Begleitende Hinweise zu der Anlage Auftragsverarbeitung

Leitfaden

bitkom

Herausgeber

Bitkom e. V.
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
Albrechtstraße 10 | 10117 Berlin

Ansprechpartner

Susanne Dehmel | Mitglied der Geschäftsleitung Vertrauen und Sicherheit
T 030 27576-223 | s.dehmel@bitkom.org

Verantwortliches Bitkom-Gremium

AK Datenschutz

Satz & Layout

Sabrina Flemming | Bitkom

Titelbild

vadim yerofeyev – iStock.com

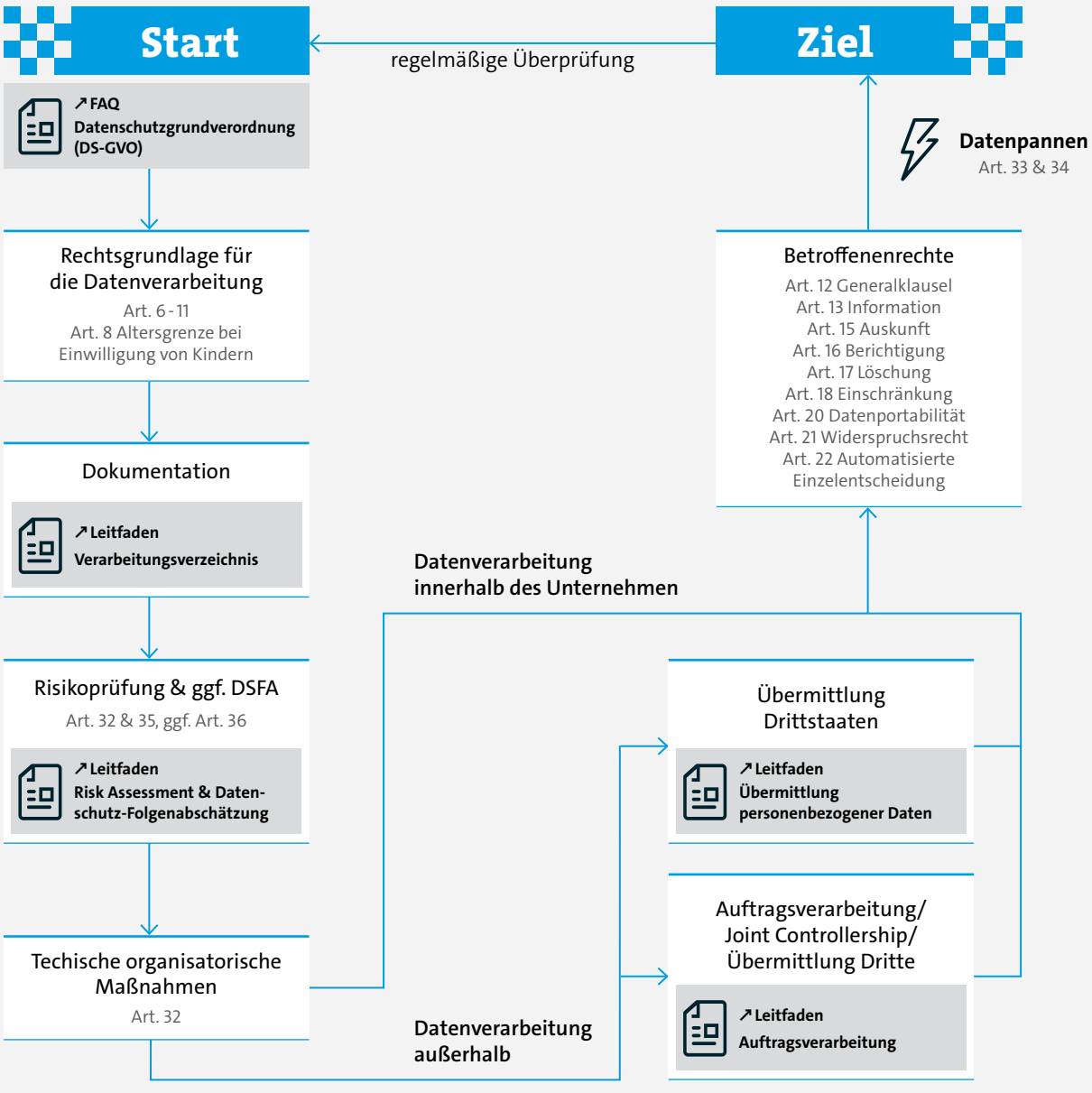
Begleitende Hinweise zu der Anlage Auftragsverarbeitung

Leitfaden

Datenschutzkonforme Datenverarbeitung

nach der EU-Datenschutz-Grundverordnung (DS-GVO)*

Art. 5 Datenschutzprinzipien & Art. 25 Datenschutz durch Technikgestaltung



*alle Artikel sind solche der DS-GVO

bitkom

Inhaltsverzeichnis

Vorwort 4

Definitionen 6

Executive Summary 8

Gegenüberstellung BDSG und DS-GVO 11

Einleitung 14

1 Wann liegt eine Auftragsverarbeitung vor? 17

1.1 Abgrenzung Übermittlung – Auftragsverarbeitung 17

1.2 Gemeinsam Verantwortliche (»Joint Controllership«) 19

1.2.1 Begriffe 19

1.2.2 Gemeinsame Verantwortung 20

1.2.3 Folgen 21

1.3 Wartung und Prüfung 22

1.4 Nebenleistungen 23

2 Verantwortung und Umsetzung 25

2.1 Auswahl des Auftragsverarbeiters (»hinreichende Garantien«) 25

2.2 Sicherheitsmaßnahmen gemäß DS-GVO 25

2.3 Dokumentationspflichten 27

2.3.1 Dokumentationspflichten gegenüber dem Auftraggeber (Verantwortlichen) 28

2.3.2 Dokumentationspflichten gegenüber der Datenschutzaufsichtsbehörde 29

2.4 Einbeziehung von Subunternehmern durch den Auftragsverarbeiter 29

2.5 Mögliche zusätzliche Kostenregelungen 30

2.6 Mögliche zusätzliche Haftungsregelungen 30

3 Übergangsregelungen 34

4 Erläuterungen zu den Regelungen der Anlage 37

Anlage 41

Vorwort

Die aktualisierte Version 1.1 wurde im Mai 2017 auf Basis der EU-Datenschutz-Grundverordnung erstellt und löst den bisherigen Leitfaden ab. Die Datenschutz-Grundverordnung ist ab 25. Mai 2018 anzuwenden.

Für die Aktualisierung danken wir insbesondere folgenden Mitgliedern des Arbeitskreises:

- Josef Beck, Atos Information Technology GmbH
- Mareike Böddeker, Bertelsmann SE & Co. KGaA
- Sebastian Brüggemann, IBM Deutschland GmbH
- Giovanni Brugugnone, Hewlett-Packard Europa
- Almuth Flunkert, Hewlett-Packard GmbH
- Markus Frowein, Telefónica Germany GmbH & Co. OHG
- Hens Gehrandt, arvato direct services Münster GmbH
- Wulf Kamlah, SKW Schwarz Rechtsanwälte
- Rudi Kramer, Datev eG
- Ilona Lindemann, gkv informatik GbR
- Regina Mühlich, Teqcycle Solutions GmbH
- Karolina Rozek, Robert Bosch GmbH
- Martin Schweinoch, SKW Schwarz Rechtsanwälte
- Sylle Schreyer-Bestmann, CMS Hasche Sigle Partnerschaft von Rechtsanwälten und Steuerberatern mbB
- Andreas Splittgerber, Olswang Germany LLP
- Hendrik Tamm, HSH Soft- und Hardware Vertriebs GmbH
- Florian Thoma, Accenture GmbH
- Christian Wagner, Nokia and Networks GmbH & Co. KG
- Stephan Weinert, Computacenter AG & Co. oHG

Zur ursprünglichen Version des Leitfadens hatten maßgeblich beigetragen: Rudi Kramer, Lars Marten Kripko, Ilona Lindemann, Catrin Peter, Hermann-Josef Schwab, Christian Wagner, Stephan Weinert.

Der Arbeitskreis Datenschutz besteht aus Experten der Bitkom-Mitgliedsfirmen und befasst sich mit aktuellen Themen und datenschutzspezifischen Aspekten der Informations- und Kommunikationstechnik. Ein Profil des Arbeitskreises befindet sich am Ende des Leitfadens.

Als weitere Publikationen des Arbeitskreises Datenschutz sind erhältlich:

- Grafik Datenschutzkonforme Datenverarbeitung nach der EU-Datenschutz-Grundverordnung. (Siehe Seite 2) Stand April 2017. Download möglich auf Webseite.

- FAQ – Was muss ich wissen zur EU-Datenschutz Grundverordnung? Stand September 2016. Download möglich auf Bitkom Webseite: ↗ **https://www.bitkom.org/Bitkom/Publikationen/FAQ-zur-Datenschutzgrundverordnung.html**

- Leitfaden Risk Assessment und Datenschutz-Folgenabschätzung. Stand April 2017. Download möglich auf Bitkom Webseite: ↗ **https://www.bitkom.org/Bitkom/Publikationen/Risk-Assessment-und-Datenschutz-Folgenabschätzung**

- Übermittlung personenbezogener Daten – Inland, EU-Länder, Drittländer. Stand 2016.* Download möglich auf Bitkom Webseite: ↗ **https://www.bitkom.org/Bitkom/Publikationen/Uebermittlung-personenbezogener-Daten-Inland-EU-Laender-Drittlaender-2.html**

- Das Verarbeitungsverzeichnis (Version 4.0). Stand Mai 2017. Download möglich auf Bitkom Webseite: ↗ **https://www.bitkom.org/Bitkom/Publikationen/Das-Verarbeitungsverzeichnis.html**

Berlin, Mai 2017

*Diese beiden Publikationen werden derzeit an die Anforderungen der Datenschutz-Grundverordnung angepasst.

Definitionen

Personenbezogene Daten

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, vgl. Art. 4 Nr. 1 DS-GVO.

Auftragsverarbeiter

Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet, vgl. Art. 4 Nr. 8 DS-GVO.

Datenverarbeitung im Auftrag

Es gibt keine Legaldefinition des Begriffs der Auftragsverarbeitung in der DS-GVO. Art. 28 DS-GVO legt lediglich die Anforderungen fest, bei dieser Art der arbeitsteiligen Datenverarbeitungen bestehen. Demnach ist eine Datenverarbeitung im Auftrag die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter (Auftragnehmer) nach Weisung und im Auftrag des Verantwortlichen (Auftraggeber).

Weisung

Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt; der Autraggeber hat ein Weisungsrecht im Rahmen dieser vereinbarten Leistung.

Subunternehmer

Als Auftragnehmer des Auftragsverarbeiters im Sinne der DS-GVO ist der Subunternehmer ein »weiterer Auftragsverarbeiter«, vgl. Art. 28 Abs. 4 DS-GVO. Zur Vermeidung von Missverständnissen aufgrund der Erinnerung an § 11 Abs. 5 BDSG alt, sollte eine weitere Auftragsverarbeiter nur bei der Teil- oder vollständigen Übernahme der Hauptleistung definiert werden.

Dritter

Der Ausdruck »Dritter« bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten (Art. 4 Nr. 10 DS-GVO).

Datenübermittlung

Phase der Datenverarbeitung, in der personenbezogenen Daten von dem Verantwortlichen an andere Personen oder Stellen (Dritte) bekannt oder weitergegeben gegeben werden; im BDSG definiert in § 3 Abs. 4 Nr. 3. Die Bekanntgabe kann durch aktive Weitergabe, gleich in welcher Form, oder durch Einsicht eines Dritten oder Abruf der Daten durch einen Dritten erfolgen. Demgegenüber verwendet die DS-GVO eine umfassendere, weniger differenzierte Begriffsbestimmung der Verarbeitung (Art.4 Nr. 2 DS-GVO), der die Übermittlung umfasst.

