Bayerisches Landesamt für Datenschutzaufsicht

in der Regierung von Mittelfranken

Auftragsdatenverarbeitung nach § 11 BDSG
- Gesetzestext mit Erläuterungen -

Stand: Dezember 2009

Impressum:
Bayerisches Landesamt für Datenschutzaufsicht in der Regierung von Mittelfranken
Promenade 27
91522 Ansbach

Telefon: (0981) 53-0
Telefax: (0981) 53-5301
E-Mail: datenschutz@reg-mfr.bayern.de
Internet: http://www.regierung.mittelfranken.bayern.de

§ 11 Absatz 1 BDSG

(1) Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§ 6, 7 und 8 genannten Rechte sind ihm gegenüber geltend zu machen.

Erläuterungen:

Die verantwortliche Stelle bedient sich im Falle von § 11 einer anderen Stelle, die für sie im Auftrag und weisungsabhängig personenbezogene Daten erhebt, verarbeitet oder nutzt.

Es darf sich nur um datenverarbeitende Hilfsfunktionen nach Weisungen des Auftraggebers handeln, die z. B. in einem Rechenzentrum, einem Direktwerbeunternehmen, einem Callcenter, einem Systembetreuungsunter-nehmen, einem Datenerfassungsbüro oder einem Datenträgerentsorgungs-unternehmen vorgenommen werden, und wo die insoweit betroffene Aufgabe/Funktion beim Auftraggeber verbleibt.

Beispiele:
- Lohnabrechnung durch ein Dienstleistungsrechenzentrum,
- Einscannen des schriftlichen Posteingangs durch einen Dienstleister,
- Werbeadressenpflege und -ausdruck sowie Werbepostversand durch einen Lettershop,
- Kontaktdatenerhebung durch ein Callcenter,
- Wartung/Fernwartung durch ein Softwarehaus,

usw.

Die Auftrag gebende Stelle bleibt im vollem Umfang für den Umgang mit ihren personenbezogenen Daten beim Dienstleister verantwortlich.

Datenbewegungen zwischen Auftraggeber und Auftragnehmer stellen keine Datenübermittlungen im Sinne des BDSG dar. Sie werden gesetzlich einer internen Nutzung gleichgestellt.

Gegensatz:

Übertragung einer Aufgabe (sog. Funktionsübertragung), die über eine datenverarbeitende Hilfsfunktion hinausgeht, zur eigenverantwortlichen Wahrnehmung durch eine andere Stelle.

Beispiele:
- Personalverwaltung durch ein zentrales Konzernunternehmen,
- Buchhaltung und Steuerberatung durch einen Steuerberater,
- Kontoführung durch eine Bank,
- Versicherungsbetreuung/-beratung durch selbständige Handelsvertreter,

etc.

Die Zulässigkeit der dabei gegebenen Datenübermittlungen ist an Hand der allgemeinen Vorschriften des BDSG (§ 4 Abs. 1 BDSG) zu beurteilen.

§ 11 Absatz 2 Satz 1 und Satz 2 BDSG

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen **sorgfältig auszuwählen**. Der Auftrag ist **schriftlich** zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:

1. der Gegenstand und die Dauer des Auftrags,

Erläuterungen:

Gegenstand:

Lohnabrechnung, Finanzbuchhaltung, Werbeaussendungen, Callcenterdienste, Telefonwerbung, Kundenbefragungen im Auftrag, Videoüberwachung im Auftrag, Internet-Providing, E-Mail-Account, DV-System-Betreuung, Wartung/Fernwartung, Datenträgerentsorgung usw.

Dauer:

einmalig, befristet bis ..., unbefristet mit Kündigungsmöglichkeit ab ...

2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,

Erläuterungen:

a) Umfang, Art, Zweck

- Welche Leistungen sind im einzelnen zu erbringen (Leistungsverzeichnis, Pflichtenheft).
- Auftragsdatenverarbeitung nur im Inland, auch im EU-/EWR-Bereich oder auch in Drittstaaten.
- Welche Leistungsphasen sollen außer Haus gegeben werden.
- Vorübergehende oder dauernde Speicherung von Daten beim Dienstleister.
- Welche Menge an Daten, Datensätzen, Datenträgern.
- Umfang und Dauer einer Videoüberwachung.
- Nur Verwendung von Telefondaten oder E-Mail-Adressen mit einem nachweisbaren Werbe-Opt-In

usw.

b) Art der Daten

Personaldaten, Vertragsdaten/Bestelldaten, Werbedaten, Werbewidersprüche, Befragungsergebnisse, Gesundheitsdaten, Videoaufzeichnungsdaten, Nutzungsdaten aus Telemediendiensten oder Telekommunikationsdiensten, Telefongesprächsaufzeichnungen, DV-Protokollierungsdaten, usw.

c) Kreis der Betroffenen

Mitarbeiter, Stellenbewerber, Kunden, Interessenten, Lieferanten, Werbekontakte, Besucher/Gäste, Passanten, Systemnutzer usw.

