Stand 02.11.2015

Mustervertrag zur Auftragsdatenverarbeitung

zwischen öffentlichen Stellen in Niedersachsen

und öffentlichen oder nicht-öffentlichen Auftragnehmern

erstellt von der Landesbeauftragten für den Datenschutz Niedersachsen (LfD) in Zusammenarbeit mit den Netzwerken Nord-West und Süd-Ost der kommunalen Datenschutzbeauftragten des Landes Niedersachsen

Nachfolgender Vertrag für die Verarbeitung personenbezogener Daten im Auftrag nach § 6 Niedersächsisches Datenschutzgesetz (NDSG) ist nur ein Muster, das im Einzelfall inhaltlich aufgabenspezifisch anzupassen ist!

Hinweise zur Auftragsvergabe:
Ein Auftrag darf nur vergeben werden, wenn weder gesetzliche Regelungen über Berufs- oder besondere Amtsgeheimnisse noch überwiegende schutzwürdige Belange entgegenstehen. Zudem wird auf die Ausführungen zur sog. „Funktionsübertragung“ in der Handreichung „Datenschutzrechtliche Grundlagen bei Auftragsdatenverarbeitung/Outsourcing in der öffentlichen Verwaltung“ verwiesen (s. Arbeitspapier des Arbeitskreises Grundsatzfragen der Verwaltungsmodernisierung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Stand 08/09.10.2008; eingestellt auf der Homepage des LfD Nds. www.lfd.niedersachsen.de unter der Rubrik „Themen/Auftragsdatenverarbeitung“).

Soweit nicht § 6 NDSG, sondern spezialgesetzliche Regelungen für die Daten, die im Auftrag verarbeitet werden sollen, maßgeblich sind (s. § 2 Abs. 6 NDSG), ist zunächst zu prüfen, ob eine Auftragsdatenverarbeitung zulässig ist (s. u. a. § 50 S. 3 Beamtenstatusgesetz, § 30 Abgabenordnung, § 203 Strafgesetzbuch).
Ggf. sind spezialgesetzliche Regelungen bei der Vertragsgestaltung zu berücksichtigen (s. z. B. bei Sozialdaten § 80 SGB IX, § 51 SGB II).

In den in § 6 Abs. 4 Satz 2 NDSG genannten Fällen hat die Auftraggeberin / der Auftraggeber die zuständige Datenschutzkontrollbehörde über die Beauftragung zu unterrichten.

Auf Nr. 4.1 ff der Verwaltungsvorschriften zu § 6 des Niedersächsischen Datenschutzgesetz (VV NDSG, Gem. RdErl. des MI, der StK u. d. übr. Min. vom 26.06.2002, Nds. MBl. S. 640) sowie auf den aktuellen Kommentar des LfD zu § 6 NDSG (s. Broschüre „Das NDSG, Text und Kommentar) wird verwiesen.

Vereinbarung

zwischen dem/der

- nachstehend Auftraggeberin/Auftraggeber genannt –

und dem/der

- nachstehend Auftragnehmerin/ Auftragnehmer genannt –

§ 1 Gegenstand der Vereinbarung

(1) Die Auftragnehmerin / Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrage der Auftraggeberin / des Auftraggebers.

(2) Der Auftrag umfasst folgende Tätigkeiten:

(Definition der Aufgaben)

§ 2 Pflichten der Auftraggeberin / des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der die Auftraggeberin / der Auftraggeber verantwortlich.

(2) Die Auftraggeberin / Der Auftraggeber erteilt alle Aufträge oder Teilaufträge schriftlich. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und schriftlich festzuhalten.

(3) Die Auftraggeberin / Der Auftraggeber hat das Recht, in folgendem Umfang Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen:

.....

Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.

Weisungsberechtigte Personen der Auftraggeberin / des Auftraggebers sind:

.....
(Name, Vorname, Funktion, Telefon, E-Mail-Adresse)

Weisungsberechtigte Personen der Auftraggeberin / des Auftraggebers im Vertretungsfall sind:

.....
(Name, Vorname, Funktion, Telefon, E-Mail-Adresse)

Weisungsempfänger bei der Auftragnehmerin /dem Auftragnehmer sind:

.....
(Name, Vorname, Funktion, Telefon, E-Mail-Adresse)

Weisungsempfänger bei der Auftragnehmerin /dem Auftragnehmer im Vertretungsfall sind:

.....
(Name, Vorname, Funktion, Telefon, E-Mail-Adresse)

Bei einem Wechsel oder einer längerfristigen Verhinderung der Kontaktperson ist der Vertragspartnerin / dem Vertragspartner unverzüglich schriftlich die Nachfolge- bzw. die Vertretungsregelung mitzuteilen.

