an Fachkunde und Unabhängigkeit des Beauftragten für den Datenschutz nach § 4f Abs. 2 und 3 Bundesdatenschutzgesetz (BDSG)“[9]) konkretisiert z.B. durch das Berufsleitbild des BvD (Kapitel 1) in seiner jeweils aktuellen Fassung.

- Eine Ausbildung nach GDD-Cert oder einer in Inhalt und Umfang vergleichbaren Ausbildung gewährleistet die Fachkunde. Eine vergleichbare Fachkunde kann auch durch Berufserfahrung oder nachgewiesene Fortbildung erworben werden. Die Vergleichbarkeit sollte belegt werden.

- Ausgewählte Prozesse und die angebotene Leistung werden stichprobenartig in angemessenen Zeitabständen auf ihre Datenschutzkonformität kontrolliert. Dabei werden die herrschende Meinung in der Literatur, die Rechtsprechung und die Stellungnahmen der zuständigen Aufsichtsbehörde sowie des Düsseldorfer Kreises einbezogen.

- Ein Prozess zur regelmäßigen Kontrolle von Unterauftragnehmern, die für die Leistungserbringung wesentlich sind oder Zugriff auf Auftragsdaten erhalten, ist beschrieben und im Wirkbetrieb. Bei der Kontrolle wird auch überprüft,

    - ob alle für den konkreten Unterauftrag relevanten Vorgaben dieses Standards durch Unterauftragnehmer eingehalten werden,

    - ob die Verträge mit Unterauftragnehmern die in den Verträgen mit Auftraggebern festgelegten Datenschutzpflichten durchreichen,

    - ob die Vorgaben von § 11 BDSG eingehalten werden,

    - ob Auftraggeber nach § 11 Abs. 2 S. 2 Nr. 6 BDSG über neue oder ausgeschiedene Unterauftragnehmer informiert werden,

[9] URL: https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2010/Mindestanforderungen_an_Datenschutzbeauftragte/Mindestanforderungen_an_DSB_nach_4f_II_und_III_BDSG.pdf

- ob sich die technischen und organisatorischen Maßnahmen substantiell verändert haben, so dass das IT-Sicherheitskonzept des Auftragnehmers angepasst werden muss,
- ob bei einer Anpassung des IT-Sicherheitskonzepts des Auftragnehmers die Auftraggeber informiert werden müssen,
- ob für jeden Unterauftragnehmer erforderliche Zustimmungen der Auftraggeber vorliegen.

- Die Kontrollen von Unterauftragnehmern kann auf geeignete Weise jederzeit Auftraggebern nachgewiesen werden.
- Der Datenschutzbeauftragte besitzt keine Interessenskonflikte (z.B. gleichzeitig Leiter IT, Leiter Personal oder Dienstleister in anderen Rollen).
- Der Datenschutzbeauftragte verfügt über eine angemessene Ressourcenausstattung hinsichtlich Fortbildungsbudget, Arbeitsmaterialien, aktuelle Literatur und Hilfspersonal.

4.7.3 Anforderungen

- Bestellungsurkunde des Datenschutzbeauftragten liegt vor.
- Nachweise der Kontrolltätigkeit liegen vor.
- Eine Beschreibung des Datenschutz-Managementsystem liegt vor.
- Der Prozess Kontrolle von Unterauftragnehmern ist beschrieben.

4.7.4 Best Practice Beispiele

Weitergehende wertvolle Anregungen gibt die Praxishilfe der GDD „Praxishilfe IV Datenschutzmanagement und -organisation“.

4.7.4.1 Musterprozess „Kontrolle des Datenschutzkonzepts“

Der Musterprozess zeigt wesentliche Prozessschritte und Verantwortlichkeiten zwischen Auftraggeber und Auftragnehmer. Der Schwerpunkt liegt auf dem Auftragnehmer, so dass die Tätigkeiten des Auftraggebers nicht detailliert betrachtet werden. Daraus darf nicht der Schluss gezogen werden, dass auf Seiten des Auftraggebers keine Aktivitäten notwendig sind. Er trägt die Verantwortung für die Rechtmäßigkeit der Datenverarbeitung durch den Auftragnehmer.

