Auftragsdatenverarbeitung

Orientierungshilfe und Checkliste

Landesbeauftragter für den Datenschutz Niedersachsen

Vorbemerkung

Zunehmende Spezialisierung in Hardware, Software und Personal sowie mögliche Kosteneinsparungen und hohe Flexibilität sind heute Gründe, bestehende Verfahrensabläufe zu überdenken. Immer häufiger wird in Wirtschaft und Verwaltung das Modell „Outsourcing" gewählt. Der Begriff stammt aus dem amerikanischen Wirtschaftsleben und setzt sich aus den Worten *„Outside Resource Using = Mittel von außen gebrauchen zusammen"*. Dabei scheint die verbreitete Grundeinstellung zu „Outsourcing" negativ, zumindest skeptisch zu sein. Auf Gesetzesebene wird dies am deutlichsten im SGB X, wo die Datenverarbeitung im Auftrag unverkennbar als nicht immer vermeidbares Übel eingestuft ist. Für die Auftragsdatenverarbeitung sprechen bei aller Skepsis auch gute Gründe, so:

- hohe Qualität der Verarbeitung durch Spezialisierung,
- Interessenferne der Auftragnehmer gegenüber den Daten der Betroffenen,
- Geschäftsinteresse an untadeligem Image und
- effektive Sicherheitssysteme durch optimale Betriebsgröße.

Datenschutzrechtlich zu unterscheiden sind die Auftragsdatenverarbeitung und die Funktionsübertragung. Bei der Auftragsdatenverarbeitung bleibt die datenschutzrechtliche Verantwortung für die Verarbeitung und Nutzung der personenbezogenen Daten beim Auftraggeber. Er schreibt die technischen und organisatorischen Maßnahmen zur Datensicherung und zur Gewährleistung der Vertraulichkeit beim Auftragnehmer vor. Dem Serviceunternehmen wird nur die tatsächliche Verarbeitung oder Nutzung nach Weisung und unter materieller Verantwortung des Auftraggebers übertragen. Bei der Datenverarbeitung im Auftrag wird damit lediglich eine „Hilfsfunktion" der eigentlichen Aufgabe ausgelagert.

Werden dagegen die der Verarbeitung zugrunde liegenden Aufgaben oder Geschäftszwecke ganz oder teilweise abgegeben, erbringt der Auftragnehmer über die technische Durchführung hinaus materielle Leistungen mit Hilfe der überlassenen Daten, dann spricht die Kommentarliteratur von einer „Funktionsübertragung". In diesem Fall wird also dem Dienstleister eine ganze Aufgabe übertragen, die er eigenverantwortlich wahrnimmt.

Deutliche Erkennungsmerkmale sind bei

Auftragsdatenverarbeitung

- fehlende Entscheidungsbefugnis des Auftragnehmers
- weisungsgebundene Unterstützung
- fehlende (vertragliche) Beziehung des Auftragnehmers zum Betroffenen
- Umgang nur mit Daten, die der Auftraggeber zur Verfügung stellt

Funktionsübertragung

- Überlassung von Nutzungsrechten an den Daten
- eigenverantwortliche Sicherstellung von Zulässigkeit und Richtigkeit der Daten durch den Dienstleister
- Sicherstellen der Rechte von Betroffenen (Benachrichtigungspflicht, Auskunftsanspruch).

Die Abgrenzung, ob eine Outsourcing-Regelung Auftragsdatenverarbeitung oder Funktionsübertragung ist, lässt sich nur im Einzelfall entscheiden. Im Folgenden wird nur noch die Fallgestaltung der Auftragsdatenverarbeitung betrachtet.

Soll eine Dienstleistung durch ausländische Stellen erbracht werden, gelten die Regelungen der Datenverarbeitung im Auftrag nicht. In diesen Fällen finden die jeweiligen Regelungen über die Übermittlung von personenbezogenen Daten an Stellen außerhalb der Bundesrepublik Deutschland Anwendung (§ 14 NDSG/ § 4b BDSG). Dies bedeutet für die Nutzung der Datenverarbeitungskapazitäten im Ausland, dass der Auftragnehmer als Dritter anzusehen ist, dass rechtlich unselbständige Zweigstellen als Dritte in Bezug zur inländischen Muttergesellschaft anzusehen sind und dass die grenzüberschreitende Übertragung personenbezogener Daten eine Übermittlung ist.

