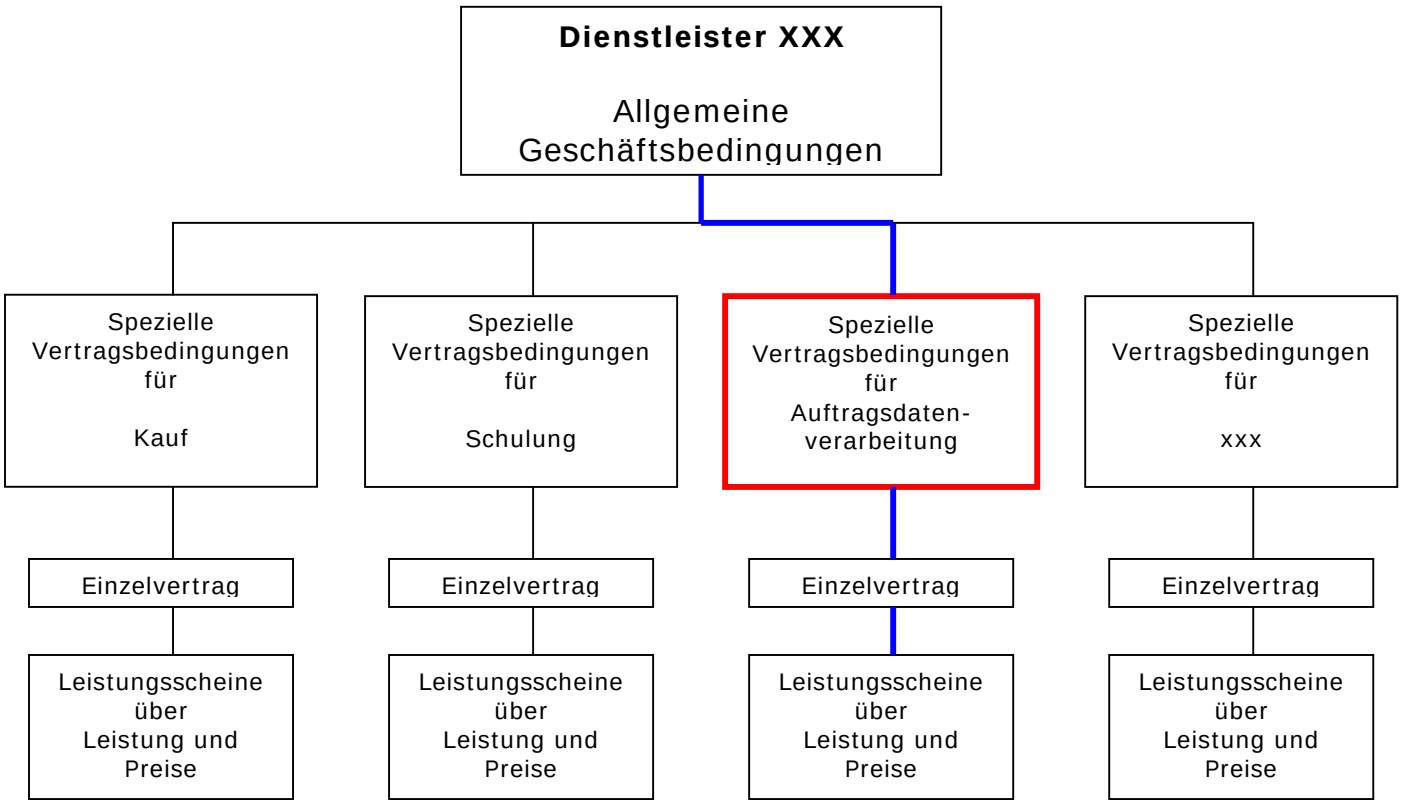
Stand: 09.01.2004

Ergänzende Hinweise zu den
Speziellen Vertragsbedingungen für die Auftragsdatenverarbeitung

Einleitung

Die speziellen Vertragsbedingungen für die Auftragsdatenverarbeitung sind ein den allgemeinen Geschäftsbedingungen (AGB) nachgeordneter Vertragsteil, der sich ausschließlich mit den datenschutzrechtlichen Vereinbarungen für die Auftragsdatenverarbeitung befasst.