»Funktionsübertragung«

Übertragung einer ganzen Funktion zur eigenverantwortlichen Wahrnehmung durch den Auftragnehmer (in Abgrenzung zur Datenverarbeitung im Auftrag).

Mit diesem Begriff, der weder im BDSG, der RL 95/46 EG noch in der DS-GVO definiert wird, wird seit seiner Erwähnung in einer Gesetzesbegründung zum BDSG im Jahr 1989 eine weisungsabhängige, primär technische Dienstleistung (Auftragsverarbeitung) von einer (weitgehend) weisungsfreien, dabei eigene Aufgaben erfüllende Leistungserbringung abgegrenzt. Der Dienstleister wird dabei auch wegen der eigenen verfolgten Zwecke damit zu einem Verantwortlichen (Beispiele: Rechtsanwalt, Steuerberater Wirtschaftsprüfer oder auch Gutachter). Die Rechtmäßigkeitsgrundlage für die Übermittlung (Verarbeitung) der personenbezogenen Daten an solche Funktionsübernehmer ist meistens das überwiegende berechtigte Interesse (bisher nach § 28 Abs. 1 Nr. 2 BDSG). Dieses Konstrukt ermöglicht auch die DS-GVO in Art. 6 Abs. 1 lit. f) DS-GVO.

Drittland

Ein Land, das sich außerhalb der EU/EWR befindet. Die Voraussetzungen der Datenübermittlung in ein Drittland sind ausführlich dargestellt in der Bitkom Publikation »Übermittlung personenbezogene Daten - Inland, EU-Länder, Drittländer« (Version 1.1). (Download möglich auf der Bitkom Webseite: **↗ https://www.bitkom.org/Bitkom/Publikationen/Uebermittlung-personenbezogener-Daten-Inland-EU-Laender-Drittlaender-2.html**). In der DS-GVO wird diese Thematik im 5. Kapitel behandelt.

Executive Summary

Änderungen an der Auftragsverarbeitung durch die Datenschutz-Grundverordnung

Anpassung der Begrifflichkeiten: Es haben sich teilweise die Begrifflichkeiten geändert. So spricht man zukünftig nur noch von »Auftragsverarbeitung« und »Auftragsverarbeiter« und nicht mehr von »Auftragsdatenverarbeitung« und »Auftragsdatenverarbeiter« oder kurz von dem »Verantwortlichen« und nicht mehr »dem für die Verarbeitung Verantwortlichen«.

Auftragsverarbeitung kann zukünftig auch außerhalb der EU stattfinden: Bisher war die Auftragsverarbeitung durch das BDSG auf den EU/EWR beschränkt. Diese Einschränkung ergab sich jedoch nicht aus der EU-Richtlinie 95/46, sodass in anderen EU-Mitgliedsstaaten auch schon bisher für die Übermittlung innerhalb der EU und an einen Drittstaat im Ausgangspunkt die gleichen Anforderungen galten. Durch die DS-GVO werden die Anforderung europaweit einheitlich geklärt. Unter der DS-GVO kann die Datenverarbeitung im Auftrag auch außerhalb der EU stattfinden, da die Definition des Auftragsverarbeiters in Art. 4 Abs.8 DS-GVO keine Beschränkung mehr vorsieht.

Die Auftragsverarbeitung kann zukünftig auch im elektronischen Format erfolgen: Nach Art. 28 Abs. 9 DS-GVO besteht die Verpflichtung den Vertrag schriftlich abzufassen, was auch im elektronischen Format (Textform) erfolgen kann d.h. eine Auftragsverarbeitung kann auch ohne eigenhändige Unterschrift bzw. elektronisch qualifizierte Signatur abgeschlossen werden. Dies war zwar auch bisher unter der Richtlinie 95/46 (»schriftlich o. in anderer Weise dokumentiert«) nach europarechtskonformer Auslegung möglich, allerdings fehlte in Deutschland diesbezüglich eine Klarstellung, sodass ein strenges Schriftformerfordernis nach §126a BGB in das BDSG hineininterpretiert wurde.

Neben der Auftragsverarbeitung gibt es zukünftig auch die »Joint Controllership«: Die »Joint Controllership«, bei der zwei verantwortliche Stellen gemeinsam Daten mit jeweils vertraglich festgelegten Verantwortlichkeiten verarbeiten, war dem BDSG ebenfalls nicht bekannt (jedoch schon in der EU-Richtlinie enthalten)(mehr Infos unter 1.2).

Die EU-Kommission kann zukünftig auch Standardvertrasgklauseln für die Auftragsverarbeitung veröffentlichen: Sowohl EU-Kommission als auch Aufsichtsbehörden können unter der DS-GVO Standardvertragsklauseln veröffentlichen.

Nachweis von Garantien des Datenverarbeiters können durch Zertifizierung und genehmigte Verhaltensregeln erfolgen: Die DS-GVO nimmt erstmalig spezifische Vorschriften zur Zertifizierung und Codes of Conduct auf (mehr Infos unter 2.3.1).

Mehr Spielraum bei der Kontrollpflicht des Auftragsverarbeiters: Die DS-GVO schafft mehr Rechtsklarheit bei der Kontrollpflicht des Auftragsverarbeiters. In der Vergangenheit war nach § 11 Abs. 2 BDSG die Überprüfung der technischen und organisatorischen Maßnahmen und deren Dokumentation durch den Verantwortlichen vor Aufnahme sowie regelmäßig während der Datenverarbeitung vorgeschrieben. Dabei war beispielsweise umstritten, ob der Auftraggeber dieser Kontrollpflicht persönlich oder vor Ort nachkommen musste. In der DS-GVO wird die Kontrolle nicht vorab, regelmäßig und auch nicht vor Ort gefordert. Sie kann auch, so nun explizit klargestellt, durch Prüfung von Zertifikaten oder ähnlichen Nachweisen, die als Garantien dienen, erfolgen. Die Dokumentationspflichten ergeben sich aus den Nachweispflichten. Insbesondere eine fehlende Überprüfung der technischen und organisatorischen Maßnahmen und deren Dokumentation vor Aufnahme der Datenverarbeitung war nach BDSG noch bußgeldbewährt (mehr Infos unter 2.3.1).

Auch Auftragsverarbeiter haben zukünftig Dokumentationspflichten: Auch Auftragsverarbeiter müssen künftig eine schriftliche bzw. elektronische Dokumentation ihrer Verarbeitungstätigkeiten führen (Verarbeitungsverzeichnis, das bisher nur für Verantwortliche verpflichtend war) und auf Verlangen der Aufsichtsbehörde zur Verfügung stellen. Die Pflicht zur Führung eines solchen Verzeichnisses besteht nur für Unternehmen oder Einrichtungen, die 250 oder mehr Mitarbeiter beschäftigen, solange durch die Verarbeitung keine Risiken für den Betroffenen bestehen. Bei der Verarbeitung von sensiblen Daten besteht diese Pflicht immer (mehr Infos unter 2.3).

Kein öffentliches Verzeichnis und keine Meldepflicht mehr: Ein öffentlich für jedermann zugängliches Verzeichnis zu den eingesetzten automatisierten Verfahren für die Verarbeitung personenbezogener Daten ist dagegen weder für den Verantwortlichen noch für den Auftragsverarbeiter unter der DS-GVO vorgesehen. Auch die Meldepflichten unter § 4d und § 4de BDSG für manche Unternehmen entfallen.

Auftragsverarbeiter haben zukünftig eine Unterstützungsfunktion: Der Verantwortliche kann sich seiner Verpflichtungen gegenüber Betroffenen (Kapitel III) oder der Verpflichtungen nach Artt. 32 – 36 DS-GVO nicht dadurch entziehen, dass er auf die Einbindung eines Auftragsverarbeiters verweist. Bindet er einen Auftragsverarbeiter ein, muss er mit diesem eine Unterstützungspflicht vereinbaren, wenn er seinen Verpflichtungen nicht alleine nachkommen kann oder will. Der Auftragsverarbeiter muss dann den Verantwortlichen im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche Betroffener gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Artt. 33 bis 36 DS-GVO genannten Pflichten z. B. der Datenschutz-Folgenabschätzung unterstützen.

Der Auftragsverarbeiter haftet zukünftig direkt gegenüber dem Betroffenen: Nach Art. 82 Abs. 1, 4 DS-GVO haftet im Gegensatz zur bisherigen Rechtslage nicht nur der Verantwortliche, sondern auch der Auftragsverarbeiter z. B. bei Datenpannen gegenüber dem Betroffenen im Außenverhältnis gesamtschuldnerisch auf Schadenersatz (mehr Infos unter 2.6).

Aufsichtsbehörden können Sanktionen zukünftig auch direkt gegen den Auftragsverarbeiter verhängen: Nicht nur die möglichen Geldbußen für Verstöße wurden drastisch nach Art. 83 DS-GVO erhöht – auf bis zu 2 Prozent des weltweiten Umsatzes pro Verstoß. Aufsichtsbehörden können die Sanktionen auch direkt gegenüber Auftragsverarbeitern verhängen.

Keine spezifische Regelung unter der Datenschutz-Grundverordnung zu Wartung und Prüfung: Anders als im BDSG (§ 11 Abs. 5 BDSG) sieht die DS-GVO keine spezifische Regelung mehr für den Fall der Prüfung und Wartung automatisierter Verfahren oder Datenverarbeitungsanlagen und der dabei möglichen Kenntnisnahme von personenbezogenen Daten vor (mehr Infos unter Punkt 1.3).

Keine spezifische Regelung unter der Datenschutz-Grundverordnung zum Datengeheimnis: Das BDSG hat bisher in § 5 Unternehmen dazu verpflichtet, die Mitarbeiterinnen und Mitarbeiter vor Beginn ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Eine solche explizite Regelung zum »Datengeheimnis« enthält die DS-GVO nicht mehr. Eine Vertraulichkeitsverpflichtung lässt sich aber auch weiterhin aus Art. 24 und Art. 28 Abs.3 lit. b) DS-GVO begründen (mehr Infos unter Punkt 2.1 Siehe auch Bitkom Muster zur Vertraulichkeitsverpflichtung).

Gegenüberstellung BDSG und DS-GVO

BDSG	DS-GVO	Hinweise
§ 3 Abs. 8 S. 3 und 11 Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.	Art. 4 Nr. 10 DS-GVO	DS-GVO enthält keine Beschränkung der Privilegierung der AV auf den EU-/EWR-Raum[1].
§ 11 Abs. 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.	Art. 28 Abs. 1	Verstößt der Auftragsverarbeiter gegen die Weisungen seines Auftragsgebers, wird er auch zur verantwortlichen Stelle (Art. 28 Abs. 10 DS-GVO) mit allen Folgen wie z. B. der Erfüllung der Betroffenenrechte.
Die in den §§ 6, 7 und 8 genannten Rechte sind ihm gegenüber geltend zu machen.	Art. 28 Abs. 1 e)	Der Auftragsverarbeiter unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DS-GVO genannten Rechte des Betroffenen, soweit vereinbart.
§ 11 Abs. 2 Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen.	Art. 28 Abs. 1, 3	Als Beleg können auch genehmigte Verhaltensregeln (Art. 40 DS-GVO) und Zertifizierung (Art. 42 DS-GVO) herangezogen werden.
Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:	Art. 28 Abs. 9	Elektronisches Format (Textform) ist ausreichend.
1. der Gegenstand und die Dauer des Auftrags,	Art. 28 Abs. 3	
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarttbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,	Art. 28 Abs. 3	
3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,	Art. 28 Abs. 1, Abs. 3 c)	Technische und Organisatorische Maßnahmen nach Art. 32 DS-GVO.
4. die Berichtigung, Löschung und Sperrung von Daten,	Art. 28 Abs. 1, Abs. 3 g)	
5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,		

1 Schon die Datenschutzrichtlinie 95/46 enthielt keine Beschränkung wie in §3 Abs. 8 S.3 und 11 BDSG.

BDSG	DS-GVO	Hinweise
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,	Art. 28 Abs. 2, Abs. 3 d), Abs. 4	
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,	Art. 28 Abs. 3 h)	
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,	Art. 33 Abs. 2	
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,	Art. 29	
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.	Art. 28 Abs. 3 g)	
Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.		Keine Vorabkontrolle mehr. Kontrolle kann auch durch Prüfung von Zertifikaten oder ähnlichen Nachweisen, die als Garantien dienen, erfolgen. Die Dokumentationspflichten ergeben sich aus den Nachweispflichten.
§ 11 Abs. 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.	Art. 28 Abs. 3 g), Art. 28 Abs. 3 S. 3	Auch unverzügliche Meldung des Auftragsverarbeiters an Verantwortlichen bei Datenpannen nach Art. 33 Abs. 2 DS-GVO.
§ 11 Abs. 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.		Wartung und Prüfung nicht mehr in DS-GVO geregelt. Mit Aufsichtsbehörden zu diskutieren wie man mit solchen Fällen zukünftig umgehen soll (vgl. Fusnnote 3).