Der Musterprozess muss an die Gegebenheiten im Unternehmen angepasst werden. Aktivitäten dürfen aber nur dann weggelassen werden, wenn sie sachlich nicht notwendig sind.

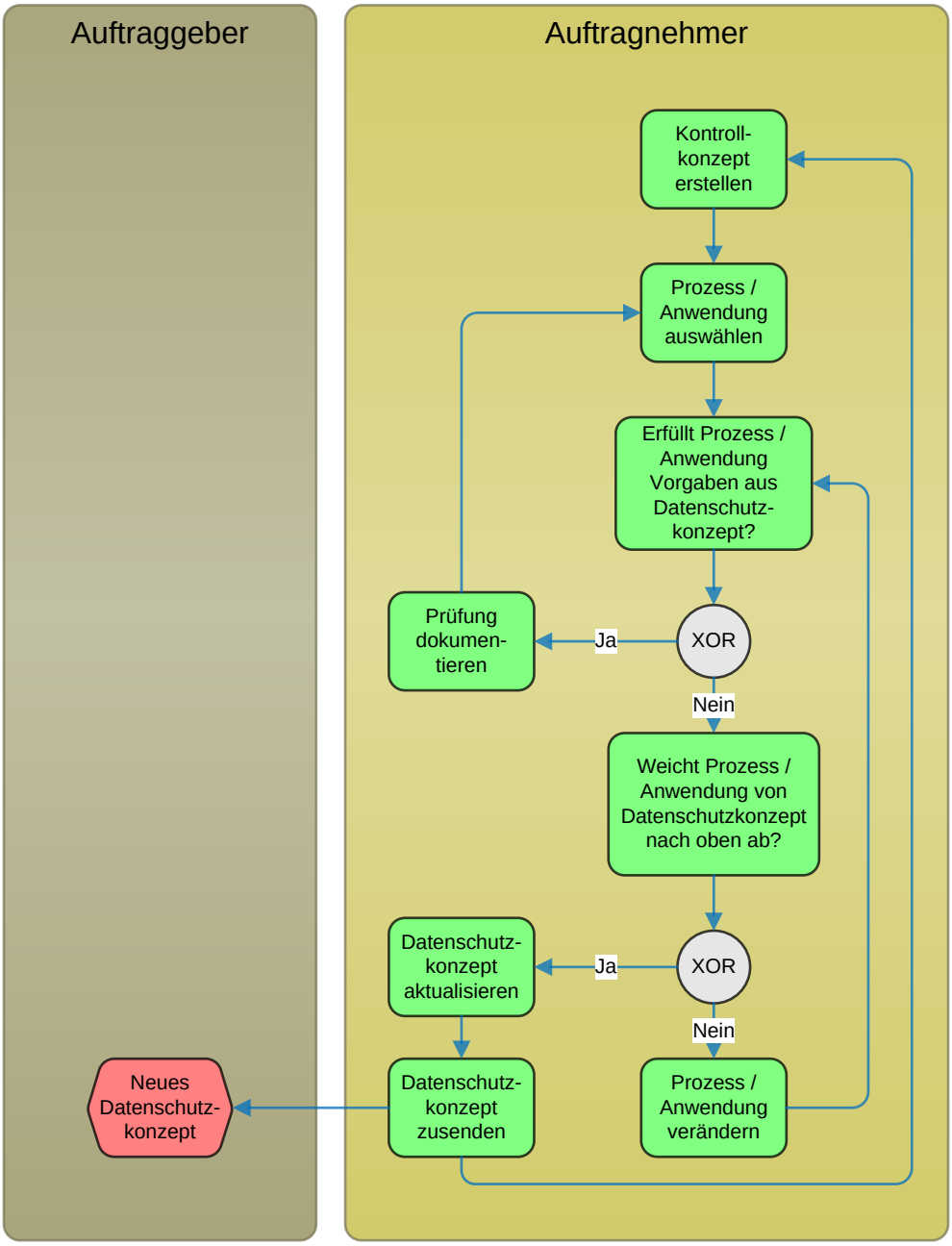

Abbildung 3: Musterprozess „Kontrolle des Datenschutzkonzepts“

4.7.4.2 Musterprozess „Kontrolle von Unterauftragnehmern“

Der Musterprozess zeigt wesentliche Prozessschritte und Verantwortlichkeiten zwischen Auftraggeber und Auftragnehmer. Der Schwerpunkt liegt auf dem Auftragneh-

mer, so dass die Tätigkeiten des Auftraggebers nicht detailliert betrachtet werden. Daraus darf nicht der Schluss gezogen werden, dass auf Seiten des Auftraggebers keine Aktivitäten notwendig sind. Er trägt die Verantwortung für die Rechtmäßigkeit der Datenverarbeitung durch den Auftragnehmer.

