Seminararbeit

Auftragsdatenverarbeitung

|  |  |
| --- | --- |
| Hochschule: | FH Dortmund |
| Modul: | IT-Recht |
| Verfasser 1: | Ayana, Denis 7095563 |
| Verfasser 2: | Kappenberg, Gorden 7090778 |
| Verfasser 3: | Runge, Marvin 7092120 |
| Verfasser 4: | Schewtschuk, Nikita 7092122 |
| Abgabedatum: |  |

Inhaltsverzeichnis

[1. Einleitung - Schewtschuk 2](#_Toc505674525)

[2. Begriffserklärung - Schewtschuk 3](#_Toc505674526)

[Bundesdatenschutzgesetz 4](#_Toc505674527)

[Aufteilung des BDSG 4](#_Toc505674528)

[3. Auftragsdatenverarbeitung - Runge 5](#_Toc505674529)

[Kriterien zur Auftragsdatenverarbeitung 7](#_Toc505674530)

[Beispiele zur Auftragsdatenverarbeitung 8](#_Toc505674531)

[4. Haftung - Ayana 9](#_Toc505674532)

[Begriffserklärung BDSG 9](#_Toc505674533)

[Haftung nach BDSG 9](#_Toc505674534)

[Schadensersatz nach BDSG 9](#_Toc505674535)

[Schadensersatz bei automatisierter Datenverarbeitung durch öffentliche Stellen nach BDSG 9](#_Toc505674536)

[Bußgeld- und Strafvorschriften nach BDSG 9](#_Toc505674537)

[Begriffserklärung DS-GVO 10](#_Toc505674538)

[Haftung nach DS-GVO 10](#_Toc505674539)

[Geldbußen nach DS-GVO 10](#_Toc505674540)

[5. DSGVO - Schewtschuk 12](#_Toc505674541)

[DSGVO Änderrungen gegenüber BDSG 12](#_Toc505674542)

[6. Erläuterung des Vertrags - Kappenberg 15](#_Toc505674543)

[7. Quellen 19](#_Toc505674544)

[8. Anhang 20](#_Toc505674545)

# Einleitung *- Schewtschuk*

# Begriffserklärung *- Schewtschuk*

* **personenbezogene Daten**: Dazu gehören Beispielsweise Name, Adresse, Geburtstag, Telefonnummer, Kontodaten, E-Mail Adresse und KFZ-Kennzeichen. Grundsätzlich alle Daten, die zu einer bestimmten Person zurückführen können. Ab dem DSVGO gilt das auch für IP-Adressen.
* **Frage nach Rechtmäßigkeit**: Regelt wann eine Datennutzung, Datenerhebung oder Datenverarbeitung angebracht ist. Dabei wird von ausgegangen, dass alle genannten Datenoperationen rechtswidrig sind. Es sei denn, eine andere rechtliche Regelung erlaubt es.
* **Beweislastumkehr**: Kennt man normalerweise bei Verbrauchsgütern, oder bei Immobilien. Man kann sich die Beweislastumkehr leicht an einem Beispiel erklären: Person A kauft eine Immobilie von Unternehmen B. Nach dem Gefahrenübergang(Person unterzeichnet den Kaufvertrag) hat Person A die Immobilie gekauft. Wenn nun Mängel auftreten, gehen diese zu Lasten der Person A. Wenn aber die Mängel schwerwiegend sind und nach einer Abschätzung diese Mängel bereits vor dem Kauf der Immobilie vorhanden waren, liegt Unternehmen B nun in der Beweislastumkehr. Im Kontext des BDSG heißt dies: Wenn ein Unternehmen beschuldigt wird, seinen Pflichten in Sachen Datenschutz nicht nachzukommen, steht die Person die beschuldigt nicht in der Beweispflicht, sondern das Unternehmen.[umschulden-leicht.de]
* **Verbotsprinzip mit Erlaubnisvorbehalt**: Die Nutzung, Verarbeitung oder Speicherung von personenbezogenen Daten ist immer verboten. Es sei denn, eine andere Regelung erlaubt dies.
* **Datensparsamkeit und Datenvermeidung**: Das Sammeln von Daten ist auf das Minimalste zu reduzieren. Anwendungen dürfen nur so viel Daten verarbeiten/sammeln wie sie zum Betrieb brauchen.
* **Zweckbindung** Das Sammeln/Verarbeiten ist von Daten ist auf den angegebenen Zweck beschränkt.
* **Datenrichtigkeit** Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neusten Stand sein.(§35 BSDG)
* **Datensicherheit** //TODO[it-recht-kanzlei/DSGVO vs BDSG]

Ist ein gesuchter Begriff nicht aufgeführt, empfehlen wir den Art. 4 DSGVO (Begriffsbestimmung).

# Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz (BDSG) gilt in der Bundesrepublik Deutschland und ist somit ein Bundesgesetz. Seine ursprüngliche Fassung wurde am 27. Januar 1977 verfasst. Zu diesem Zeitpunkt(23. Januar 2018) gilt die Fassung vom 30. Juni 2017. Sie wird am 25. Mai 2018 von der europäischen DSGVO ersetzt. Auf diese werden wir im Kapitel DSGVO tiefer eingehen.

Den Zweck dieses Gesetzes fasst der §1 Absatz 1 BDSG zusammen:

Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. [§1 Absatz 1 BDSG]

Daraus schließt sich, dass das Gesetz sich hauptsächlich um die Regelungen und Umgang der personenbezogenen Daten beschäftigt. Dabei folgt das Gesetz zwei Grundprinzipien. Zu einem ist das es **Verbotsprinzip mit Erlaubnisvorbehalt** und zum anderen die **Datensparsamkeit und Datenvermeidung**.

# Aufteilung des BDSG

Das Gesetz ist in 6 Abschnitte unterteilt.

\* 1: Allgemeine und gemeinsame Bestimmungen (§§ 1 - 11)

\* 2: Datenverarbeitung der öffentlichen Stellen (§§ 12 - 26)

\* 3: Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen (§§ 27 - 38a)

\* 4: Sondervorschriften (§§ 39 - 42a)

\* 5: Schlussvorschriften (§§ 43 - 44)

\* 6: Übergangsvorschriften (§§ 45 - 48)

Wir gehen in dieser Arbeit hauptsächlich nur auf den ersten Abschnitt, Allgemeine und gemeinsame Bestimmungen, ein. //TODO

# Auftragsdatenverarbeitung *- Runge*

Eine Auftragsdatenverarbeitung liegt vor, wenn personenbezogene Daten eines Auftraggebers von einem Auftragnehmer erhoben, verarbeitet oder genutzt werden. Geschieht dies, muss ein entsprechender Vertrag nach § 11 Bundesdatenschutzgesetz abgeschlossen werden. Oft kommt es zu solchen Verträgen, wenn ein Unternehmen Aufgaben und Strukturen, wie zum Beispiel die Personalverwaltung, auf externe Dienstleister auslagert. (Outsourcing) Die Verantwortung für die ordnungsgemäße Datenverarbeitung bleibt hier jedoch bei dem Auftraggeber und dieser ist verpflichtet einen Vertrag zu erstellen und mit dem Arbeitnehmer schriftlich abzuschließen.

§ 11 Abs. 1 Satz 1 BDSG: 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.

Erstens müssen die Dauer des Auftrags und der Gegenstand, also die Art der Dienstleistung hinterlegt sein. (§ 11 Abs. 2 Nr. 1 BDSG) Zudem wird Umfang, Art und Zweck der vorgesehenen Datenverarbeitung gefordert. (§ 11 Abs. 2 Nr. 2 BDSG) Das beinhaltet eine Auskunft darüber, welche personenbezogenen Daten im Rahmen des Auftrages bearbeiten werden und wie groß der Kreis der Betroffenen ist. Zu den Daten zählen zum Beispiel Name, Vorname, Anschrift und Telefonnummer. Außerdem wird hier belegt, dass der Auftragnehmer die verwendeten Daten geheim hält, keine unbefugten Kopien anfertigt, nur die vorgesehenen Daten verwendet entsprechend seiner Leistungsbeschreibung handelt.

§ 11 Abs. 2 Satz 1 BDSG: Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen …

Der Auftraggeber muss sicherstellen, dass die im Vertrag hinterlegten technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit berücksichtigt werden und den Auftragnehmer dementsprechend sorgfältig auswählen.

§ 11 Abs. 2 Nr. 3 BDSG: die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen

Unter technischen Maßnahmen sind alle physischen Schutzversuche zu verstehen. Das ist zum Beispiel eine Umzäunung des Geländes, also generell alle baulichen Maßnahmen wie die Sicherung von Türen und Fenstern, sowie die Installation von Alarmanlagen. Technische Maßnahmen können jedoch auch in Soft- und Hardware umgesetzt werden. Geläufig ist hier das Einsetzen von Firewalls, sicheren Verschlüsselungsverfahren, Protokollen zur Datenübermittlung, eine unabhängige Stromversorgung, Passworterzwingung und Prüfung der Passwortqualität, der Einsatz von Routern zur Bildung von Netzwerksegmenten und vieles mehr.