(4) Die Auftraggeberin / Der Auftraggeber ist berechtigt, sich vor Beginn der Datenverarbeitung und sodann regelmäßig bei der Auftragnehmerin / beim Auftragnehmer von der Einhaltung der bei getroffenen technischen und organisatorischen Maßnahmen zu überzeugen (s. § 6 dieses Vertrages). Die Auftraggeberin / Der Auftraggeber kann diese Kontrolle auch durch einen Dritten durchführen lassen.

(5) Die Auftraggeberin / Der Auftraggeber informiert die Auftragnehmerin / den Auftragnehmer unverzüglich, wenn Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse festgestellt werden.

(6) Die Auftraggeberin / Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der Auftragnehmerin / des Auftragnehmers vertraulich zu behandeln.

§ 3 Pflichten der Auftragnehmerin / des Auftragnehmers

(1) Die Auftragnehmerin / Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen der Auftraggeberin / des Auftraggebers. Sie / Er verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate werden ohne Wissen der Auftraggeberin / des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherungskopien zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung.

(2) Die Auftragnehmerin / Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu. Sie / Er sichert zu, dass die überlassenen Daten ausschließlich in der Weise verarbeitet werden, dass diese jederzeit von sonstigen Datenbeständen scharf getrennt und bereitgestellt werden können.

(3) Die Auftragnehmerin / Der Auftragnehmer erklärt sich damit einverstanden, dass die Auftraggeberin / der Auftraggeber jederzeit berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme.

(4) An der Erstellung der Verfahrensbeschreibung nach § 8 NDSG hat die Auftragnehmerin / der Auftragnehmer mitzuwirken. Sie / Er hat die erforderlichen Angaben der Auftraggeberin / dem Auftraggeber zuzuleiten.

(5) Die Verarbeitung von Daten in Privatwohnungen ist nur mit Zustimmung der Auftraggeberin / des Auftraggebers im Einzelfall gestattet.

(6) Für die Durchführung der Auftragsdatenverarbeitung nicht mehr benötigte Unterlagen mit personenbezogenen Daten und Dateien dürfen erst nach vorheriger Zustimmung durch den Auftraggeber datenschutzgerecht vernichtet werden. Gleiches gilt für Test- und Ausschussmaterial.

(7) Nach Abschluss der vertraglichen Arbeiten hat die Auftragnehmerin / der Auftragnehmer sämtliche in ihren / seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen,

☐ dem Auftraggeber auszuhändigen.

und / oder

☐ wie folgt datenschutzkonform zu löschen:

Evtl. Hinweis auf DIN 66399, Teile 1, 2 und 3 aufnehmen.
.....

Die Datenträger der Auftragnehmerin / des Auftragnehmers sind danach physisch zu löschen.

(8) [1. Alternative]
Die Einschaltung von Subauftragnehmern ist ausgeschlossen. Die Beauftragung von Subunternehmen mit der Verarbeitung von personenbezogenen Daten ist in keinem Fall zulässig.

[2. Alternative]
Die Beauftragung von Subunternehmen ist nur mit schriftlicher Zustimmung Weisungen der Auftraggeberin / des Auftraggebers zugelassen. Die Auftragnehmerin / Der Auftragnehmer hat in diesem Falle vertraglich sicherzustellen, dass die vereinbarten Regelungen auch gegenüber Subunternehmern gelten. Er hat die Einhaltung dieser Pflichten regelmäßig zu überprüfen. Die Weiterleitung von Daten ist erst zulässig, wenn die Subunternehmerin / der Subunternehmer die Verpflichtung nach § 4 erfüllt hat und Namen und Anschrift der Subunternehmerin / des Subunternehmers /der Subunternehmen mitteilt.

[Zurzeit sind die in Anlage ..... mit Namen und Auftragsinhalt bezeichneten Subunternehmerinnen / Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt.]