Der Musterprozess muss an die Gegebenheiten im Unternehmen angepasst werden. Aktivitäten dürfen aber nur dann weggelassen werden, wenn sie sachlich nicht notwendig sind.

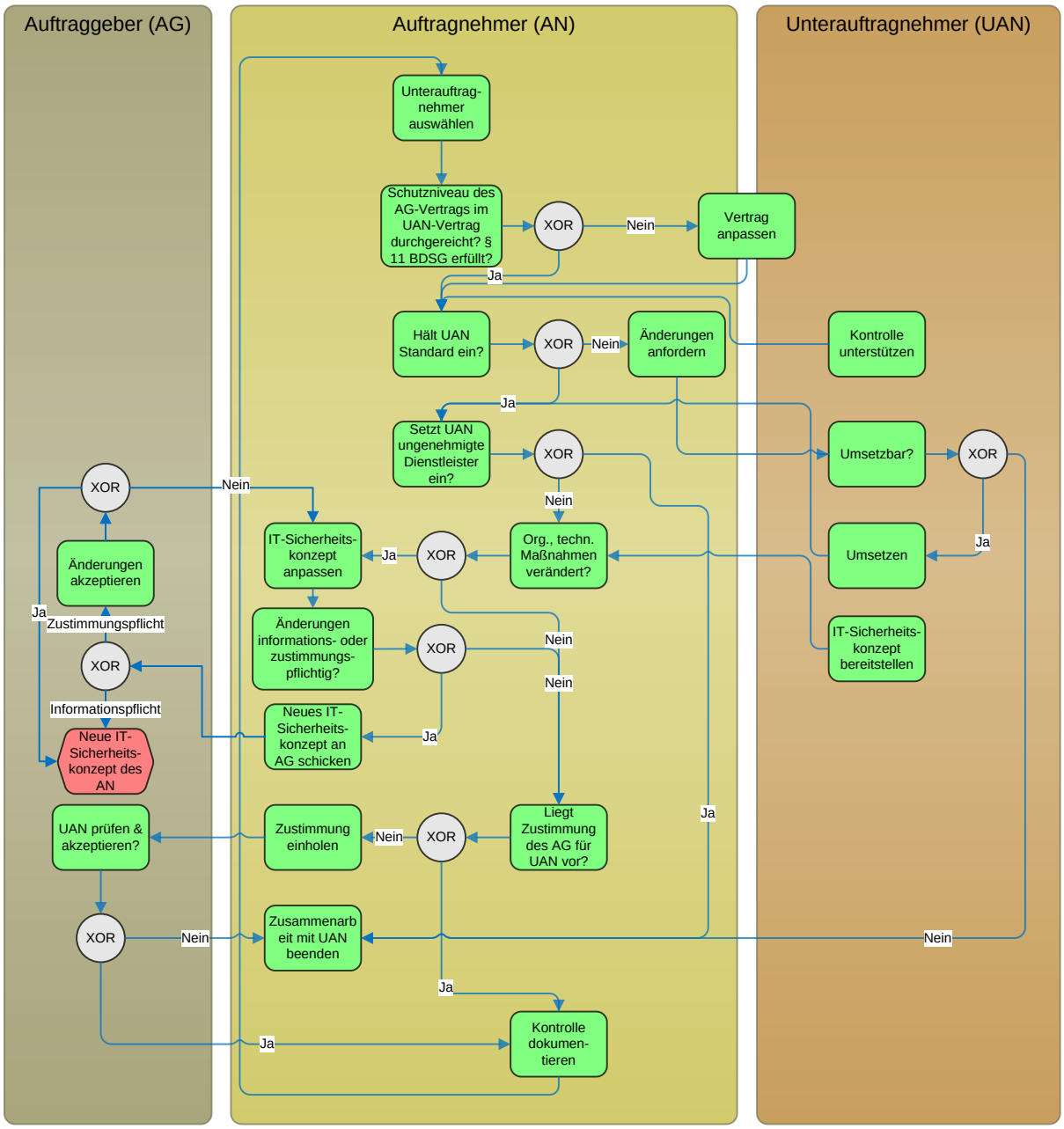

Abbildung 4: Musterprozess „Kontrolle von Unterauftragnehmern“

Aus Gründen der Übersichtlichkeit skizziert der Musterprozess „Kontrolle von Unterauftragnehmern“ die Unterstützungsaktivitäten des Unterauftragnehmers ohne sie indes vollständig in den Prozess zu integrieren. Die Aktivität „Kontrolle unterstützen“ müsste bspw. durch den Auftragnehmer getriggert werden.

Die Auftragsdatenverarbeitung stellt eine gesetzliche Privilegierung dar, die der Auftraggeber mit einer umfassenden Verantwortlichkeit und Haftung für die Handlungen des Auftragnehmers bezahlt. Je länger eine Kette von Unterauftragnehmern wird, desto unübersichtlicher wird die Verantwortlichkeit und Haftung für den Auftraggeber. Die Kette sollte z.B. durch vertragliche Regelungen begrenzt werden. Aus diesem Grund sieht der Musterprozess eine unverzügliche Beendigung des Auftragsverhältnisses mit dem Unterauftragnehmer vor, wenn dieser seinerseits ungenehmigte Unterunterauftragnehmer einsetzt.

4.8 IT-Sicherheitsmanagementsystem

4.8.1 Schutzziele

Ein funktionierendes Sicherheitsmanagementsystem ist integraler Bestandteil eines wirksamen Datenschutzes. Neben dem Nachweis der Wirksamkeit eines solchen Managementsystems sind auch die Schnittstellen zwischen Datenschutzbeauftragten und dem Sicherheitsmanagement sowie eine redundanzfreie Regelungspyramide von hoher Wichtigkeit.

4.8.2 Vorgaben

- Das Sicherheitsmanagementsystem ist umfassend dokumentiert.