Organisatorische Maßnahmen betreffen die Vorgehens- und die Verfahrensweisen der Mitarbeiter und sind in den Handlungsanweisungen enthalten. Beispielhaft für solche Maßnahmen sind die Erstellung von Passwortrichtlinien, Dokumentation von Datenvernichtungsmaßnahmen, Definitionen über die Arbeit mit personenbezogenen Daten, die Beauftragung zuverlässiger Transportunternehmen und Kontrolle von Fernwartungen.

Diese Maßnahmen sind in den vorgegebenen Anforderungen des BDSG enthalten:

|  |  |
| --- | --- |
| 1. Zutrittskontrolle 2. Zugangskontrolle 3. Zugriffskontrolle 4. Weitergabekontrolle | 1. Eingabekontrolle 2. Auftragskontrolle 3. Verfügbarkeitskontrolle 4. Trennungsgebot |

Falls der Auftragsdatenverarbeitungsvertrag nicht abgeschlossen wird oder inhaltlich nicht den gesetzlichen Vorgaben entspricht, handelt der Auftraggeber ordnungswidrig.

§ 43 Abs. 1 Nr. 2b BDSG: Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen § 11 Absatz 2 Satz 2 einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt […].

Müssen Berichtigungen, Löschungen oder Sperrungen von personenbezogenen Daten vorgenommen werden, dürfen die Auftragnehmer nur nach vorheriger Zustimmung des Auftraggebers handeln. (§11 Abs. 2 Nr. 4 BDSG)

Der Auftragnehmer muss sich außerdem verpflichten seine Mitarbeiter mit den maßgebenden Bestimmungen des Datenschutzes vertraut zu machen und das Datengeheimnis laut § 5 BDSG zu wahren. Auch eine Überwachung der Vorschriften ist Pflicht. (§11 Abs 2. Nr. 5 BDSG)

Falls für gewisse Arbeiten, wie zum Beispiel eine Wartung oder Prüfung der automatisierten Verarbeitungen, muss für diese Unterauftragnehmer eine schriftliche Zustimmung des Auftraggebers vorhanden sein. Die vereinbarten Datenschutzregelungen müssen dann vom Auftragnehmer gegenüber dem Unterauftragnehmer vertraglich sichergestellt sein. (§11 Abs. 2 Nr. 6 BDSG)

Es folgen die Kontrollrechte des Auftraggebers. (§ 11 Abs. 2 Nr. 7 BDSG) Der Auftraggeber wird in diesem Abschnitt des Vertrages dazu berechtigt Kontrollen bezüglich der vertraglichen Vereinbarungen und der Einhaltung der Vorschriften des Datenschutzes durchzuführen.

Kommt es zu Verstößen gegen die Vorschriften zum Schutz personenbezogener Daten oder die im Auftrag getroffenen Festlegungen, ist dies laut §11 Abs. 2 Nr. 8 BDSG dem Auftragnehmer unverzüglich mitzuteilen. Hier wird auch erwähnt, wer im Falle eines Schadens Ersatz leisten muss.

Im vorletzten Punkt erklärt der Auftragnehmer sich damit einverstanden personenbezogene Daten nur der Weisungen des Auftraggebers entsprechend zu erheben, zu verarbeiten oder zu nutzen. (§11 Abs. 2 Nr. 9 BDSG)

Als letztes wir im Vertrag hinterlegt, was bei der Beendigung des Auftrags passiert. Dazu gehört die Löschung sämtlicher genutzter Daten, beziehungsweise die Rückgabe der Daten. Dabei können Sicherheitskopien ausgeschlossen werden, weil sie zur Erfüllung von Haftungs- und Gewährleistungsansprüchen dienen. Diese sind dann aber so zu sperren, dass der Auftragnehmer diese nicht mehr nutzen kann. (§11 Abs. 2 Nr. 10)

Fällt dem Auftragnehmer auf, dass eine Weisung des Arbeitgebers nicht dem Gesetz oder anderen Vorschriften des Datenschutzes entspricht, hat er den Auftraggeber unverzüglich darauf hinzuweisen. (§11 Abs. 3)

Kriterien zur Auftragsdatenverarbeitung

Es ist wichtig zu erkennen, wann eine Auftragsdatenverarbeitung vorliegt, denn oft ist es schwierig sie von der Funktionsübertragung abzugrenzen. Dazu gibt es in Aufsichtsbehörden oder auch in der Literatur Kriterienkataloge, die die wichtigsten Punkte beschreiben. Ein wichtiger Aspekt ist, dass der Auftragnehmer keine Entscheidungsbefugnis über die übermittelten Daten hat und ihm die Nutzung der persönlichen Daten verboten ist, solange es sich nicht um den vereinbarten Überlassungszweck handelt. Außerdem ist der Auftragnehmer verpflichtet dem Auftraggeber darüber zu informieren, was mit den Daten geschieht. Damit ist also der Auftraggeber für alle Daten nach außen hin verantwortlich. Ein weiteres Kriterium besagt, dass der Auftragnehmer in keiner vertraglichen Beziehung zum Betroffenen stehen darf.

