

NOVELLIERUNG DES BUNDESDATENSCHUTZGESETZES ÄNDERUNGEN SEPTEMBER 2009

TEIL 1: AUFTRAGSDATENVERARBEITUNG

Autoren: Daniela Weller (DIIR e.V.)
In Zusammenarbeit mit Uwe Dieckmann (GDD e.V.)
und Volker Hampel (DIIR e.V.)

Oktober 2009
Frankfurt am Main

Der vorliegende Artikel basiert auf einer persönlichen Einschätzung der Autoren. Er gibt nicht die Meinung des DIIR und der GDD wieder.

1. EINLEITUNG

Ab dem 1. September 2009 ist die **BDSG Novelle II** in Kraft getreten. Sie beinhaltet

1. Erweiterte Anforderungen an die **Auftragsdatenverarbeitung** (§ 11 BDSG)
2. Eine Neuregelung zum Arbeitnehmerdatenschutz (§ 32 BDSG),
3. Informationspflichten bei Datenschutzpannen (§ 42a BDSG)
4. Eine Änderung der Anlage zu § 9 BDSG / die Stärkung des Grundsatzes der Datenvermeidung
5. Die Einschränkung der Zulässigkeit personalisierter Werbung (§ 28 Abs. 3 und 3a BDSG)
6. Die Stärkung der Rechtsstellung des betrieblichen Datenschutzbeauftragten (§ 4f Abs. 3 BDSG) sowie
7. Erweiterte Kompetenzen der Aufsichtsbehörden (§ 38 BDSG)

Dieser Teil der DIIR Artikelreihe BDSG setzt sich alleinig mit den **erweiterte Anforderungen an die Auftragsdatenverarbeitung (§ 11 BDSG) – Punkt 1** - auseinander.

2. HINTERGRUND

Die neuen Regelungen zur Auftragsdatenverarbeitung können erhebliche Auswirkungen auf Revisionsaktivitäten in folgenden Bereichen haben:

- Prüfungen mit **Outsourcing-Schwerpunkt** oder Organisationseinheiten, die sehr stark mit Outsourcing-Partnern zusammenarbeiten
- Prüfungen hinsichtlich der **zentralisierten Personalverwaltung/-buchhaltung**
- Prüfungen **zentraler Kundendatenbanken** oder **Shared Service Centern** in Konzernen bzw. bei Unternehmen mit unterschiedlichen rechtlichen Einheiten.

Die Regelungen beinhalten neue weitreichende **Anforderungen an die Vertragsgestaltung**. Für Auftraggeber ergibt sich aus den Regelungen auch die explizite Pflicht zur Kontrolle/ Prüfung der vertraglichen Festlegungen vor und in regelmäßigen Abständen auch während des Outsourcings. Darüber hinaus besteht die Pflicht, die Ergebnisse dieser Kontrollen/Prüfungen entsprechend zu dokumentieren.

Neu sind insbesondere auch drohende Geldbußen im Falle der Nichtbeachtung der getroffenen Regelungen. Als **Geldbußen** können hier bis zu 50.000 Euro verhängt werden. Die Auftragsdatenverarbeitung betreffenden Regelungen aus der BDSG Novelle II gelten **seit 01.09.2009 ohne Übergangsregelung**.

Im Folgenden sind die wesentlichen Elemente der neuen Regelungen zur Auftragsdatenverarbeitung praxisgerecht aufgearbeitet. In Zusammenarbeit mit der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) werden praktische Fragestellungen zur Vertrags- und Prozessgestaltung behandelt und dargestellt.

3. AUFTRAGSDATENVERARBEITUNG – WAS HEIßT DAS?

Im §11 Abs. 1 BDSG ist geregelt, dass eine verantwortliche Stelle (Auftraggeber) bestimmte Datenverarbeitungen durch eine andere Stelle (Auftragnehmer - AN) vornehmen lassen kann. Dabei bleibt der Auftraggeber „Herr der Daten“ und ist verantwortlich für die Einhaltung regulatorischer Vorschriften. Im rechtlichen Sinne wird der Auftragnehmer nicht als Dritter, sondern als „Teil der verantwortlichen Stelle“ (Privilegierungseffekt) betrachtet.