Insbesondere muss die Auftraggeberin / der Auftraggeber berechtigt sein, Kontrollen vor Ort bei der Subunternehmerin / dem Subunternehmer / den Subunternehmen durchzuführen oder durch Dritte durchführen zu lassen. Die Auftragnehmerin / Der Auftragnehmers hat die Einhaltung der Pflichten regelmäßig zu überprüfen.

Optional bei Einbindung Dritter: Hinweis der Auftragnehmerin / des Auftragnehmer auf Gesetzesverstoß durch Subunternehmerin / dem Subunternehmer / den Subunternehmen an die Auftraggeberin / der Auftraggeber.

(9) Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit der Auftraggeberin / dem Auftraggeber abzustimmen. Es gilt die Leistungsbeschreibung.

(10) Sonstige konkrete Vorgaben für die o. g. Überprüfungen:

.....

(11) Die Auftragnehmerin / Der Auftragnehmer verpflichtet sich die Daten auf EU-Servern zu speichern.

§ 4 Datengeheimnis

(1) Die Auftragnehmerin / Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten der Auftraggeberin / des Auftraggebers das Datengeheimnis gemäß § 5 NDSG zu wahren.
Sie /Er verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie der Auftraggeberin / dem Auftraggeber obliegen, insbesondere § 203 StGB oder besondere Berufsgeheimnisse.

(2) Die Auftraggeberin /Der Auftraggeber verpflichtet sich, der Auftragnehmerin / dem Auftragnehmer die im Einzelfall zu beachtenden spezialgesetzlichen Datenschutzbestimmungen zu benennen. Die Auftragnehmerin / Der Auftragnehmer verpflichtet sich, diese auch gegen sich gelten zu lassen.

(3) Die Auftragnehmerin / Der Auftragnehmer bestätigt, dass ihr / ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Die Auftragnehmerin / Der Auftragnehmer sichert zu, dass sie / er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiterinnen und Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht. Sie /Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

(4) Auskünfte an Dritte oder an Betroffene darf die Auftragnehmerin / der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch die Auftraggeberin / den Auftraggeber erteilen.

Ggf. Konkretisierung/ Sog. „W-Fragen“ stellen

§ 5 Kontrollrechte der Landesbeauftragten für den Datenschutz (LfD)

(1) Die Auftragnehmerin / Der Auftragnehmer verpflichtet sich, der oder dem jeweils gesetzlich zuständigen Landesbeauftragten für den Datenschutz und den von ihr oder ihm eingesetzten Bediensteten sowie von ihr oder ihm beauftragten Stellen Zugang zu den Arbeitsräumen zu gewähren und unterwirft sich der Kontrolle nach Maßgabe des NDSG in seiner jeweiligen Fassung.

(2) Soweit Daten in einer Privatwohnung verarbeitet werden, ist der Zugang der oder des LfD und der von ihm eingesetzten Bediensteten vorher mit der Auftragnehmerin / dem Auftragnehmer abzustimmen.

§ 6 Technische und organisatorische Maßnahmen nach § 7 NDSG

(1) Die Auftragnehmerin / Der Auftragnehmer hat die in spezialgesetzliche Regelungen sowie die in § 7 NDSG getroffenen Festlegungen zu technischen und organisatorischen Maßnahmen umzusetzen.

(2) Die Auftragnehmerin / Der Auftragnehmer sichert in ihrem Verantwortungsbereich die Umsetzung und Einhaltung der gesetzlich vorgeschriebenen und vertraglich vereinbarten Datensicherheitsmaßnahmen zu. Die Auftragnehmerin / Der Auftragnehmer entwickelt ein Sicherheitskonzept, dass die erforderlichen technischen und organisatorischen Maßnahmen im Sinne von § 7 NDSG darstellt, setzt dieses um und ermöglicht der Auftraggeberin / dem Auftraggeber eine Überprüfung gem. § 6 Abs. 2 NDSG. Die Überprüfung ist vor Ort vorzunehmen. Die Auftragnehmerin / Der Auftragnehmer passt das Sicherungskonzept an veränderte Rahmenbedingungen an und stellt eine zeitnahe Realisierung sicher; der Auftraggeberin / dem Auftraggeber ist Gelegenheit zur Überprüfung zu geben. Insbesondere wird die Auftragnehmerin / der Auftragnehmer ihre / seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