Bei einer Funktionsübertragung hingegen, werden die Nutzungsrechte der persönlichen Daten dem Auftragnehmer überlassen. Dieser trägt damit die eigenverantwortliche Sichererstellung von Zuverlässigkeit und Richtigkeit der Daten. Damit ist der Dienstleister nun dafür zuständig die Rechte des Betroffenen zu berücksichtigen. Das sind zum Beispiel die Benachrichtigungspflicht und der Auskunftsanspruch.

Trotz dieser Kriterien, ist es oft nicht eindeutig, welcher Fall vorliegt. Es gibt einige Sonderfälle, wie zum Beispiel die Wartung und Prüfung von automatisierten Verarbeitungen, bei denen ein Auftragsdatenverarbeitungsvertrag notwendig ist, weil der Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. (§11 Abs. 5 BDSG)

Beispiele zur Auftragsdatenverarbeitung

1. Beauftragung eines Callcenters zur Kundenkommunikation
2. Ablage von personenbezogenen Daten auf extern gehosteten Servern. (Egal ob für Produktivsysteme oder Backups)(Gola/Schomerus verneinen hier ADV, da er Hoster ja nichts mit der eigentlichen DV zu tun hat. Anm. d. A: Der Hoster wird aber für die Wartung der Systeme verantwortlich sein, dabei kann eine Kenntnisnahme nicht ausgeschlossen werden, also doch ADV?)
3. Wartungsdienstleistungen, bei denen nicht ausgeschlossen werden kann, dass während der Wartung personenbezogene Daten zur Kenntnis gelangen
   * Wartung von IT-Systemen
   * Wartung von TK-Anlagen
4. Entsorgung von Akten oder Datenträgern durch externe Unternehmen

**Keine ADV** liegt per Definition beim Postversand oder Bankgeschäften vor.

# Haftung *- Ayana*

### Begriffserklärung BDSG

* Verantwortliche Stelle: Nach §3 Abs. 7 BDSG ist eine verantwortliche Stelle jede Person oder Stelle, die personenbezogen Daten erhebt, verarbeitet oder nutzt oder dies durch einen Auftrag von einem anderen gemacht wird.
* Öffentliche und nicht-öffentliche Stellen: In §2 BDSG wird unterschieden in öffentliche Stellen des Bundes, öffentliche Stellen der Länder, Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder und nicht-öffentliche Stellen, welche alle natürlichen und juristischen Personen sind, die nicht in den Abs. 1-3 genannt wurden.

## Haftung nach BDSG

Laut §11 Abs. 1 Satz 1 BDSG ist nur der Auftraggeber dafür verantwortlich, dass bei der Auftragsdatenverarbeitung die gesetzlichen Vorschriften des Bundesdatenschutzgesetzes und andere Vorschriften des Datenschutzes eingehalten werden.

### Schadensersatz nach BDSG

Sollte eine verantwortliche Stelle einem Betroffenen Schaden zu fügen, in dem Sie seine personenbezogenen Daten unzulässig oder unrichtig erhebt, verarbeitet oder nutzt, so ist Sie nach §7 BDSG dazu verpflichtet Schadensersatz zu leisten.

### Schadensersatz bei automatisierter Datenverarbeitung durch öffentliche Stellen nach BDSG

Wenn eine verantwortliche öffentliche Stelle einer Person Schaden, durch eine unzulässige oder unrichtige Erhebung, Verarbeitungen oder Nutzung der personenbezogen Daten vornimmt, so ist der Träger dem Betroffenen nach §8 Abs. 1 BDSG zum Schadensersatz verpflichtet. Der Gesamtbetrag der Schadensersatzleistung ist nach §8 Abs. 3 auf maximal 130.000€ begrenzt. Sollten mehrere Person zu Schaden gekommen sein, so ist die Schadensersatzleistung des einzelnen so zu verringern, dass der Gesamtbetrag im Verhältnis zum Höchstbetrag steht. Sollte der die betroffene Person an dem Entstehen des Schadens eine Mitschuld haben, so gilt §254 des Bürgerlichen Gesetzbuchs. Auch die Verjährung für unerlaubte Handlungen ist dem Bürgerlichen Gesetzbuch zu entnehmen.

### Bußgeld- und Strafvorschriften nach BDSG

Wer ordnungswidrig handelt in dem er vorsätzlich oder fahrlässig die in §43 Abs.1 BDSG genannten Taten begeht, kann nach §43 Abs. 3 Satz 1 BDSG mit einer Geldstrafe von bis zu 50.000€ geahndet werden. Sollte er die in §43 Abs. 2 genannten Taten begehen, so kann die Geldstrafe auf bis zu 300.000€ erhöht werden. Auf jeden Fall soll die Geldstrafe den wirtschaftlichen Nutzen den der Täters aus der Ordnungswidrigkeit gezogen hat übertreffen. Sollten 50.000€, bzw. 300.000€ nicht ausreichen, so dürfen nach §43 Abs.3 Satz 3 BDSG die Geldstrafen auch erhöht werden.

Wer die Straftaten in §43 Abs. 2 gegen Bezahlung oder mit der Absicht sich oder andere zu bereichern oder jemanden zu schädigen begangen hat, kann nach §44 Abs. 1 BDSG mit einer Freiheitsstrafe von bis zu zwei Jahren oder einer Geldstrafe bestraft werden.

### Begriffserklärung DS-GVO

* Verantwortlicher: Der in der DS-GVO genannte Verantwortliche ist mit dem Auftraggeber aus dem BDSG gleichzusetzen.
* Auftragsverarbeiter: Der in der DS-GVO genannte Auftragsverarbeiter ist mit dem Auftragsnehmer aus dem BDSG gleichzusetzen.

## Haftung nach DS-GVO

Nach Artikel 83 Abs. 1 DS-GVO kann ein Schadensersatz nun gegenüber dem Verantwortlichen oder dem Auftragsverarbeiter in Anspruch genommen werden. Grundsätzlich ist nach Artikel 82 Abs.2 DS-GVO jeder, an der Verarbeitung beteiligte, Verantwortliche haftbar. Sofern der Auftragsverarbeiter seine Pflichten verletzt hat oder gegen die Anweisung des Verantwortlichen gehandelt hat ist auch dieser haftbar. Sollte der Verantwortliche oder der Auftragsverarbeiter seine Unschuld an der Entstehung des Schadens beweisen können, ist dieser nach Artikel 82 Abs. 3 DS-GVO von der Haftung ausgeschlossen. Sind sowohl der Verantwortliche als auch der Auftragsverarbeiter für den Schaden verantwortlich, so haftet nach Artikel 82 Abs. 4 jeder der beiden für den Gesamtschaden, damit die vom Schaden betroffene Person einen angemessenen Schadensersatz erhält. Nach Artikel 82 Abs. 5 kann ein Verantwortlicher oder Auftragsverarbeiter, wenn er den vollständigen Schadensersatz gezahlt hat, von den andern, an der Verarbeitung, Verantwortlichen oder Auftragsverarbeitern, sofern diese nach Artikel 82 Abs. 2 einen Anteil an der Entstehung des Schadens haben, Teile des Schadensersatzes zurückfordern.

### Geldbußen nach DS-GVO

Je nach Verstoß sieht Artikel 83 DS-GVO unterschiedliche Bußgelder, aber keine Freiheitsstrafen vor.

Liegt ein Verstoß gegen die unter Artikel 83 Abs. 4a-c genannten Bestimmungen vor, so wird dieser mit bis zu 10.000.000€ oder sofern es sich um ein Unternehmen handelt, 2% des weltweit erzielten Jahresumsatzes des vorangegangen Geschäftsjahrs. Bezieht sich der Verstoß auf die in Artikel 83 Abs. 5a-e genannten Bestimmungen, so kann ein Bußgeld in Höhe von bis zu 20.000.000€ oder sofern es sich um ein Unternehmen handelt, 4% des weltweit erzielten Jahresumsatzes des vorangegangen Geschäftsjahrs.

Des Weiteren sieht die DS-GVO vor, dass ein Missachten der Weisungen einer Aufsichtsbehörde mit einem Bußgeld in Höhe von 20.000.000 oder sofern es sich um ein Unternehmen handelt, 4% des des weltweit erzielten Jahresumsatzes des vorangegangen Geschäftsjahrs.

# DSGVO *- Schewtschuk*

Die Datenschutzgrundverordnung(DSGVO) ist eine neue EU-Verordnung. Sie soll den Umgang von personenbezogenen Daten(siehe Begriffsdefinitionen) vereinheitlichen und sich dem digitalen Zeitalter anpassen. Dabei wirft es viele bereits beschlossenen Regelungen um.

Betroffen sind Unternehmen/Anbieter, die mit personenbezogenen Daten arbeiten. Auch Unternehmen außerhalb der EU können von der DSGVO betroffen sein, wenn sie: 1. Mit den Daten von EU-Bürgern arbeiten. 2. Eine Niederlassung in der EU haben.

Die Verordnung ist bereits am 25. Mai 2016 in Kraft getreten. Allerdings soll sie erst ab dem 25. Mai 2018 angewendet werden. Da es eine Vorordnung ist, müssen die gestellten Anforderungen von den Unternehmen spätestens 25. Mai 2018 realisiert sein.

## DSGVO Änderrungen gegenüber BDSG

Die DSGVO ist in vielen Punkten schärfer und genauer als der BDSG. Es wird viel über den Haufen geworfen und neues Eingeführt.

Einer der wohl größten Punkte des DSGVO ist das **Recht auf Löschung** (oft auch **Recht auf Vergessenwerden** genannt). Danach muss jeder Anbieter, der personenbezogene Daten speichert, eine leichte Möglichkeit für seine Nutzer bieten um ihre personenbezogenen Daten löschen zu können. Je nach angebotenem Service kann sich das allerdings nur schwer umsetzen. Am Beispiel von Google: Jede Privatperson hat dadurch das Recht alle gefundenen Eintrage, die dessen Namen erwähnen, löschen zu lassen. Wie man sich vorstellen kann ist der Aufwand für die technische Umsetzung enorm.[welt/Google überfordert]

Dies ist allerdings bereits Realität. Am Mai. 2014 hatte der Spanier Mario Costeja González gegen Google geklagt, weil Google einen Zeitungsartikel über ihn nicht aus den Suchtreffern entfernen wollten.

Kurzer Einschub zu dem Mario Costeja González Fall: Mario Costeja González ist ein Schriftexperte und Professor. 1998 veröffentlichte eine katalanische Zeitung „La Vanguardia“ eine Liste von Immobilien die gepfändet werden mussten. Dabei kam der Name vom Herren González vor. Daraufhin wurde der mit dem unschönen Thema "Pfändung" in Verbindung gebracht. Dies schadete seinem Beruf. Zuerst ging González gegen die Zeitung „La Vanguardia“ ins Gericht und verlor. Daraufhin klagte er gegen Google.[welt/Fall González]

Google verlor vor Gericht. Somit war Google der erste Anbieter, der das Recht auf Löschung umsetzen musste.

Nach dem Art. 17 DSGVO müssen folgende Punkte zutreffen, um das Recht auf Löschung geltend zu machen:

Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.

Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.

Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2 Widerspruch gegen die Verarbeitung ein.

Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.

Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.

Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.

Eine weitere größe Neuerung ist das **Recht auf Datenübertragbarkeit**(Datenportabilität). Diese soll den Nutzer die Möglichkeit geben, mit seinen Daten leicht zu anderen Anbietern wechseln zu können. Dabei müssen alle Anbieter die Daten in einem "gängigem Format" anbieten.

Gängige Einsatzzwecke sollen beispielsweise der Wechsel der Bank, Arbeitsgebers oder sozialen Netzwerken sein. Die Rechenschaftspflichten von Unternehmen ändert sich laut Art. 22 auch. Danach müssen je nach Art der Daten „geeignete technische und organisatorische Maßnahmen“ ergriffen werden, um sicherzustellen und den Nachweis dafür erbringen zu können, dass personenbezogene Daten in Übereinstimmung mit den neuen EU-Regelungen verarbeitet werden.[heise/Änderrungen] Dabei sind Unternehmen, die beschuldigt werden rechtswidrig mit den Daten umzugehen, zu einer **Beweislastumkehr** verpflichtet.

Die **Datenschutz-Folgenabschätzung** ist ebenfalls eine Neuerung. Diese ist in Art. 34 geregelt und sieht eine "vorherige Konsultation" durch einen Datenschutzbeauftragten vor. Somit müssten größere Projekt, die mit personenbezogenen Daten umgehen, eine Konsultation durch einen Datenschutzbeauftragten haben. Diese Regelung gab es bereits in dem BDSG, sie ist allerdings von der Mitarbeiterzahl abhängig. Danach brauchte man einen Datenschutzbeauftragten erst bei 10 oder mehr Mitarbeitern. Dieser Punkt wird auch oft von Kritikern kritisiert, da sich dadurch die agile Softwareentwicklung abgebremst und eine Innovationshemmung stattfindet.

Was sich auch ändert sind die Strafen bei Verletzung der DSGVO Gesetze. Diese werden in den folgenden Kapiteln noch erläutert.

# Erläuterung des Vertrags *- Kappenberg*

Der Auftragsdatenverarbeitungsvertrag nach §11 des BDSG oder kurz ADV-Vertrag genannt, beinhaltet Rechte und Pflichten des Auftragnehmers und des Auftraggebers, die im Laufe des Auftrags eingehalten werden müssen um eine Einhaltung des geltenden Datenschutzes garantieren zu können.