Die Regelungen zur Auftragsdatenverarbeitung (ADV) gelten sowohl für **externe Outsourcing-Dienstleister** als auch für **rechtlich selbständige Organisationseinheiten** innerhalb eines Konzerns oder Unternehmensverbunds. Im Konzernverbund sind damit auch z.B. Übertragung, Verarbeitung oder Speicherung von Daten einer Tochtergesellschaft an eine andere Tochtergesellschaft oder den Mutterkonzern betroffen. Daher ist in den exemplarisch aufgeführten Fällen der Abschluss eines Vertrages zur Auftragsdatenverarbeitung unumgänglich. Darüber hinaus reicht ein reiner Geschäftsbesorgungsvertrag oder Dienstleistungsvertrag in der Regel trotz Vertraulichkeitsbestimmungen nicht aus, weil darin der Umgang mit **personenbezogenen Daten** nicht notwendig geregelt ist. Um bestehende Verträge nicht ändern zu müssen, ist der ADV-Vertrag häufig ein **Zusatzvertrag** oder ein Anhang zu bestehenden Verträgen

Auftragsdatenverarbeitung setzt voraus, dass der Auftrag nach den vorgegebenen Regeln des Auftraggebers abgearbeitet wird. Im Gegensatz dazu existiert die sogenannte „Funktionsübertragung“ (Business Process Outsourcing), die eine zusätzliche eigenständige geistige Leistung des Vertragspartners erfordert, z.B. komplette Abwicklung aller Personalverwaltungsangelegenheiten. Daher gelten die Regelungen der Auftragsdatenverarbeitung für **Funktionsübertragungen (Business Process Outsourcing)** nicht. Daher ergibt sich hier wiederum u.a. die Verpflichtung, dass die betroffenen Personen von der Datenspeicherung benachrichtigt werden müssen.

4. WELCHE NEUERUNGEN GIBT ES?

4.1 Konkretisierung der Mindestinhalte eines ADV-Vertrages

Im Gesetzestext¹ wurden die Mindestinhalte eines ADV-Vertrages konkretisiert. Diese sind:

- der Gegenstand und die Dauer des Auftrags
- der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten sowie die Art der Daten und der Kreis der Betroffenen,
- die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen
- die Berichtigung, Löschung und Sperrung von Daten,
- die bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
- die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
- die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
- mitzuteilende Verstöße des Auftragnehmers gegen Datenschutzvorschriften oder gegen die im Auftrag getroffenen Festlegungen oder der bei ihm beschäftigten Personen gegen Vorschriften

¹ (§ 11 Abs. 2 Sätze 2 und 4 BDSG, nachzulesen unter <https://www.gdd.de/nachrichten/arbeitshilfen/BDSG-Gesetzestext%20mit%20Novelle%20I-III.pdf>)

- der Umfang der Weisungsbefugnisse,
- die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

4.2 Bußgeldbewährung

Ein mögliches Bußgeld ist gemäß § 43 Abs. 1 Nr. 2b BDSG (Neu) geregelt:

Ordnungswidrig handelt, wer **vorsätzlich oder fahrlässig**

- einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt oder
- sich nicht vor Beginn der Datenverarbeitung über die Einhaltung der beim AN getroffenen technischen und organisatorischen Maßnahmen überzeugt

Eine Geldbuße bis zu 50.000 Euro sowie zusätzlich die Zahlung einer sog. „**Gewinnabschöpfung**“ sind möglich. Wurde also ein wirtschaftlicher Vorteil aus der Ordnungswidrigkeit gezogen, soll die Geldbuße nach § 43 Abs. 3 BDSG den wirtschaftlichen Vorteil übersteigen (Gewinnabschöpfung). Das kann dazu führen, dass die Geldbuße sogar die normale Grenze von **50.000 Euro übersteigt**.

4.3 Überprüfung und Dokumentation der Technisch-Organisatorischen-Maßnahmen

Der Auftraggeber hat sich nach § 11 Absatz 2 Satz 4 BDSG bereits vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.