BDSG	DS-GVO	Hinweise
§ 5 Datengeheimnis	Art. 28 Abs. 3 b)	Verpflichtung zur Vertraulichkeit (evtl. weitere gesetzlich geregelte Geheimnisse wie Telekommunikationsgeheimnis, Berufsgeheimnis) bleibt weiterhin bestehen.
	Art. 28 Abs. 5	Vorhandensein genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens; Pflicht zur Aktualisierung der Zertifikate und zur Unterrichtung des Verantwortlichen.
§ 7 Abs. 3 Schadensersatz	Art. 82	Neu: Haftung von Auftragsverarbeitern.

Einleitung

Die Auslagerung von Datenverarbeitungsprozessen oder deren Übertragung auf einen Dienstleister, eine unternehmensfremde Stelle, ist für viele Unternehmen eine wichtige Möglichkeit, externes Spezialwissen zu nutzen, höhere Sicherheitsstandards zu erreichen und effektiver und flexibler zu wirtschaften.

Nach der EU-Datenschutz-Grundverordnung (»DS-GVO«, Verordnung (EU) 2016/679 vom 27. April 2016, ABI.L119/1) trägt das Unternehmen die datenschutzrechtliche Gesamtverantwortung für die Verarbeitung personenbezogener Daten, das über die Zwecke und Mittel der Verarbeitung entscheidet (»Verantwortlicher«). Die DS-GVO erkennt an, dass in der Realität viele Prozesse arbeitsteilig verlaufen, und eröffnet dafür mit Art. 28 DS-GVO die **Auftragsverarbeitung** sowie mit Art. 26 DS-GVO die **gemeinsame Verantwortung**.

Die Auftragsverarbeitung verlangt eine vertragliche Regelung (oder ein anderes »Rechtsinstrument« nach dem Recht der Union oder der Mitgliedsstaaten, Art. 28 Abs. 3 DS-GVO) zwischen Auftraggeber und Auftragnehmer. Im Gegenzug darf das Unternehmen die Daten vom Auftragnehmer verarbeiten lassen, ohne dass es einer weiteren Rechtsmäßigkeitsgrundlage nach Art. 6 DS-GVO bedarf: der Auftragsverarbeiter wird unter der Verantwortung und Kontrolle des Verantwortlichen tätig, weil er durch den Vertrag gebunden wird (Erwägungsgrund 81); es liegt keine »Übermittlung« von Daten an den Auftragnehmer nach Art. 4 Nr. 2 DS-GVO vor und es ist weder die Zustimmung der betroffenen Person noch eine Interessensabwägung erforderlich. Diese Argumentation lässt sich auch auf die Meinung der Art. 29-Datenschutzgruppe zur Auftragsverarbeitung in der Datenschutzrichtlinie 95/46 stützen.[2] Da sich gegenüber der Richtlinie in der DS-GVO weder textlich noch konzeptionell auch in der Definition des Auftragsverarbeiters wie des Verantwortlichen etwas Grundlegendes in diesem Bereich ändert, ist auch weiterhin von einer solchen Legitimation der Auftragsverarbeitung auszugehen.

Textform des Vertrages

Nach Art. 28 Abs. 9 DS-GVO besteht die Verpflichtung den Vertrag schriftlich abzufassen, was auch im elektronischen Format (Textform) erfolgen kann d.h. eine Auftragsverarbeitung kann auch ohne eigenhändige Unterschrift bzw. elektronisch qualifizierte Signatur abgeschlossen werden. Dies war zwar auch bisher unter der Richtlinie 95/46 (»schriftlich o. in anderer Weise dokumentiert«) nach europarechtskonformer Auslegung möglich, allerdings fehlte in Deutschland diesbezüglich eine Klarstellung, sodass ein strenges Schriftformerfordernis nach §126a BGB in das BDSG hineininterpretiert wurde.

2 »Die Rechtmäßigkeit der Datenverarbeitungstätigkeit des Auftragsverarbeiters wird somit durch den von dem vom Verantwortlichen erteilten Auftrag bestimmt. Ein Auftragsverarbeiter, der den Rahmen der ihm übertragenen Aufgaben überschreitet und eine nennenswerte Rolle bei der Entscheidung über die Zwecke und die wesentlichen Mittel der Verarbeitung übernimmt, ist als (gemeinsam) für die Verarbeitung Verantwortlicher einzustufen und nicht als Auftragsverarbeiter.« (Art. 29-Datenschutzgruppe in WP 169, S. 31).

Mindestanforderungen an den Vertrag

Folgende Gegenstände sind gem. Art. 28 Abs. 2 und 3 DS-GVO im Vertrag zu regeln:

- Gegenstand und Dauer der Verarbeitung
- Art und Zweck der Verarbeitung
- Art der personenbezogenen Daten
- Kategorien betroffener Personen
- Pflichten und Rechte des Verantwortlichen
- Umfang der Weisungsbefugnisse
- Verpflichtung der zur Verarbeitung befugten Personen zur Vertraulichkeit
- Sicherstellung von technischen & organisatorischen Maßnahmen
- Hinzuziehung von Subunternehmern
- Unterstützung des Verantwortlichen bei Anfragen und Ansprüchen Betroffener
- Unterstützung des Verantwortlichen bei der Meldepflicht bei Datenschutzverletzungen und der Datenschutz-Folgenabschätzung
- Rückgabe oder Löschung personenbezogener Daten nach Abschluss der Auftragsverarbeitung
- Rückgabe oder Löschung personenbezogener Daten nach Abschluss der Auftragsverarbeitung
- Regelung wie der Nachweis der Einhaltung der in Art. 28 niedergelegten Pflichten erfolgt. Dies kann auch durch Überprüfungen und Inspektionen auch durch einen beauftragten Prüfer vereinbart werden.
- Pflicht des Auftragsverarbeiters, den Verantwortlichen unverzüglich zu informieren, falls eine Weisung gegen Datenschutzrecht verstößt

Darüber hinaus zu regelnde Inhalte:

- Haftung

1 Wann liegt eine Auftragsverarbeitung vor?

1 Wann liegt eine Auftragsverarbeitung vor?

Wenn Daten nicht von der verantwortlichen Stelle (allein) verarbeitet werden, sondern eine andere rechtliche Einheit involviert ist, kommen drei grundsätzliche Konstellationen in Frage, die jeweils unterschiedliche formale und materielle Rechtmäßigkeitsvoraussetzungen haben:

Auftragsverarbeitung	Joint Controllership	Übermittlung (Funktionsübertragung)
Erlaubnistatbestand für Verarbeitung durch verantwortliche Stelle	Erlaubnistatbestand für Verarbeitung durch beide verantwortliche Stellen	Erlaubnistatbestand für die Übermittlung vom einen Verantwortlichen zum anderen
+	+	+
Vertrag/sonstiges Rechtsinstrument gemäß Art. 28 III DS-GVO als Rechtmäßigkeitsvoraussetzung für Verarbeitung durch Auftragsverarbeiter	Vereinbarung gemäß Art. 26 DS-GVO zur Verteilung der Pflichten	Erlaubnistatbestand für Verarbeitung bei der anderen verantwortlichen Stelle

1.1 Abgrenzung Übermittlung – Auftragsverarbeitung

Nicht jede Konstellation, in der ein Unternehmen sich eines Dritten zur Datenverarbeitung bedient, stellt zugleich eine Auftragsverarbeitung dar. Die Frage, ob eine solche vorliegt, ist jedoch von erheblicher Bedeutung für die Absicherung der Rechtsmäßigkeit der Datenverarbeitung. Liegt eine Auftragsverarbeitung vor, ist zwingend eine Auftragsverarbeitungsvereinbarung abzuschließen.

»Auftragsverarbeitung ist auch zwischen den verschiedenen rechtlichen Einheiten innerhalb eines Konzerns möglich.«

Immer dann, wenn von der Übertragung einer Aufgabe auf eine andere, rechtliche Einheit (innerhalb oder außerhalb der Unternehmensgruppe) auch personenbezogene Daten betroffen sind, sind daher die folgenden **Fragen** zu stellen:

- Ist das wesentliche Element der Dienstleistung auf die Verarbeitung personenbezogener Daten für Zwecke des Auftraggebers gerichtet und besteht kein eigenes Interesse des Dienstleisters an den Daten?
- Legt das beauftragende Unternehmen die Zwecke und Mittel der Verarbeitung im Wesentlichen selbst fest?
- Hat die datenverarbeitende Stelle ausschließlich eine (technsiche) Hilfs- oder Unterstützungsfunktion?

Sind diese Fragen zu bejahen, wird in der Regel eine **Auftragsverarbeitung** vorliegen. Diese ist nach »unten« abzugrenzen: ist Zweck des arbeitsteiligen Zusammenwirkens nicht die Datenverarbeitung, sondern erfolgt die Weitergabe personenbezogener Daten nur als Mittel zur Erbringung anderer Leistungen, so liegt noch keine Auftragsverarbeitung vor.

Spielt die Datenverarbeitung hingegen nur eine untergeordnete Rolle bei der Aufgabenübertragung, kann z. B. eine vollkommen anders zu handhabende **Funktionsübertragung** vorliegen (wie beispielsweise bei der Finanzbuchführung oder Gehaltsabrechnung durch einen Steuerberater). Die Grundlage für diese Übermittlung zur eigenverantwortlichen Ausführung des Auftrags findet sich im Regelfall in Art. 6 Abs. 1 lit. f) DS-GVO (bislang § 28 Abs. 1 Nr. 2 BDSG) – der Wahrung berechtigter Interessen.

Von der Auftragsverarbeitung können alle Aspekte der **Verarbeitung** personenbezogener Daten nach Art. 4 Nr. 2 erfasst sein, d. h. jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verarbeitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Diese Verarbeitungszwecke können für die Erfüllung der Aufgaben und Geschäftszwecke des Verantwortlichen, räumlich oder ideell, ausgelagert werden. Der **Auftragnehmer** hat dementsprechend nur eine unterstützende Funktion, in der er dem Auftraggeber in einer oder mehreren Phasen der Verarbeitung behilflich ist. Er wird gleichsam als »verlängerter Arm« des Auftraggebers tätig, weil keine Aufgabe in ihrer Vollständigkeit, sondern lediglich ihre technische Ausführung übertragen wird. Behörde, Einrichtung oder andere Auftragsverarbeiter kann nach Art. 4 Nr. 8 DS-GVO eine natürliche oder juristische Person, Stelle sein, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Wirkt der Dienstleister hingegen nennenswert an der Festlegung von Zwecken und Mitteln der Verarbeitung mit, insbesondere wenn die den Verarbeitungsvorgängen zugrunde liegenden Aufgaben ganz oder teilweise (mit) abgegeben werden – etwa in Form ganzer Geschäftsprozesse – oder erfüllt der Dienstleister überwiegend eigene Geschäftszwecke, dann **wird er selbst zum Verantwortlichen**. Der Auftragnehmer wird dann auch wegen der eigenen verfolgten Zwecke bzw. wegen des Fehlens ausreichender Kontroll- und Steuerungsmöglichkeiten des Auftraggebers (z. B. Steuerberater, Rechtsanwalt, Wirtschaftsprüfer oder auch Gutachter, soweit sie jeweils ihre Fachkunde einbringen und /oder eine berufsrechtlich vorgegebene eigenständige Rolle wahrnehmen) zu einem Verantwortlichen. In solchen Fällen bedarf es sowohl für die Weitergabe der Daten an den Auftragnehmer wie auch für dessen eigenes Tätigwerden jeweils einer Rechtmäßigkeitsgrundlage. Die Grundlage für diese Übermittlung zur eigenverantwortlichen Ausführung des Auftrags findet sich im Regelfall in Art. 6 Abs. 1 lit. f)DS-GVO (bislang § 28 Abs. 1 Nr. 2 BDSG) – der Wahrung berechtigter Interessen.