3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,

Erläuterungen:

Vgl. im Einzelnen die Anlage zu § 9 Abs. 1 BDSG, wobei die Maßnahmen konkret sachverhaltsbezogen anzusprechen sind, z. B.

- Festlegung der Transportwege und -verfahren für die Daten (manuell, elektronisch) mit den dabei zu treffenden Sicherheitsmaßnahmen.

- Technische Vorsorgemaßnahmen zur Ausfallsicherheit (Ersatzrechenzentrum, Notfalleinrichtungen).

- Verfahrensweise zur Trennung der Daten verschiedener Auftraggeber.

- Festlegungen zu Protokollierungen der Verarbeitungen beim Dienstleister und zu Sicherheitsspeicherungen/Backup, sichere Lagerung solcher Datenträger.

- Festlegungen zur Aufbewahrung von zu entsorgenden Datenträgern und der Sicherheitsstufe für die Löschung/Vernichtung.

- Regelungen zum Technik-Einsatz in Callcentern zum Schutz vor Datenunterschlagungen.

4. die Berichtigung, Löschung und Sperrung von Daten,

Erläuterungen:

- Mitwirkung des Dienstleisters bei Anträgen von Betroffenen an den Auftraggeber nach § 35 BDSG.
- Führung von Werbesperrlisten für den Auftraggeber.

- Sperrung oder Löschung von Daten nach Abarbeitung von Einzel-Dienstleistungen, sichere Löschverfahren.

- Löschungsfristen für Daten bei Videoüberwachung, für Nutzungsdaten beim Internet- oder E-Mail-Provider.

usw.

5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,

Erläuterungen:

Aus § 11 Abs. 4 BDSG sind insoweit folgende Vorschriften relevant:

§ 5 BDSG – Datengeheimnis

§ 9 BDSG – Datensicherheit

§ 4f, § 4g BDSG – Datenschutzbeauftragter

z. B.

- Verpflichtung der Beschäftigten des Dienstleisters auf das Datengeheimnis (einschließlich entsprechender Belehrung) und Bestellung eines Datenschutzbeauftragten beim Dienstleister, Name und Kontaktdaten des Datenschutzbeauftragten.
- Kontrollmaßnahmen beim Dienstleister (dessen Revision, dessen Datenschutzbeauftragter, externe Auditierungen) zur Einhaltung des Datenschutzes und der Datensicherheit, Prüfungsberichte.
- Kontrolle der Arbeitsergebnisse durch den Dienstleister.
- Kontrollen des Dienstleisters bei Subunternehmen.

6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,

Erläuterungen:

Z. B.

- Subunternehmerbeauftragungen unzulässig bzw. unter welchen Bedingungen und nach vorheriger Genehmigung durch den Auftraggeber zulässig, Namhaftmachung der Subunternehmer.

- Subunternehmer nur aus dem Inland, auch aus dem EU-/EWR-Raum oder auch aus Drittstaaten.

- Subunternehmer für welche Zwecke, in welchem Fall, in welchem Umfang, auch Sub-Subunternehmer.

Als Datenverarbeitung von Subunternehmen werden nicht sog. notwendige Nebenleistungen von Externen beim Dienstleister angesehen, wie Reinigungsleistungen, Telekommunikationsleistungen, Wartungsarbeiten etc.

7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,

Erläuterungen:

- Umfang der Kontrollrechte, mit bzw. ohne Vorankündigung.

- Insoweit vom Dienstleister einzuräumende Duldungs- und Mitwirkungspflichten.

- Kontrollen vor Ort beim Dienstleister und auch bei eventuellen Subunternehmen.

- Wer führt welche Kontrollen von Seiten des Auftraggebers durch (Fachbereiche, Revision, Datenschutzbeauftragter, externe Sachverständige) und wer wirkt beim Dienstleister mit (Ansprechpartner).

- Einsichtsrechte des Auftraggebers in DV-Protokolle, in Berichte der Revision und des Datenschutzbeauftragten des Dienstleisters, in externe Audits für den Dienstleister.

- Mitlesen am Kontrollbildschirm bei Fernwartung.

- Kontrolle des Opt-In bei Werbemaßnahmen.

- Zutrittsrechte in Privatwohnungen bei Telearbeit/Heimarbeit.

usw.

8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,

Erläuterungen:

Neuer Regelungsbereich in § 11 Abs. 2 BDSG wegen der neuen Verpflichtungen des Auftraggebers aus § 42a BDSG (Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten).
Z. B.

- Welche Art, welcher Grad von Verstößen ist mitzuteilen (Fehlversendungen, verlorengegangene Datenträger, unterschlagene Daten, Zugangsberechtigungs-/Passwortoffenlegungen usw.).

- Nicht nur Verstöße des Auftraggebers und seiner Beschäftigten, sondern auch rechtswidrige Handlungen von Dritten (Subunternehmer, Hacker, Einbrecher).