- Qualifikations- und Fortbildungsnachweis des IT-Sicherheitsverantwortlichen ist vorhanden.
- Ein Prozess zur kontinuierlichen Verbesserung ist wirksam etabliert.

4.8.3 Anforderungen

ISO 27001 oder vergleichbares Zertifikat liegt vor. Alternativ: Ein Sicherheitsmanagementsystem ist etabliert, dokumentiert und dessen Wirksamkeit wird regelmäßig überprüft.

4.8.4 Best Practice Beispiele

- Es finden regelmäßige Konsultationen zwischen IT-Sicherheitsbeauftragtem und Datenschutzbeauftragtem statt, um die Zusammenarbeit hinsichtlich des beide betreffenden Bereichs IT-Sicherheit abzustimmen.
- Die Vorgaben der beiden Disziplinen werden miteinander abgestimmt bzw. bauen aufeinander auf (redundanzfreie Regelungspyramide).

4.9 Auftragsmanagementsystem

4.9.1 Schutzziele

Das Modul Auftragsmanagementsystem stellt die Auftragskontrolle in den Mittelpunkt. Nr. 6 der Anlage zu § 9 S. 1 BDSG versteht unter Auftragskontrolle „zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können“.

4.9.2 Vorgaben

- Alle für die Leistungserbringung relevanten Prozesse sind schriftlich beschrieben und im Wirkbetrieb.
- Alle mit der Leistungserbringung betrauten Personen sind mit den relevanten Prozessen vertraut.
- Die Wirksamkeit des Auftragsmanagementsystems kann auf geeignete Weise jederzeit Auftraggebern nachgewiesen werden.
- Eine angemessene Prüfmöglichkeit durch den Auftraggeber besteht.
- Ein Ablauf existiert, der sicherstellt, dass Protokolle aus dem Datenschutz- und Sicherheitskonzept auf Anforderung dem Auftraggeber übergeben werden können. Alle Angaben über Daten anderer Kunden sind vor der Übergabe zu entfernen. Die Namen der Mitarbeiter des Auftragnehmers sind durch Pseudonyme zu ersetzen.