Im Wesentlichen muss der Auftragsdatenverarbeitungsvertrag zunächst zwei Aspekte der Auftragsdatenverarbeitung abdecken. Aus ihm muss hervorgehen, dass der Auftragnehmer zu jedem Zeitpunkt weisungsbefugt handelt. Das bedeutet, dass dem Auftragnehmer zu jedem Arbeitsschritt der Auftragsdatenverarbeitung eine Anweisung des Auftraggebers vorliegt. Den zweiten Aspekt, den der Vertrag darstellen muss, ist die Verantwortlichkeit des Auftraggebers eine Garantie Garantie geben zu können, dass die Auftragsdatenverarbeitung nicht die Zustimmung der Personen, deren Daten bearbeitet werden, überschreitet. Der Auftraggeber ist damit weiterhin für die Einhaltung des Datenschutzgesetzes verantwortlich. Um dies zu garantieren trifft den Auftraggeber eine Kontrollpflicht, die die Einhaltung der in §11 BDSG genannten Punkte beinhaltet. [1]

Damit ein Auftragsdatenverarbeitungsvertrag gültig ist, muss dieser in schriftlicher Form zwischen Auftraggeber und Auftragnehmer abgeschlossen werden. Des Weiteren gibt es einige Punkte, die in jedem Vertrag behandelt werden sollten. Diese Punkte werden im folgendem aufgezählt und mit dem vorliegenden Mustervertrag abgeglichen.

Einige allgemeine Punkte, wie der Gegenstand und die Dauer der Vereinbarung, sowie Art, Zweck, betroffenen Personen und die personenbezogenen Daten werden in einem allgemeinen Teil des Vertrags unter Abschnitt 1 geklärt. [2]

Verantwortliche für die Datenverarbeitung: Die für die Datenverarbeitung verantwortlichen Personen sind im Mustervertrag mit in die Rechte und Pflichten des Auftragnehmers in Abschnitt 3 aufgenommen. Wie in Punkt (3) darrgestellt stimmt der Auftragnehmer zu, dass die Datenverarbeitung ausschließlich durch Beschäftigte seiner Firma erfolgen darf.

Umfang der Weisungsbefugnis: Der Umfang der Weisungsbefugnis ist im Mustervertrag unter Abschnitt 4 „Rechte und Pflichten des Auftraggebers“ vereinbart. In den Punkten (1) und (2) wird zunächst abgesprochen, dass alle Weisungen an den Auftragnehmer vom Auftraggeber in Schriftform vorliegen müssen. Des Weiteren wird hier der Umfang der Weisungen auf die Verarbeitung der Daten beschränkt, dies soll dem Auftraggeber das Recht dazu geben die Art der Verarbeitung der Daten zu beeinflussen. Es soll aber auch gleichzeitig den Auftragnehmer davor schützen, dass der Auftraggeber in seine internen Geschäftsprozesse eingreifen kann.

Für beide Vertragspartner wurden in Abschnitt 1 weisungsbefugte Personen benannt. Die dort genannten Personen sind ausschließlich befugt Weisungen entgegenzunehmen und auszusprechen.

Verpflichtung zur Vertraulichkeit der zur Verarbeitung befugten Personen: Der Auftragnehmer wird in Abschnitt 3 unter Punkt (2) verpflichtet die personenbezogenen Daten nur innerhalb des Auftrags zu bearbeiten. Dies verpflichtet ihn dazu, die Daten nur nach den Weisungen des Auftraggebers zu behandeln. Des Weiteren ist in Punkt (4) desselben Abschnittes vereinbart, dass der Auftragnehmer nicht ohne den Auftraggeber in Kenntnis zu setzen Duplikate der Daten anfertigen darf.

Sicherstellung von technischen und organisatorischen Maßnahmen für den Datenschutz: Um die Einhaltung der technischen und organisatorischen Maßnahmen sicherzustellen, verpflichtet sich der Auftragnehmer in Abschnitt 3 Punkt (1) dazu, diese einzuhalten. Des Weiteren verpflichten sich Auftragnehmer und Auftraggeber zu einer gemeinsamen Durchsetzung dieser Maßnahmen durch Kontrollen. Die Art der Maßnahmen sind in Abschnitt 2 genauer erläutert.

Etwaige Hinzuziehung von Subunternehmern: Das beauftragen von Subunternehmern ist im Mustervertrag unter Abschnitt 5 „Unterauftragsverhältnisse“ geklärt. Hier wird zunächst definiert welche Umstände erfüllt sein müssen, damit ein Unterauftragsverhältnis mit einem Subunternehmer zustande kommt. Danach werden einige Punkte aufgezählt, welche zu beachten sind, wenn der Auftragnehmer einen Unterauftrag durchführen will. Der wichtigste Punkt dabei ist sowohl die mündliche Zustimmung des Auftraggebers, als auch die schriftliche. In der Praxis ist es zum Teil üblich Unterauftragsverhältnisse von Beginn an auszuschließen. Dies wird im Mustervertrag allerdings zu Gunsten des Auftragnehmers verhindert. Stattdessen werde strikte Vorgaben zu den Umständen eines solchen Verhältnisses gemacht.

