Datenschutz
Einfach
Digital
Gestalten

Ratgeber
Knackpunkt IT-(Fern)Wartung

Die Wartung der eigenen IT durch externe Anbieter und IT-Berater ist gerade für kleine und mittlere Unternehmen nicht nur ein Kosteneinsparungspotential, sondern gestattet auch den Fokus auf das eigentliche Kerngeschäft. Gerade in der digitalen Aufbruchszeit werden Software und Applikationen vermehrt in die Betriebsabläufe eingebunden. Die Nutzung steht dabei im Vordergrund und nicht mehr der Besitz der Anwendungen oder gar der Hardware, vor allem die der Server. Externes Hosting und Daten aus der Cloud revolutionieren das papiergebundene Büro. Durch diesen Trend steigt folglich der Wartungs- und Pflegeaufwand von Soft- und Hardware sowie die Anforderungen an die Mitarbeiter, ganz gleich ob Administrator oder Anwender.

Die (Fern)Wartung als Alternative zu einem eigenen IT-Mitarbeiter. Insbesondere kleinere Betriebe profitieren von dieser Alternative. Nicht nur die Kostenoptimierung im Vergleich zu einem eigenen Mitarbeiter spielt eine Rolle, sondern vor allem der Mangel an qualifizierten Experten in deren Gunst kleinere Unternehmen oft das Nachsehen im direkten Wettbewerb zu Großkonzernen haben.

Dabei bringt die digitale Zeit nicht nur neue Anforderungen an die Technik und deren Umgang, sondern auch im Bereich des Datenschutzes mit sich. Wurde der Datenschutz und ein funktionierendes Management dahinter bisher eher vernachlässigt, so trifft die Unternehmen mit der Umstellung auf „Digital“ die volle Wucht der Anforderungen und deren Umsetzungen.
Die Erfahrung zeigt, dass gerade der Datenschutz in der Budget- und Umsetzungsplanung nicht berücksichtigt und im Grunde viel zu spät in die Planungen eingebunden wird. Eine Kostenexplosion und Zeitverzögerungen bei der Umsetzung sind die Folgen.

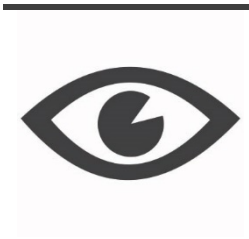
Lassen Sie sich bei Ihrem Vorhaben daher nicht Überraschen

Ihr
Marc Weber

Wartung und Pflege von Hard- und Software

Wie im Intro bereits beschrieben stellt die Digitalisierung nicht nur neue Anforderungen an die Anwender, sondern vor allem an die Entwickler und die IT-Administratoren. Zusammenhänge und Integrationen werden zunehmend komplexer und die Updatefristen verkürzen sich zunehmend. Um konstant auf eine einwandfrei funktionsfähige Infrastruktur zurückgreifen zu können sind besonders qualifizierte Experten unabdingbar. Dies stellt jedoch gerade kleine und mittlere Unternehmen vor neue Herausforderungen. Auf der einen Seite werden durch die Digitalisierung vorhandene Betriebsprozesse effizienter gestaltet und dem modernen Kundenanforderungen entsprochen, auf der anderen Seite fehlt das eigene Personal für eine optimale Umsetzung und anschließende Wartung.
An dieser Stelle kommen zunehmend externe IT-Dienstleister zum Tragen, die bei Bedarf oder in einem festen Wartungsintervall die IT-Aufgaben übernehmen und für einen reibungslosen Betrieb sorgen.

Nicht neu und doch neuartig. Waren es früher eher Hardwareprobleme, die vor Ort beim Kunden gelöst wurden, verlagert sich der Service zunehmend auch auf Applikationen und die Fernwartung über einen Remotezugriff. Hinzu kommen diverse Auslagerungen der Infrastruktur wie externe Server, Datenspeicher aus der Cloud, cloudbasierte IuK-Anlagen oder das klassische Voll-Service-Leasing von Multi-Funktionsgeräten. Die Folge sind nun zahlreiche externe Anbieter, die die Wartung und Pflege für ihre jeweiligen Produkte übernehmen. Nicht einfach hier noch den Überblick zu bewahren. Ein zentrales IT- und Vertragswesen ist auch für kleine Unternehmen unabdingbar geworden.



