



Auftragsdatenverarbeitung nach § 11 BDSG

- Gesetzestext mit Erläuterungen
- Formulierungshilfe für datenschutzrechtliche Vertragsregelungen
- Kurz-Prüfliste Merkmale für die Abgrenzung

Herausgeber:

Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27
91522 Ansbach

Telefon: (0981) 53 - 1300
Telefax: (0981) 53 - 5300
E-Mail: poststelle@lda.bayern.de
Webseite: www.lda.bayern.de

Stand: März 2016

§ 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. Die Auftrag gebende Stelle bleibt im vollen Umfang für den Umgang mit ihren personenbezogenen Daten beim Dienstleister verantwortlich. Datenbewegungen zwischen Auftraggeber und Auftragnehmer stellen keine Datenübermittlungen im Sinne des BDSG dar (vgl. insoweit § 3 Abs. 8 Satz 3 BDSG). Sie werden gesetzlich einer internen Nutzung gleichgestellt und insoweit privilegiert.

Es darf sich dabei nur um datenverarbeitende **Hilfsfunktionen** nach Weisungen des Auftraggebers handeln, wobei die insoweit betroffene Aufgabe/Funktion beim Auftraggeber verbleibt. Die Hilfstätigkeit bzw. dv-technische Unterstützung muss im Kern die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten betreffen, und nicht Dienstleistungen völlig anderer Art. Siehe auch Urteil des OLG Düsseldorf vom 13.02.2015, Az. I-16 U41/14: „Wahrnehmung bloßer technischer Hilfsfunktionen“.

Was ist Auftragsdatenverarbeitung im Sinne von § 11 BDSG?

Auftragsdatenverarbeitung sind regelmäßig z. B. folgende Dienstleistungen

- die dv-technischen Arbeiten für die Lohn- und Gehaltsabrechnungen oder die Finanzbuchhaltung,
 - Outsourcing personenbezogener Datenverarbeitung im Rahmen von Cloud-Computing,
 - die Werbeadressenverarbeitung in einem Lettershop,
 - die Kontaktdatenerhebung durch ein Callcenter,
 - die Auslagerung eines Teils des eigenen Telekommunikationsanlagenbetriebs (soweit nicht TKG),
 - die Auslagerung der E-Mail-Verwaltung oder von sonstigen Datendiensten zu Webseiten,
 - die Datenerfassung, die Datenkonvertierung oder das Einscannen von Dokumenten,
 - die Backup-Sicherheitspeicherung und andere Archivierungen,
 - die Datenträgerentsorgung,
- usw.

Wenn an einen Dienstleister nicht nur der datenverarbeitungstechnische Umgang mit personenbezogenen Daten des Auftraggebers übertragen worden ist, sondern in eng eingegrenztem Umfang weitere **weisungsgebundene** Hilfeleistungen anderer Art (z. B. die technische Organisation von Dienstreisen oder Versetzungen, Callcenter-Tätigkeiten), kann der Umgang mit den personenbezo-

genen Daten des Auftraggebers unter Umständen ebenfalls noch als Auftragsdatenverarbeitung nach § 11 BDSG eingeordnet werden, wenn der Umgang mit den vom Auftraggeber überlassenen Daten beim Dienstleister vertraglich streng weisungsgebunden festgelegt ist.

Für die **Prüfung oder Wartung (z. B. Fernwartung, externer Support)** automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen gelten kraft Gesetzes (§ 11 Abs. 5 BDSG) die Regelungen zur Datenverarbeitung im Auftrag nach § 11 BDSG **entsprechend**, wenn bei diesen Tätigkeiten ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Was ist keine Auftragsdatenverarbeitung im Sinne von § 11 BDSG?

Keine Auftragsdatenverarbeitung sind z. B.

- die Auslagerung von Aufgaben/Funktionen oder
- die externe Inanspruchnahme von Fachleistungen, wie Personalverwaltung, Mitarbeiterrekrutierung, Vertragskundenbetreuung, Finanzberatung, Steuerberatung, Unternehmensberatung, Wirtschaftsprüfung, Inkassotätigkeit mit Forderungsübertragung, Sachverständigen- bzw. Gutachterbeauftragung, usw. an/von einem Dritten (auch verbundenes Unternehmen) mit dort eigenverantwortlicher Wahrnehmung.

