

Bericht

zum Rezertifizierungsaudit nach dem

DATENSCHUTZSTANDARD DS-BVD-GDD-01 "Anforderungen an Auftragnehmer nach § 11 BDSG"

für

Pix Software GmbH

über die Leistungen

„Hosting von Atlassian-Produkten nach deutschem Datenschutzrecht“ in der Ausprägung „Standard Hosting“ mit dem IT-Sicherheits-Standard „BSI-Grundschutz: normal“

Berichtersteller Thomas Müthlein
Zertifizierungsnummer DSZ 005
Anschrift DMC Datenschutz Management & Consulting GmbH & Co. KG
Zur Mühle 2-4
50226 Frechen
Berichts-Datum 10.10.2016



Inhaltsverzeichnis

1. Einführung	3
1.1. Ziel und Inhalt des Folgeaudits	3
1.2. Anwendungsbereich der Zertifizierung Reg.Nr. A-001 / A-005	4
2. Management Summary / Zusammenfassung	6
3. Obligatorische Anforderungen / Scoping	7
3.1. Prüfungsrelevante Kernmodule	7
3.2. Prüfungsrelevante Module in Abhängigkeit des Leistungsumfangs.....	8
3.3. Genehmigte Ausnahmen.....	8
4. Erneut auditierte Bereiche & Feststellungen	8
4.1. Kernmodule.....	8
4.1.1. Leistungsbeschreibung.....	8
4.1.2. Herstellung	9
4.1.3. Datenschutzkonzept.....	10
4.1.4. IT-Sicherheitskonzept	11
4.1.5. Managementsysteme	11
4.2. Module in Abhängigkeit des Leistungsumfangs	13
5. Prüfergebnis / Prüfvermerk	14
Bemerkungen der DSZ Datenschutz Zertifizierungsgesellschaft mbH	15

1. Einführung

Dieser Bericht wurde von RA THOMAS MÜTHLEIN erstellt und beschreibt die Tätigkeiten bzgl. unten stehender Auditaktivitäten:

Organisation	Erstprüfung / Verlängerung	Audittermin (Start)
Pix Software GmbH An der Beek 255 41372 Niederkrüchten	<input type="checkbox"/> Erstprüfung	Start: 09. September 2016
	<input checked="" type="checkbox"/> Verlängerung	Dauer: 24 Stunden

1.1. Ziel und Inhalt des Folgeaudits

Das Ziel des Folgeaudits war die erneute Überprüfung der im Anwendungsbereich beschriebenen Leistung, um zu gewährleisten, dass die im Anwendungsbereich getroffenen Maßnahmen und erforderlichen Umsetzungen nach dem DATENSCHUTZSTANDARD DS-BVD-GDD-01 "Anforderungen an Auftragnehmer nach § 11 BDSG" und sonstigen Vorgaben der Zertifizierungsgesellschaft auch zwei Jahre nach dem ursprünglichen Audit erfüllt werden. Es mündet in der Empfehlung hinsichtlich der Weiterführung einer Zertifizierung.

Das Folgeaudit fand auf Basis der abgeschlossenen Zertifizierung und des zugehörigen Prüfberichts vom 23.10.2014 statt, welcher den vorliegenden Bericht ergänzt. Im Zuge des ursprünglichen Audits wurden Empfehlungen zur Verbesserung in diversen Bereichen ausgesprochen sowie der spätere Nachweis des Funktionierens gerade angelaufener Prozesse vorgemerkt, welches nun überprüft wurde. Die einzeln betroffenen Aspekte sind Gliederungspunkt 4 zu entnehmen. Ohne Beanstandung erfüllte und nicht geänderte Punkte aus dem ursprünglichen Bericht sind nicht erneut überprüft worden.

Das Audit mit dem Ziel der Zertifizierung nach dem DATENSCHUTZSTANDARD DS-BVD-GDD-01 "Anforderungen an Auftragnehmer nach § 11 BDSG" dient folgenden Aspekten:

- Auftraggeber können die Zertifizierung ihrem eigenen Kontrollermessen gemäß § 11 Abs. 2 BDSG zugrunde legen.
- Das Unternehmen signalisiert als Auftragnehmer sein gesetzskonformes Datenschutzniveau.

Dieses Vor-Ort durchgeführte Audit basiert auf Stichproben. Es kann somit nicht ausgeschlossen werden, dass Abweichungen nicht erkannt werden.