Die Vertragsstruktur stellt sich wie folgt dar:



Rechtsgrundlage für die Auftragsdatenverarbeitung öffentlicher Stellen in Niedersachsen ist § 6 des Niedersächsischen Datenschutzgesetzes (NDSG). Danach kann eine öffentliche Stelle eine andere öffentliche oder private Stelle beauftragen, für sie personenbezogene Daten zu verarbeiten. Die beauftragende Stelle (Auftraggeber) bleibt jedoch weiterhin Herr der Daten. Der Auftragnehmer arbeitet ausschließlich nach den Weisungen des Auftraggebers. Er hat keinen eigenen Beurteilungs- oder Entscheidungsspielraum.

Die Zurverfügungstellung der zu verarbeitenden personenbezogenen Daten stellt keine Datenübermittlung im Sinne der §§ 11 bis 14 NDSG dar. Eine ermächtigende Rechtsgrundlage ist daher nicht erforderlich.

Der Auftraggeber hat bereits die Wahl des Auftragnehmers sorgfältig zu treffen. Er ist in jeder Phase der Verarbeitung für die Einhaltung der Datenschutz-Vorschriften verantwortlich. Ansprüche von Betroffenen sind ausschließlich gegen ihn zu richten.

Der Auftraggeber überwacht, ob der Auftragnehmer die technisch und organisatorischerforderlichen Maßnahmen im Einzelfall einhält. Diese sind im Einzelnen in § 7 NDSG beschrieben.

Alle Aufträge und Anweisungen sind schriftlich festzuhalten.

Zu den Bestimmungen im Einzelnen:

Zu 1.1 Beauftragt wird ausschließlich Auftragsdatenverarbeitung. Folgende Merkmale müssen erfüllt sein:

- fehlende Entscheidungsbefugnis des Auftragnehmers,
- weisungsgebunden gegenüber dem Auftraggeber in jeglicher Art,
- fehlende Beziehung des Auftragnehmers zum Betroffenen,
- erwirbt kein Eigentum an den zur Verfügung gestellten Daten.

Im Gegensatz dazu steht die Funktionsübertragung, die hier nicht abgedeckt wird, mit ihren Merkmalen:

- Überlassung von Nutzungsrechten an den Daten,
- eigenverantwortliche Sicherstellung der Zulässigkeit und Richtigkeit der Daten und Verarbeitungsschritte/-wege durch den Auftragnehmer,
- Sicherstellen der Rechte von Betroffenen (Benachrichtigungspflicht, Auskunftspflicht) durch den Auftragnehmer.

Zu 1.2 Die Auftragsdatenverarbeitung (Tätigkeiten) im Einzelnen ist nicht Gegenstand dieser speziellen Vertragsbedingungen. Hier werden nur allgemein gültige Regelungen festgelegt. In jedem Einzelfall werden die zu erledigenden Arbeiten im Einzelvertrag (siehe vorstehende Zeichnung)detailliert beschrieben.

Zu 2.1 Der Auftragnehmer wird vollkommen unselbständig tätig. Er darf keine eigenen Entscheidungen treffen. Alle Weisungen bezüglich der Verarbeitung erhält er vom Auftraggeber. Das ist auch dann der Fall, wenn der Auftraggeber z.B. eine vom Auftragnehmer erstellte Software benutzt. Der Auftragnehmer hat hier zwar alle Verarbeitungsschritte festgelegt, die Anweisung ob, dass und wann diese erfolgen, wird ausschließlich vom Auftraggeber erteilt. Dies begründet dann auch den Anspruch von Betroffenen, ihre Rechte ausschließlich beim Auftraggeber geltend zu machen (§ 6 Abs. 1 Satz 2 NDSG). Damit sind die im 3. Abschnitt des NDSG (§§ 16 bis 20 NDSG) genannten Rechte, wie:

- Auskunft, Einsicht in die Akten

- Berichtigung, Löschung und Sperrung
- Widerspruchsrecht
- Schadenersatz
- Anrufung des Landesbeauftragten für den Datenschutz
- Verzicht auf Rechte

gemeint.
Gegen den Auftraggeber werden auch eventuelle Maßnahmen nach §§ 28 und 29 NDSG (Ordnungswidrigkeiten und Straftaten) zu richten sein.