(theoretischer) Zugriff auf personenbezogene Daten während der Wartung/Pflege

Was hat nun die IT-Infrastruktur und deren Wartung mit dem Datenschutz zu tun?
Gerade im Geschäftsleben können personenbezogene Daten recht schnell anfallen. Insbesondere im Onlinezeitalter, wo ein direkter Kontakt zum Endverbraucher zustande kommt – nicht zuletzt durch den Betrieb eines Onlineshops, fallen personenbezogene Daten an und in der Aufbruchsstimmung der Digitalisierung werden diese Daten auch folgerichtig digital gespeichert.

Und hier liegt die Problematik verborgen, wenn IT-Anlagen, auf denen personenbezogene Daten gespeichert sind von externen Dritten gewartet werden. In diesem Fall kommt § 11 Abs. 5 BDSG zum Tragen *„…(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. …“

Besonders zu berücksichtigen ist hierbei der vorhandene – theoretische – Zugriff auf die gespeicherten Datenbestände. Damit ist es unerheblich, ob ein Zugriff auf die Daten Vertragsgegenstand ist oder nicht. Sollte im Zuge von Wartungs- oder Pflegearbeiten ein Zugriff theoretisch möglich sein, so ist die Anforderung des BDSG umzusetzen.

Hinweis:
Die Umsetzung des § 11 BDSG ist nicht an eine bestimmte Betriebsgröße gebunden!

(Fern)Wartung = Auftragsdatenverarbeitung

Auf Basis von § 11 Abs. 5 BDSG kann nun eine Auftragsdatenverarbeitung im Sinne des Datenschutzes vorliegen. Trotz einiger weniger Ausnahmen, bei denen ein Zugriff auf personenbezogene Daten – auch theoretisch – nicht möglich ist, zeigt die Praxis, dass die meisten Wartungs- und Pflegeverträge ein Auftragsdatenverarbeitungsverhältnis darstellen. Der Auftraggeber ist hier gefordert, eine rechtlich einwandfreie Grundlage für die Wartung durch externe IT-Dienstleister zu schaffen. Neben der Umsetzung eines geordneten IT-und Vertragswesen ist auch das Datenschutzmanagement von zentraler Bedeutung.

Oftmals fehlende Vertragsgrundlagen

In der Praxis werden mit externen IT-Dienstleistern zumeist detaillierte Wartungs- und Pflegeverträge geschlossen, die den Fokus auf den Umfang und die Vergütung der Leistung werfen. Datenschutzrechtliche Aspekte werden selten festgehalten oder begründen auf wohlwollend vordefinierte Vereinbarungen durch den Auftragnehmer. Eine vom Auftraggeber ausformulierte schriftliche Vereinbarung ist selten anzutreffen. Dabei sollten Auftraggeber stets berücksichtigen, dass sie die verantwortliche Stelle sind und gegebenenfalls auch bei datenschutzrechtlichen Verstößen des IT-Dienstleisters haften.

Anforderungen des Datenschutzes

Der § 11 Abs. 5 BDSG sieht nun bei einer (Fern)Wartung mit einem möglichen Zugriff durch den Dienstleister auf personenbezogenen Daten der verantwortlichen Stelle eine Reihe von Anforderungen für das Verhältnis zwischen Auftragnehmer und Auftraggeber vor. In den Absätzen 1 bis 4 sind Rechte und Pflichten wie verbindliche Vorgaben festgehalten. Insbesondere § 11 Abs. 2 S. 2 BDSG hält einen verbindlichen (jedoch nicht abschließenden) 10-Punkte-Katalog vor, der vollumfänglich bei einer Vereinbarung über eine Auftragsdatenverarbeitung umzusetzen ist. Nachdem eine (Fern)Wartung entsprechend auch eine Form der Auftragsdatenverarbeitung darstellt, ist dieser 10-Punkte-Katalog verbindlich zu berücksichtigen und mit dem Dienstleister schriftlich festzuhalten.