(3) Die Auftragnehmerin / Der Auftragnehmer informiert die Auftraggeberin / den Auftraggeber unverzüglich über geplante Veränderungen in der Organisation der Datenverarbeitung und den angewandten Verfahren, soweit sie für die Auftragsdatenverarbeitung sicherheitsrelevant sind. Entsprechendes gilt in Fällen von schwerwiegenden Betriebsstörungen, bei Verdacht auf Datenschutzverletzungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten der Auftraggeberin / des Auftraggebers. Die Auftragnehmerin / Der Auftragnehmer stellt sicher, dass die datenschutzrechtlichen Rahmenbedingungen auch bei Einsatz von Telearbeitsplätzen oder mobilem Zugriff seiner Mitarbeiter auf Datenverarbeitungssysteme oder Daten des Auftragnehmers beachtet werden.

(4) Die in den o. g. Rechtsvorschriften vorgeschriebenen Regelungen zu technischen und organisatorischen Maßnahmen sind im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung anzupassen. Wesentliche Änderungen sind schriftlich zu vereinbaren.

(4.1) Soweit die bei der Auftragnehmerin / beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen der Auftraggeberin / des Auftraggebers nicht mehr genügen, benachrichtigt er den Auftraggeber unverzüglich. Entsprechendes gilt für Störungen sowie bei Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten.

(4.2) Sie / Er unterrichtet die Auftraggeberin / den Auftraggeber unverzüglich, wenn eine von der Auftraggeberin / vom Auftraggeber erteilte Weisung nach ihrer / seiner Meinung zu einem Verstoß gegen gesetzliche Vorschriften führen kann. Die Weisung braucht nicht befolgt zu werden.

(5) Sollten Sicherheit oder Verfügbarkeit der Daten bzw. Eigentum der Auftraggeberin / des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse möglicherweise gefährdet sein, so hat die Auftragnehmerin / der Auftragnehmer die Auftraggeberin / den Auftraggeber unverzüglich zu unterrichten und der Auftraggeberin / dem Auftraggeber alle erforderlichen Auskünfte zur Sicherung der Daten selbst sowie ihrer Verfügbarkeit zu erteilen.

§ 7 Zusammenarbeit

(1) Die Vertragspartner stellen sicher, dass die Übergabeformate der zu verarbeitenden Daten in den Einzelverträgen verlässlich geregelt werden.

(2) Die Vertragspartner definieren klare Schnittstellen und Verantwortlichkeiten (Netzwerkkomponenten, Verfahrensdurchführung, Fernwartung).

§ 8 Vertragsdauer

(1) Der Vertrag

- beginnt am ..... und endet am ...../

- mit Auftragserledigung /

- wird auf unbestimmte Zeit geschlossen.

Er ist mit einer Frist von ..... Monaten zum Quartalsende kündbar.

(2) Die Auftraggeberin / Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß der Auftragnehmerin / des Auftragnehmers gegen die Bestimmungen des NDSG oder dieses Vertrages vorliegt, die Auftragnehmerin / der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder die Auftragnehmerin / der Auftragnehmer den Zutritt der Auftragnehmerin / des Auftraggebers oder der Niedersächsischen Landesbeauftragten für den Datenschutz vertragswidrig verweigert.

§ 9 Vergütung

...

§ 10 Haftung

(1) Die Auftragnehmerin / Der Auftragnehmer haftet der Auftraggeberin / dem Auftraggeber für Schäden, die die Auftragnehmerin / der Auftragnehmer, seine Mitarbeiterinnen und Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der verträglichen Leistung schuldhaft verursachen.

(2) Für den Ersatz von Schäden, die eine Betroffene oder ein Betroffener wegen einer nach dem NDSG oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist die Auftraggeberin / der Auftraggeber gegenüber den Betroffenen verantwortlich. Soweit die Auftraggeberin / der Auftraggeber schuldhaft zum Schadensersatz gegenüber der oder dem Betroffenen verpflichtet ist, bleibt ihr / ihm der Rückgriff bei der Auftragnehmerin / beim Auftragnehmer vorbehalten.