Für das Vorliegen einer Auftragsverarbeitung spricht es, wenn

- dem Auftragnehmer die Entscheidungsbefugnis über die Daten fehlt.
- der Auftragnehmer mit der Datenverarbeitung keine eigenen Geschäftszwecke verfolgt.
- der Auftragnehmer einem ausdrücklichen Nutzungsverbot in Bezug auf die zu verarbeitenden Daten unterliegt.
- der Auftrag auf die Durchführung einer Datenverarbeitung gerichtet ist, die aber nach außen hin vom Auftraggeber verantwortet wird.
- der Auftragnehmer im Zusammenhang mit der Auftragsverarbeitung in keinerlei vertraglichen Beziehungen zu den von der Datenverarbeitung Betroffenen steht.

Eine Auftragsverarbeitung liegt zum Beispiel regelmäßig vor bei:

- Telefonmarketing und andere Callcenterleistungen soweit nicht vom Unternehmen selbst durchgeführt.
- externer Datenhaltung, insbesondere beim teilweisen oder gesamten Outsourcing eines Rechenzentrums.
- Implementierung neuer IT-Systeme mit Migration bestehender Datenbanken durch den Auftragnehmer.
- Nutzung von Cloudsystemen zur Personal- oder Kundenverwaltung.
- externe Druckdienstleistung.
- manuellem oder elektronischem Archivierungsservice.
- Aktenvernichtung, Vernichtung von Datenträgern.

Hinweis

Wenn Sie Zweifel haben, wie die Aufgabenübertragung richtig einzuordnen ist, sollten Sie sich unbedingt an den Datenschutzbeauftragten Ihres Unternehmens wenden.

1.2 Gemeinsam Verantwortliche (»Joint Controllership«)

1.2.1 Begriffe

Wie in 1.1 dargestellt geht die DS-GVO in Art. 4 Nr. 7 davon aus, dass Verantwortlicher derjenige ist, der »allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (...)«. Auftragsverarbeiter ist diejenige Person oder Stelle, die (so Art. 4 Nr. 8) »personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet«. Damit sind die beiden wesentlichen Rollen, die prägend für die DS-GVO sind (vgl. Kapitel 2: »Verantwortung und Umsetzung«), umrissen.

Aus Art. 4 Nr. 7 DS-GVO ergibt sich zunächst, dass neben der alleinigen Verantwortung auch ein **arbeitsteiliges Zusammenwirken** möglich ist. Ohne ein solches Zusammenarbeiten kommen selbst kleinere und mittlere Unternehmen heute nur noch selten aus, denn es ermöglicht die Inanspruchnahme besonderer Kenntnisse und Erfahrungen und vermeidet unverhältnismäßige Investitionen. Dabei ist das Zusammenwirken nicht zahlenmäßig beschränkt: Art. 26 DS-GVO, die Kernbestimmung über gemeinsam Verantwortliche, nennt »zwei oder mehr Verantwortliche« und verzichtet damit sinnvollerweise auf eine Obergrenze.

Von der gemeinsamen Verantwortung zu unterscheiden ist damit einerseits die alleinige Verantwortung einer Stelle, die die Entscheidungen über Zwecke und Mittel der Verarbeitung selbst und unabhängig von anderen Stellen trifft, und andererseits die Auftragsverarbeitung (dazu bereits oben in 1.1).

»Die Zwecke der und die Mittel zur Verarbeitung« sind dabei nicht ausdrücklich in der DS-GVO definiert. Es ist naheliegend, bezüglich der **Zwecke** auf Art. 5 zurückzugreifen; dort werden die übergreifenden Grundsätze für die Verarbeitung aufgestellt. Es handelt sich demnach um die festgelegten, eindeutigen und legitimen Zwecke, für die personenbezogene Daten verarbeitet werden. Beispiele wären die Personalgewinnung, Personalverwaltung, das Marketing, die Vertragsabwicklung, wobei sich die Zwecke ggf. auch noch genauer spezifizieren lassen. Es geht in allen diesen Fällen also um die Frage, welche Daten für bestimmte Aktivitäten von wem verarbeitet werden müssen.

Bei den **Mitteln der Verarbeitung** geht es um die Maßnahmen, Instrumente, Werkzeuge und Hilfsmittel, mit denen der Zweck (oder die Zwecke) der Verarbeitung erreicht werden sollen. Der Begriff ist relativ weit, jedoch stets mit Bezug auf personenbezogene Daten zu verstehen: so sind etwa die zur Verarbeitung eingesetzte Hard- und Software oder Services (im Sinne des »as a service« Ansatzes) Mittel, nicht aber Elemente, die mit Daten nicht in Berührung kommen (etwa die Kühlung eines Rechenzentrums). Gleichwohl bleibt der Dienstleister bei der Wahl seiner Mittel frei, wenn der Auftraggeber als Verantwortlicher nichts vorgibt: beispielsweise welche Telefonanlage ein Callcenter einsetzt, welches Druckermodell verwendet wird etc.

1.2.2 Gemeinsame Verantwortung

Die gemeinsame Verantwortung entsteht nicht notwendigerweise aus einem gemeinsamen Willen, diese Verantwortung gemeinsam zu tragen bzw. in einer bestimmten Weise aufzuteilen – maßgeblich ist ein **faktisches Verhalten**, das in der gemeinsamen Festlegung von Zwecken und/oder Mitteln besteht.

Beispiel: Ein Unternehmen beauftragt einen Dienstleister, im Rahmen eines Personalbedarfsplanes bei der Besetzung offener Stellen zu unterstützen. Der Dienstleister schreibt die Stellen aus, sichtet Bewerbungsunterlagen und führt eine erste Runde von Gesprächen; einige Kandidaten werden dann in die engere Auswahl genommen und dem Unternehmen vorgeschlagen, das dann eigene Gespräche führt. Das Unternehmen überlässt es dem Dienstleister, geeignete Personalfragebögen zu entwickeln und Medien auszuwählen. Beide wirken faktisch an einem einheitlichen Prozess mit und haben gemeinsam festgelegt, wer welche Teilaufgaben wahrnimmt. Beiden kommen bestimmte Entscheidungskompetenzen zu.

Beispiel: Ein Versicherungskonzern muss aus regulatorischen Gründen für unterschiedliche Sparten unterschiedliche Unternehmen einrichten, die aber gemeinsam auf eine Kundendatenbank zugreifen können.

Dabei sollten untergeordnete Entscheidungen eines der beteiligten Unternehmens, die keine nennenswerten Auswirkungen haben oder die aufgrund von üblichen Standards festgelegt werden können, unberücksichtigt bleiben. Ein Auftragsverarbeiter wird nicht bereits dadurch gemeinsam Verantwortlicher, weil er zwischen verschiedenen Möglichkeiten (z. B. Verschlüsselungsalgorithmen, Rechenzentrumsstandorten, Aktenentsorgern), die dem Stand der Technik entsprechen, eine Auswahl trifft.

Fragestellungen:

- Trifft der Dienstleister Entscheidungen, legt er Dinge fest, beschließt er eigenständig? Oder handelt es sich um Empfehlungen, die sich der Auftragnehmer noch zu eigen machen muss?
- Ist der Auftraggeber fachlich in der Lage (und willens), selbst die wesentlichen Entscheidungen zu treffen, oder besteht daran kein Interesse, geht es vielmehr darum, mit umfangreicheren (Teil-) Prozessen »nichts zu tun zu haben«?
- Ist nach der Vertragsgestaltung der Auftragnehmer der verlängerte Arm, der an den Auftraggeber gebunden ist, oder kommen ihm größere Spielräume zu?
- Handelt es sich um gemeinsame Festlegungen der Beteiligten oder um klare Vorgaben eines Beteiligten? (Dabei kommt es eher auf die Substanz als auf die Form an – allein dass es sich um Abreden in einem Vertrag handelt reicht nicht zur Bejahung der gemeinsamen Festlegung, weil Verträge notwendigerweise von mehreren Beteiligten geschlossen werden.)
- Handelt es sich um ein abgestimmtes Vorgehen oder nimmt sich ein Dienstleister mehr heraus als ihm zusteht?
- Hat der Dienstleister eigene Nutzungsmöglichkeiten an den erhobenen Daten? (Im Beispiel: kann der Dienstleister Kandidaten, die nicht für einen Auftraggeber geeignet sind, anderen Kunden vorschlagen?)

1.2.3 Folgen

Als Folge der gemeinsamen Festlegung von Zwecken und/oder Mitteln entsteht eine gemeinsame Verantwortung, die nach Art. 26 in einer Vereinbarung zu dokumentieren ist. Darin sind u. a. zu regeln:

- wer welche Verpflichtung nach der DS-GVO erfüllt,
- insb. wer für die Wahrung welcher Rechte der Betroffenen verantwortlich ist,
- wer welche Informationspflichten nach Artt. 13 und 14 erfüllt.

Art. 26 ist aber keine Rechtmäßigkeitsgrundlage für die Übermittlung und Verarbeitung der Daten zwischen den gemeinsam für die Verarbeitung Verantwortlichen. Für die Rechtmäßigkeitsgrundlage wird idR Art. 6 Abs. 1 lit. f) heranzuziehen sein.

Die gemeinsam Verantwortlichen sind stets auch Verantwortliche im Sinne von Art. 4 Nr. 7, d. h. sie sind verpflichtet, die einen Verantwortlichen treffenden Pflichten zu erfüllen.

Die Festlegungen sollen dabei den tatsächlichen Verantwortungsbereichen gegenüber den Betroffenen Rechnung tragen; eine Zusammenfassung (nicht die Vereinbarung selbst) ist den Betroffenen zur Verfügung zu stellen (Abs. 2). Ungeachtet der Absprachen können sich Betroffene weiterhin an beide/alle gemeinsam Verantwortliche wenden, um ihre Rechte geltend zu machen, weil ihnen u.U. die Abgrenzungen nicht ausreichend klar sein werden und sie nicht zwischen den Beteiligten hin- und hergeschickt werden sollen (Abs. 3).

1.3 Wartung und Prüfung

Aufträge über Wartung oder Prüfung von IT-Systemen stellen keine Auftragsverarbeitung dar, sofern Gegenstand des Vertrages keine Datenverarbeitung ist, sondern allein auf die Supportleistung abzielt. Es kann zwar nicht ausgeschlossen werden, dass durch die Systemprüfung auch personenbezogene Daten durch den IT-Dienstleister zur Kenntnis genommen werden, nach DS-GVO müssen aber deswegen keine den ADV-Vorgaben entsprechende Regelungen wie nach § 11 Abs. 5 BDSG geschlossen werden. Vielmehr müssen Wartung und Prüfung so organisiert und geregelt werden, dass die Daten entsprechend den in Art. 24 festgelegten Pflichten des Verantwortlichen angemessen geschützt sind. Vorsorglich sollte in solchen Konstellationen ggf. eine Verschwiegenheitsverpflichtung vereinbart werden.

Hinweis

Ohne Belang ist, ob die Wartungsmaßnahmen vor Ort oder per Fernwartung durchgeführt werden (Remote – Zugriff des Auftragnehmers auf personenbezogene Daten beim Auftraggeber).