Gleichwohl sollte der Auftraggeber in solchen Ländern, die über keine oder z.B. nur bereichsspezifische Datenschutzregelungen verfügen, folgende Punkte vertraglich festlegen:

- verbindliche Festlegung des Verwendungszwecks
- Auskunftsrechte gegenüber dem Datenempfänger
- Einräumung der Rechte auf Benachrichtigung, Sperrung und Löschung
- Regelung der Benachrichtigungspflicht
- Festlegung von Datensicherungsmaßnahmen
- Vereinbarung zur Verminderung bestehender Kontrolldefizite im Ausland

Bei einer Übermittlung von personenbezogenen Daten ohne vertragliche Regelungen verliert der Betroffene seine Rechtsposition, die ihm durch die datenschutzrechtlichen Regelungen der Bundesrepublik Deutschland zugestanden wird.

Datenschutz

Bei einer Auftragsdatenverarbeitung sind die datenschutzrechtlichen Anforderungen für Stellen der Wirtschaft im Bundesdatenschutzgesetz (BDSG) und für öffentliche Stellen des Landes Niedersachsen im Niedersächsische Datenschutzgesetz (NDSG) geregelt. Bereichsspezifische Vorschriften gehen dem allgemeinen Datenschutzrecht vor, so z.B.

- § 80 Abs. 2 bis 5 SGB X bei der Verarbeitung von Sozialdaten im Auftrage,
- § 5 NStatG, der bei Vergabe statistischer Auswertungen die Kenntnisnahme von Hilfsmerkmalen untersagt,
- besondere Berufsgeheimnisse wie z.B. § 203 StGB für Ärzte, Apotheker, Angehörige der privaten Kranken-, Unfall- oder Lebensversicherungen, Rechtsanwälte, Steuerberater u.a.,
- § 30 Abgabenordnung (Steuergeheimnis).

Die Auftraggeber in Wirtschaft und Verwaltung sind in gleicher Weise verpflichtet, die zu übertragende Datenverarbeitung, die vom Auftragnehmer einzuhaltenden technischen und organisatorischen Datensicherungsmaßnahmen sowie etwaige Unterauftragsverhältnisse schriftlich festzulegen. Neben diesen Mindestfestlegungen sollten auch die folgenden Pflichten festgelegt werden:

- Externe Personen oder Stellen, die mit der Auftragsdatenverarbeitung betraut sind, haben nach den Weisungen des Auftraggebers zu arbeiten.
- Der Auftraggeber hat vor Beginn der Arbeiten sicherzustellen, dass der Auftragnehmer personenbezogene Daten nur zur Kenntnis nehmen kann, soweit dies unvermeidbar ist.
- Die Auftragnehmer haben die technischen und organisatorischen Maßnahmen nach § 9 BDSG bzw. § 7 NDSG zu treffen, die erforderlich sind, um eine datenschutzgerechte Verarbeitung personenbezogener Daten sicherzustellen.

Weiter hat der Auftragnehmer allgemeine Sicherungsziele zu gewährleisten, wie Gewährleistung der Vertraulichkeit der Daten, Sicherstellung der Integrität der Daten, Gewährleistung der Authentizität der Daten, Gewährleistung der Authentifikation von Benutzern, Gewährleistung der sicheren Zustellung, Sicherstellung der Verfügbarkeit und Sicherstellung der Revisionsfähigkeit.

Gefahren- und Risikoanalyse

Auftragsdatenverarbeitung schafft neben vielen Vorteilen auch Gefahren und Risiken für die genannten Sicherungsziele. Konkrete Gefahren können dadurch entstehen, dass :

- zusätzliche Akteure auftreten, die das Missbrauchspotential erhöhen,
- die Datenschutzkontrolle durch die Auslagerung kompliziert und verschlechtert wird,
- personenbezogene Daten mit hohem Schutzbedürfnis Betroffener Serviceunternehmen bekannt werden und
- Kernbereiche staatlicher Tätigkeit berührt sein können.