§ 11 Vertragsstrafe

Bei Verstoß gegen die Abmachungen dieses Vertrages, insbesondere gegen die Einhaltung des Datenschutzes, wird eine Vertragsstrafe von .. *Euro/ Prozent des Gesamtauftragswertes des Vorjahres* vereinbart.

Von der Vertragsstrafe bleiben darüber hinausgehende Rechte der Auftraggeberin / des Auftraggebers unberührt.

§ 12 Nichterfüllung der Leistung

.....

§ 13 Sonstiges

(1) Die Auftragnehmerin / Der Auftragnehmer übereignet der Auftraggeberin / dem Auftraggeber zur Sicherung die Datenträger, auf denen sich Dateien befinden, die Daten der Auftraggeberin / des Auftraggebers enthalten. Diese Datenträger sind besonders zu kennzeichnen.

(2) Für Nebenabreden ist die Schriftform erforderlich.

(3) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen *[Hinweis: Diese Klausel muss wegen § 309 Nr. 2 BGB gesondert vereinbart werden!].*

§ 14 Salvatorische Klausel

Sollte eine Bestimmung dieses Vertrags unwirksam oder undurchführbar sein oder werden, bleibt die Wirksamkeit des Vertrags im Übrigen unberührt. Die Beteiligten werden an Stelle der änderungsbedürftigen Regelung eine wirksame treffen, die dem ursprünglich Gewallten so weit wie möglich entspricht. Gleiches gilt, wenn sich der Vertrag als lückenhaft erweisen sollte.

Ort, Datum

.....
Unterschrift/Stempel der Vertragspartner

Anlage zum Mustervertrag

I. Definitionen und Hinweise auf Regelungen

Auftraggeber:
Öffentliche Stelle in Niedersachsen (s. § 2 Abs. 1 und § 3 Abs. 3 NDSG), die einen Auftrag gemäß § 6 NDSG erteilt hat oder erteilen wird (s. a. Definition „verantwortliche Stelle“).

Auftragnehmer:
Natürliche Person oder Stelle (z. B. Unternehmen), die einen Auftrag gemäß § 6 NDSG angenommen hat oder annehmen will (s. § 3 Abs. 4 S. 3 NDSG). Auftragnehmer müssen gemäß § 6 Abs. 3 S. 1 NDSG Gewähr für die Einhaltung der technischen und organisatorischen Maßnahmen nach § 7 NDSG bieten.

Auftragskontrolle:

Werden personenbezogene Daten automatisiert verarbeitet, so sind gemäß § 7 Abs. 2 Nr. 9 NDSG Maßnahmen zu treffen, die je nach Art der Daten und ihrer Verwendung geeignet sind, zu gewährleisten, dass Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen der Auftraggeber verarbeitet werden können (Auftragskontrolle), s. a. § 6 Abs. 2 und Abs. 3 S. 2 NDSG.

Daten verarbeitende Stelle:
Daten verarbeitende Stelle ist gemäß § 3 Abs. 3 NDSG jede Stelle, die personenbezogene Daten selbst verarbeitet oder durch andere im Auftrag verarbeiten lässt. Sofern die Vorschriften dieses Gesetzes auf Auftragnehmer keine Anwendung finden, hat die Daten verarbeitende Stelle die Auftragnehmerin / den Auftragnehmer zu verpflichten, jederzeit vom Auftraggeber veranlasste Kontrollen zu ermöglichen (§ 6 Abs. 4 S. 1 NDSG).

Datenverarbeitung:
Datenverarbeitung ist gemäß § 3 Abs. 2 S. 1 NDSG das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen und Nutzen personenbezogener Daten. Im NDSG sind alle Phasen des Umgangs mit Daten unter dem Oberbegriff zusammengefasst).
Achtung: Siehe davon abweichende Legaldefinition im BDSG!

Personenbezogene Daten:
Personenbezogene Daten sind gemäß § 3 Abs. 1 NDSG Einzelangaben über persönliche oder sachliche Verhältnisse von bestimmten oder bestimmbaren natürlichen Personen (Betroffene).

Verantwortliche Stelle:
Werden personenbezogene Daten im Auftrag öffentlicher Stellen verarbeitet, so bleiben diese für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich (§ 6 Abs. 1 S. 1 NDSG).