4.9.3 Anforderungen

- Prozessbeschreibungen aller für die Auftragsbearbeitung notwendigen manuellen und technisch unterstützten Prozesse liegen vor.
- Der Prozess Weisungsbearbeitung (Change Management) ist beschrieben.

- Der Prozess Kontrolle der ordnungsgemäßen Bearbeitung ist beschrieben.

4.9.4 Best Practice Beispiele

4.9.4.1 Musterprozess „Change Management“

Der Musterprozess zeigt wesentliche Prozessschritte und Verantwortlichkeiten zwischen Auftraggeber und Auftragnehmer. Der Schwerpunkt liegt auf dem Auftragnehmer, so dass die Tätigkeiten des Auftraggebers nicht detailliert betrachtet werden. Daraus darf nicht der Schluss gezogen werden, dass auf Seiten des Auftraggebers keine Aktivitäten notwendig sind. Er trägt die Verantwortung für die Rechtmäßigkeit der Datenverarbeitung durch den Auftragnehmer.

Der Musterprozess muss an die Gegebenheiten im Unternehmen angepasst werden. Aktivitäten dürfen aber nur dann weggelassen werden, wenn sie sachlich nicht notwendig sind.

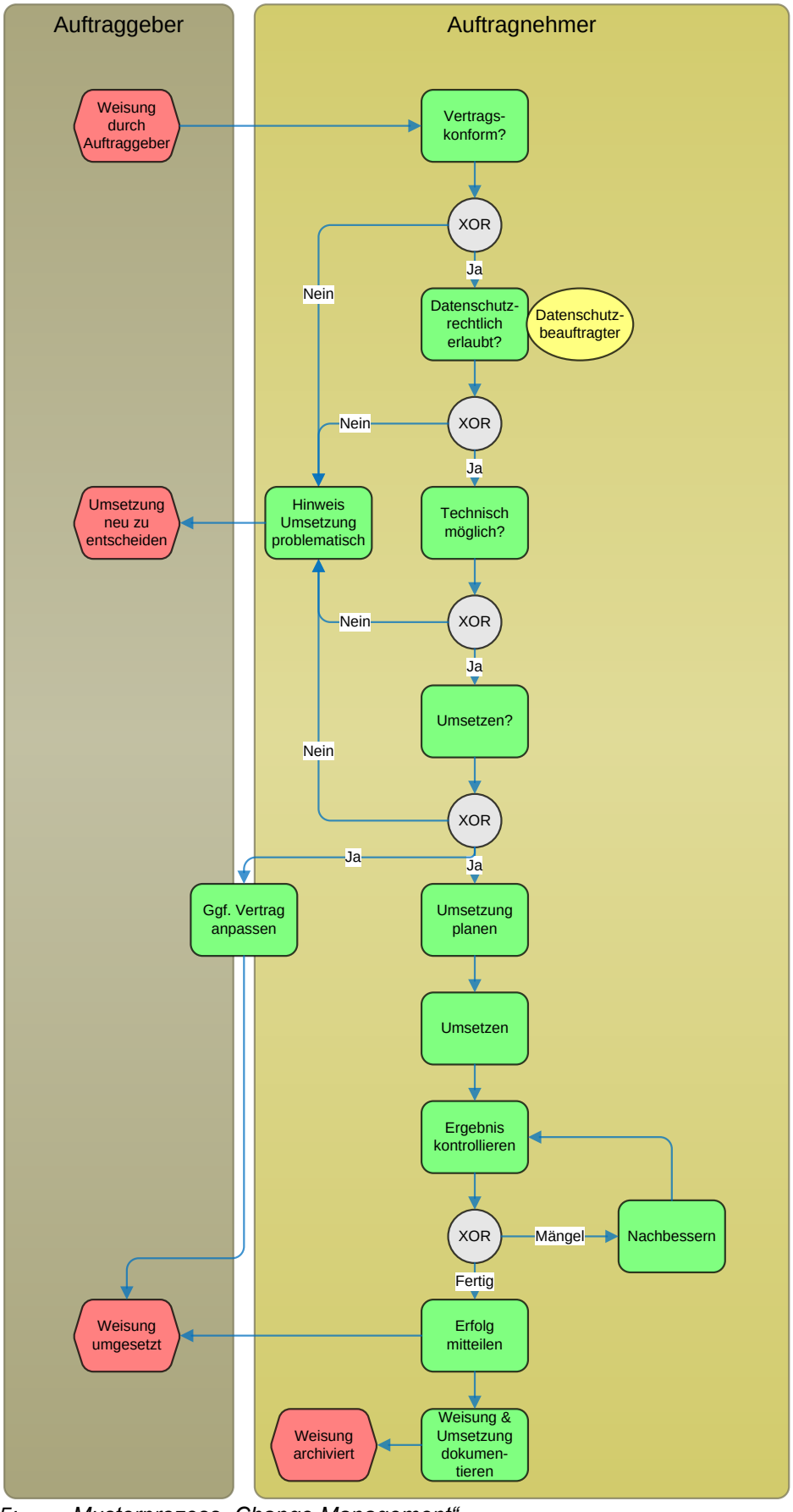

Abbildung 5: Musterprozess „Change Management“

4.9.4.2 Musterprozess „Kontrolle Auftragsbearbeitung“

Der Musterprozess zeigt wesentliche Prozessschritte und Verantwortlichkeiten zwischen Auftraggeber und Auftragnehmer. Der Schwerpunkt liegt auf dem Auftragnehmer, so dass die Tätigkeiten des Auftraggebers nicht detailliert betrachtet werden. Daraus darf nicht der Schluss gezogen werden, dass auf Seiten des Auftraggebers keine Aktivitäten notwendig sind. Er trägt die Verantwortung für die Rechtmäßigkeit der Datenverarbeitung durch den Auftragnehmer.

Der Musterprozess muss an die Gegebenheiten im Unternehmen angepasst werden. Aktivitäten dürfen aber nur dann weggelassen werden, wenn sie sachlich nicht notwendig sind.