Wenn Sie diesen Auditbericht an Dritte weiterleiten möchten, sind alle Teile des Berichtes zu übermitteln. Auszüge oder Teile des Berichts dürfen nicht an Dritte weitergeleitet werden.

1.2. Anwendungsbereich der Zertifizierung Reg.Nr. A-001 / A-005

Ort	Auditierte Leistung
Pix Software GmbH, An der Beek 255 41372 Niederkrüchten	„Hosting von Atlassian-Produkten nach deutschem Datenschutzrecht“ in der Ausprägung „Standard Hosting“ mit dem IT-Sicherheits-Standard „BSI-Grundschutz: normal“
<p>Zertifiziert werden soll die Leistung "Hosting". Die Leistung ist wie folgt definiert:</p> <ul style="list-style-type: none"> • Vermietung einer technisch definierten virtuellen Maschine, • Vorinstallation eines Atlassian Produktes (Confluence oder Jira) und • Betrieb der vermieteten virtuellen Maschine. <p>Es erfolgt ein Support bei Betriebsstörungen der virtuellen Maschine.</p> <p>Die Art der verarbeiteten Daten, der Kreis der Betroffenen und der Zweck liegen in der Verantwortung des Kunden und sind Pix Software i.d.R. nicht bekannt.</p> <p>Folgende Geräte und Anwendungen sind nicht mehr im Scope der Leistung Hosting:</p> <ul style="list-style-type: none"> • Abrechnungssystem • Tools zur Softwareentwicklung • Heimarbeitsplätze inkl. private Netzwerke* • Webseite • Terminal Server <p>Folgende Tätigkeiten und Leistungen sind nicht Teil der Leistung Hosting:</p> <ul style="list-style-type: none"> • Beratung • Projekte • Support von Atlassian Produkten* • Softwareentwicklung • Design-Individualisierung • Schulung, Workshops • Übernahme von Daten in virtuelle Maschinen <p>Verantwortung des Kunden</p> <ul style="list-style-type: none"> • Rechteverwaltung • Datenerhebung, Verarbeitung, Löschung, Archivierung <div data-bbox="304 1361 1442 1756" style="text-align: center;"> <pre> graph LR subgraph Rechenzentrum subgraph Kunden_VM [Kunden VM] Jira_DB[Jira DB] Attachments Confl_DB[Confl DB] end Pix_System1[Pix System] Storage1[Storage] Jira_DB --> Pix_System1 Attachments --> Pix_System1 Confl_DB --> Pix_System1 Pix_System1 -- "Verschlüsselte Tagessicherung mit BoxBackup" --> Storage1 end subgraph Internet Internet_Cloud((Internet)) end subgraph Reserverechenzentrum Pix_System2[Pix System] Storage2[Storage] Pix_System2 -- "Ablage auf verschlüsselte Festplatte" --> Storage2 end Pix_System1 -- "Verschlüsselte Übertragung" --> Internet_Cloud Internet_Cloud -- "Verschlüsselte Übertragung" --> Pix_System2 </pre> </div>	

* Erläuterung:

Die Aspekte „Heimarbeitplätze inkl. private Netzwerke“ sowie „Support von Atlassian Produkten“ können aus folgenden Gründen aus dem Scope ausgenommen werden:

- Die Leistung „Hosting“ ist soweit abgeschottet, dass es keinen administrativen Zugriff auf die jeweilige virtuelle Maschine gibt.
- Der Support von Atlassian Produkten ist nicht Gegenstand der Hosting-Dienstleistung und bedarf einer optionalen gesonderten Beauftragung.
- Ein Support durch den Hersteller Atlassian der gehosteten Applikation ist nicht vorgesehen. Dieser wäre durch den Auftraggeber selbst in eigener Verantwortung zu realisieren.
- Die Softwarelizenz ist alleiniges Eigentum des Auftraggebers.

2. Management Summary / Zusammenfassung

Das Rezertifizierungsaudit „Hosting von Atlassian-Produkten nach deutschem Datenschutzrecht“ in der Ausprägung „Standard Hosting“ mit dem IT-Sicherheits-Standard „BSI-Grundschutz: normal“ wurde im Zeitraum vom 09.09.2016 – 04.10.2016 durchgeführt. Hierbei stand dem Auditor die komplette Dokumentation im stets aktuellen Online-Portal der Pix Software GmbH (Pix) zur Verfügung. Weitere Dokumente und Auskünfte wurden auf Anforderung ohne Vorbehalte erteilt bzw. übergeben. Im Vor-Ort Termin wurden die Fragen des Auditors vollumfänglich ohne Vorbehalte fachkundig beantwortet und auf Wunsch durch Demonstrationen im System belegt.