Kontrollrechte des Auftraggebers und Unterstützung durch den Auftragnehmer: Da der Auftraggeber während der Verarbeitung der Daten weiterhin die verantwortliche Person für den Datenschutz bleibt, werden die Kontrollrechte und die Unterstützung bei der Ausführung durch den Auftragnehmer in den Rechten und Pflichten beider Parteien im Mustervertrag mit aufgenommen. In Abschnitt 3, in welchem es um die Rechte und Pflichten des Auftragnehmers geht, wird in den Punkten (9), (10), (11) und (12) die Mitarbeit an den Kontrollen durch den Auftragnehmer vereinbart. Zunächst verpflichtet er sich dazu, den Auftraggeber unverzüglich bei ihm bekannten Verstößen gegen das Datenschutzrecht zu informieren. Danach wird geklärt in welchem Umfang seine Mitarbeit stattfindet. Er gewährleistet Prüfungen und Kontrollen durch den Auftraggeber sowie ein Informationsrecht des Auftraggebers. Damit der Auftragnehmer durch die Kontrollen und Prüfungen keinen wirtschaftlichen Schaden erleidet, steht ihm, laut Vertrag eine Vergütung für die Mithilfe zu. In Punkt (10) wird dem Auftragnehmer das Recht eingeräumt die Auftragsdatenverarbeitung zu stoppen, wenn er von einem Verstoß gegen das Datenschutzrecht ausgeht. Dies soll ihm vor einer Vertragsstrafe durch die nicht Ausführung des Auftrags schützen.

Dem Auftraggeber wird laut Abschnitt 4 Punkt (4) das Recht zugesprochen die Prüfungen durchzuführen und zu diesem Zweck externe Firmen zu beauftragen. Des Weiteren werden ihm in diesem Abschnitt die Umfänge dieser Kontrollen und die Mithilfe des Auftragnehmers gewährleistet. Er verpflichtet sich zudem dazu die Einhaltung der technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung der Daten durch ein Konzept des Auftragnehmers zu überprüfen. In Punkt (3) sichert er zu dem Auftragnehmer bei seinen Rechten und Pflichten zu helfen, indem er Informationen zur Verfügung stellt.

Informationspflicht des Auftragnehmers gegenüber dem Auftraggeber: Der Auftragnehmer verpflichtet sich neben den Informationspflichten zu Kontrollzwecken ausdrücklich dazu den Auftraggeber zu informieren, falls durch ihn eine Verletzung des Datenschutzrechts entstanden ist. Dies ist notwendig, da der Auftraggeber gegenüber einer geschädigten Person haftbar gemacht werden kann und sich durch einen solchen Verstoß gegenüber dem Geschädigten verantworten muss.

Behandlung personenbezogener Daten durch den Auftragnehmer: Der Auftragnehmer verpflichtet sich nach dem Mustervertrag dazu die personenbezogenen Daten des Auftraggebers durchgehend zu markieren und strikt von anderen Daten zu trennen. Siehe Abschnitt 3, Punkte (7) & (8). Des Weiteren verpflichtet er sich dazu, die Daten nach der Bearbeitung oder zu einem früheren Zeitpunkt aufgrund einer Aufforderung dem Auftraggeber auszuhändigen oder zu löschen. Das Löschen muss laut Vertrag unter der Einhaltung des Datenschutzrechts geschehen und dokumentiert werden.

Dies sind die wichtigsten Punkte, die in jedem ADV-Vertrag stehen sollten. Unter dem Abschnitt 6 wird zudem noch einmal eindeutig definiert, welche Partei gegenüber wem haftet. Zu beachten ist, dass ein solcher Vertrag nicht die Service Leistung beschreibt. Daher ist in dem Vertrag auch nicht geklärt, welche Vergütungen für die Leistung anfallen oder unter welchen Punkten die Service Leistung ungültig ist. Gegenstand des Auftragsdatenverarbeitungsvertrags ist lediglich die Haftung bezogen auf das gültige Datenschutzgesetz.

# Quellen

|  |  |
| --- | --- |
| [1] | Jens Eckhardt, Rudi Kramer *Auftragsdatenverarbeitung*, Datenschutz und Datensicherheit – DuD, 01.09.2013 |
| [2] | https://it-service.network/blog/2017/09/28/auftragsdatenverarbeitung-adv-vertag-aendert-sich/, Zugriff am 05.02.2018 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Anhang

Mustervertrag zur Auftragsdatenverarbeitung.