Dies geht über DV-Hilfstätigkeiten bzw. dv-technische Unterstützungen hinaus und betrifft extern in Anspruch genommene fachlich-intellektuelle Tätigkeiten von Spezialisten; die hierzu notwendige Weitergabe von Daten durch die verantwortliche Stelle bedarf einer speziellen Rechtsgrundlage nach § 4 Abs. 1 BDSG (entweder § 28 Abs. 1 Satz 1 Nrn. 1 und 2 BDSG mit transparenter Information der Betroffenen oder Einwilligung der Betroffenen).

Die insoweit mit dem Aufgabenübernehmer zu treffenden vertraglichen Vereinbarungen müssen im Hinblick auf die zu berücksichtigenden Interessenlagen der betroffenen Personen und die Zweckbindung für die Daten (vgl. § 28 Abs. 5 BDSG) oft einen ähnlichen Inhalt wie Verträge nach § 11 BDSG haben.

Keine Auftragsdatenverarbeitung im Sinne von § 11 BDSG sind auch

extern in Anspruch genommene Tätigkeiten, die im eigentlichen Kern nicht den Umgang (Erhebung, Verarbeitung, Nutzung) mit personenbezogenen Daten betreffen, sondern in denen andere Dienstleistungsschwerpunkte im Vordergrund stehen und der dabei notwendigerweise mit verbundene Kontakt mit personenbezogenen Daten nur ein unvermeidliches "Beiwerk" darstellt, oder eine Kenntnisnahme personenbezogener Daten bei der Leistungserbringung nicht ausgeschlossen ist.

Beispiele:

- Transportleistungen von Post- oder Kurierdiensten
- Transportleistungen von öffentlichen Telekommunikationsdiensten
- Bankdienstleistungen als "Verwaltungs- und Transportleistungen von Geld"
- Bewachungsdienste
- Reinigungsdienstleistungen
- Handwerkereinsätze in Unternehmen

Wenn hier keine besonderen gesetzlichen oder vertraglichen Geheimhaltungsverpflichtungen bestehen, wie Postgeheimnis, Telekommunikations-/Fernmeldegeheimnis, Bankgeheimnis, ist eine spezielle Geheimhaltungsverpflichtung des Arbeitgebers der externen Personen (Bewachungs-/Reinigungspersonal, Handwerker etc.) notwendig, die sich inhaltlich an der Verpflichtung auf das Datengeheimnis nach § 5 BDSG orientieren kann. Je nach Sachverhalt kann im Hinblick auf die zu berücksichtigenden Interessenlagen der betroffenen Personen und auf die Zweckbindung für die Daten (vgl. § 28 Abs. 5 BDSG) auch eine vertragliche Vereinbarung mit dem Leistungserbringer nach den Grundsätzen von § 11 BDSG geboten sein (z. B. bei privaten Kurierdiensten).

§ 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 (fehlt eine schriftliche Auftragserteilung, so dürfen keine Daten an den Auftragnehmer weitergegeben werden, siehe Urteil des VG Wiesbaden vom 20.01.2015, Az. 6 K 1567/14.WI), wobei insbesondere im Einzelnen festzulegen sind:*

1. Gegenstand und die Dauer des Auftrags

Erläuterungen:

a) Gegenstand:

Lohnberechnung, Adressenverarbeitung, Datenerhebung, DV-System-Betreuung, Wartung/Fern-wartung, Datenträgerentsorgung, usw.

b) Dauer:

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

2. Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, Art der Daten und 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
 - Datenmenge, Anzahl der Datensätze und Datenträger
 - Nur Verwendung von Telefondaten oder E-Mail-Adressen für Werbung mit einem nachweisbaren Werbe-Opt-In
- usw.

b) Art der Daten:

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

c) Kreis der Betroffenen

Mitarbeiter, Stellenbewerber, Kunden, Interessenten, Lieferanten, Werbekontakte, Systemnutzer, usw.

3. Nach § 9 zu treffende technische und organisatorische 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 Sicherheits-speicherungen/Backup, sichere Lagerung solcher Datenträger
- Festlegungen zur Aufbewahrung der zu entsorgenden Datenträger und der Sicherheitsstufe für die Löschung/Vernichtung
- Regelungen zum Technik-Einsatz in Callcentern zum Schutz vor Datenunterschlagungen

4. Berichtigung, Löschung und Sperrung von Daten

Erläuterungen:

- Sperrung oder Löschung von Daten nach Abarbeitung von Einzel-Dienstleistungen, sichere Lösungsverfahren
- Mitwirkung des Dienstleisters bei Anträgen von Betroffenen an den Auftraggeber nach § 34 oder § 35 BDSG

5. Nach Absatz 4 bestehende 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

Beispiele:

- 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. Etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen

Erläuterungen:

- Subunternehmerbeauftragungen unzulässig bzw. unter welchen Bedingungen und nach vorheriger Genehmigung durch den Auftraggeber zulässig
- Subunternehmer nur aus dem Inland, auch aus dem EU-/EWR-Raum oder auch aus Drittstaaten
- welche Subunternehmer (Namhaftmachung der Subunternehmer) für welche Zwecke, in welchem Fall, in welchem Umfang, auch Sub-Subunternehmer

7. Kontrollrechte des Auftraggebers und entsprechende 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:

Unterrichtung des Auftraggebers wegen dessen Verpflichtung aus § 42a BDSG und § 15a TMG (Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten).

Beispiele:

- Welche Art, welcher Grad von Verstößen ist mitzuteilen (Fehlversendungen, verlorengangene Datenträger, unterschlagene Daten, Datenhacking, Zugangsberechtigungs-/Passwort-offenlegungen usw.)
- Nicht nur Verstöße des Auftragnehmers und seiner Beschäftigten, sondern auch rechtswidrige Handlungen von Dritten (Subunternehmer, Hacker, Einbrecher)

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

Erläuterungen:

Weil der Auftraggeber für die an einen Auftragnehmer nach § 11 BDSG ausgelagerten Arbeiten weiterhin verantwortlich nach dem BDSG bleibt, muss er sich ein umfassendes Weisungsrecht einräumen lassen.

Beispiele:

- Einzelweisungen zur Auftrags erledigung, 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

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

Erläuterungen:

Bei einer Auftragsvergabe nach § 11 BDSG muss auch an das Ende der Vertragsbeziehung gedacht und müssen entsprechende Regelungen dazu getroffen werden.

Beispiele:

- Was ist wann zurückzugeben und was ist wie zu löschen bzw. zu vernichten (elektronische Datenträger, Papierunterlagen)
- Weitere Verwendung von elektronischen Datenträgern

§ 11 Absatz 2 Satz 3 BDSG

Enthält Regelung für öffentliche Stellen.

§ 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 Kontrollpflichten des Auftraggebers gegenüber dem Dienstleister beziehen sich darauf, 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 Rechenzentren, Dienstleistern und Systemhäusern mit gutem Ruf können Vor-Ort-Prüfungen eher entfallen als bei bisher unbekanntem 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 es, die Ergebnisse der Prüfungsüberlegungen sowie der eigentlichen Prüfungen angemessen zu dokumentieren. Dies nützt zum einen bei Verantwortlichkeits- und Haftungsfragen des Auftraggebers, zum anderen bei 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.

Erläuterungen:

Wegen der grundsätzlich strikten gesetzlichen Bindung des Auftragnehmers an Weisungen des Auftraggebers stellt sich die Frage, wie sich der Auftragnehmer bei Zweifeln an der Rechtmäßigkeit von bestimmten Auftraggeber-Weisungen verhalten muss.

§ 11 Abs. 3 Satz 2 BDSG gibt dem Auftragnehmer eine Hinweispflicht auf seine Zweifel an der Rechtmäßigkeit einer Weisung auf.

Besteht in einem solchen Fall der Auftraggeber trotz des Hinweises auf der fraglichen Weisung, trifft den Auftragnehmer insoweit regelmäßig keine weitere Verantwortlichkeit.

§ 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**.*

Erläuterungen:

Auch wenn bei einer Datenverarbeitung im Auftrag nach § 11 BDSG der Auftraggeber die verantwortliche Stelle bleibt, treffen den Auftragnehmer bestimmte Rahmenregelungen des BDSG, nämlich

- § 5, Datengeheimnis, Verpflichtung,
- § 9, zu treffende technische und organisatorische Sicherheitsmaßnahmen,
- bestimmte Bußgeld- und Strafvorschriften aus § 43 und § 44 BDSG,
- §§ 4f und 4g, Bestellung und Tätigkeit eines Datenschutzbeauftragten und
- § 38 mit den Regelungen zur Aufsichtsbehörde.

§ 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.*

Erläuterungen:

Wie oben zu § 11 Abs. 1 schon dargelegt, bezieht das BDSG die Sachverhalte der Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen (einschließlich Support, Softwaretests usw.) kraft Gesetzes mit ein, wenn dabei ein Zugriff auf personenbezogenen Daten nicht ausgeschlossen werden kann, auch wenn hier die Zielrichtung des Auftrags gar nicht auf die Verarbeitung personenbezogener Daten geht.

Formulierungshilfe für datenschutzrechtliche Vertragsregelungen nach § 11 BDSG:

Auftraggeber:

Auftragnehmer:

1. Gegenstand und Dauer der Vereinbarung

Der Auftrag umfasst Folgendes:

(Gegenstand des Auftrages, konkrete Beschreibung der Dienstleistungen)

Der Auftragnehmer erhebt / verarbeitet / nutzt dabei personenbezogene Daten im Auftrag des Auftraggebers nach § 11 BDSG.

oder

Bei Durchführung des Auftrags kann der Auftragnehmer mit personenbezogenen Daten in Berührung kommen. (z. B. bei Systembetreuung/Support oder Wartung/Fernwartung, § 11 Abs. 5 BDSG)

Dauer des Auftrags

Der Vertrag beginnt am und endet am

oder

wird auf unbestimmte Zeit geschlossen. Kündigungsfrist ist

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

2. Umfang, Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung:

(nähere Beschreibung, ggf. Verweis auf Leistungsverzeichnis als Anlage etc.)

Art der Daten:

Kreis der Betroffenen:

3. Technische und organisatorische Maßnahmen nach § 9 BDSG

Für die auftragsgemäße Verarbeitung personenbezogener Daten nutzt der Auftragnehmer schwerpunktmäßig folgende DV-Technik und Softwareprodukte:

Die im Anhang beschriebenen Datensicherheitsmaßnahmen/Das als Anlage beigefügte Datensicherheitskonzept des Auftragnehmers werden/wird als verbindlich festgelegt.

Der Auftragnehmer beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

Die Datensicherheitsmaßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden.

Wesentliche Änderungen sind vom Auftragnehmer mit dem Auftraggeber schriftlich abzustimmen.

4. Regelungen zur Berichtigung, Löschung und Sperrung von Daten

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder zu sperren, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechnigte Interessen des Auftragnehmers dem nicht entgegenstehen.

5. Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers. Der Auftragnehmer verwendet die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Eingang und Ausgang werden dokumentiert.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Auftraggeber abzustimmen.

Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

Der Auftragnehmer hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber insbesondere folgende Kontrollen in seinem Bereich durchzuführen:

Das Ergebnis der Kontrollen ist zu dokumentieren.

An der Erstellung der Verfahrensverzeichnisse des Auftraggebers hat der Auftragnehmer mitzuwirken.

Er hat die erforderlichen Angaben dem Auftraggeber zuzuleiten.

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der

Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Sicherheitskontrollen vor Ort.

Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt. Hierzu wird bis auf weiteres folgendes vereinbart:

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit) ist nur mit Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen.

Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften des BDSG bekannt sind. Der Auftragnehmer bestätigt, dass ihm auch folgende datenschutzrechtliche Vorschriften bekannt sind:

Der Auftragnehmer verpflichtet sich, bei der auftragungsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers das Datengeheimnis zu wahren.

Er verpflichtet sich, auch folgende Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen:

(z. B. Bankgeheimnis, Fernmeldegeheimnis, Sozialgeheimnis, etc.)

Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und sie auf das Datengeheimnis schriftlich verpflichtet. Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Weisung oder Zustimmung durch den Auftraggeber erteilen.

Beim Auftragnehmer ist als Beauftragte(r) für den Datenschutz Herr/Frau

.....
(Vorname, Name, Organisationseinheit, Telefon)

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

oder

Ein betrieblicher Datenschutzbeauftragter ist beim Auftragnehmer nicht bestellt, da die gesetzliche Notwendigkeit für eine Bestellung nicht vorliegt.

6. Unterauftragsverhältnisse

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist nur mit schriftlicher Zustimmung des Auftraggebers zugelassen. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von § 9 BDSG sorgfältig auswählt.

Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, angemessene Kontrollen vor Ort bei Subunternehmern durchzuführen oder durch beauftragte Dritte durchführen zu lassen.

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach § 11 BDSG erfüllt hat.

Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) regelmäßig wie folgt zu überprüfen:

.....
.....
.....

Das Ergebnis der Überprüfungen ist zu dokumentieren.

Zurzeit sind für den Auftragnehmer die in Anlage mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden. Kommt bei einem künftig geplanten neuen Subunternehmer-Einsatz keine Einigung zustande, hat der Auftraggeber ein außerordentliches Kündigungsrechts dieses Vertrags.

7. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Datenerhebung / -verarbeitung / -nutzung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich festzulegen.

Der Auftraggeber erteilt alle Aufträge oder Teilaufträge in der Regel schriftlich. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.

Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

8. Weisungsberechtigte des Auftraggebers

Weisungsberechtigte Personen des Auftraggebers sind:

(Vorname, Name, Organisationseinheit, Telefon)

Weisungsempfänger beim Auftragnehmer sind:

(Vorname, Name, Organisationseinheit, Telefon)

Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitzuteilen.

9. Mitteilungspflichten des Auftragnehmers

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregel-

mäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Informationspflichten des Auftraggebers nach § 42 a BDSG sowie § 15a TMG. Der Auftragnehmer sichert zu, den Auftraggeber bei seinen Pflichten nach § 42 a BDSG zu unterstützen.

10. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags

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

dem Auftraggeber auszuhändigen.

oder

wie folgt datenschutzgerecht zu löschen bzw. zu vernichten:

Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich zu bestätigen.

11. Vergütung

12. Haftung

Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung schuldhaft verursachen.

Für den Ersatz von Schäden, die ein Betroffener wegen einer nach dem BDSG oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber dem Betroffenen verantwortlich. Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff beim Auftragnehmer vorbehalten.

13. Vertragsstrafe

Bei Verstoß des Auftragnehmers gegen die Abmachungen dieses Vertrages, insbesondere gegen die Einhaltung des Datenschutzes, wird eine Vertragsstrafe von Euro vereinbart.

14. Sonstiges

Beispiele:

Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

Für Nebenabreden ist die Schriftform erforderlich.

Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Unterschriften

Auftraggeber

Auftragnehmer

Hinweis:

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

- http://www.datenschutz.hessen.de/mustervereinbarung_auftrag.htm
- <https://www.gdd.de/nachrichten/news/neues-gdd-muster-zur-auftragsdatenverarbeitung-gemas-a7-11-bdsg>
- <https://www.bitkom.org/Bitkom/Publikationen/Aktualisierte-Mustervertragsanlage-zur-Auftragsdatenverarbeitung.html>

Kurz-Prüfliste

Merkmale für die Abgrenzung einer Auftragsdatenverarbeitung nach § 11 BDSG von einer Aufgabenausgliederung/Funktionsübertragung bzw. einer externen Inanspruchnahme von Fachleistungen

Maßgebend für die Einordnung unter die gesetzlich privilegierte Auftragsdatenverarbeitung (keine nach BDSG zu prüfende Datenübermittlung) sind die objektiven Zwecke des Auftrags, nicht die subjektiven Vorstellungen der Vertragspartner.

A

B

Weisungsgebundene Datenerhebung, -verarbeitung oder -nutzung im Auftrag nach § 11 BDSG

Aufgabenausgliederung/Funktionsübertragung bzw. externe Inanspruchnahme von Fachleistungen mit Datenübermittlung nach § 4 Abs. 1 BDSG, § 28 BDSG etc.

Hilfs-/Unterstützungstätigkeit in it-technischer Hinsicht für die auftraggebende verantwortliche Stelle (siehe auch Urteil des OLG Düsseldorf vom 13.02.2015, Az. I-16 U 41/14: „bloße technische Hilfsfunktionen“).

Fachlich-intellektuelle Aufgabenwahrnehmung, über eine it-technische Unterstützung hinaus.

Auftragnehmer wird weisungsgebunden tätig.

Einbringung eigener fachlicher Kompetenz über reine IT-Leistungen hinaus, eigene Entscheidungskompetenz.

Auftragnehmer hat meist keinen direkten Kontakt und keine Vertragsbeziehung zu den Betroffenen (Ausnahme z. B. bei Datenerhebung im Auftrag, wie bei Interviewunternehmen für Forschungseinrichtungen).

In vielen Fällen auch Kontakt mit den Betroffenen (z. B. bei externer Personalverwaltung/-rekrutierung, bei Forderungsverkauf an Inkassounternehmen).

Auftragnehmer hat kein eigenes fachliches Interesse an den verarbeiteten personenbezogenen Daten.

Die personenbezogenen Daten dienen der Erfüllung der übernommenen bzw. angebotenen Fachaufgaben.

Auftragnehmer hat keine Verantwortlichkeit für die Daten zur Erfüllung der Betroffenenrechte (§§ 33 bis 35 BDSG).

Es besteht eine eigene Verantwortlichkeit für die Daten zur Erfüllung der Betroffenenrechte (§§ 33 bis 35 BDSG)