Nach den Erkenntnissen der Dokumentenprüfung und des Vor-Ort-Audits ist das Verfahren „Hosting von Atlassian-Produkten nach deutschem Datenschutzrecht“ in der Ausprägung „Standard Hosting“ mit dem IT-Sicherheits-Standard „BSI-Grundschutz: normal“ weiterhin hinreichend schlüssig im Hinblick auf Datenschutz- und IT-Sicherheitsaspekte des DATENSCHUTZSTANDARDS DS-BVD-GDD-01 "Anforderungen an Auftragnehmer nach § 11 BDSG" durch Pix dokumentiert und wirksam implementiert.

Den Empfehlungen des Ursprungsaudits wurde im großen Umfang gefolgt. Geforderte Nachweise werden, nachdem neu eingeführte Prozesse den vollständigen PDCA-Zyklus inzwischen durchlaufen haben, geführt und vorgelegt. Sie sind in dem PDCA-Zyklus integriert und bilden die Grundlage zur Aufdeckung und Verbesserung von Schwachstellen.

3. Obligatorische Anforderungen / Scoping

3.1. Prüfungsrelevante Kernmodule

		Modul	relevant
4.1	Leistungsbeschreibung	4.1.1 Beschreibung der Leistung	ja
		4.1.2 Beschreibung der Auftragsbearbeitung (Herstellung)	ja
4.2	Input-Management		nein
4.3	Auftragsmanagement		ja
4.4	Output-Management		ja
4.5	Datenschutzkonzept	4.5.1 Eingabekontrolle	ja
		4.5.2 Trennungsgebot	ja
		4.5.3 Auftragskontrolle	ja
		4.5.4 Prozessbeschreibung Auskunft	ja
		4.5.5 Prozessbeschreibung Berichtigung	ja
		4.5.6 Prozessbeschreibung Sperrung	ja
		4.5.7 Prozessbeschreibung Löschung	ja
		4.5.8 Prozessbeschreibung Sicherheitsvorfall	ja
4.6	IT-Sicherheitskonzept	4.6.2.1 Erstellung und Verwendung des IT-Sicherheitskonzeptes	ja
		4.6.2.2 Mindeststandard Gebäudesicherheit	ja
		4.6.2.3 Mindeststandard Zutrittsschutz	ja
		4.6.2.4 Mindeststandard Zugangsschutz	ja
		4.6.2.5 Mindeststandard Zugriffsschutz	ja
		4.6.2.6 Mindeststandard Verfügbarkeit	ja
		4.6.2.7 Mindeststandard Datenübertragung	ja
4.7	Datenschutz-Managementsystem	4.7.4.1 Der Datenschutzbeauftragte	ja
		4.7.4.2 Kontrolle des Datenschutzkonzeptes	ja
		4.7.4.3 Kontrolle der Unterauftragnehmer	ja
4.8	IT-Sicherheitsmanagementsystem		ja
4.9	Auftragsmanagementsystem		ja

3.2. Prüfungsrelevante Module in Abhängigkeit des Leistungsumfangs

Modul		relevant
5.1	Vertrag	ja
5.2	Beendigung der Leistungsbeziehung	ja

3.3. Genehmigte Ausnahmen

Es wurden keine Ausnahmen im Folgeaudit beantragt.

4. Erneut auditierte Bereiche & Feststellungen

4.1. Kernmodule

4.1.1. Leistungsbeschreibung

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.1.1 Beschreibung der Leistung	Im Rahmen des Moduls Leistungsbeschreibung werden die Vorgaben und Anforderungen des Standards vollständig und aktuell umgesetzt.
Prüfmethode / Prüfhandlung	
Die für die Beschreibung der Leistung erforderlichen Dokumente, insbesondere Leistungsbeschreibungen, Musterverträge und Datenschutz- /IT-Sicherheitskonzepte liegen vor. Zusätzlich zu den Feststellungen des Zertifizierungsaudits wurde - wie empfohlen – das Gütesiegel DATENSCHUTZSTANDARD DS-BVD-GDD-01 mit der entsprechenden Zertifikatsseite verlinkt. Das Vertragsmuster wurde bereits auf die Datenschutz-Grundverordnung angepasst. Für dieses Muster gelten die Feststellungen des Zertifizierungsaudits. Prüfhandlung: Dokumentensichtung, Vertragssichtung, Interview, Demonstration / Prüfung einzelner Prozesse Vor-Ort	

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.1.2 Beschreibung der Herstellung	Im Rahmen des Moduls Leistungsbeschreibung werden die Vorgaben und Anforderungen des Standards vollständig und aktuell umgesetzt.
Prüfmethode / Prüfhandlung	
Es fand ein Umzug der Back-up-Server (Housing) in ein neues Rechenzentrum statt (ebenfalls Housing unter Beibehaltung der IT-Sicherheitsarchitektur). Die Portunity GmbH ist daher kein RZ-Betreiber (Housing) mehr,	

sondern auch hier nun die myLoc managed IT AG (Inhaber des Rechenzentrums ist wiederum Telia Company AB). Eine sorgsame Auswahl des neuen Housing-Anbieters und eine Kontrolle durch den IT-Sicherheitsbeauftragten und den Datenschutzbeauftragten wurden durchgeführt, dokumentiert und sich hieraus ergebende Maßnahmen umgesetzt.

Prüfhandlung:

Dokumentensichtung, Interview

4.1.2. Herstellung

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.2 Input-Management	Nicht einschlägig
Prüfmethode / Prüfhandlung	
<p>Die Dienstleistung umfasst das Hosting einer Applikation auf einer dedizierten VM. Dazu erhält der Auftraggeber vom Auftragnehmer einen Admin-Zugang für die Applikation, mit dessen Hilfe er selbst die Benutzer anlegen und verwalten kann. Die Dateneingabe (Input) erfolgt in alleiniger Verantwortung des Auftraggebers.</p> <p>Ein Input-Management gehört deshalb nicht zum Leistungsumfang.</p>	

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.3 Auftragsmanagement	<p>Im Rahmen des Auftragsmanagements sind Verbindlichkeit, Handlungssicherheit und aktueller Status für jeden Auftrag bei allen Beteiligten jederzeit sichergestellt.</p> <p>Prozesse zur Steuerung und Kontrolle von Unterauftragnehmern sind eingeführt und aktiv.</p>
Prüfmethode / Prüfhandlung	
<p>In das vorliegende Auftragsverhältnis (Hosting) werden nur der Auftraggeber und der Auftragnehmer einbezogen. Unterauftragnehmer im Sinne des § 11 BDSG werden nicht zur Leistungserbringung eingesetzt. Die für die Auftragsabwicklung notwendigen Schnittstellen zwischen den beteiligten Stellen und Unternehmen und die vollständige Kontrolle über den jeweiligen Status eines Auftrags sind über ein revisionssicheres Auftragsmanagement sichergestellt. Zentrales Kommunikations- und Dokumentationsmittel ist dabei das Ticket-System.</p> <p>Im Bereich des Housings, bei dem keine Unteraufträge im Sinne des § 11 BDSG vorliegen, werden diese Maßnahmen und Prozesse für Unterauftragnehmer entsprechend angewendet und umgesetzt.</p>	
<p>Prüfhandlung:</p> <ul style="list-style-type: none"> • Dokumentensichtung, Interview, Demonstration einzelner Prozesse Vor-Ort 	

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.4 Output-Management	Es ist hinsichtlich der Vertraulichkeit und Integrität bei der Weitergabe von Daten vom Auftragnehmer zum Auftraggeber oder an eine dritte Stelle sichergestellt, dass dies ausschließlich von hierfür autorisierten Personen durchgeführt wird.
Prüfmethode / Prüfhandlung	
<p>Bezüglich des Ursprungsaudits sind keine relevanten Änderungen erfolgt.</p> <p>Prüfhandlung:</p> <ul style="list-style-type: none"> • Dokumentensichtung, Interview 	

4.1.3. Datenschutzkonzept

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.5 Datenschutzkonzept	<p>Pix hat ein angemessenes Datenschutzkonzepts für die angebotene Leistung „Hosting“ auf der Basis des DATENSCHUTZSTANDARDS DS-BVD-GDD-01 dokumentiert und implementiert.</p> <p>Soweit insbesondere Schnittstellen zu schaffen, Verantwortlichkeiten zu regeln und Prozesse zu implementieren sind, ist dies auf Auftragnehmerseite hinreichend geschehen.</p>
Prüfmethode / Prüfhandlung	
<p>Im Bereich des Datenschutzkonzepts erfolgt die Beschreibung der Erfüllung datenschutzrechtlicher Vorgaben. Im Hinblick auf die zu auditierende Leistung "Hosting" ist der Einfluss des Auftragnehmers auf den tatsächlichen Umgang mit personenbezogenen Daten Betroffener sehr gering.</p> <p>Die Empfehlung, auf die Problematik der Sperrung bei Wiedereinspielung von Backups hinzuweisen, wurde im neuen ADV Vertragsmuster in § 17 umgesetzt.</p> <p>Prüfhandlung:</p> <p>Dokumentensichtung, Vertragsprüfung, Prüfung Arbeitsvertrag und Verpflichtungserklärung, Interview sowie Demonstration einzelner Prozesse Vor-Ort</p>	

4.1.4. IT-Sicherheitskonzept

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.6 IT-Sicherheitskonzept	Pix hat ein angemessenes IT-Sicherheitskonzept basierend auf der angebotenen Leistung „Hosting“ auf der Basis des BSI-Standards 100-2 „IT-Grundschutz-Vorgehensweise“ dokumentiert und implementiert.
Prüfmethode / Prüfhandlung	
<p>Pix hat sein IT-Sicherheitskonzept auf dem BSI-Standard 100-2 aufgebaut. Es hat dabei - für die Auftraggeber ersichtlich - den BSI Grundschutz - "normal" zugrunde gelegt.</p> <p>Die Dokumentation greift die hieraus erwachsenden Maßnahmen vollständig auf. Beim IT-Sicherheitskonzept "Hosting" wird der der Umstand des Colocation / Housings der physischen Server hinreichend berücksichtigt. Die Maßnahmen der Dienstleister werden in das eigene IT-Sicherheitskonzept integriert und in dessen Rahmen offen kommuniziert. Auf Schwächen, die sich aus der Einbindung der Colocation- / Housing-Geber ergeben können, wird durch andere - ggf. kompensierend wirkende - Maßnahmen wie z. B. Einsatz von Verschlüsselungen reagiert.</p> <p>Es wurden mehrere Empfehlungen zur Verbesserung der Dokumentation aus dem vergangenen Audit aufgenommen und umgesetzt:</p> <p>Die Dokumentation der Außenhautsicherung der RZ wurde aufgenommen im Dokument "IT-Sicherheitsmaßnahmen durch Rechenzentrum".</p> <p>Eine Dokumentation bezüglich der Token der Rechenzentren ist erfolgt (Dokument "Token für RZs in Düsseldorf).</p> <p>Die angeregte Nutzung unterschiedlicher Kombinationen der Zahlenschlösser wurde umgesetzt.</p> <p>Es existiert ein Passwortkonzept mit Bildungs- und Aufbewahrungsregeln.</p> <p>Die Empfehlung zur Dokumentation des Umgangs mit dem Passwort Safe ist in der Prozessbeschreibung „Prozess 1Passwort-Safe- Sicherung“ umgesetzt worden.</p> <p>Prüfhandlung: Dokumentensichtung, Interview sowie Vor-Ort-Prüfung</p>	

4.1.5. Managementsysteme

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.7 Datenschutz-Managementsystem	Pix hat ein Datenschutz-Managementsystem zur nachhaltigen Sicherstellung des Datenschutzes, so wie er im Datenschutzkonzept definiert worden ist, dokumentiert und eingeführt.
Prüfmethode / Prüfhandlung	
<p>Ausgewählte Prozesse und Leistungen werden in angemessenen Zeitabständen auf ihre Datenschutzkonformität sowie hinsichtlich der Funktionsweise des IT-Sicherheitskonzeptes überprüft. Dies konnte im unternehmensinternen Ticketsystem nachgewiesen werden.</p> <p>Der Nachweis der Kontrolltätigkeiten durch den betrieblichen Datenschutzbeauftragten und IT-Sicherheitsbeauftragten konnte ebenfalls geführt werden.</p>	

<p>Stichproben wurden insbesondere entnommen für:</p> <ul style="list-style-type: none"> • Schulungskonzept • Lieferantenänderung • Auftragskontrolle <p>Prüfhandlung: Einsicht in das Ticketsystem, Interview.</p>

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.8 IT-Sicherheitsmanagementsystem	Ein angemessenes IT-Sicherheitsmanagementsystem ist eingeführt und dokumentiert.
Prüfmethode / Prüfhandlung	
<p>Prozesse zur stichprobenartigen Kontrolle ausgewählter Prozesse und der angebotene Leistung im Hinblick auf IT-Sicherheitsmaßnahmen sind dokumentiert.</p> <p>Ein Prozess zur kontinuierlichen Verbesserung der IT-Sicherheit ist etabliert. Diesbezügliche Nachweise sind aus dem Ticketsystem ersichtlich.</p> <p>Prüfhandlung: Einsicht in das Ticketsystem, Interview</p>	

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.9 Auftragsmanagementsystem	Pix hat wirksame Prozesse und Maßnahmen dokumentiert, um im Rahmen des Auftragsmanagementsystems zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.
Prüfmethode / Prüfhandlung	
<p>Pix hat Prozesse und Maßnahmen dokumentiert, um im Rahmen des Auftragsmanagementsystems zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.</p> <p>Die fachliche und organisatorische Einweisung in den Arbeitsplatz findet statt und konnte über Schulungsbelege bei Ersteinstellung nachgewiesen werden.</p> <p>Die Wirksamkeit des Auftragsmanagementsystems kann Kunden gegenüber mithilfe von Prüfprotokollen im Kundenbereich des unternehmensweiten Informationssystems eingesehen werden.</p> <p>Prüfhandlung: Dokumentensichtung, Prüfung von Checklisten, Interview</p>	

4.2. Module in Abhängigkeit des Leistungsumfangs

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
5.1 Vertrag	<p>Die Bewertung erfolgt summarisch ohne Rechtsprüfung:</p> <p>Der von Pix angebotene Mustervertrag zur Auftragsdatenverarbeitung ("Angebot 2.9f.pdf") greift alle nach § 11 BDSG zu regelnden Aspekte auf. Es ist nicht offensichtlich, dass Auftraggeberrechte oder -pflichten, die aus dem BDSG erwachsen, durch vertragliche Regeln behindert werden. Die zur Umsetzung der Auftraggeberrechte oder -pflichten erforderlichen Prozesse und Maßnahmen sind, wie im Rahmen des Audits überprüft, dokumentiert und eingeführt.</p>
Prüfmethode / Prüfhandlung	
<p>Es existiert ein Prozess bei Beendigung des Leistungsbezuges, der auch das Löschen oder die Rückgabe der Auftragsdaten an den Auftraggeber umfasst.</p> <p>Wie in der Präambel des ADV Vertrag ausgeführt, sollen auch die Vorgaben der DS-GVO bereits jetzt erfüllt werden. Damit sollen bereits jetzt die Vorgaben des Art. 28 DS-GVO umgesetzt werden. Diese Anforderungen der DS-GVO sind allerdings - bislang - nicht von der Prüfung umfasst.</p> <p>Für die Beschreibung der angebotenen Leistung wird direkt auf das betroffene Angebotsdokument verwiesen und insofern eine Empfehlung des Audits umgesetzt.</p> <p>Die Empfehlung zur eindeutigeren Fassung der Regelung zur Löschung beim Hosting ist im neuen ADV Muster unter § 16 umgesetzt.</p> <p>Prüfhandlung: Dokumentensichtung, Vertragsprüfung, Interview</p>	

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
5.2 Beendigung der Leistungsbeziehung	<p>Es liegen eindeutige Vereinbarungen für den Fall der Beendigung eines Auftrages im Hinblick darauf, was mit den beim Auftraggeber vorhandenen Daten geschehen soll, vor. Ein Prozess zur Auftragsbeendigung (Löschprozess der gehosteten VM) ist eingeführt und dokumentiert.</p>
Prüfmethode / Prüfhandlung	
<p>Das verwendete Vertragsmuster setzt die Vorgaben des § 11 BDSG sowie des Art. 28 DS-GVO um. Die Anforderungen des Art. 28 DS-GVO sind allerdings - bislang - nicht von der Prüfung umfasst.</p> <p>Die Empfehlungen des Zertifizierungsaudits wurden aufgegriffen.</p> <p>Prüfhandlung: Dokumentensichtung, Vertragsprüfung, Interview</p>	

5. Prüfergebnis / Prüfvermerk

Die im Scope des Audits stehende Leistung

*„Hosting von Atlassian-Produkten nach deutschem Datenschutzrecht“ in der Ausprägung
„Standard Hosting“ mit dem IT-Sicherheits-Standard „BSI-Grundschutz: normal“*

wird nach Erkenntnissen des Audits nach den Maßgaben des DATENSCHUTZSTANDARD DS-BVD-GDD-01 "Anforderungen an Auftragnehmer nach § 11 BDSG" angeboten und erbracht.

Daher wird die Verlängerung des Zertifikats empfohlen.



Bemerkungen der DSZ Datenschutz Zertifizierungsgesellschaft mbH

Das Siegel wird erteilt

Nummer des Zertifikats: U-001

Gültigkeit des Zertifikats: 20.11.2018