Zu den Besonderheiten zählt, dass der Auftragnehmer die personenbezogenen Daten des Auftraggebers gerade nicht planmäßig verarbeitet oder nutzt. Häufig verlassen die personenbezogenen Daten auch nicht die IT-Systeme des Auftraggebers.[3]

Im Rahmen der Dienstleistungserbringung muss darauf geachtet werden, dass der Rahmen der Tätigkeiten Wartung oder Prüfung nicht verlassen wird. Entwickelt sich die Dienstleistung dagegen zu einer Auftragsverarbeitung gem. Art. 28 DS-GVO, ist eine entsprechende Vereinbarung zu treffen.

3 Hinweis: In dem Papier zur Auftragsverarbeitung vom 26.10.2016 geht das Bayrische Landesamt für Datenschutz auch davon aus, dass »bestimmte Tätigkeiten, wie eine rein technischen Wartung, unter Umständen nicht zu einer Qualifikation als Aufgtragsverarbeitung und Anwendung von Art. 28 DS-GVO führen.« Sei der Auftragsgegenstand der (Fern-) Wartung allerdings gerade der Umgang mit Datensätzen mit personenbezogenen Daten, so handele es sich weiter um eine Auftagsverarbeitung nach Art. 28 DS-GVO.

In der Konsequenz führt das dazu, dass bei vielen Dienstleistungen der ITK-Branche die gesetzlichen Anforderungen an eine Auftragsverarbeitung nicht zur Anwendung kommen. Betroffen sind zum Beispiel:

- Installation und Wartung von Netzwerken, Hardware (inkl. Telekommunikationsanlagen) sowie Pflege von Software u.a. (Betriebssysteme, Middleware, Anwendungen),
- Parametrisieren von Software,
- Programmentwicklungen, Programmanpassungen bzw. -umstellungen, Fehlersuche und Tests,
- wenn dabei eine Kenntnis von personenbezogenen Daten nicht ausgeschlossen werden kann.

Beispiel Wartung

Die technischen und organisatorischen Maßnahmen der Datensicherung sind wartungsspezifisch zu treffen.

1.4 Nebenleistungen

Eine Auftragsverarbeitung liegt ebenfalls nicht vor, wenn

- die Dienstleistung in speziellen Gesetzen geregelt ist, z. B. Telekommunikationsdienstleistungen oder Postdienstleistungen,
- fremd in Anspruch genommene Tätigkeiten beauftragt werden, die im eigentlichen Kern nicht den Umgang (Verarbeitung) mit personenbezogenen Daten betreffen, sondern in denen andere Dienstleistungsschwerpunkte im Vordergrund stehen und der dabei notwendigerweise verbundene Umgang mit personenbezogenen Daten nur ein unvermeidliches »Beiwerk« darstellt (z. B. Pförtnerdienstleistungen, Wachschutz, Reinigungsdienstleistungen, Handwerkereinsätze in Unternehmen, Hauspostverteilung).

2 Verantwortung und Umsetzung

2 Verantwortung und Umsetzung

2.1 Auswahl des Auftragsverarbeiters (»hinreichende Garantien«)

Liegt eine Auftragsverarbeitung vor, so ist der Auftraggeber für die Einhaltung der gesetzlichen Datenschutzvorschriften allein verantwortlich. Dementsprechend ist der Auftraggeber verpflichtet, den Auftragnehmer sorgfältig auszuwählen und er hat sich von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zum Schutz der betroffenen personenbezogenen Daten zu überzeugen.

Der Umsetzung dieser Anforderungen soll die vorliegende »Mustervereinbarung AV« als Anlage zum Vertrag dienen, die zugleich noch weitere im Zusammenhang mit der Auftragsverarbeitung häufig auftauchende Fragen regelt.

Der Auftragnehmer muss seinerseits sicherstellen, dass die Datenverarbeitung nach den, durch den Auftraggeber erteilten, Weisungen erfolgt. Er hat außerdem in seinem Verantwortungsbereich die technischen und organisatorischen Maßnahmen nach Art. 32 DS-GVO (siehe 2.2) selbständig umzusetzen und einzuhalten, die für den Schutz der betroffenen personenbezogenen Daten angemessen sind und die mit dem Auftraggeber vereinbart wurden. Seine Mitarbeiter sind von ihm zur Vertraulichkeit zu verpflichten. Verweise auf Rechtsvorschriften in der Vereinbarung sind an das jeweils geltende nationale Recht anzupassen.

Die nachfolgend beschriebenen Maßnahmen führen beispielhaft die Mindestanforderungen an die zu treffenden Sicherheitsvorkehrungen im Rahmen einer Auftragsverarbeitung auf. Sie sind für den konkreten Fall entsprechend anzupassen und soweit nicht bereits im Vertrag (zum Beispiel in der Anlage zur Leistungsbeschreibung) festgelegt, in der »Mustervereinbarung AV« in § 3 Abs. 2 aufzuführen und damit zu vereinbaren.

2.2 Sicherheitsmaßnahmen gemäß DS-GVO

Maßnahmen der Informationssicherheit (technisch-organisatorische Maßnahmen (TOMs)) werden in Art. 32 der DS-GVO beschrieben. Dort gibt der europäische Gesetzgeber rudimentäre Informationen, nach welchen Kriterien diese zu wählen sind, um ein angemessenes Schutzniveau zu gewährleisten.

Technische und organistorische Maßnahmen nach Anlage zu §9 BDSG

Bisher legte § 9 BDSG technische und organisatorische Maßnahmen fest. Diese sollten verhältnismäßig zum angestrebten Schutzzweck sein und wurden in Form umzusetzender Kontrollen (Zugangskontrolle, Zutrittskontrolle ...) in der Anlage zu § 9 BDSG aufgezählt. Viele Beschreibungen der TOMs in Verträgen zur Auftragsdatenverarbeitung orientierten sich sehr schematisch an dieser Anlage.

Sicherheitsmaßnahmen nach Art. 32 DS-GVO

Nach der DS-GVO ist die Systematik zur Ermittlung geeigneter TOMs nun explizit auf eine Bewertung anhand der ermittelten Risiken ausgerichtet (risikobasierter Ansatz). Eine solche Bewertung und Ableitung von Maßnahmen anhand von Risiken ist in vielen Unternehmen keine neue Methode, bspw. haben viele Unternehmen bereits ein Risikomanagement für Informationssicherheitsrisiken. Jedoch unterscheidet sich der Ansatz in der DS-GVO etwas von der reinen Betrachtung aus der Perspektive der Informationssicherheit. Wie eine solche Risikobewertung aussehen kann, können Sie im Bitkom Leitfaden Risikoabschätzung und Datenschutz-Folgenbschätzung nachlesen.

Art. 32 Abs. 1 verlangt vom Verantwortlichen und vom Auftragsverarbeiter konkret, dass zum Schutz personenbezogener Daten angemessene Sicherheitsmaßnahmen ergriffen werden müssen: »Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten;«

Abhängig vom Risiko müssen also geeignete TOMs ausgewählt und eingesetzt werden, die darauf abzielen müssen, das ermittelte Risiko soweit wie möglich zu minimieren. Diese Maßnahmen schließen gem. Art. 32 Abs. 1 S. 2 lit. a) – c) unter anderem Folgendes ein:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Dabei werden als technische Maßnahmen nur die Pseudonymisierung und Verschlüsselung konkret in der DS-GVO hervorgehoben. Für weitere Maßnahmen kann der Auftragsverarbeiter als Orientierung selber einen beliebigen Maßnahmenkatalog heranziehen, sofern die Aspekte des Art. 32 Abs. 1 S. 2 lit a) – c) DS-GVO beachtet werden und neben den reinen Sicherheitsmaßnahmen auch datenschutzspezifische technische Maßnahmen ausgewählt werden. Angesichts hoher Bußgeldrisiken empfiehlt es sich, im Unternehmen einen allgemein anerkannten Maßnahmenkatalog zu verwenden.

In der **Informationssicherheit** werden bspw. die folgenden Maßnahmenkataloge eingesetzt:

- ISO/IEC DIS 29151: Leitfaden für den Schutz personenbezogener Daten
- ISO/IEC 27001: Anhang A und ISO/IEC 27002 als Leitfaden zur Auslegung der Maßnahmen. Zusätzlich kann auf sektorspezifische Ergänzungen der ISO/IEC 27002 zurückgegriffen werden
- Maßnahmenkataloge der IT-Grundschutz-Kataloge des BSI

Für beide Kataloge gibt es Mapping-Tabellen für Überleitungsrechnungen und sind damit untereinander kompatibel.[4]

Im **Datenschutz** gibt es im BDSG lediglich die Anlage zu § 9 Satz 1 BDSG. Konkrete Maßnahmen zur Umsetzung der Kontrollziele werden von der Literatur vorgeschlagen. Auch gibt es Zuordnungstabellen, um Informationssicherheitsmaßnahmen den Kontrollzielen des BDSG zuzuordnen.[5]

Neben dem Einsatz von Maßnahmenkatelogen sollten beim Technikeinsatz generell parallel auch die Grundsätze zu Datenschutz durch Technikgestaltung und Voreinstellungen (Art. 25 DS-GVO) beachtet und umgesetzt werden, sofern möglich.

Hinweis

In Anlage 1 finden Sie eine Gegenüberstellung der bisherigen Anlage zu § 9 und den Voraussetzungen der DS-GVO als Hilfestellung.

2.3 Dokumentationspflichten

Der Auftragsverarbeiter unterliegt nach der DS-GVO mehreren Dokumentationspflichten, um nachzuweisen, dass die von ihm vorgenommene Verarbeitung personenbezogener Daten den Vorschriften der DS-GVO entspricht. Zum einen besteht die **Dokumentationspflicht im Binnenverhältnis mit seinem Auftraggeber (Verantwortlicher)**. So wird zwischen dem Verantwortlichen und dem Auftragsverarbeiter vertraglich festgehalten, dass der Auftragsverarbeiter alle erforderlichen Informationen zur Einhaltung der in Art. 28 DS-GVO genannten Pflichten nachzuweisen und deren Überprüfung zu ermöglichen hat. Im Außenverhältnis hat der Auftragsverarbeiter ein **Verzeichnis seiner Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DS-GVO** zu führen, welches er auf Anforderung der Datenschutzaufsichtsbehörde vorzulegen hat.

Die Dokumentation ist schriftlich zu führen, was auch ein elektronisches Format (Textform) beinhaltet.

4 Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz, BSI, Abrufbar auf Webseite: ↗ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Doku/Vergleich_ISO27001_GS.pdf?__blob=publicationFile.

5 Maßnahmen der IT-Grundschutzkataloge, BfDI, Abrufbar auf Webseite: ↗ http://www.bfdi.bund.de/SharedDocs/Publikationen/Arbeitshilfen/ErgaenzendeDoks/MassnahmeGS-Kat.pdf?__blob=publicationFile.

2.3.1 Dokumentationspflichten gegenüber dem Auftraggeber (Verantwortlichen)

Der Auftragsverarbeiter hat dem Auftraggeber (Verantwortlicher) alle erforderlichen Informationen zur Einhaltung der in Art. 28 DS-GVO genannten Pflichten nachzuweisen und deren Überprüfung zu ermöglichen. Insbesondere muss er nachweisen, dass technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftragsgebers getroffen wurden (siehe Punkt 2.1 und 2.2). Dem Auftragsverarbeiter steht es generell frei zu entscheiden, auf welche Art und Weise er diesen Nachweis erbringt. Als Instrumente zum Nachweis der getroffenen Vorkehrungen kann der Auftragsverarbeiter erleichtert entweder auf genehmigte Verfahrensregeln (Art. 40 DS-GVO) oder Zertifizierungsverfahren (Art. 42 DS-GVO) zurückgreifen.

- Verfahrensregeln können von Verbänden oder Vereinigungen für bestimmte Branchen oder Datenverarbeitungsvorgänge ausgearbeitet und von Aufsichtsbehörden genehmigt werden. Auftragsverarbeiter, die sich genehmigten Verfahrensregeln unterwerfen, können so die Einhaltung ihrer Pflichten nach DS-GVO nachweisen. Die Einhaltung von Verfahrensregeln wird durch Aufsichtsbehörden oder akkreditierte Stellen geprüft.