5. PRAKTISCHE FRAGESTELLUNGEN: VERTRAGSGESTALTUNG

5.1 Welche Regelungen müssen angepasst werden?

Anpassungsbedarf an die neuen Vorschriften ergibt sich bei allen Auftraggebern, auch bei denen, die bisher schon eine Mustervereinbarung zur ADV verwendet haben.

Die Nutzung eines **BDSG-konformen Vertragsmusters** zur Beauftragung des Dienstleisters ist nunmehr dringend zu empfehlen, um der Gefahr der Unrichtigkeit, Unvollständigkeit oder Unvorschriftsmäßigkeit des Auftrags und der damit verbundenen Geldbuße zu entgehen. Das erste offizielle Vertragsmuster von einer Datenschutzbehörde wurde am 30.9. veröffentlicht (RP Darmstadt)². Die GDD wird am 12.10.2009 auf ihrer Homepage eine Mustervereinbarung zur ADV präsentieren.

Bei der ADV Vertragsgestaltung besteht insbesondere **Konkretisierungsbedarf** für

- die nach § 9 BDSG zu treffenden technischen und organisatorischen Datensicherheitsmaßnahmen
- die Begründung von Unterauftragsverhältnissen

² http://www.rp-darmstadt.hessen.de/irj/RPDA_Internet?cid=cc0eeb29fc27e29efe4d7d34acc1e89e

- Kontrollmaßnahmen durch Auftraggeber und Auftragnehmer (auch beim Unterauftragnehmer)
- Umfang der Weisungsbefugnisse des Auftraggebers
- Maßnahmen bei Beendigung des Auftrags hinsichtlich Rückgabe bzw. Vernichtung überlassener Datenträger und Löschung der Daten beim Auftragnehmer.

5.2 Wie sind Altverträge zu behandeln?

Alte ADV-Verträge, die dem bisherigen § 11 BDSG entsprechen, werden **nicht** ab dem 01.09.2009 **automatisch ungültig**. Weil das Gesetz jedoch keine Übergangsfristen vorsieht, sollten auch **Alt-Verträge grundsätzlich** auf Anpassungsbedarf **geprüft** werden.

Unsere Empfehlung lautet hier: **Priorisierung bestehender ADV-Verhältnisse**. Wie kritisch ist die jeweilige ADV nach Art und Umfang der verarbeiteten Daten?

Werden besonders **sensible personenbezogene Daten** verarbeitet oder handelt es sich um eine Datenverarbeitung mit hoher Komplexität und vielen Schnittstellen, ist von einer kritischen Datenverarbeitung auszugehen. Kritische ADV-Verhältnisse sollten intensiver, weniger kritische ADV-Verhältnisse können ggf. im Rahmen turnusgemäßer Überprüfungen abgedeckt werden.

Grundsätzlich hat die Anpassung der Aufträge Priorität, deren Daten auf fremden IT-Systemen verarbeitet werden und damit nicht mehr der eigenen Kontrollsphäre unterliegen. Zu solchen Auftragnehmern gehören z.B. Rechenzentren, Archivierungsdienstleister, Marktforschungsinstitute, Adressdienstleister, Lettershops.

5.3 Sind Rahmenvereinbarungen weiterhin zulässig?

Die Regel in den Unternehmen ist, dass Fremdleistungen schon allein wegen der Preisabsprache schriftlich fixiert sind. Das gilt erst recht für Fremdleistungen, die auf eine gewisse Dauer angelegt sind. Soweit diese Leistungen sehr unterschiedlich sind oder zu unterschiedlichen Zeitpunkten fällig werden, sind lediglich Rahmenvereinbarungen vorhanden, die jeweils vertraglich ergänzt werden hinsichtlich der Einzelleistungen. Soweit in der Rahmenvereinbarung auch datenschutzrechtliche Vereinbarungen enthalten sind, kann in dem mit den Einzelleistungen verbundenen schriftlichen Auftrag nach § 11 BDSG auf die Rahmenvereinbarung verwiesen werden. Wichtig ist in diesem Zusammenhang, dass bei Abruf der Leistungen nach dem 31.08.2009 das neue BDSG Anwendung findet.