Zu 2.2 Da der Auftragnehmer keine eigenen Entscheidungen bezüglich der Verarbeitung fällen darf, muss seine Tätigkeit im Einzelvertrag detailliert beschrieben sein. Alle möglichen Verarbeitungsschritte und Handlungsanweisungen sind schriftlich festzuhalten.

Zu 2.3 In seinem eigenen Interesse sollte der Auftraggeber regelmäßig, zumindest stichprobenweise, die Arbeitsergebnisse kontrollieren, um weitere Schäden und Ersatzansprüche durch Betroffene von sich abzuwenden. Nur durch regelmäßige Kontrolle kann er dazu beitragen, dass die Arbeitsergebnisse fehlerfrei werden und bleiben.

Zu 2.4 Der Auftraggeber sollte sich in jedem Fall ein vom Auftragnehmer entwickeltes und realisiertes Sicherheitskonzept in schriftlicher Form vorlegen lassen. Anhand dieses Konzeptes (siehe auch Nr. 3.7 dieser Vereinbarung) prüft der Auftraggeber, ob die in § 7 NDSG vorgeschriebenen technischen und organisatorischen Maßnahmen für diesen Einzelfall richtig festgelegt und umgesetzt wurden. Wichtig dabei ist, dass die zu treffenden Maßnahmen individuell verschieden sein können. Sie hängen von der jeweiligen Verarbeitung und den räumlichen und derzeitigen technischen Gegebenheiten ab.

Zu 3.1 Eine eigenständige Nutzung der zu verarbeitenden Daten durch den Auftragnehmer ist nicht zulässig. Alle Verarbeitungsschritte müssen vom Auftraggeber veranlasst und bestimmt sein. Eine zweckfremde Nutzung ist untersagt. Kopien der überlassenen Daten dürfen nur für und auf Anweisung des Auftraggebers erstellt werden. Sicherheitskopien dürfen erstellt werden, wenn sie für die ordnungsgemäße Datenverarbeitung erforderlich sind. Die Datensicherung (Form, Anzahl und jeweiliger Zeitpunkt) sollte Bestandteil des Datensicherheitskonzeptes sein. Zu regeln wäre in diesem Zusammenhang auch, wann erstellte Sicherungskopien zu löschen bzw. durch neue Sicherungen zu überschreiben sind.

Zu 3.2 Eine physikalische Trennung von anderen Datenbeständen ist nicht zwingend erforderlich, wenn das benutzte Datenbanksystem eine sichere logische Trennung gewährleistet. Der Auftragnehmer hat lediglich sicherzustellen, dass der Auftraggeber jederzeit in den Besitz der ihm gehörenden Daten kommen kann.

Zu 3.3 Wie diese Kontrolle im Einzelnen aussieht, sollte zwischen Auftraggeber und Auftragnehmer im Einzelvertrag oder im Sicherheitskonzept (Nr. 3.7) detailliert beschrieben bzw. geregelt werden. Die Kontrolle korrespondiert mit Nr. 2.4.

Zu 3.4 Hierbei kann es sich um Zwischenergebnisse bzw. erstmalig zur Einspielung in eine Datenbank übergebene Datensätze bzw. zu erfassende Unterlagen handeln. Ob und wie diese Materialien vernichtet

werden, ist mit dem Auftraggeber abzustimmen. Die Abstimmung kann, soweit vorhersehbar, auch im Vorhinein abstrakt im Einzelvertrag oder im Sicherheitskonzept vereinbart werden. Diese Regelung realisiert die Vorschrift, dass der Auftraggeber in jedem Zeitpunkt der Verarbeitung Herr der Daten sein muss.