Vor der Entscheidung, ob und welche Art der Leistung in Zukunft durch Auftragsdatenverarbeitung betrieben werden soll, hat der Auftraggeber zu prüfen, ob und in welchem Umfang wegen der Art

und des Umfangs der zu verarbeitenden Daten oder der Verwendung neuer Technologien Gefahren für die Rechte der Betroffenen verbunden sind. Auftragsdatenverarbeitung darf nur durchgeführt werden, soweit derartige Gefahren durch technische und organisatorische Maßnahmen wirksam beherrscht werden können.

Technische und organisatorische Maßnahmen

Eine ausreichend sichere Form der Auftragsdatenverarbeitung wird erreicht, wenn die vertraglichen Vereinbarungen und die getroffenen technischen und organisatorischen Maßnahmen einen hinreichenden Schutz bieten. Art und Umfang der erforderlichen und angemessenen Sicherungsmaßnahmen richten sich dabei nach der Sensibilität der verarbeiteten Daten. Wird eine dieser Maßnahmen vernachlässigt, ist eine sichere Auftragsdatenverarbeitung nicht möglich.

Neben meiner Orientierungshilfe und Checkliste zur Auftragsdatenverarbeitung empfehle ich meine Materialsammlung im Internet. Unter der Adresse www.lfd.niedersachsen.de finden Sie dort weitere datenschutzrelevante Rechtsvorschriften, Empfehlungen, Orientierungshilfen, Checklisten sowie sonstige Materialien zum „Downloading".

Handlungsempfehlungen

Die Orientierungshilfe weist auf Gefahren und Risiken bei der Datenverarbeitung im Auftrag hin und gibt konkrete Empfehlungen für vertragliche Vereinbarungen sowie technische und organisatorische Sicherungsmaßnahmen. Im Hinblick auf die Vielschichtigkeit der Auftragsdatenverarbeitung, von der schlichten Datenerfassung über das Bereitstellen von Rechnerleistung, die Verarbeitung im Rahmen eines umfassenden Hardware- und Softwarekonzeptes, bis hin zur individuellen Entwicklung und Implementierung komplexer automatisierter Verfahren, ergeben sich im Einzelfall Fragestellungen und Forderungen. Es ist jedoch sinnvoll, anhand der folgenden Checkliste zu prüfen, ob die im Einzelfall bestehenden oder beabsichtigten vertraglichen Vereinbarungen den datenschutzrechtlichen Anforderungen entsprechen. Der regelungsfreie Raum sollte möglichst klein gehalten werden.

Die Orientierungshilfe will
- Geschäfts- und Behördenleitung,
- Personalleitung und Personalvertretung sowie
- Organisations- und DV-Leitung

in die Lage versetzen, die erforderlichen Regelungen zu treffen.

Checkliste

Die folgende Checkliste soll eine Hilfestellung für die Erarbeitung datenschutzgerechter Lösungen bei der Ausgestaltung der vertraglichen Vereinbarungen leisten. Ausschließlich datenschutzrechtliche Überlegungen liegen der Checkliste zugrunde.

Zur Beantwortung der Checklisten-Fragen wird es in der Regel ausreichen, jeweils anzukreuzen
- Erfüllt
- Nicht erfüllt
- Trifft nicht zu.

Anlage 1

Checkliste
- Datenschutz bei Auftragsdatenverarbeitung -

1.	Allgemeine Anforderungen	
	Welche Stellen verarbeiten im Auftrag der überprüfen Stelle personenbezogene Daten?	
	Für welche Stellen werden personenbezogene Daten im Auftrag verarbeitet?	
	Wird der Auftrag im Ausland ausgeführt (wenn ja: EU oder außerhalb der EU?)?	
	Gibt es Unterauftragsverhältnisse?	
	Ggf. Zusatzfrage:	