- Der Auftragsverarbeiter kann seine Datenverarbeitungsvorgänge von einer akkreditierten Zulassungsstelle und einer Aufsichtsbehörde zertifizieren lassen, um gegenüber seinem Auftraggeber den Nachweis für die Einhaltung seiner Pflichten nach DS-GVO zu erbringen.[6] Eine **Zertifizierung** ist höchstens drei Jahre gültig und wird veröffentlicht. Sie mindert nicht die Verantwortung des Auftragsverarbeiters für die Einhaltung seiner Pflichten nach der DS-GVO.

Kommt der Auftragsverarbeiter seinen Nachweispflichten gegenüber dem Auftraggeber nicht nach, kann er nach Art. 82 Abs. 2 DS-GVO für den von ihm dadurch verursachten Schaden haftbar gemacht werden (siehe 2.6).

Die DS-GVO schafft mehr Rechtsklarheit bei der Kontrollpflicht des Auftragsverarbeiters. In der Vergangenheit war nach § 11 Abs. 2 BDSG die Überprüfung der technischen und organisatorischen Maßnahmen und deren Dokumentation durch den Auftraggeber vor Aufnahme sowie regelmäßig während der Datenverarbeitung vorgeschrieben. Dabei war beispielsweise umstritten, ob der Auftraggeber dieser Kontrollpflicht persönlich oder vor Ort nachkommen musste.[7]
In der DS-GVO ist die Kontrolle nicht vorab, regelmäßig und auch nicht vor Ort gefordert. Eine solche Kontrolle kann je nach Bedarf in den AV-Vertrag mitaufgenommen werden. Sie kann aber auch, so explizit in der DS-GVO klargestellt, durch Prüfung von Zertifikaten oder ähnlichen Nachweisen, die als Garantien dienen, erfolgen. Insbesondere eine fehlende Überprüfung der technischen und organisatorischen Maßnahmen und deren Dokumentation vor Aufnahme der Datenverarbeitung war nach BDSG noch bußgeldbewährt.

6 Mehr zur Akkreditierung siehe BDSG-neu.

7 Vgl. Borges et al., Datenschutzrechtliche Lösungen für Cloud Computing, S.7; Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe Cloud Computing S.9, Weichert, Cloud Computing und Datenschutz.

2.3.2 Dokumentationspflichten gegenüber der Datenschutzaufsichtsbehörde

Unabhängig von Ihren Dokumentationspflichten gegenüber dem Verantwortlichen hat der Auftragsverarbeiter ein Verzeichnis seiner Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DS-GVO zu führen. Dieses Verzeichnis beinhaltet folgende Angaben:

- den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;
- die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Art. 49 Abs. 1 Unterabs. 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1.

Der Auftragsverarbeiter hat **der Datenschutzaufsichtsbehörde das Verzeichnis auf Anforderung zur Verfügung** zu stellen. **Stellen mit weniger als 250 Mitarbeitern**: Die Pflicht, ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DS-GVO zu führen, entfällt, wenn der Auftragsverarbeiter weniger als 250 Mitarbeiter beschäftigt und folgende Bedingungen erfüllt sind:

- Die Verarbeitung der personenbezogenen Daten birgt kein Risiko für die Rechte und Freiheiten der betroffenen Personen.
- Die Verarbeitung der personenbezogenen Daten nur gelegentlich erfolgt.
- Die Verarbeitung nicht besondere Datenkategorien gem. Art. 9 Abs.1 sowie Art. 10 DS-GVO einbezieht.

2.4 Einbeziehung von Subunternehmern durch den Auftragsverarbeiter

Der Auftragsverarbeiter kann ebenfalls Prozesse auslagern und weitere Auftragsverarbeiter (sogenannte »Subunternehmer« oder »Unterauftragsnehmer«) für die Erfüllung bestimmter Aufgaben beauftragen. Dabei legt er seinen Subunternehmern dieselben Datenschutzpflichten auf, die aus dem Vertrag zwischen ihm und dem Verantwortlichen hervorgehen.

Auch der Auftragsverarbeiter muss seine Auftragnehmer sorgfältig auswählen und prüfen, ob diese angemessene technische und organisatorische Maßnahmen gewährleisten (siehe Punkt 2.2).

Die letztendliche Entscheidungsgewalt über die Subunternehmer liegt beim Verantwortlichen, der in der Verarbeitungskette immer die datenschutzrechtliche Gesamtverantwortung für die Verarbeitung personenbezogener Daten behält. Er muss der Einschaltung von Subunternehmern durch den Auftragsverarbeiter gem. Art. 28 Abs.2 DS-GVO entweder durch eine **spezifische oder generelle schriftliche Genehmigung** zustimmen. Diese kann auch in einem elektronischen Format (Textform) erfolgen. Im letzteren Fall muss der Auftragsverarbeiter den Verantwortlichen über eine beabsichtigte weitere Auftragsvergabe an einen Subunternehmer informieren, sodass dieser die Möglichkeit erhält einer solchen Änderung zu wiedersprechen.

2.5 Mögliche zusätzliche Kostenregelungen

Dem Auftraggeber und Auftragsverarbeiter wird empfohlen, sich bei Vertragsschluss darüber einig zu sein, ob für die Unterstützungsleistungen des Auftragsverarbeiters, beispielsweise die Unterstützung bei der Erfüllung der Betroffenenrechte nach Art. 33 - 36 DS-GVO, eine Kostenerstattung geregelt werden soll. Eine solche Kostenregelung ist nicht zwingend notwendig, aber im Hauptvertrag möglich. Laut BayLDA ist beispielsweise eine Kostenregelung bezüglich des Aufwands, der dem Auftragsverarbeiter bei Vor-Ort-Kontrollen durch das Zur Verfügungsstellen von Personal entsteht, keine datenschutzrechtliche, sondern eine zivilrechtliche Streitfrage zur Auslegung eines Vertrags für nicht konkret geregelte Sachverhalte (Kernfrage: Was ist dem Auftragnehmer an Aufwand entschädigungslos zumutbar, damit der Auftraggeber seine BDSG-Kontrollpflichten erfüllen kann, und ab wann besteht ein unzumutbarer Aufwand, für den der Auftragnehmer einen angemessenen Aufwand-Ersatz verlangen kann?). Am besten sei hier eine Festlegung im Vertrag dazu.[8] Hinweise zur möglichen Vergütungsregelung finden Sie auch in der Mustervertragsanlage.

2.6 Mögliche zusätzliche Haftungsregelungen

Die DS-GVO enthält ausdrücklich normierte und detaillierte Haftungsregelungen für das Außen- und Innenverhältnis der Verantwortlichen und Auftragsverarbeiter, wobei eine weitergehende Haftung der an der Verarbeitung Beteiligten nicht ausgeschlossen ist (EW 146 S. 4). Das Haftungssystem insgesamt gibt insbesondere Anreize zur sauberen und klaren Regelung von Pflichten und Rechten in der Auftragsverarbeitungsvereinbarung, sowie auch in der Vereinbarung zwischen gemeinschaftlich Verantwortlichen.

8 So Bay LDA zu Kostenverteilung Vor-Ort-Kontrollen bei ADV, GDD, Datenschutz Newsbox, S.8 ↗ https://www.rdv-online.com/newsletter/newsbox_10_2016.pdf.

Nach Art. 82 Abs. 1, 4 DS-GVO haften der Verantwortliche und Auftragsverarbeiter gegenüber dem Betroffenen im Außenverhältnis gesamtschuldnerisch auf Schadensersatz. Diese Haftung gilt auch für gemeinsame Verantwortliche entsprechend Art. 26 DS-GVO, so dass insoweit kein Unterschied zwischen gemeinsam Verantwortlichen und Auftragsverarbeiter besteht. Ketten von Verarbeitungsvorgängen sind damit grundsätzlich haftungsrechtlich gleichgestellt ohne Ansehung der Stellung als Verantwortlicher oder Auftragsverarbeiter; eine Exkulpation ist – wie bisher – entsprechend Art. 82 Abs. 2 bei Nichtverschulden möglich.

Alle Beteiligten an der Verarbeitungskette haften gegenüber dem Betroffenen voll, d.h. Sie müssen im Außenverhältnis den kompletten Schaden ersetzen, Art. 82 Abs. 4. Erfüllt ein Beteiligter den Anspruch des Betroffenen voll, so kann er über Art. 82 Abs. 5 DS-GVO Rückgriff bei den anderen Beteiligten entsprechend des Verantwortungsbeitrags nehmen.

Beschränkt wird die Haftung des Auftragsverarbeiters im Gegensatz zum gemeinsam Verantwortlichen jedoch auf Verstöße gegen spezifisch ihm betreffende Pflichten aus der Verordnung oder bei Handeln gegen rechtmäßig erteilte Weisungen bzw. bei Handeln unter Nichtbeachtung dieser (Art. 82 Abs. 2 S.2 DS-GVO). Entsprechend des Wortlauts haftet der Auftragsverarbeiter damit gegenüber dem Betroffenen im Umkehrschluss nicht für ihm vertraglich auferlegte Pflichten über die Anforderungen nach Art. 28 Abs. 3, 4 und 5 DS-GVO hinaus.

Der Auftragsverarbeiter verantwortet daher insbesondere, aber auch nur:

- Die weisungs- und zweckgemäßige sowie mittelkonforme Verarbeitung der Daten, inkl. Hinweispflicht bei rechtswidrigen Weisungen
- Die Vertrauchlichkeitsverpflichtung der beteiligten befugten Personen,
- Die ergriffenen technischen und organisatorischen Schutzmaßnahmen,
- Die ordnungsgemäße Beauftragung von Unterauftragnehmern,
- Die Mithilfe bei Wahrnehmung von Betroffenenrechten – soweit vereinbart,
- Unterstützung bei Meldung von Datenschutzvorfällen,
- Unterstützung bei Durchführung von Datenschutz-Folgeabschätzungen – soweit vereinbart,
- Erstellung und Führung eines Verarbeitsungsverzeichnisses der Verarbeitungstätigkeiten im Rahmen der Auftragsverarbeitungen,
- Die Bestellung eines eigenen Datenschutzbeauftragten,
- Ordnungs- und vertragsgemäße Löschung und / oder Rückgabe von Daten nach Abschluss der Verarbeitung sowie,
- Duldung und Mitwirkung bei Prüfungen und Audits des für die Verarbeitung Verantwortlichen.[9]

9 Aufzählung des Art. 28 Abs. 3 a) bis h) und Art. 4. Sowie Art. 30 Abs. 2, Art. 37 Abs. 1.

Geriert sich ein Auftragsverarbeiter durch eigenständige Bestimmung der Zwecke und Mittel der Verarbeitung als Verantwortlicher (Exzess), so haftet er auch als solcher ohne die Beschränkung des Art. 82 Abs. 2 S. 2 DS-GVO (Art. 28 Abs. 10 DS-GVO). Der Auftragsverarbeiter hat damit einen Anreiz, klar dokumentierte Weisungen zu verlangen und diese auch strikt einzuhalten, da er ansonsten seine vorgenannte Haftungsprivilegierung verliert.

Die Abgrenzung zwischen rechtswidriger Verarbeitung eines Auftragsverarbeiters und Gerierung als Verantwortlicher ist im Außenverhältnis nicht bedeutsam, da der betreffende Beteiligte in der Verarbeitungskette in beiden Fällen durch den Betroffenen voll in Anspruch genommen werden kann. Allerdings wird die Bestimmung des genauen Verstoßes des Auftragsverarbeiters im Rahmen des Ausgleichsanspruchs untereinander bedeutsam sein.

Zu empfehlen ist folglich in jedem Fall eine klare Regelung der DS-GVO im Rahmen der Auftragsverarbeitungsvereinbarung, insbesondere der Art, Zwecke und der Mittel der Datenverarbeitung, um beiden Seiten Rechtssicherheit im Zusammenhang mit der Verarbeitung zu geben und die Haftungsrisiken entsprechend der übernommenen Rollen zu verteilen.

