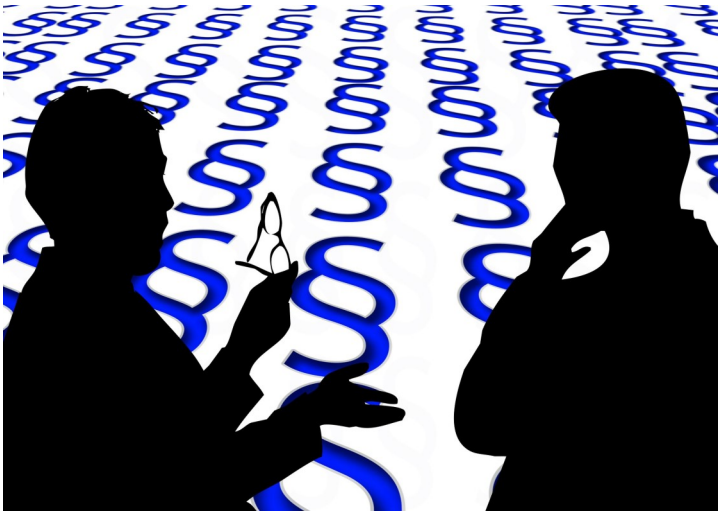
amendos

Newsletter 04/2018

Inhalt:

DSGVO – ein halbes Jahr danach – mit Fokus auf IT-Outsourcing

Seit 25. Mai 2018 gilt in Deutschland die Datenschutz-Grundverordnung (DSGVO). Jüngste Studien zeigen aber, dass sich hinsichtlich ihrer Umsetzung in den meisten Unternehmen noch viel zu wenig getan hat (siehe z. B. Bitkom, *Kaum Fortschritt bei der Umsetzung der Datenschutz-Grundverordnung*[1]). Gerade in Unternehmen mit Multi-Providerumgebung haben sich die Herausforderungen jedoch potenziert. Wir wollen deshalb dieses Thema noch einmal aufgreifen und bezüglich IT-Outsourcing den „roten Faden“ skizzieren, was von wem zu tun ist.



DSGVO und IT-Outsourcing

Die DSGVO[2] umfasst 11 Kapitel mit insgesamt 99 Artikeln und einer Vielzahl von Absätzen (zur besseren Orientierung siehe die nachfolgende Tabelle). Sie unterscheidet zwischen dem Verantwortlichen (Auftraggeber) und dem Auftragsverarbeiter (Provider im Falle eines

Outsourcings). Die Aufgabenverteilung ist im Wesentlichen in Kapitel IV geregelt.

Kapitel		Artikel
I	Allgemeine Bestimmungen	1 – 4
II	Grundsätze	5 – 11
III	Rechte der betroffenen Person	12 – 23
IV	Verantwortlicher und Auftragsverarbeiter	24 – 43
V	Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen	44 – 50
VI	Unabhängige Aufsichtsbehörden	51 – 59
VII	Zusammenarbeit und Kohärenz	60 – 76
VIII	Rechtsbehelfe, Haftung und Sanktionen	77 – 84
IX	Vorschriften für besondere Verarbeitungssituationen	85 – 91
X	Delegierte Rechtsakte und Durchführungsrechtsakte	92 – 93
XI	Schlussbestimmungen	94 – 99

Tabelle1: Gliederung der DSGVO

Betroffen sind alle Outsourcing-Aktivitäten, bei denen personenbezogene Daten – definiert in Kapitel I der DSGVO – im Spiel sind. Wir zeigen die notwenigen Schritte auf, mit denen der Auftraggeber seine Providerbeziehungen auf einen DSGVO-konformen Stand bringt.