6. PRAKTISCHE FRAGESTELLUNGEN: PROZESSGESTALTUNG

6.1 Wann soll kontrolliert werden?

Eine **Erstkontrolle** muss zwingend vor Beginn der Datenverarbeitung erfolgen, da sonst Bußgeldbewehrung droht. **Laufende Kontrollen** sollten je nach Sensibilität und Umfang der Datenverarbeitung in jeweils angemessenen Zeiträumen erfolgen. Als Maßstab könnten hier bspw. die reversionstypischen **Prüfungszyklen** verwendet werden, die üblicherweise im jeweiligen Unternehmen gemäß Risikoeinordnung (s. „Priorisierung“ oben) verwendet werden, (i.d.R. je nach Risiko alle 1-3 Jahre).

Sinnvoll ist auch die Erarbeitung eines **Prüfkonzepts**, das sowohl Kontrollen als Auftraggeber als auch Kontrollen als Auftragnehmer enthält und somit zur Sicherstellung der Erst- und auch der laufenden Kontrollen dient.

6.2 Was soll kontrolliert werden?

Vor der Prüfung sind Festlegungen erforderlich, **welche Art der Kontrollen** vorgesehen sind und wie man diese prüfungstechnisch abbilden möchte.

Insbesondere bei der laufenden Kontrolle sind auch **Teil- und Schwerpunktprüfungen** denkbar.

6.3 Wer soll kontrollieren?

Nach dem Gesetzestext hat der Auftraggeber sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. In der Regel delegiert der Auftraggeber die Aufgabe auf die **Fachabteilung**, die für den Prozess und für das interne Kontrollsystem verantwortlich ist.

Nach der Gesetzesbegründung ist eine persönliche oder Vorort-Kontrolle jedoch nicht zwingend erforderlich. Eine schriftliche Auskunft des Auftragnehmers kann ausreichen, wenn diese im Rahmen der Erstkontrolle auf Plausibilität geprüft wird. Gut geeignet ist auch die Vorlage eines Testats bzw. Zertifikats eines Sachverständigen (z.B. Interne Revision oder der Datenschutzbeauftragte des Auftragnehmers, Externe Prüfer).

Wir empfehlen bei persönlicher Prüfung eine gestufte Beteiligung des betrieblichen Datenschutzbeauftragten. Bei ADV mit geringer Sensibilität beispielsweise ist eine Kontrolle durch die Fachseite nach Vorgaben, z.B. in Form von Checklisten möglich. Bei ADV mit mittlerer Sensibilität ist die Kontrolle mit unmittelbarer Unterstützung durch den **Datenschutzbeauftragten** empfehlenswert. Bei Datenverarbeitungen mit hoher Sensibilität ist eine Kontrolle unter Beteiligung des Datenschutzbeauftragten und (ggf. externer) Sachverständiger fast unumgänglich.

7. PRAKTISCHE FRAGESTELLUNGEN: DOKUMENTATION

Was sollte die Dokumentation zur Prüfung beinhalten?

Die **Dokumentation** zur Prüfung von ADV sollte folgende Informationen enthalten:

- Angaben zu den **Beteiligten** (Verfahrensverantwortlicher, konkreter Prüfer, DSB, CIO)
- Angaben zur betroffenen **ADV** (AN, Beginn/Ende, Art der ADV, Sensibilität, wo wird ADV-Vertrag vorgehalten?)
- Angaben zur **Kontrolle** (Wann, Wo, Prüfer, Erstkontrolle/ laufende Kontrolle, Zeitpunkt der letzten Kontrolle)
- Art und **Umfang** der Kontrolle (vor Ort, schriftlich, vollständig, Schwerpunktprüfung)
- **Feststellungen** (vertragliche, gesetzliche, techn. organisatorische Anforderungen: eingehalten/nicht eingehalten?; sonstige Verstöße; Verfahrensmeldung aktuell/zu überarbeiten)
- Weitere **Maßnahmen** (Zeitpunkt der nächsten Kontrolle/Nachkontrolle)
- **Name des Prüfers, ggf. Unterschrift**