9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,

Erläuterungen:

- Einzelweisungen zur Auftragserledigung, zu (zusätzlichen) Sicherheitsmaßnahmen, zum Vorgehen bei Datenschutzverstößen.

- Weisungen zur Gestaltung bzw. Beendigung von Subunternehmerverhältnissen.

- Wer erteilt die Weisungen von Seiten des Auftraggebers und an wen sind die Weisungen beim Dienstleister zu richten, in welcher Form erfolgen die Weisungen

usw.

10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Erläuterungen:

- Was ist wann zurückzugeben und was ist wie zu löschen bzw. zu vernichten (elektronische Datenträger, Papierunterlagen).

- Weitere Verwendung von elektronischen Datenträgern

usw.

§ 11 Absatz 2 Satz 3 BDSG

Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden.

§ 11 Absatz 2 Satz 4 BDSG

Der Auftraggeber hat sich **vor Beginn der Datenverarbeitung und sodann regelmäßig** von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

Erläuterungen:

Die schon bisher bestehenden Kontrollpflichten des Auftraggebers gegenüber dem Dienstleister wurden dadurch herausgehoben, dass der Auftraggeber

einerseits vor Beginn der Datenverarbeitung und

andererseits anschließend regelmäßig

beim Dienstleister die Einhaltung der gebotenen Sicherheitsmaßnahmen zu prüfen hat.

Zuständig für diese Prüfungen ist die Leitung der verantwortlichen Stelle, die daraus bestimmte Prüfungsaufgaben je nach Art den Fachabteilungen, der Revision, ihrem Datenschutzbeauftragten oder auch einem externen Sachverständigen übertragen kann.

Vor-Ort-Kontrollen werden nach der Gesetzesbegründung zu der BDSG-Änderung 2009 nicht allgemein erwartet, sondern es können im Einzelfall auch ein vom Dienstleister vorgelegtes schlüssiges Datensicherheitskonzept oder ein dort durchgeführtes externes Audit genügen.

Bei bekannten/großen Rechenzentren, Dienstleistern und Systemhäusern, Internet-/E-Mail-Providern, mit gutem Ruf können Vor-Ort-Prüfungen eher entfallen als bei kleineren/unbekannten Callcentern, Direktwerbeunternehmen oder Datenträgerentsorgern.

Für den Prüfungsturnus in laufenden Auftragsverhältnissen können je nach Sachverhalt Prüfungsfristen zwischen ein und drei Jahren angemessen sein, wobei auch die öffentliche Berichterstattung zu Datenschutzverletzungen sowie eigene und fremde Erfahrungen mit einem Dienstleister bzw. einer Branche berücksichtigt werden sollten.

§ 11 Absatz 2 Satz 5 BDSG

Das Ergebnis ist zu **dokumentieren**.

Erläuterungen:

Besonders wichtig ist, die Ergebnisse der Prüfungsüberlegungen und von konkreten Prüfungen angemessen zu dokumentieren, zum einen für eigene Verantwortlichkeits- und Haftungsfragen des Auftraggebers, zum anderen für Kontrollen der Datenschutzaufsichtsbehörden, anderen Aufsichts- und Prüfungsinstitutionen oder Nachfragen des Betriebsrats.

§ 11 Absatz 3 BDSG

(3) Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

§ 11 Absatz 4 BDSG

(4) Für den Auftragnehmer gelten neben den **§§ 5, 9, 43** Abs. 1 Nr. 2, 10 und 11, Abs. 2 Nr. 1 bis 3 und Abs. 3 sowie **§ 44** nur die Vorschriften über die Datenschutzkontrolle oder die Aufsicht, und zwar für

1. a) öffentliche Stellen,
   b) nicht-öffentliche Stellen, bei denen der öffentlichen Hand die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht und der Auftraggeber eine öffentliche Stelle ist,

   die §§ 18, 24 bis 26 oder die entsprechenden Vorschriften der Datenschutzgesetze der Länder,

2. die übrigen **nicht-öffentlichen Stellen**, soweit sie personenbezogene Daten im Auftrag als Dienstleistungsunternehmen geschäftsmäßig erheben, verarbeiten oder nutzen,

   die **§§ 4f, 4g und 38**.

§ 11 Absatz 5 BDSG

(5) Die Absätze 1 bis 4 gelten entsprechend, wenn die **Prüfung oder Wartung** automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Hinweis:

Formulierungsvorschläge für Vertragsregelungen nach § 11 Abs. 2 BDSG finden sich z. B. unter

http://www.rp-darm-stadt.hessen.de/irj/servlet/prt/portal/prtroot/slimp.CMReader/HMdI_15/RPDA_Internet/med/c76/c7640de8-bd84-0421-b30b-cd44e9169fcc,22222222-2222-2222-2222-222222222222,true.doc

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

http://www.bitkom.org/de/publikationen/38336_45940.aspx