Lese-Tipp:
DSGVO – Missverständnisse und rechtliche Unsicherheiten

Verzeichnis aller Verarbeitungstätigkeiten erstellen

In Kapitel IV, Art. 30, fordert die DSGVO, dass der Auftraggeber ein vollständiges Verzeichnis aller Verarbeitungstätigkeiten personenbezogener Daten führen muss. Hier werden auch die externen Provider vermerkt, wenn sie innerhalb einer Tätigkeit Zugang zu Daten bekommen und sie verarbeiten. Dieses Verzeichnis bildet den Ausgangspunkt für alle weiteren Betrachtungen. (Nicht zu vergessen: Auch die Daten der verschiedenen Ansprechpartner auf Seite der Provider sind personenbezogen und müssen gleichermaßen betrachtet werden.)

Risikoanalyse durchführen

Jede Datenverarbeitungstätigkeit sollte der Auftraggeber einer Risikoanalyse hinsichtlich des Datenschutzes unterziehen, wie wir es z. B. in unserem Newsletter 1/2016 beschrieben haben.

Lese-Tipp:
Compliance-Risiken beim IT-Outsourcing minimieren

(In bestimmten Fällen ist sogar zwingend eine Datenschutz-Folgeabschätzung durchzuführen; vgl. Kapitel IV, Art. 35).

Maßnahmen ableiten

Aus der Risikoanalyse lassen sich die Technischen und Organisatorischen Maßnahmen (TOM) ableiten, um Risiken zu minimieren und sich so DSGVO-konform aufzustellen. Die DSGVO bleibt in Art. 32 zur Ausgestaltung eher vage: „(1) Unter Berücksichtigung des Stands der Technik […] treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, […]". Konkretere Hinweise findet man z. B. auf über 70 Seiten in der *Handreichung zum „Stand der Technik" technischer und organisatorischer Maßnahmen* des Bundesverbandes IT-Sicherheit[3] und weiteren Quellen zur IT-Sicherheit.

Die TOM sind je Verarbeitungstätigkeit zu definieren und im Verzeichnis der Verarbeitungstätigkeiten zu dokumentieren. Daraus ergibt sich, welche Maßnahmen von welchem Provider umgesetzt werden müssen.

Interne Zuständigkeiten festlegen

Damit die Provider die TOM im Sinne des Auftraggebers umsetzen und DSGVO-Konformität herstellen, ist ein straffes Providermanagement notwendig. Die Komplexität des Vorhabens hat zur Folge, dass in dessen Phasen (siehe Abbildung 1) verschiedene Expertisen und Rollen benötigt werden, z. B.:

- Geschäftsführung
- Datenschutzbeauftragter

- Vertragsmanagement, Einkauf, Rechtsabteilung
- IT-Sicherheit
- Projektmanager, der die TOM umsetzt
- ITIL-Rollen (Incident Manager, Change Manager, …)
- (operative) Providermanager

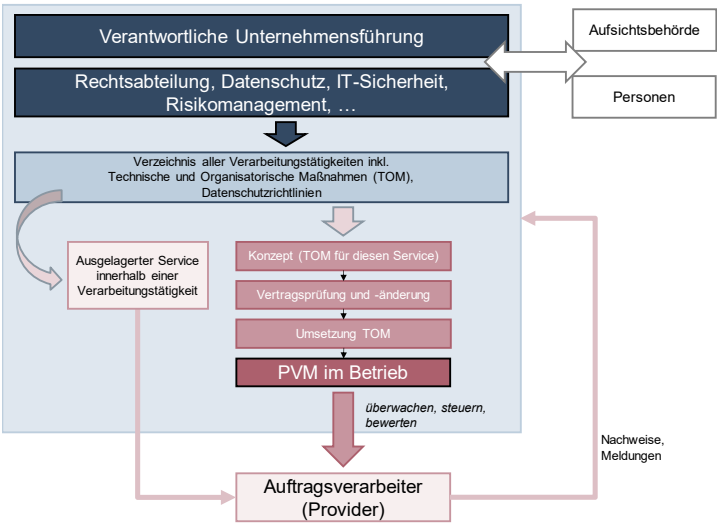


Abbildung 1: Umsetzung der DSGVO beim IT-Outsourcing

Die Regelung von Zuständigkeiten erfolgt idealerweise als Ergänzung einer bestehenden RACI-Matrix.

Providerverträge prüfen

Anhand der definierten TOM (Soll-Zustand) muss dann für jeden einzelnen Providervertrag (Ist-Zustand) mittels Gap-Analyse geprüft werden, ob und welche Vertragsanpassungen jeweils erforderlich sind. Diese müssen generell die DSGVO-Konformität sicherstellen, aber gegebenenfalls auch zusätzliche individuelle Datenschutzrichtlinien des Auftraggebers adressieren. (Im ungünstigsten Fall lassen sich diese nicht durchsetzen – vor allem bei großen Providern außerhalb der EU – sodass ein

Providerwechsel oder ein Insourcing erforderlich wird.)

Bei den Vertragsanpassungen müssen der spätere Betrieb und notwendigen Steuerungsinstrumente des Providermanagements bereits berücksichtigt werden.

Maßnahmen umsetzen

Die Umsetzung der Maßnahmen kann Projektcharakter haben und erfordert somit ein professionell arbeitendes (Multi-)Projektmanagement. Es überwacht die Umsetzung von Maßnahmen der einzelnen Provider, leitet Eskalationen bei Abweichungen ein und koordiniert, wenn mehrere Parteien involviert sind.

Providermanagement-Aufgaben im Betrieb

Aus der DSGVO resultieren z. B. die folgenden Aufgaben, für die auf Auftraggeber-Seite die jeweilige Zuständigkeit festgelegt werden muss:

- Verwaltung von Nachweisen, die die in Art. 28 geforderten „hinreichenden Garantien“ belegen (z. B. aktuelles ISO 27001-Zertifikat).
- Kontrollen, dass jeder Provider seinerseits ein Verzeichnis von Verarbeitungstätigkeiten führt (Art. 30).
- Kontrollen, dass jeder Provider festgelegte Verhaltensrichtlinien (Art. 40) umsetzt.

- Providersteuerung und -überwachung bei Prozessen zur Wahrung der Rechte von Betroffenen (Kapitel III, Art. 12 bis 23, Rechte auf Informationen und Auskünfte, Widerspruch, Berichtigung und Löschung von Daten, Einschränkung der Verarbeitung, Datenübertragbarkeit) und bei Beschwerden (Art. 77).

Seminare 1. Halbjahr 2019

PM	**IT-Projekte erfolgreich aus der Krise führen** Hamburg, 28.01.-29.01.2019 **Project Management Offices im IT-Umfeld** Hamburg, 31.01.-01.02.2019 **Kommunikationskompetenz in Projektkrisen** Hamburg, 04.02.-05.02.2019 **Soft Skills für Projektleiter/innen** Hamburg, 06.02.-07.02.2019
ITSM	**Einführung in die Prozessoptimierung** Hamburg, 28.03.-29.03.2019 **Prozessdokumentation gestalten** Hamburg, 01.04.2019 **IT Service Management und Agilität** Hamburg, 01.04.2019 **Erstellung von IT-Servicekatalogen** Hamburg, 02.04.2019
Outsourcing	**Grundlagen IT-Providermanagement** Hamburg, 20.02.-21.02.2019 **IT-Providerwechsel** Hamburg, 22.02.2019 **IT-Providermanagement – live im Betrieb** Hamburg, 25.02.-26.02.2019 **IT-Outsourcing** Hamburg, 16.05.-17.05.2019 **Öffentliche IT-Ausschreibungen** Hamburg, 06.05.-07.05.2019

www.amendos.de/seminare

- Mitwirkung bei der Entgegennahme von Informationen vom Provider (Art. 33, Abs. 2) und der Risikobewertung dazu, bei den Meldepflichten gegenüber Aufsichtsbehörden (Art. 33), für die i. d. R. eine Frist von 72 Stunden gilt, und der Information von Betroffenen (Art. 34).
- Bei Schadensersatzforderungen betroffener Personen (Art. 82) kann es um „abschreckende“ Geldbußen gehen (Art. 83). Hierzu müssen vertragliche Regelungen zwischen Auftraggeber und den Providern getroffen werden. Im operativen Betrieb sollte das Providermanagement notwendige Fakten zusammenstellen, um für den Streitfall vorbereitet zu sein.

- Im operativen Betrieb müssen z. B. providerseitige Changes und Sicherheits-Bulletins von Providern auf ihre datenschutzseitigen Auswirkungen hin geprüft werden.

Kernaufgabe bleibt die Providerbewertung

Im Kontext der DSGVO sollten neue KPIs aufgenommen und regelmäßig geprüft werden:

- Reaktionszeiten des Providers bei der Umsetzung von TOM
- Zuverlässigkeit bei der Bereitstellung von Garantien gemäß Art. 28 und Zugriff auf das Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30
- Reaktionszeiten bei Prozessen zur Wahrung der Rechte von Betroffenen, ggf. aufgeschlüsselt nach Prozess
- Anzahl der Meldungen gemäß Art. 33, Abs. 2 (nach Periode, nach Schweregrad, …)
- Anzahl DSGVO-relevanter Changes auf Providerseite

Fazit

DSGVO in Bezug auf IT-Outsourcing ist ein hochkomplexes Thema, das nicht nur juristische, datenschutzrechtliche und IT-sicherheitstechnische Belange umfasst, sondern auch tiefgehende Kenntnisse im Providermanagement erfordert. Erfolgsfaktoren sind dabei klare Regelungen der Zuständigkeiten, aber auch ein solides ganzheitliches Verständnis: Providermanager müssen die juristische Dimension der DSGVO verstehen. Der Datenschutzbeauftragte wiederum muss wissen, wie Provider bei einem IT-Outsourcing hinsichtlich der Einhaltung des Datenschutzes gesteuert werden.

Michael Schneegans

[1] Bitkom: *Kaum Fortschritt bei der Umsetzung der Datenschutz-Grundverordnung.* [Zugriff am: 21.11.2018]. Verfügbar unter: https://www.bitkom.org/Presse/Presseinformation/Kaum-Fortschritt-bei-der-Umsetzung-der-Datenschutz-Grundverordnung.html

[2] DSGVO, Verfügbar unter: https://ec.europa.eu

[3] TeleTust – Bundesverband IT-Sicherheit e. V.: *IT-Sicherheitsgesetz und Datenschutz-Grundverordnung: Handreichung zum „Stand der Technik" technischer und organisatorischer Maßnahmen.* [Zugriff am: 19.11.2018]. Verfügbar unter: https://www.teletrust.de/publikationen/broschueren/stand-der-technik/

ANGEBOT

Sie benötigen Hilfe bei der Provider-bezogenen Implementierung der DSGVO?

amendos bietet Ihnen die Konzeption einer DSGVO-konformen Implementierung an und begleitet die Umsetzungsphase.

Sie wollen Ihre DSGVO-Implementierung auf Vollständigkeit prüfen lassen?

amendos bietet Ihnen eine strukturierte Prüfung inklusive Dokumentation von Ergebnissen und Maßnahmenempfehlungen an.

Fordern Sie bei uns ein unverbindliches Angebot an!

DSGVO bei der Nutzung von Cloud-Services

Die DSGVO stellt an Unternehmen hinsichtlich des Datenschutzes zahlreiche neue Anforderungen. Dies gilt umso mehr, wenn das betreffende Unternehmen Cloud-Services nutzt. Welche neuen Anforderungen ergeben sich für Auftraggeber und Auftragnehmer? Was ist bei der Vertragsgestaltung mit einem Cloud-Provider zu beachten? Dies und mehr wird im folgenden Artikel betrachtet.

Die DSGVO bringt keine grundlegende Veränderung in der Frage, welche Verarbeitung personenbezogener Daten zulässig oder unzulässig ist. Die Rechtsgrundlage ändert sich zwar, aber die Prinzipien bleiben grundsätzlich die gleichen. Die Bußgeldhöhe für Verstöße gegen die DSGVO steigt allerdings deutlich an: So beträgt die maximale Geldbuße bis zu 20 Millionen Euro oder bis zu 4% des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahr; abhängig davon, welcher Wert der höhere ist.

Der eigentliche, durch die DSGVO ausgelöste Paradigmenwechsel im Datenschutzrecht besteht darin, dass das Datenschutzrecht jetzt umfassende Dokumentations-, Organisations- und Transparenzpflichten vorsieht. Der Auftraggeber muss seine Verarbeitung von personenbezogenen Daten untersuchen. Diese ist auf Unzulässigkeit hin zu überprüfen und/oder verarbeitungsbedingte Risiken sind zu identifizieren und angemessene Maßnahmen zur Ri-

sikoreduzierung zu planen und umzusetzen. Daneben gibt es auch Änderungen für bestehende Alt-Verträge sowie veränderte Haftungsregeln.

Im Folgenden werden die wichtigsten Cloud-spezifischen Neuerungen angesprochen:

Alt-Verträge

Nach Erwägungsgrund 171 der DSGVO gilt, dass seit 25.Mai 2018 eine Verarbeitung personenbezogener Daten nur noch dann Datenschutz-konform ist, wenn sie den Anforderungen der DSGVO genügt. Somit müssen auch bereits bestehende Verträge mit Cloud-Providern entsprechend der DSGVO gegebenenfalls neu ausgestaltet oder mit Zusätzen versehen werden. Es ist zu überprüfen, ob die eingesetzten Cloud-Provider ihre Verträge

selbstständig an die Erfordernisse anpassen und ihre Kunden darüber informieren. Falls nicht, ist die erforderliche Anpassung einzufordern.

Die insgesamt 173 Erwägungsgründe werden zur Auslegung der 99 DSGVO-Artikel herangezogen.

Vorgabe für die Auftragsverarbeitung

Die Auftragsdatenverarbeitung (BDSG-alt) heißt unter der DSGVO nun Auftragsverarbeitung. Bei der Nutzung von Cloud-Services

kommt ihr aus datenschutzrechtlicher Sicht eine zentrale Rolle zu. Die Auftragsverarbeitung wird zum größten Teil in den Artikeln 28 und 29 der DSGVO geregelt.

Jede Vereinbarung zwischen Auftraggeber und Service-Provider über Auftragsverarbeitung muss den neuen Anforderungen der Art. 28 / 29 DSGVO genügen.

Gerade im Cloud-Umfeld stellen sich zwei neue Herausforderungen:

- Die Beauftragung von Subunternehmern durch den Auftragnehmer (zum Beispiel für den Cloud-Provider ein Rechenzentrumsbetreiber – IaaS) wird durch Art. 28 DSGVO an strengere Vorgaben geknüpft. Der Auftragnehmer seinerseits hat jetzt dafür Sorge zu tragen – und haftet auch dafür – dass seine Subunternehmer ebenfalls DSGVO-konform vorgehen (Art. 28, Abs. 4 DSGVO). Hierbei ist zu beachten, dass der Verantwortliche (Auftraggeber) den Einsatz von Subunternehmern genehmigen muss (Art. 28, Abs. 2, DSGVO).
- Der Auftragnehmer wird nach Art. 28, Abs. 3e DSGVO unter anderem stärker in die Pflicht genommen, so dass er „… den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen

Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte [Informationspflicht, Berichtigung, Löschung u.a.] der betroffenen Person nachzukommen“.

Diesem Umstand sollte bei der Vertragsgestaltung unbedingt Beachtung geschenkt werden. Dies umzusetzen kann allerdings bei den größtenteils hoch standardisierten Cloud-Service-Verträgen der Provider eine Herausforderung sein.