Die 10-Punkte in der Übersicht:

1. der Gegenstand und die Dauer des Auftrags,

2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,

3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,

4. die Berichtigung, Löschung und Sperrung von Daten,

5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,

6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,

7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,

8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,

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

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

Auswahl des IT-/Software-Dienstleisters

Mit den durch das BDSG gestellten Anforderungen an Auftragsdatenverhältnisse, sind die Auftraggeber bei der Auswahl der Dienstleister in eine besondere Pflicht genommen. Dabei hält § 11 Abs. 2 eindeutig fest *„Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen …“*. Hinter dieser Formulierung verbirgt sich eine Reihe von Gesichtspunkten, die es vor der Auftragsvergabe zu prüfen und vor allem zu dokumentieren gilt. Wesentlich ist zum einen der Themenblock der Technik und der Maßnahmen zur Sicherheit (digitale und physische Sicherheit) wie auch der organisatorische Block (Management und Mitarbeiter). Je nach Struktur und Größe des Dienstleisters und der Kategorie der zugrunde liegenden personenbezogenen Daten, kann dies zu einer umfassenden Prüfung führen. Erst nach Auswertung der wesentlichen Kontroll- und Prüfpunkte ist eine Vergabe empfehlenswert. Der Maßstab über den erforderlichen Schutzstandard stellt die Kerngröße für den Umfang der Prüfung und der Auswertung dar. Anderweitige Gesichtspunkte wie bspl. Gebührenstruktur oder räumlicher Nähe können daher in keinem relevanten Ausmaß in die Bewertung einfließen.

TOM – technisch organisatorische Maßnahmen

Die technisch organisatorischen Maßnahmen sind ein zentrale Baustein im Datenschutz und bilden gerade bei der Auftragsdatenverarbeitung einen bedeutenden Kern. Dabei gilt es diese Maßnahmen unter zwei unterschiedlichen Betrachtungsweisen zu berücksichtigen. Zum einen haben Sie vor der Auftragsvergabe im Rahmen des Auswahlverfahrens den künftigen IT-Dienstleister auf die vorhandenen technischen und auch den organisatorischen Maßnahmen hin zu prüfen. Dieses Abbild des Ist-Zustandes erleichtert die Einschätzung der Eignung des bewerbenden Dienstleisters.
Ist die Entscheidung gefallen, sind entsprechend dem 10-Punkte-Katalog die technisch organisatorischen Maßnahmen schriftlich in der Vereinbarung über eine Auftragsdatenverarbeitung festzuhalten. Hier eröffnet sich dem Auftraggeber die Möglichkeit, dem Auftragnehmer Standards detailliert vorzugeben, die unter der Berücksichtigung des erforderlichen Schutzniveaus der Datenbestände erforderlich sind. § 11 Abs. 2 S. 2 Nr. 3 BDSG verweist direkt auf § 9 BDSG und in diesem Rahmen auf die zu § 9 BDSG gehörige Anlage mit zu berücksichtigenden Anforderungen. Auszug aus der Anlage zu § 9 BDSG:

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren

(**Zutrittskontrolle**),

2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**),

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**),

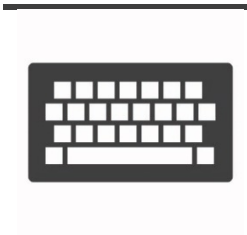
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (**Weitergabekontrolle**),

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**),

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),

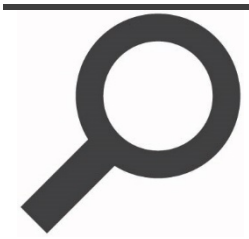
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**),

8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.



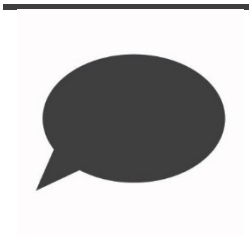
ADV den Besonderheiten einer (Fern)Wartung anpassen

Die Absätze 1 bis 4 aus § 11 BDSG haben vornehmlich eine klassische Auftragsdatenverarbeitung im Sinn, wonach ein Auftragnehmer direkt mit personenbezogenen Daten des Auftraggebers umgeht. Erst durch den Nachgang des Absatzes 5 wird die Auftragsdatenverarbeitung auch auf Fälle ausgeweitet, denen im Rahmen einer Systemwartung kein direkter Umgang mit personenbezogenen Daten zugrunde liegt, jedoch ein ähnliches Gefährdungspotential beigemessen wird. Daher ist es empfehlenswert, dieser gesonderten Grundlage des Verhältnisses Rechnung zu tragen und die notwendigen Vereinbarungen auf diese Besonderheit anzupassen.



Laufende Kontroll- und Überwachungspflichten des Auftraggebers

Neben einer ausführlichen Kontrolle und Bewertung externer Dienstleister vor der Auftragsvergabe kommen dem Auftraggeber auch während des Auftragsverhältnisses weitere Pflichten zu. So ist der Auftraggeber als verantwortliche Stelle dazu angehalten, die eingesetzten IT-Dienstleister regelmäßig zu kontrollieren. In einem besonderen Fokus stehen dabei die getroffenen technisch organisatorischen Maßnahmen und deren konstante Umsetzung sowie Anpassung an den Stand der Technik. Die laufenden Nachkontrollen sind anlassunabhängig durchzuführen und können nach einem eigenen, pflichtgemäß ermessenen Intervall erfolgen. Die entsprechenden Ergebnisse der Kontrollen sind zu dokumentieren.



Fazit

Die scheinbar bequem einfache Lösung, die Wartung der IT-Infrastruktur auszulagern um sich dem Kerngeschäft ganzheitlich widmen zu können, birgt bei genauer Betrachtung einige datenschutzrechtliche Stolpersteine. Nachdem die (Fern)Wartung als eine Auftragsdatenverarbeitung einzustufen ist, sollten neue Vereinbarungen die geforderten Anforderungen ganzheitlich berücksichtigen. Zudem ist es empfehlenswert bereits bestehende Vereinbarungen und Verträge unter den datenschutzrechtlichen Aspekt zu prüfen und im Bedarfsfall anzupassen. Ein Hauptaugenmerk sollte in jedem Fall auf den technisch organisatorischen Maßnahmen liegen und deren Vereinbarkeit mit dem jeweils aktuellen Stand der Technik.

Zahlreiche Musterverträge im Internet oder in Fachbüchern können die Vertragsgestaltung vereinfachen und als eine Orientierung in Formulierungsfragen dienen. Derartige Vorlagen sollten jedoch nicht ohne eine genaue Prüfung und auf den Zweck optimierte Anpassungen genutzt werden. In den seltensten Fällen sind exakt passende und aktuelle Muster frei verfügbar.

Impressum:

Herausgeber:
Datenschutz | Einfach | Digital | Gestalten
eine Initiative der
Marc Weber Management GmbH

Autor:
Marc Weber

Bezugsquelle:
Marc Weber Management GmbH
Lackerbauerstraße 23
81241 München
www.datenschutz-einfach-digital-gestalten.de
datenschutz@marcweber.de
Telefon 089 66 62 86 0
Fax 089 66 62 86 25

Stand:
Oktober 2017

Bildnachweis:
Titelseite: Grundgrafik mohamed1982eg – pixabay, Modifizierung durch Marc Weber Management GmbH
Piktogramme: IO-Images – pixabay