Weitere Auftragsverarbeiter (Subdienstleister) gehören im Innenverhältnis dem Haftungsverbund des beauftragten Auftragsverarbeiters an, Art. 28 Abs. 4 S. 2 DS-GVO. Etwaige anteilige Haftung wird damit dem Auftragsverarbeiter im Rahmen des Innenausgleichs nach Art. 82 Abs. 5 DS-GVO zugerechnet. Steigert der Auftragsverarbeiter das Risiko für den Betroffenen durch eine Unterbeauftragung, so steigert er gleichzeitig sein eigenes Risiko am eventuellen Schaden beteiligt zu werden. Dies setzt Anreize für die Auftragsverarbeiter zur sorgfältigen Entscheidung über und die Auswahl von Unterauftragsverarbeitern und entlastet den Verantwortlichen.

Entsprechend der heute herrschenden Meinung wird die Haftung aus Art. 82 DS-GVO die strafrechtliche Verantwortlichkeit oder zivilrechtliche Haftung gegenüber dem Betroffenen nicht ausschließen.

3 Übergangsregelungen

3 Übergangsregelungen

Die Frage nach Übergangsregelungen lässt sich noch nicht abschließend beantworten. Hier kommt es sehr stark auf den Einzellfall an, was beispielsweise bislang unter dem bestehenden Vertrag vereinbart wurde und welche Leistung in der Auftragsverarbeitung konkret erbracht wird. Es wird daher sehr unterschiedliche Szenarien geben, bei denen mal mehr und mal weniger in der AV-Vereinbarung angepasst werden muss. Der Bitkom empfiehlt, sich hier rechtlichen Rat einzuholen. In diesem Papier werden nur ein paar derzeitige Vorüberlegungen mitaufgenommen, die das Bitkom-Muster betreffen:

- Solange mit den Aufsichtsbehörden nicht geklärt ist, dass eine Weitergeltung der ADV-Vereinbarung nach Bitkom-Muster auch die Anforderungen an eine AV-Vereinbarung nach DS-GVO vollständig erfüllt, besteht Notwendigkeit, die von der DS-GVO geforderten Inhalte (Art. 28 Abs. 3) mit dem Kunden vollständig zu vereinbaren.

- Dann ist zivilrechtlich zwischen den Vertragspartnern in ihren Rollen als Auftraggeber und Auftragsdaten-/Auftragsverarbeiter die notwendige Änderung der Vereinbarung zur Auftragsdaten-/Auftragsverarbeitung umzusetzen. Dies kann auf sicherem Weg wohl nur über eine Zustimmung des jeweils anderen Vertragspartner zu einer entsprechenden Vertragsänderung erfolgen. Für diese Zustimmung können im bestehenden Auftragsdatenverarbeitungsvertrag formale Anforderungen vereinbart sein (einfache oder doppelte Schriftform), die zu beachten sind. Insbesondere kann sich der Verwender eines Templates gegenüber seinem Vertragspartner nicht auf eine Unwirksamkeit unveränderter Regelungen in diesem Template berufen.

- Nachdem das BDSG bislang den schriftlichen Abschluss einer Auftragsdatenverarbeitungsvereinbarung verlangt (11 Abs. 2 BDSG), wurde üblicherweise auch eine Schriftformklausel verwendet. Daher werden Änderungen grundsätzlich auch nur schriftlich möglich sein. Dies ist unabhängig davon, dass die DS-GVO auch den Abschluss einer Auftragsverarbeitungsvereinbarung in elektronischer Form ermöglicht.

- Die Vertragspartner müssten vor diesem Hintergrund üblicherweise eine neue Vereinbarung über die Auftragsverarbeitung oder zumindest eine Änderung der bestehenden Vereinbarung um die inhaltlichen Veränderungen schriftlich vereinbaren. Der schriftliche Abschluss der entsprechenden Vereinbarung kann dabei grundsätzlich nicht durch eine stillschweigende oder unterstellte Zustimmung des anderen Vertragspartners ersetzt werden.

- Um die notwendige Änderung umzusetzen, sollte ein neues Vereinbarungsdokument an den anderen Vertragspartner, typischerweise den Auftraggeber, versendet werden mit der Bitte, diesem bis zu einem bestimmten Termin oder innerhalb einer angemessenen Frist durch unterzeichnete Rückleitung zuzustimmen, die auch elektronisch in eingescannter Form oder per Telefax möglich ist. Dann ist die entsprechende gegengezeichnete Rückleitung notwendig, außer es wurde darauf verzichtet (§ 151 BGB).

- Falls eine nach DS-GVO notwenige Auftragsverarbeitungsvereinbarung nicht rechtzeitig vor deren Inkrafttreten abgeschlossen worden ist, müsste der Auftragnehmer seine datenschutzrechtliche Berechtigung zur weiteren Leistungserbringung für den Auftragnehmer kritisch prüfen. Soweit diese Prüfung nicht zu einem positiven Ergebnis führt, hat der Auftragnehmer aufgrund des Verbotsprinzips (Art. 6 Abs. 1 DS-GVO) die weitere Leistungserbringung einzustellen, auch um einer möglichen Verantwortung wegen Überschreitung eines bestehenden Auftrags zu entgehen (Art. 28 Abs. 10 DS-GVO).

4 Erläuterungen zu den Regelungen der Anlage

4 Erläuterungen zu den Regelungen der Anlage

Das Muster ist im Einzelfall aufgabenspezifisch anzupassen. Soweit spezialgesetzliche Regelungen für die Daten, die im Auftrag verarbeitet werden, Anwendung finden, ist zunächst zu prüfen, ob eine Auftragsverarbeitung zulässig ist. Ggf. sind die spezialgesetzlichen Regelungen bei der Vertragsgestaltung (z. B. Beihilfe,- Personal-, Sozial- und Gesundheitsdaten) zu berücksichtigen.

Diese Mustervertragsanlage und die Erläuterungen richten sich an den Erfordernissen des 28 Abs. 3 DS-GVO aus. Sie müssen jedoch **prüfen**, ob Sie ggf. **einem Gesetz mit anderen bzw. weitergehenden Vorschriften** unterliegen. Weitergehende Vorschriften enthalten beispielsweise die Regelungen zur Auftragsverarbeitung im § 80 des SGB (Sozialgesetzbuch) X für Sozialdaten und einige Landesdatenschutzgesetze. Dabei ist vor allem zu beachten, dass einige dieser Gesetze im Gegensatz zur DS-GVO bei der Auftragsverarbeitung eine **Anzeigepflicht** des Auftraggebers gegenüber seiner Aufsichtsbehörde vorsehen. Zudem enthalten §80 SGB X und einige der Landesdatenschutzgesetze ein Weisungsrecht des Auftraggebers auch bezüglich der technisch-organisatorischen Maßnahmen, wie es die DS-GVO nicht kennt.[10]

Anwendungsbereich

Die Anlage kann im Zusammenhang mit allen Verträgen Verwendung finden, die innerhalb Deutschlands oder zwischen einem deutschen Unternehmen und einem Unternehmen der Mitgliedsstaaten der Europäischen Union bzw. des Europäischen Wirtschaftsraums geschlossen werden. Aufgrund der direkten Anwendung der DS-GVO wird keine Unterscheidung mehr getroffen zwischen einer Auftragsverarbeitung in der EU oder in einem Staat außerhalb (sog. Drittland). Eine Beschränkung der Privilegierung der Auftragsverarbeitung ergab sich bisher aus §3 Abs. 8 S.2 BDSG. Bei einer **Datenübermittlung in ein sog. Drittland** muss jedoch ein angmessenes Datenschutzniveau sichergestellt sein (durch Standardvertragsklauseln, BCR, Privacy Shield o. ä.)

Hinweis

Die Voraussetzungen der Datenübermittlung in ein Drittland sind ausführlich dargestellt in der Bitkom Publikation »Übermittlung personenbezogener Daten – Inland, EU-Länder, Drittländer« (Version 1.1). (Download möglich auf Bitkom Webseite: ↗ https://www.bitkom.org/Bitkom/Publikationen/Uebermittlung-personenbezogener-Daten-Inland-EU-Laender-Drittlaender-2.html

10 Hinweis: Dieses Gesetz wird derzeit angepasst.

Hauptvertrag und Anlage

Im Hauptvertrag, der in aller Regel ein Dienst- oder Werkvertrag sein wird, ist in allen Einzelheiten die Leistung des Auftragnehmers beschrieben, aus der sich das Vorliegen einer Auftragsverarbeitung ergibt. Der Hauptvertrag und insbesondere die dortige Leistungsbeschreibung stellen auch den Rahmen bzw. die Grundlage für die Weisungen des Auftraggebers dar. Die Weisungen des Auftraggebers an den Auftragnehmer dienen der Sicherstellung der ordnungsgemäßen und datenschutzgerechten Erfüllung der vertraglich geschuldeten Leistung. In Art. 28 Abs.3 DS-GVO ist festgelegt, dass der Auftragnehmer die Daten »nur auf dokumentierte Weisung« des Auftraggebers verarbeiten darf. Der Auftraggeber bleibt bei der Auftragsverarbeitung also verantwortlich für den Datenschutz.

Hinweis

Beachten Sie bitte den Grundsatz der Datenminimierung. Die Planung, Gestaltung und Auswahl informationstechnischer Produkte und Verfahren haben sich an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu verarbeiten, Art. 5 Abs. 1 lit. c) DS-GVO.

Der Auftragnehmer muss dementsprechend sicherstellen, dass die Datenverarbeitung nur nach den festgelegten Weisungen erfolgt und die technischen und organisatorischen Maßnahmen gemäß der Anlage eingehalten werden.

§ 3 Pflichten des Auftragnehmers

Der Auftragnehmer muss den Weisungen des Auftraggebers folgen. Verstößt er gegen diese Pflicht der weisungsgebundenen Verarbeitung, indem er die Daten des Auftraggebers für eigene Zwecke oder Zwecke Dritter verarbeitet, wird er nach Art. 28 Abs.10 DS-GVO selbst zum Verantwortlichen mit allen rechtlichen Folgen z. B. auch zur Erfüllung der Betroffenenrechte.

Genehmigte Verhaltensregeln nach Art. 40 DS-GVO und Zertifizierung nach Art. 42 DS-GVO werden zum Zeitpunkt der Anwendung der DS-GVO am 25. Mai 2018 sehr wahrscheinlich noch nicht vorliegen. Es kann daher vorübergehend nur auf andere Zertifikate zurückgegriffen werden. Diese Option ist in §3 Abs. 2 Var. 3 formuliert (siehe hierzu auch §6 Abs. 1 Var. 6)).

Für die Verschwiegenheits-/Vertraulichkeitsverpflichtung in § 3 Abs. 4 kann das Bitkom Muster genutzt werden.[11]

§ 4 Pflichten des Auftraggebers

Da in der DS-GVO auch spezielle Haftungsregelungen für den Auftragsverarbeiter bei Datenschutzverletzungen hinzugekommen sind, wonach der Betroffene direkt vom Auftragsverarbeiter Schadenersatz fordern kann, muss der Verantwortliche den Auftragsverarbeiter bei der Abwehr des Anspruchs unterstützen.

11 Hinweis: Dieses Muster wird nach der offiziellen Verabschiedung des DSAnpUG-EU veröffentlicht.

§ 5 Anfragen betroffener Personen

Die Person, deren personenbezogene Daten verarbeitet werden (sog. betroffene Person), kann seine Rechte (z. B. Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung, vgl. Kapitel III der DS-GVO) gegenüber seinem Vertragspartner oder gegenüber dem Unternehmen geltend machen, mit dem er in Beziehung steht. Bei einer Auftragsverarbeitung bleibt daher der Auftraggeber Adressat dieser Ansprüche. Dies hat zur Folge, dass ein Verfahren zwischen Auftraggeber und Auftragnehmer festgelegt werden sollte, das sicherstellt, den Rechten der betroffenen Personen nachkommen zu können. Die Verantwortung hierfür und auch die entstehenden Kosten trägt der Auftraggeber.