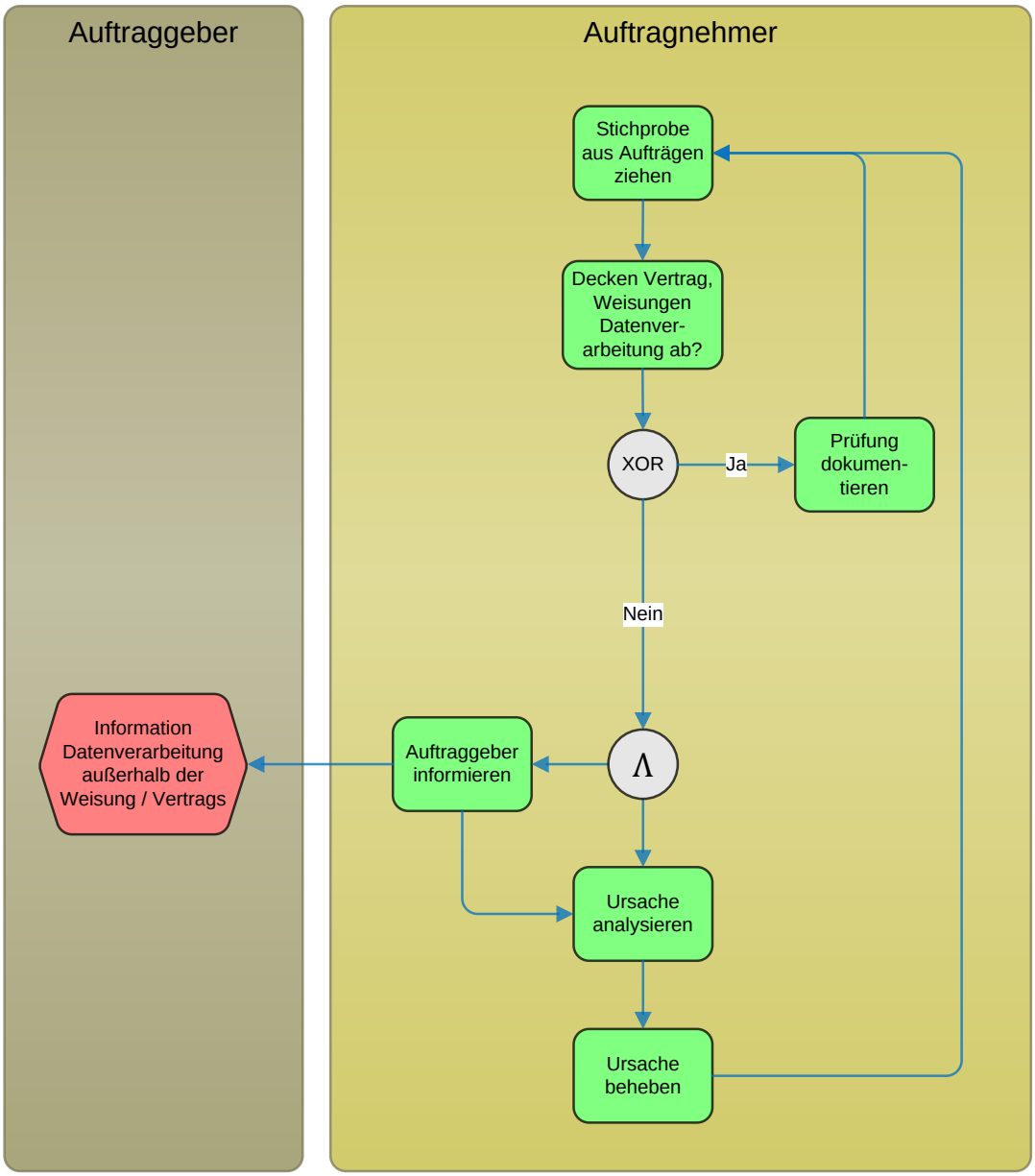

Abbildung 6: Musterprozess „Kontrolle Auftragsbearbeitung“

4.9.4.3 Protokollierung

Eine Protokollierung der Administrator- oder Nutzerzugriffe sollte folgende Anforderungen erfüllen:[10]

- **Strenge Zweckbindung:** Die Protokollierung dient ausschließlich zum Nachweis der ordnungsgemäßen Auftragserfüllung unter Datenschutzaspekten. Sie darf nicht für eine automatisierte Leistungs- und Verhaltenskontrolle der an der Datenverarbeitung beteiligten Personen herangezogen werden. Lesezugriffe für andere Zwecke müssen unterbunden werden.
- **Vollständigkeit:** Die zu protokollierenden Aktivitäten müssen jederzeit zuverlässig aufgezeichnet werden.
- **Datensparsamkeit:** Es soll nur so viel protokolliert werden, wie für den Nachweis eines ordnungsgemäßen Umgangs mit Auftragsdaten notwendig ist.
- **Revisionsfest:** Ein nachträgliches Ändern von Protokolldaten muss ausgeschlossen sein.
- **Enge Zugriffsmöglichkeit:** Nur ausgewählte Berechtigte dürfen Protokolldaten lesen. Dabei sollte technisch sichergestellt sein, dass die zu überwachenden Personen die Protokolldaten nicht ändern oder löschen können.

Protokolldaten sollen Auskunft geben über

- den Zeitpunkt einer Tätigkeit bzw. eines Ereignisses,
- die zutreffende Bezeichnung einer Tätigkeit oder eines Ereignisses,
- die mit der Tätigkeit oder dem Ereignis befasste Person bzw. Systemkomponente und
- den Zweck der Tätigkeit.

Kryptographische Verfahren zur Verschlüsselung und Signierung helfen, die Anforderungen an Vertraulichkeit, Integrität und Authentizität von Protokolldaten umzusetzen.

[10] Siehe Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2009): Orientierungshilfe „Protokollierung“. URL: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/070328_Datenschutzrechtliche_Protokollierung_beim_Betrieb_IT-Systeme/OH_Datenschutzrechtliche_Protokollierung_beim_Betrieb_ITSysteme.pdf

Umfang der Protokollierung:

- Administrative Tätigkeiten wie z.B. Installation, Modifikation und Konfiguration von Hard- und Software sollten protokolliert werden.
- Nutzaktivitäten wie z.B. Authentifizierung und Autorisierung, Dateneingabe und -veränderung, Dateneinsicht, Datenübermittlung und Datenlöschung sollten je nach Schutzbedarf der Auftragsdaten detailliert protokolliert werden.