Zu 3.5 Diese Vorschrift kommt sowohl beim regulären als auch beim vorzeitigen Ende des Auftragsverhältnisses zum Tragen und korrespondiert in der Ausführung mit Nr. 3.4. Hinweise zur „datenschutzgerechten Vernichtung“ findet man u.a. unter www.bsi.bund.de.

Zu 3.6 Eine Unterbeauftragung bedarf nach § 6 Absatz 3 NDSG der Schriftform. Sie muss auch im Sicherheitskonzept beschrieben sein. Nur so ist es dem Auftraggeber möglich, die ihm vorgeschriebenen Kontrollen auch hier vorzunehmen und jederzeit darüber Auskunft zu erteilen, wo, wie und durch wen in seinem Eigentum befindliche personenbezogene Daten gehalten und verarbeitet werden. Selbstverständlich ist, dass die zwischen dem Auftraggeber und dem Auftragnehmer vereinbarten Regelungen auch im Unterauftragsverhältnis Anwendung finden müssen. Dazu zählt auch die Verpflichtung auf das Datengeheimnis nach Nr. 4.

Zu 3.7 Derzeit sind nach §7 Absatz 2 NDSG sind folgende technischen und organisatorischen Maßnahmen im Sicherheitskonzept im Einzelnen zu beschreiben und zu realisieren:

- Zugangskontrolle:
  Unbefugten ist der Zugang zu den Verarbeitungsanlagen zu verwehren.
- Datenträgerkontrolle:
  Es ist zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden.
- Speicherkontrolle:
  Es ist eine unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter Daten zu verhindern.
- Benutzerkontrolle:
  Das Benutzen der Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte ist zu verhindern.
- Zugriffskontrolle:
  Innerhalb eines Datenverarbeitungssystems dürfen nur Berechtigte auf die, Ihrer Zugriffsberechtigung unterliegenden, Daten zugreifen .
- Übermittlungskontrolle:
  Es muss überprüft und festgestellt werden können, welche Daten zu welcher Zeit an wen übermitteln worden sind.
- Eingabekontrolle:
  Es muss überprüft und festgestellt werden können, welche Daten zu
  welcher Zeit von wem eingegeben worden sind.
- Verfügbarkeitskontrolle:
  Der Schutz personenbezogener Daten gegen zufällige Zerstörung oder gegen Verlust muss gewährleistet sein.
- Auftragskontrolle:

Daten, die im Auftrag verarbeitet werden, dürfen nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

- Transportkontrolle:
  Bei der Übertragung von Daten sowie beim Transport von Datenträgern muss gewährleistet sein, dass diese nicht unbefugt gelesen, kopiert oder gelöscht werden können.
- Organisationskontrolle:
  Die innerbehördliche oder innerbetriebliche Organisation ist so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

Der Auftraggeber kontrolliert sowohl das Konzept als auch seine Realisierung. Der Auftragnehmer hat dies nicht nur zu gestatten, sondern auch zu unterstützen.

Zu 3.8 Der Auftraggeber muss unbedingtes Vertrauen in die Tätigkeit des Auftragnehmers haben. Deshalb werden ihm nicht nur betriebsbedingte Änderungen des Sicherheitskonzeptes mitgeteilt, sondern er wird auch unverzüglich über sämtliche Dinge in Kenntnis gesetzt, die nicht vereinbarungsgemäß ablaufen. Telearbeitsplätze sind mit den Bediensteten so zu vereinbaren, dass der Auftraggeber jederzeit seine Kontrollrechte wahrnehmen kann.

´Zu 3.9 Sollte es zur Nichtzahlung der vereinbarten Vergütung seitens des Auftraggebers kommen, berechtigt dies den Auftragnehmer nicht dazu, die überlassenen Datenbestände zwecks Sicherung seines Anspruchs zurückzubehalten.