II. Erläuterungen zu § 6 des Mustervertrags „Datensicherungsmaßnahmen/Schutzziele“

In dem Vertrag müssen die technischen und organisatorischen Maßnahmen gemäß § 7 NDSG festgelegt werden, die bei der Datenverarbeitung umzusetzen sind.

Rechtsgrundlage ist § 6 Abs. 2 S. 2 NDSG, in dem beschrieben ist, welche Prüfungen eine Auftraggeber / ein Auftraggeber vor einer Auftragsvergabe durchzuführen hat („Auftraggeber

haben sich über...zu vergewissern“). Die Auftragnehmerin / Der Auftragnehmer sollte unter besonderer Berücksichtigung der Zuverlässigkeit und der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt werden.

Im Auftrag sind insbesondere die Weisungen zu technischen und organisatorischen Maßnahmen schriftlich festzulegen, die geeignet sind zu gewährleisten, dass

1. nur Befugte auf Verfahren und Daten zugreifen und zur Kenntnis nehmen können (**Vertraulichkeit)**,
2. Daten unversehrt, vollständig, zurechenbar und aktuell bleiben (Integrität),
3. Verfahren und Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (**Verfügbarkeit**),
4. die Verarbeitung von personenbezogenen Daten mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden kann (**Transparenz**).
5. personenbezogene Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können (**Nichtverkettbarkeit**) und
6. Verfahren so gestaltet werden, dass sie den Betroffenen die Ausübung der ihnen zustehenden Rechte (z. B. nach den §§ 16 ff NDSG) wirksam ermöglichen (**Intervenierbarkeit**).

Im Einzelfall ist zu fordern, dass

- jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (**Authentizität**, Teil der Integrität),
- festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (**Revisionsfähigkeit**, Teil der Transparenz).

a) Grundsätzlich sind technische Datensicherungsmaßnahmen gegenüber organisatorischen Maßnahmen vorzuziehen. Bei der Auswahl der technischen Maßnahmen sollten sicherheitsüberprüfte und zertifizierte Produkte bevorzugt werden. Einen aktuellen Nachweis über sicherheitsüberprüfte Produkte führt das Bundesamt für Sicherheit in der Informationstechnik (BSI), Godesberger Allee 183, 53133 Bonn (Internet: www.bsi.bund.de).

Die IT-Grundschutzkataloge des BSI beschreiben mögliche Gefahren und bieten einen umfangreichen Katalog geeigneter Datensicherungsmaßnahmen. Reichen auf Grund eines höheren Schutzbedarfes Grundschutzmaßnahmen nicht aus, sind weitergehende Zusatzmaßnahmen zu treffen.

Die BSI-Standards 100-x bieten zudem umfassende Orientierung für die Organisation eines Informationssicherheitsprozesses (BSI-Standard 100-1: Managementsysteme für Informationssicherheit – ISMS, BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise, BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz und BSI-Standard 100-4: Notfallmanagement).

b) Wenn die Auftragnehmerin / der Auftragnehmer ein Datensicherheitskonzept aus technischen und organisatorischen Maßnahmen besitzt, muss die Auftraggeberin / der Auftraggeber prüfen und schriftlich festlegen, ob es ihren / seinen Anforderungen entspricht (s. o.). Insbesondere bei der Verarbeitung sensibler Daten sind in der Regel zusätzliche Maßnahmen erforderlich. Das Datensicherungskonzept muss in seiner Gesamtheit einen hinreichenden Schutz der Daten vor unsachgemäßer Handhabung gewährleisten. Ist das Konzept nicht ausreichend, sind ergänzende Maßnahmen zu vereinbaren. Das daraus resultierende Sicherheitskonzept sollte zum Vertragsbestandteil gemacht werden. In diesem

Fall kann darauf verzichtet werden, im Sicherheitskonzept genannte Maßnahmen im Vertragstext zu wiederholen.

c) Besonders wichtig sind Regelungen zu folgenden Sachverhalten:

Verantwortlichkeiten: Aus unklaren Aufgabenverteilungen, beispielsweise bei der Vergabe von Zugriffsrechten, resultieren Schwachstellen mit hohen Risiken. Bsp.:

- **Abschottung von Netzen**: Es müssen Maßnahmen ergriffen werden, um ein unberechtigtes Eindringen in Rechnernetze soweit möglich zu verhindern. Da meist keine absolute Sicherheit zu erreichen ist, müssen derartige Versuche erkannt werden. Technische Komponenten, die in Betracht kommen, sind Firewalls oder Intrusion Detection Systeme.