Die Löschfrist orientiert sich am Zweck der Protokollierung. Sie sollte deshalb zusammen mit dem Zweck festgelegt werden. Protokollierungen aus

- Sicherheitsgründen können i.d.R. nach wenigen Tagen gelöscht werden,
- aus Dokumentationsgründen der ordnungsgemäßen Auftragserfüllung können oft nach dem Ablauf etwaiger aus dem Auftrag resultierender Anspruchsfristen gelöscht werden.

Siehe für weitere Empfehlungen:

- Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2009) Orientierungshilfe „Protokollierung“. URL:

  https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/070328_Datenschutzrechtliche_Protokollierung_beim_Betrieb_IT-Systeme/OH_Datenschutzrechtliche_Protokollierung_beim_Betrieb_IT-Systeme.pdf .

5 Module in Abhängigkeit des Leistungsumfangs

5.1 Vertrag

Gemäß § 11 BDSG sind Aufträge zur Erhebung, Verarbeitung oder Nutzung schriftlich zu erteilen. Es ist ein Vertrag zur Auftragsdatenverarbeitung zu schließen. Dieser Vertrag muss den Anforderungen des § 11 BDSG entsprechen und die Weisungen zu den technischen und organisatorischen Maßnahmen entsprechend der Anlage des § 9 BDSG in angemessener Weise beinhalten.

5.1.1 Schutzziele

- Sicherstellung der Rechtskonformität von ADV Verträgen.
- Vollständige Umsetzung der Anforderungen der §§ 9 und 11 BDSG.
- Wirksame vertragliche Bindung von Unterauftragnehmern an die Weisungen des Auftraggebers.

5.1.2 Vorgaben

- Die verwendeten Vertragsmuster setzen die Vorgaben des § 11 BDSG in angemessener Form um.
- Auftraggeberrechte oder -pflichten, die aus dem BDSG erwachsen, dürfen nicht behindert werden.

5.1.3 Anforderungen

Vorlage des rechtskonformen Vertragsmusters.

5.1.4 Best Practice Beispiele

Anregungen zur Vertragsgestaltung finden sich

- in der Praxishilfe der GDD „Neue Anforderungen an die Auftragsdatenverarbeitung nach § 11 BDSG“[11] und

[11] URL: https://www.gdd.de/nachrichten/news/neues-gdd-muster-zur-auftragsdatenverarbeitung-gemas-a7-11-bdsg

- in der „Mustervereinbarung zum Datenschutz und zur Datensicherheit in Auftragsverhältnissen nach § 11 BDSG“, erstellt vom Regierungspräsidium Darmstadt und mit Hinweisen des LDI NRW für Stellen mit Sitz in Nordrhein-Westfalen versehen.[12]

5.2 Beendigung der Leistungsbeziehung

5.2.1 Schutzziele

Nach Beendigung eines Auftrages müssen klare Regelungen zwischen Auftragnehmer und Auftraggeber bestehen, was mit den beim Auftraggeber vorhandenen Daten geschehen soll (Löschung, Rückgabe, Archivierung oder Weiterverwendung im Rahmen eines Folgeauftrags).

5.2.2 Vorgaben

Es existiert ein Prozess zur Auftragsbeendigung, der auch das Löschen oder Zurückgeben der Auftragsdaten an den Auftraggeber umfasst. Dies schließt sämtliche Daten bei etwaigen Unterauftragnehmern mit ein.

5.2.3 Anforderungen

Entsprechende Musterklauseln oder -Verträge müssen vorgelegt werden.

5.2.4 Best Practice Beispiele

Hilfreiche Anregung gibt die GDD Praxishilfe „Datenträgerentsorgung“. Hinweise zum Aufbau eines Löschkonzepts gibt die „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“ des DIN - Deutsches Institut für Normung e.V.

[12] URL: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Auftragsdatenverarbeitung/Inhalt/Mustervereinbarung_zur_Auftragsdatenverarbeitung_nach___11_BDSG/Mustervereinbarung_zur_Auftragsdatenverarbeitung_nach___11_BDSG.php