Zu 3.10 Um dem Auftraggeber frühzeitig zu ermöglichen, das Recht an seinen Daten geltend zu machen bzw. diese möglichst vor dem drohenden Ereignis in seinen Zugriff zu bekommen, ist es unverzichtbar, dass der Auftragnehmer dieser Unterrichtungspflicht nachkommt. Im Falle der Insolvenz verzichtet der Insolvenzverwalter zunächst auf die Verwertung von Datenträgern, wenn der Auftraggeber seine Rechte daran rechtzeitig geltend gemacht hat. Noch wichtiger ist die rechtzeitige Unterrichtung bei drohenden Beschlagnahmen, da die beschlagnahmende Stelle Rechte an den Daten zunächst unberücksichtigt lässt und eine Verfügbarkeit der Daten somit nicht gewährleistet ist. Siehe in diesem Zusammenhang auch Ziffer 3.2, in der die Möglichkeit der jederzeitigen logischen Trennung und Bereitstellung der Datenbestände des Auftraggebers verlangt wird.

Zu 4.1 Es erfolgt eine Gleichstellung der Bediensteten des Auftraggebers mit denen des Auftragnehmers. Diese haben im Rahmen des Auftrags bekannt gewordene Informationen nur in diesem Rahmen zu verarbeiten. Sie dürfen diese nicht anderweitig offenbaren. Die Geheimhaltung nach § 5 NDSG gilt über den Auftrag hinaus, selbst wenn der Bedienstete mittlerweile ausgeschieden ist. Die für den einzelnen Auftrag geltenden spezialgesetzlichen Datenschutzbestimmungen sollten aufgelistet und Bestandteil des Einzelvertrages werden.

Zu 4.2 Die Wahrung des Datengeheimnisses nach § 5 NDSG bzw. sonstiger datenschutzrechtlicher Spezialbestimmungen ist für jeden am Auftrag beteiligten Bediensteten zwingend vorgeschrieben. Auch wenn die gesetzliche Verantwortung zur Einhaltung der Datenschutzvorschriften eindeutig beim Auftraggeber liegt, sollte dieser vom Auftragnehmer

dadurch unterstützt werden, dass die entsprechenden Vorschriften den am Auftrag mitwirkenden Mitarbeitern bekannt gegeben werden und deren Einhaltung überwacht wird.

Zu 5.1 Übergabeformate sind mit der Definition der einzelnen Felder Bestandteil des Einzelvertrages. Es kann auch die Übergabe der beim Auftraggeber vorhandenen und noch überzuleitenden Daten formuliert werden. Wichtig ist, dass jeder Vertragspartner seine Aufgaben zugewiesen bekommt und dass dieses ausreichend schriftlich festgehalten wird.

Zu 5.2 Es soll schriftlich festgelegt werden, wer an welcher Stelle verantwortlich ist. Insbesondere bei Netzen muss festgelegt werden, bis wohin der Auftraggeber und ab wann der Auftragnehmer für die Daten verantwortlich ist. Dies gilt auch für das Verfahren der Vergabe von Zugriffsberechtigungen. Das Verfahren der Fernwartung, insbesondere die aktive Beteiligung des Auftraggebers bei Online-Verfahren, ist detailliert zu beschreiben. Dazu gehört auch die Erstellung von Protokollen und deren Aufbewahrung.

Zu 5.3 Ein schwerwiegender Verstoß gegen das Datenschutzrecht liegt u.a. dann vor, wenn die Geheimhaltungspflicht nach § 5 NDSG oder anderer gesetzlicher Vorschriften (z.B. des Sozialgeheimnisses nach § 35 SGB I) verletzt wird oder die zur Verfügung gestellten Daten, anders als im Auftragsdatenverhältnis geregelt, genutzt werden. Darüber hinaus ist ein schwerwiegender Verstoß dann anzunehmen, wenn ein Straf- bzw. Ordnungswidrigkeitentatbestand nach den §§ 28 oder 29 NDSG erfüllt wird.