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Die Pflicht zum Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen trifft nach Art. 25 DSGVO formal den Auftraggeber. Diese Pflicht, geeignete technische und organisatorische Maßnahmen bei der Datenverarbeitung zu ergreifen, wird allerdings faktisch auf den Cloud-Provider „durchschlagen“, da die Umsetzung nicht durch die Nutzung des Cloud-Services allein sichergestellt werden kann. Im besten Fall ist dies bereits im Vertrag geregelt.

Lese-Tipp:
amendos Spezial „Cloud Services“

Cloud-Services außerhalb der EU

Die Übermittlung personenbezogener Daten in Länder außerhalb der EU (sog. Drittstaaten) wird durch die DSGVO in Art. 44 ff. geregelt. Unverändert bleibt die Zweistufigkeit der Prüfung der Zulässigkeit einer Verarbeitung in Drittstaaten:

- Ist die Verarbeitung durch den Cloud-Provider zulässig (siehe Auftragsverarbeitung – Art. 28)?
- Darf die Verarbeitung im oder der Zugriff aus dem Drittstaat erfolgen (Art. 44 ff. DSGVO)?

Diese Prüfung ist entsprechend für jeden Subunternehmer durchzuführen. Bei Cloud-Services würde das bedeuteten: hat ein Provider kein eigenes Rechenzentrum, dann ist der Rechenzentrumsbetreiber der Subunternehmer.

Eine erfreuliche Situation ergibt sich durch Erwägungsgrund 171 DSGVO. Dieser sieht vor, dass ältere Beschlüsse der EU-Kommission grundsätzlich auch über den An-

wendungsbeginn der DSGVO hinaus wirksam bleiben. Das bedeutet insbesondere, dass EU-US Privacy Shield, EU-Standard-verträge und die bereits erfolgte Anerkennung von Drittstaaten mit angemessenem Datenschutzniveau nicht automatisch entfällt, sondern grundsätzlich gilt.

Ausweitung der Haftung des Cloud-Providers durch die DSGVO

Nach dem alten Bundesdatenschutzgesetz hatte der Auftragsverarbeiter eine komfortable Haftungssituation. Ansprüche waren von Betroffenen gegen den Auftraggeber geltend zu machen. Dies wirkte wie eine Haftungsprivilegierung für die Auftragsverarbeiter.

Die DSGVO kennt eine solche Haftungsprivilegierung nicht mehr. Aus Art. 79 DSGVO ergibt sich, dass der Auftragsverarbeiter direkt verklagt werden kann.

Der Art. 82 Abs. 2 DSGVO geht sogar noch einen Schritt weiter: „Ist sowohl ein Auftraggeber als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt, so haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden, damit ein wirksamer Schadensersatz für die betroffene Person sichergestellt ist.“ Der Auftragsverarbeiter haftet also gegenüber der betroffenen Person auch für einen Fehler des Auftraggebers.

Fazit

Wie man sieht, sind durch die DSGVO viele neue Punkte hinzugekommen, die beim Abschluss eines Vertrags mit einem Cloud-Provider, aber auch bei bestehenden Verträgen beachtet werden müssen. Da es sich jedoch gerade im Bereich Cloud-Services oft um standardisierte Verträge handelt, kann dies durchaus eine Herausforderung darstellen und gegebenenfalls dazu führen, dass Provider ausgetauscht werden müssen. Generell sollte das Thema Datenschutz und DSGVO einen großen Bereich in einer möglichen Checkliste für eine Cloud-Migration einnehmen.

Michael Pfitzmann

Impressum:
amendos gmbh I Frankenstraße 3 I 20097 Hamburg I Tel (040) 248 276 00
Fax (040) 248 276 01 I www.amendos.de I info@amendos.de
Geschäftsführer: Dipl. Oec. Jörg Bujotzek
Handelsregister: AG Hamburg HRB 105648 I Umsatzsteueridentifikationsnummer: DE 814989917
Erscheinungsweise: 4 / jährlich I Bezug: kostenfrei als PDF