§ 6 Nachweismöglichkeiten

In § 3 Abs. 2 der vorliegenden Anlage sind die gesetzlich geforderten Maßnahmen nach Art. 32 DS-GVO wiedergegeben.

Bitte berücksichtigen Sie, dass der Verantwortliche den Auftragsverarbeiter sorgfältig auszuwählen hat und sich von dessen Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen muss. Es ist grundsätzlich nicht erforderlich, dass sich der Auftraggeber unmittelbar beim Auftragnehmer vor Ort oder selbst in Person überzeugt. Je nach Einzelfall kann es auch genügen, Selbstauskünfte des Auftragnehmers einzuholen oder sich ein Testat eines Sachverständigen (z. B. die Einhaltung eines genehmigten Zertifizierungsverfahrens) vorlegen zu lassen (siehe Punkt 2.1). Maßgeblich wird hier stets die Sensitivität der auftragsbezogenen Daten, deren Menge sowie Gefährdungspotential sein. Orientiert an diesen Kriterien ist eine der dargestellten Alternativen zu wählen. Das Ergebnis der Untersuchung ist sachgerecht zu dokumentieren. Der Gesetzgeber selbst macht keine Vorgaben hinsichtlich der Ausgestaltung und Art dieser Dokumentation. Die regelmäßige Kontrolle des Auftragsverarbeiters ist ratsam, aber nicht bußgeldbewehrt. Die geforderte Regelmäßigkeit ist daher im Einzelfall abhängig vom Gefährdungsgrad der verarbeiteten Daten und dem möglichen Schadenspotential festzulegen.

§ 7 Subunternehmer (weitere Auftragsverarbeiter)

Subunternehmer ist jedes im Rahmen des Auftrages tätig werdende Unternehmen, das nicht mit dem Auftragnehmer identisch ist. Auch konzernverbundene Unternehmen des Auftragnehmers können in diesem Sinne Subunternehmer sein.

Beauftragt der Auftraggeber selbst eine Teilleistung direkt bei einem anderen Unternehmen, wird dieses Unternehmen nicht Subunternehmer im Sinne dieser Vereinbarung. Allerdings sollten die Verantwortlichkeiten in diesem Fall dokumentiert werden.

§ 7 Abs. 1

Die »Zustimmung« ist der Oberbegriff für die Einwilligung (=vorherige Zustimmung) und die Genehmigung (=nachträgliche Zustimmung), vgl. § 182 ff BGB.

§ 7 Absatz 2

Für einzelne Tätigkeitsbereiche der Datenverarbeitung kann es notwendig sein, Subunternehmer, also Unterauftragnehmer einzuschalten (z. B. Delegierung von Arbeiten auf Ausweichrechenzentren in Fällen von Überlastung). Zwischen Auftraggeber und Auftragnehmer sollte daher die Zulässigkeit oder Nichtzulässigkeit bestehender und zukünftiger Unterauftragsverhältnisse geregelt werden. Daneben ist ggf. festzulegen, ob dem Auftragnehmer grundsätzlich das Recht zugesprochen werden soll, künftige Unterauftragsverhältnisse abzuschließen und welche Auswirkungen das auf die Beteiligten der Auftragsverarbeitung haben wird.

Die in § 7 vorgeschlagene Regelung ist daher optional. Sie steht im Zusammenhang mit § 3 Abs. 7 der Anlage und bietet zwei alternative Regelungsvorschläge. Alternative 1 stellt eine gesonderte Genehmigung aller Subunternehmer dar. Jede Änderung der Liste bedarf der Zustimmung des Verantwortlichen. Alternative 2 stellt eine allgemeine schriftliche Zustimmung dar, wonach der Auftragsverarbeiter den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter nur informieren muss. Allerdings hat der Verantwortliche bei wichtigem Grund ein Widerspruchsrecht.

§ 7 Absatz 3

Absatz 4 ist für Var.1 und Var.2 des Abs. 2 anzufügen.

Laufzeit und Kündigungsregelung

Diese ergeben sich regelmäßig aus den entsprechenden Regelungen des Hauptvertrags. Zu beachten ist, dass die Vertraulichkeit bzw. Verschwiegenheitspflicht auch nach Beendigung der Tätigkeit fortbesteht. Eine Muster für eine solche Vertraulichkeitsvereinbarung wird ebenfalls vom Bitkom veröffentlicht.

§ 9 Schadensersatz und Haftung

Regelungen zum Schadensersatz wird regelmäßig der Hauptvertrag enthalten. Unter Beachtung und Abwägung der Interessen der Vertragspartner können Höchstgrenzen einzelfallbezogen aufgenommen werden, die sich auch auf die Haftung aus Art. 82 DS-GVO beziehen. Soll gleichwohl auch in die Anlage eine Regelung zur Haftung aufgenommen werden, sollte diese sich an der Regelung des Hauptvertrages orientieren.

Anlage

Überblick zu technischen und organisatorischen Maßnahmen nach BDSG und DS-GVO

Alte Rechtslage	Neue Rechtslage
§ 9 BDSG	Art 5. Abs. 1 c), f) 24, 25, 32, 35, 36 DS-GVO
Maßnahmen **verhältnismäßig** zum angestrebten Schutzzweck. Anders als Art. 32 Abs. 1 benannte § 9 BDSG **die Kriterien zur Bestimmung des Risikos nicht ausdrücklich.**	(1) Unter Berücksichtigung des **Stands der Technik**, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten;
Checklistenbasierte Sicherheitsmaßnahmen: Auswahl der geeigneten Maßnahmen nach Anlage zu §9 BDSG	**Risikobasierte Sicherheitsmaßnahmen: Auwahl der geeigneten Maßnahmen passend zum Ergebnis der Risikoanalyse**
Umzusetzende Kontrollen in der Anlage zu § 9 BDSG	Im Gegensatz zur Anlage 1 zu § 9 BDSG sind die erforderlichen Maßnahmen nach Art. 32 allgemein umschrieben und bedürfen noch der Konkretisierung. Diese **Maßnahmen** schließen gem. Art. 32 Abs. 1 S.2 lit. a) – c) unter anderem Folgendes ein:
1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (**Zutrittskontrolle**), **Bsp**: Sicherheitsbereiche entsprechend dem Schutzbedarf(Besucherbereiche, interne Büros, IT-Räume), Einrichtungen zum Zutrittsschutz (Gebäudesicherung, Wachdienst, Einbruchmeldesystem, Karten- oder schlüsselbasierte Zutrittskontrollsystem), Zutrittsberechtigungen (Personenkreise und Rollenkonzept), Verwaltung der Zutrittsberechtigungen (Verlust der Schließmittel, Ausscheiden und Wechsel in andere Rolle), Protokollierung des Zutritts, Speicherfristen, Ausweistragepflicht, Regelungen zum Zutritt von Dienstleistern und Besuchern. 2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**), **Bsp**: Authentifizierung (User-ID, Passwort, ggf. Zweifaktor-Authentifizierung), Anforderung an Passworte und deren Kontrolle, Verbot der ungeschützten Aufzeichnung von Passworten, Sperrung	a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten; werden beispielhaft als konkrete technische Maßnahmen aufgeführt. Bei weiteren Maßnahmen können grundsätzlich beliebige Maßnahmenkataloge verwendet werden u.a. auch diejenigen, die in den Beispielen links aufgeführt sind. b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und (neu): Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen; hier können grundsätzlich beliebige Maßnahmenkataloge verwendet werden u.a. auch diejenigen, die in den Beispielen links aufgeführt sind. c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen; hier können grundsätzlich beliebige Maßnahmenkataloge verwendet werden. d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Alte Rechtslage	Neue Rechtslage
des Users nach Fehlversuchen, Vorgehensweise zur erneuten Freischaltung des Users, Rollenkonzept zur Vergabe der Zugangsberechtigungen, Vorgehensweise zur Genehmigung, Vergabe und Rücknahme von Zugangsberechtigungen, routinemäßigen Kontrolle der vergebenen Berechtigungen, Protokollierung des Zugangs und Auswertung von Fehlversuchen, Speicherfristen. Automatische Zugangssperre durch Bildschirmschoner, Anweisung zu Sperrung / Log-off bei Abwesenheit. Passworten, Sperrung des Users nach Fehlversuchen, Vorgehensweise zur erneuten Freischaltung des Users, Rollenkonzept zur Vergabe der Zugangsberechtigungen, Vorgehensweise zur Genehmigung, Vergabe und Rücknahme von Zugangsberechtigungen, routinemäßigen Kontrolle der vergebenen Berechtigungen, Protokollierung des Zugangs und Auswertung von Fehlversuchen, Speicherfristen. Automatische Zugangssperre durch Bildschirmschoner, Anweisung zu Sperrung / Log-off bei Abwesenheit. 3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Zugriffskontrolle**), **Bsp**: Beschreibung von systemimmanenten Sicherungsmechanismen, evtl. übergeordnetes Zugriffsschutzsystem, Mehraugenprinzip, automatische Prüfung der Zugriffsberechtigung, eingesetzte Verschlüsselungsverfahren, Rollenkonzept zur Vergabe der Zugriffsberechtigungen, Vorgehensweise zur Genehmigung, Vergabe und Rücknahme von Zugriffsberechtigungen, routinemäßigen Kontrolle der vergebenen Berechtigungen, Umsetzung des Rollenkonzepts in den Verfahren, Protokollierung der Zugriffe und Auswertung von Fehlversuchen, Speicherfristen. Bei Online-Zugriffen des Auftraggebers ist hier zu beschreiben, wer beim Auftraggeber für die Ausgabe und Verwaltung von Zugriffsberechtigungen verantwortlich ist. 4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (**Weitergabekontrolle**),	Datenschutzmanagementprozess muss etabliert werden. (2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden. (3)Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen. (4)Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Alte Rechtslage	Neue Rechtslage
Bsp: Beschreibung der verwendeten Einrichtungen und Übermittlungsprotokolle, z. B. Identifizierung und Authentifizierung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren und Übertragungstechniken, Regelungen zur Datenträgervernichtung oder zur sicheren Löschung vom Speichermedien, Regelungen zur sicheren Lagerung und zum sicheren Versand von Datenträgern, Regelungen zum Gebrauch von mobilen Datenträgern (CDs, USB-Sticks) zur sicheren Lagerung und zum sicheren Versand von Datenträgern, Regelungen zum Gebrauch von mobilen Datenträgern (CDs, USB-Sticks)	
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),	
Bsp: Beschreibung der Protokollierung der Systemaktivitäten, Aufbewahrung von Verarbeitungsprotokollen, Verweis auf Eingabeberechtigte (siehe Rollenkonzept), Protokollierung der Eingaben und Speicherfristen	
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),	
Bsp: Es sollte hier auf die entsprechenden Weisungen zwischen dem Auftraggeber und Auftragnehmer verwiesen werden, z. B. Weisungsberechtigte beim Auftraggeber und Empfangsberechtigte beim Auftragnehmer, Leistungsbeschreibung und Vorgehensweise bei kurzfristigen Änderungen, Betriebsstörungen, Protokollierung der Auftragsdurchführung durch den Auftragnehmer, Vorgehensweise bei Vertragsende.	
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),	
Bsp: Backup-Konzept (Redundante Systeme, Failover, unterbrechungsfreie Stromversorgung, etc.), Datensicherung (Beschreibung von Rhythmus, Medium, Aufbewahrungszeit und sicherem Aufbewahrungsort für Backupmedien), Notfallplan entsprechend möglicher Gefährdungen, Verfahren zum Wiederanlauf, Test der Notfalleinrichtungen.	
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. (Trennungskontrolle)	
Bsp: Logische Trennung der Daten auf Systemebene, Mandanten-Trennung, Trennung über Zugriffsregelung etc. gemäß Zweckbestimmung des Verfahrens.	

Bitkom vertritt mehr als 2.400 Unternehmen der digitalen Wirtschaft, davon gut 1.600 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlandsumsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, 300 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. 78 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, 9 Prozent kommen aus Europa, 9 Prozent aus den USA und 4 Prozent aus anderen Regionen. Bitkom setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom