

BIETMANN

RECHTSANWÄLTE • FACHANWÄLTE • STEUERBERATER

# Dirk Strohmeinger Rechtsanwalt



## **Die Auftragsdatenverarbeitung**

Ein Jahr nach ihrer gesetzlichen Regulierung ...

# 10.10

Die Auftragsdatenverarbeitung

Ein Jahr nach ihrer gesetzlichen Regulierung ...

... hat sich erstaunlich wenig getan. Obwohl es sich um Regelungen handelt die überall dort, wo mit Daten gearbeitet wird, hohe praktische Relevanz haben und bei Nichtbeachtung weitreichende Konsequenzen drohen, ist auf breiter Linie zu beobachten, dass ein Problembewusstsein schlichtweg nicht entwickelt ist. Grund genug sich diesem Thema ausführlich zu widmen.

Die Auftragsdatenverarbeitung ist seit der am 01.09.2009 in Kraft getretenen Novelle des Bundesdatenschutzgesetzes in § 11 BDSG geregelt. Der Absatz 1 dieser Vorschrift lautet wie folgt:

*<sup>1</sup>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. <sup>2</sup>Die in den §§ 6, 7 und 8 genannten Rechte sind ihm gegenüber geltend zu machen.*

Die Vorschrift ist relativ einfach und versteht sich von selbst. Immer wenn personenbezogene Daten von jemand anderem erhoben, verarbeitet oder genutzt werden, als von demjenigen, dem diese Daten nach außen hin zuzuordnen sind, sind die Grundsätze der Auftragsdatenverarbeitung anzuwenden.

Wie weit der Begriff Auftragsdatenverarbeitung auszulegen ist, zeigt Absatz 5 der zitierten Vorschrift:

*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.*

Somit ist praktisch jede Dienstleistung betroffen bei der Datenbestände mit personenbezogenen Daten übermittelt werden, aber auf die auch theoretisch, das heißt noch nicht einmal bestimmungsgemäß zugegriffen werden kann. Es geht also nicht nur um beispielsweise das Callcenter, das Abrechnungcenter oder die Marketingagentur, die bestimmungsgemäß personenbezogene Daten

des Auftraggebers erhalten um hiermit zu arbeiten, sondern es geht auch um EDV-Dienstleister, denen Programmierungs- oder Wartungsaufträge erteilt werden und im Rahmen dieser Tätigkeit auf personenbezogene Daten im Datenbestand des Auftraggebers zugreifen können.

Der Begriff der personenbezogenen Daten ist ebenfalls weit auszulegen. Es gilt der Grundsatz der Bestimmbarkeit. Das heißt, Daten sind personenbezogen, wenn mit deren Hilfe eine Person bestimmbar ist. Hierunter fallen zwanglos Namen und E-Mail Adressen sowie die damit verknüpften Daten. Streitig ist im Moment noch die Frage, ob es sich bei IP-Adressen auch um personenbezogene Daten handelt. Der Verfasser geht davon aus, dass sich auch in der Rechtsprechung die Auffassung durchsetzen wird, dass es sich bei IP-Adressen um personenbezogene Daten handelt. Die derzeit gängige Praxis der Gerichte im weitgehend automatisierten Verfahren Beschlüsse zu erlassen, wonach Provider anhand der IP-Adressen die Daten der Anschlussinhaber zu benennen haben, lässt nicht den Schluss zu, dass es sich um anonyme Daten handelt. Ein weiteres Argument sind immer weitergehende automatisierte Verknüpfungsmöglichkeiten. Wenn es technisch möglich ist, dass bei dem Besuch einer Website erkannt werden kann, ob der Besucher Facebook Mitglied ist oder nicht, ist eine Anonymität von IP-Adresse nicht anzunehmen. Deshalb sind aus Sicht des Verfassers selbst dann die gesetzlichen Regelungen der Auftragsdatenverarbeitung anwendbar, wenn lediglich die Übermittlung und der Zugriff auf IP-Adressen betroffen sind.

Welche Konsequenzen ergeben sich nun aus der Anwendbarkeit des § 11 BDSG?

Das Gesetz schreibt Maßnahmen vor, die der Auftragnehmer zu ergreifen hat.

Diese Maßnahmen regelt Absatz 2 des § 11 BDSG sehr detailliert:

*<sup>1</sup>Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. <sup>2</sup>Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:*

- 1. der Gegenstand und die Dauer des Auftrags,*
- 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,*
- 3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,*
- 4. die Berichtigung, Löschung und Sperrung von Daten,*
- 5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,*
- 6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,*
- 7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,*
- 8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,*
- 9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,*
- 10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.*

Dies ist ein sehr umfangreicher Katalog, der nach meiner Beobachtung dazu führt, dass in der Praxis die Existenz der gesetzlichen Regelung schlichtweg ignoriert oder auf Formulare zurückgegriffen wird, die sich im Internet herunterladen lassen und zum Teil von mehr als zweifelhafter Qualität sind.

Einschlägige Formulare sind von Verbänden und eingetragenen Vereinen entwickelt worden und gaukeln dem Betrachter eine gefährliche Sicherheit vor. Mit den oft viele Seiten langen Vertragstexten, die alle Eventualfälle abdecken sollen, glaubt der Verwender alles richtig gemacht zu haben. Hierbei wird aber nicht beachtet, dass der Gesetzgeber eine gesonderte Vereinbarung für jeden Auftrag vorsieht. Schlichtweg unzulässig ist es deshalb die Regelungen in eigenen Allgemeinen Geschäftsbedingungen aufzunehmen. Ebenso unzulässig ist aber auch eine Zusatzvereinbarung zu verwenden, die Allgemeinen Geschäftsbedingungen gleicht kommt. Allgemeine Geschäftsbedingungen sind Vertragswerke, die für eine Vielzahl von Fällen vorformuliert sind. Die gängigen Vertragsmuster sind letztlich nichts anderes. Daran ändert sich auch nichts dadurch, dass manche Muster das Ankreuzen verschiedener Alternativen zulassen. Wobei an dieser Stelle nicht unerwähnt bleiben soll, dass ich nicht erst einmal erlebt habe, dass derartige Muster in wirtschaftlich bedeutsamen Projekten verwendet wurden und nicht ein einziges Kreuz gesetzt worden ist.

Im Ergebnis ist daher von der Verwendung von Mustervereinbarungen dringend abzuraten. Absatz 2 des § 11 BDSG beschreibt sehr genau, was in jedem Vertrag, dessen Inhalt eine Auftragsdatenverarbeitung ist (sein kann), zu vereinbaren ist. Dabei kommt es immer auf den konkreten Einzelfall an. **Die Datenschutznovelle aus dem Jahre 2009 erfordert, dass sich die Vertragspartner vertieft mit der Materie der Auftragsdatenverarbeitung auseinandersetzen und nicht lediglich ein weiteres Formular blind unterschreiben.**

Allein das Erfüllen aller gesetzlicher Erfordernisse in der schriftlich abzuschließenden Vereinbarung reicht jedoch nicht. In Satz 4 des § 11 Abs. 2 heißt es insoweit:

*<sup>4</sup>Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.*

Der Einzelfall bestimmt welche Maßnahmen erforderlich sind. Diese reichen von der Aufforderung des Vertragspartners seine Sicherheitsvorkehrungen schriftlich zu bestätigen bzw. nachzuweisen bis zur Pflicht regelmäßiger Vor-Ort-Kontrollen und der Beauftragung eines Sachverständigen zur Durchführung entsprechender Kontrollen. Hier gilt der Grundsatz, dass bei Verdachtsmomenten unverzüglich zu handeln ist, während sich die regelmäßigen Prüfungspflichten nach dem Umfang und der Bedeutung des Auftrages richten.

Was passiert schließlich, wenn die gesetzlichen Erfordernisse bei der Auftragsdatenverarbeitung nicht eingehalten werden? Diese Frage ist in § 43 BDSG geregelt. Hier heißt es insoweit:

- (I) *Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig ...*  
2b) *entgegen § 11 Absatz 2 Satz 2 einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt oder entgegen § 11 Absatz 2 Satz 4 sich nicht vor Beginn der Datenverarbeitung von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt, ...*
- (II) ...
- (III) <sup>1</sup>*Die Ordnungswidrigkeit kann im Fall des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Euro, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu dreihunderttausend Euro geahndet werden. <sup>2</sup>Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. <sup>3</sup>Reichen die in Satz 1 genannten Beträge hierfür nicht aus, so können sie überschritten werden.*

Mit anderen Worten: Ein Verstoß kann mit bis zu € 50.000,00 geahndet werden ganz gleich, ob er fahrlässig oder vorsätzlich begangen wurde. § 43 Abs.3 Satz 3 BDSG gibt jedoch auch die Möglichkeit über diesen Betrag hinaus zu gehen, wenn der wirtschaftliche Vorteil diese Summe übersteigt.

Außerdem kommen Schadensersatzansprüche der Dateninhaber in Betracht.

Die dargestellten Grundsätze gelten insgesamt für eine Auftragsdatenverarbeitung in Deutschland, in einem Land der Europäischen Union oder des Europäischen Wirtschaftsraumes. Eine Auftragsdatenverarbeitung in Drittstaaten (praktisch relevant USA) erfordert ohnehin die Zustimmung des Inhabers der personenbezogenen Daten und beinhaltet eine Fülle weiterer einzuhaltender Regularien.

Im Ergebnis ist festzuhalten:

- Die seit einem Jahr gültigen Regelungen zur Auftragsdatenverarbeitung sind weitgehend unbekannt, werden ignoriert oder falsch angewendet.
- Auftragsdatenverarbeitung erfordert eine vertiefte Auseinandersetzung mit der Materie aus tatsächlicher und juristischer Sicht.
- Die wirtschaftlichen Folgen mangelhafter Umsetzung sind gravierend.
- Datenschutzrechtliche Zuverlässigkeit kann als Qualitätsmerkmal ein Akquiseinstrument sein. Obwohl die gesetzlichen Pflichten den Auftraggeber treffen, kann auch der Auftragnehmer seine datenschutzrechtliche Zuverlässigkeit bewerben und mit rechtssicheren Vereinbarungen die Auftragsentscheidung erleichtern.

23.10.2010

Dirk Strohmeier

## **Dirk Strohmenger**

Rechtsanwalt

## **BIETMANN**

RECHTSANWÄLTE · WIRTSCHAFTSPRÜFER · STEUERBERATER

[dirk.strohmenger@bietmann.eu](mailto:dirk.strohmenger@bietmann.eu)

+49.221.925900.20 Telefon

+49.221.925900.52 Telefax

Skype: dirk.strohmenger

Martinstraße 22-24, D-50667 Köln

[www.bietmann.eu](http://www.bietmann.eu)

[www.strohmenger.bietmann.eu](http://www.strohmenger.bietmann.eu)