- **Abhören der Kommunikation**: Zum Schutz gegen unberechtigtes Abhören bietet es sich an, die Daten zu verschlüsseln.

- **Abmeldeprozeduren**: Die Anmeldung am System oder Anwendung stellt die erste und wichtigste Hürde dar, die unbefugte Person überwinden müssen. An dieser Stelle müssen qualitativ hochwertige Maßnahmen ergriffen werden.

Checkliste Auftragsdatenverarbeitung

Handelt es sich um eine Auftragsdatenverarbeitung (Stichwort „Hilfstätigkeit ohne eigenen Beurteilungs- und Entscheidungsspielraum“) oder bedarf es einer Funktionsübertragung?	s. Handreichung
Welche Rechtsgrundlagen sind für die Auftragsdatenverarbeitung heranzuziehen? - Bereichsspezifische Regelungen (s. z. B. § 80 SGB X) - sonstige bereichsspezifische Regelungen - § 6 NDSG	
Welche Voraussetzungen und Anforderungen hat der Auftraggeber zu erfüllen?	
- Festlegung der Art der zu verarbeitenden Daten	Auflistung der personenbezogenen Daten, Einstufung s. Schutzstufenkonzept LfD (s. Homepage der LfD: www.lfd.niedersachsen.de)
- schriftliche Festlegung der Weisungen zur Auftragserfüllung (§ 6 Abs. 3 S. 2 NDSG)	z. B. Berichtspflicht bei besonderen Vorkommnissen (techn. oder organisatorische Unzulänglichkeiten, Verdacht auf Datenschutzverletzungen)
- Hinweis an Auftragnehmer auf geltende (nds.) Rechtsvorschriften (Spezialregelungen, ggf. NDSG)	Sog. „Unterwerfungsregelung“
Prüfung	
- Sitz Auftragnehmer	Datenschutzrechtliches Risiko?, s. a. § 13 NDSG Alternativpartner?
- Ansprechpartner vor Ort (Projektleitung/Sachbearbeitung und betrieblicher/behördlicher DSB)	Wichtig für Kontrollen und Auskunftsrecht
- Ggf. (formlose) Meldung an DSB eines anderen Bundeslandes (s. § 6 Abs. 4 S. 2 NDSG)	
- Abfrage Datenverarbeitungsstandort, Serverstandort	Alternativen? s. a. „Safe-Harbor-Urteil“ d. EuGH v. 06.10.2015 sowie Positionspapier der Konferenz der unabhängigen Datenschutzaufsichtsbehörden (DSK) v. 21.10.2015 (eingestellt auf der Homepage der LfD)
- auf welche Weise a) die Hardware in den Räumlichkeiten, b) das Gebäude und die Räume des Dienstleisters und	Stichworte: BSI-Grundschutz, ISO/IEC 27001, verschlüsselter USB-Stick,

c) Daten auf dem Transportwege vor unberechtigten Zugriffen gesichert bzw. geschützt werden.	verschlüsselte Festplatte, Zugriffskontrolle, Rollen – und Berechtigungskonzept Passwort/Kennung, abschließbare Schränke
- Werden Untervertragsverhältnisse zugelassen?	Einstufung datenschutzrechtlicher Risiken. Beauftragung nur mit vorheriger Zustimmung des Auftragnehmers zulässig?
- Dokumentationspflichten regeln	
- Festlegung	
- Datenvernichtung/Löschung klären, Geltung Datengeheimnis auch nach Beendigung des Vertragsverhältnisses	
- Vertragsrechtliche Prüfung	AGB datenschutzrechtliche Klauseln
Welche Voraussetzungen und Anforderungen hat der Auftragnehmer zu erfüllen?	
- Nur Einsatz von Beschäftigten des Auftragnehmers, die auf das gesetzlich verankerte Datengeheimnis hingewiesen und nach dem Verpflichtungsgesetz verpflichtet worden sind.	Datenschutzgeheimnis § 5 NDSG, Geheimhaltungspflicht (Berufs- und Amtsgeheimnis), s. § 203 ff StGB (s. Muster auf Homepage der LfD)