	Auftragsorganisation	Erfüllt	Nicht erfüllt	Trifft nicht zu	Bemerkung
	Die Eignung des Auftragnehmers wurde durch Überprüfung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt (§ 11 Abs. 2 BDSG).				
	Die Ergebnisse der Auftragsdatenverarbeitung werden zumindest stichprobartig auf Richtigkeit überprüft.				
	Soweit der Auftrag außerhalb des NDSG-Geltungsbereiches durchgeführt wird und der Auftraggeber dem NDSG unterliegt, wurde die zuständige Datenschutzkontrollbehörde unterrichtet (§ 6 (4) Satz 2 NDSG).				
	Es sind jeweils schriftliche Aufträge in einer der folgenden Formen erteilt worden (§ 11 Abs. 2 BDSG, § 6 (3) NDSG): - Einzelverträge oder Rahmenverträge mit Einzelaufträge (Lieferscheine, Belege, Quittungen).				
	Ggf. Zusatzfrage:				

	Vertragsgestaltung	Erfüllt	Nicht erfüllt	Trifft nicht zu	Bemerkung
	Genaue Bezeichnung des Vertragspartners.				
	Beschreibung des Gegenstandes des Vertragsverhältnisses, ggf. mit Leistungsverzeichnis, Pflichtenheft oder sonstige Unterlagen, die die Art und den Umfang der zu erbringenden Leistungen festschreiben.				
	Wichtige technische und organisatorische Sicherungsmaßnahmen bei der Auftragsabwicklung, z.B. ☐ Protokollierung ☐ Zugriffskontrolle ☐ Umgang mit nicht mehr benötigten Arbeitsergebnissen ☐ sonstige:_____				
	Vereinbarung über das Recht des Auftragnehmers, zur Erbringung der Leistungen Dritte heranzuziehen.				
	Festlegung der Unterauftragsverhältnisse				
	Genaue Bezeichnung des Speicherungs- und des Verarbeitungsortes.				
	Bestimmung der Eigentumsverhältnisse an Soft- und Hardware.				
	Regelungen über „Eigentumsvorbehalte" des Auftragnehmers an gespeicherten Daten und maschinellen Ergebnissen bei Nichterfüllung des Vertrages durch den Auftraggeber.				
	Benachrichtigungspflichten im Falle gesetzlicher Offenbarungspflichten des Auftragnehmers.				
	Vereinbarung von Laufzeiten und Kündigungsfristen.				
	Beschreibung der Pflichten, die über das Vertragsende hinausreichen.				
	Bezeichnung der Weisungsberechtigten beim Auftraggeber				
	Bezeichnung der Weisungsberechtigten beim Auftragnehmer.				
	Verantwortung ,Art, schriftliche Bestätigung, Transportkontrolle sowie Protokollierung für den Datenträgertransport.				
	Definition der verfahrensunabhängigen Plausibi-				

	Vertragsgestaltung	Erfüllt	Nicht erfüllt	Trifft nicht zu	Bemerkung
	litäts- und Sicherheitsprüfungen beim Dateneingang durch den Auftragnehmer.				
	Prüfung der Richtigkeit der Ergebnisse durch den Auftraggeber.				
	Unterrichtung des Auftraggebers bei Störungen.				
	Bereitstellung von Testmaterial durch den Auftraggeber.				
	Information des Auftragnehmers über Programm- und Verfahrensänderungen.				
	Einwilligung zu Verfahrensänderungen.				
	Festlegung des Umfangs der Verfahrens- und Programmdokumentation.				
	Nachweis der tatsächlich gespeicherten Daten.				
	Nachweis der ordnungsgemäßen Berichtigungs-, Sperrungs- und Löschungsmöglichkeiten.				
	Festlegung der Aufbewahrungsdauer der Datenbestände und der Software.				
	Verknüpfung der Datensicherungsmaßnahmen des Auftraggebers mit denen des Auftragnehmers.				
	Definition der Weisungs- und Kontrollrechte des Auftragebers/Auftragnehmers.				
	Recht zur sofortigen Kündigung bei Nichtbeachtung von Verpflichtungen, evtl. Vertragsstrafen.				
	Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis.				