Bericht

zum Zertifizierungsaudit nach

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
Zertifizierungs-nummer DSZ	005
Anschrift	DMC Datenschutz Management & Consulting GmbH & Co. KG Zur Mühle 2-4 50226 Frechen
Berichts-Datum	23.10.2014

Inhaltsverzeichnis

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 Kesseler Weg 17a 41379 Brüggen	☒ Erstprüfung ☐ Verlängerung	Start: 05. September 2014 Dauer: 5 Tage

1.1. Ziel des Audits

Das Ziel des Audits war eine 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 erfüllt werden. Es mündet in der Empfehlung hinsichtlich einer Zertifizierung.

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 gesetzeskonformes 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

Ort	Auditierte Leistung
Pix Software GmbH, Kesseler Weg 17a, 41379 Brüggen	„Hosting von Atlassian-Produkten nach deutschem Datenschutzrecht“ in der Ausprägung „Standard Hosting“ mit dem IT-Sicherheits-Standard „BSI-Grundschutz: normal“
Zertifiziert werden soll die Leistung "Hosting". Die Leistung ist wie folgt definiert: • Vermietung einer technisch definierten virtuellen Maschine, • Vorinstallation eines Atlassian Produktes (Confluence oder Jira) und • Betrieb der vermieteten virtuellen Maschine. Es erfolgt ein Support bei Betriebsstörungen der virtuellen Maschine.	

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.

Folgende Geräte und Anwendungen sind nicht mehr im Scope der Leistung Hosting:

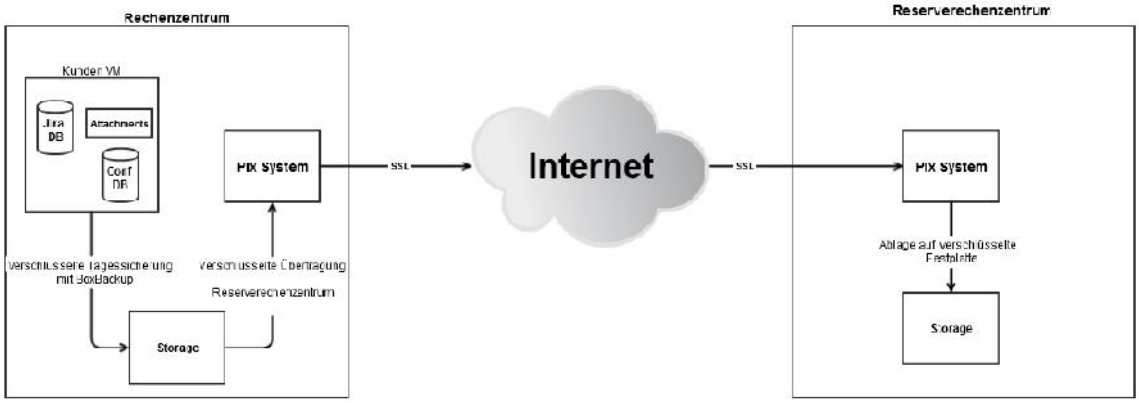
- Abrechnungssystem
- Tools zur Softwareentwicklung
- Heimarbeitsplätze inkl. private Netzwerke*
- Webseite
- Terminal Server

Folgende Tätigkeiten und Leistungen sind nicht Teil der Leistung Hosting:

- Beratung
- Projekte
- Support von Atlassian Produkten*
- Softwareentwicklung
- Design-Individualisierung
- Schulung, Workshops
- Übernahme von Daten in virtuelle Maschinen

Verantwortung des Kunden

- Rechteverwaltung
- Datenerhebung, Verarbeitung, Löschung, Archivierung



* Erläuterung:

Die Aspekte „Heimarbeitsplätze 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.
- Sie Softwarelizenz ist alleiniges Eigentum des Auftraggebers.

2. Management Summary / Zusammenfassung

Das Zertifizierungsaudit „Hosting von Atlassian-Produkten nach deutschem Datenschutzrecht“ in der Ausprägung „Standard Hosting“ mit dem IT-Sicherheits-Standard „BSI-Grundschutz: normal“ wurde im Zeitraum 5.9.2014 bis 23.10.2014 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“ 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.

Die Anpassung des Standardangebots durch Umsetzung spezieller Anforderungen oder Weisungen von Auftraggebern ist insbesondere über Change-Prozesse vorgesehen. Diese werden für interne Changes entsprechend angewendet. Hierbei ist durch die Prozessgestaltung sichergestellt, dass die Anpassungen dahingehend geprüft und gestaltet werden können, dass durch sie das auditierte Schutzniveau der Dienstleistungserbringung nicht unterschritten wird.

Die Verantwortung zur Einleitung solcher Change-Prozesse, liegt bei den Auftraggebern selbst. Die Verantwortlichkeiten zwischen Auftraggebern und Pix sind klar dokumentiert und werden – insbesondere im Hinblick auf die Verwaltung von Berechtigungen – deutlich kommuniziert. Hierzu dienen insbesondere die von Pix vorgehaltenen Vertragsmuster (s. 5.1 Vertrag).

Angemessene Maßnahmen und / oder Prozesse zu Datenschutz und IT-Sicherheit wurden durch Dokumentationen bzw. im Vor-Ort-Termin (Besichtigung der RZ, Interviews mit Fachverantwortlichen, Demonstrationen im Echt-Betrieb) schlüssig dargestellt. Dabei wurden alle Aspekte des DATENSCHUTZSTANDARDS DS-BVD-GDD-01 mit Ausnahme des Moduls 4.2 Input-Management betrachtet (nicht einschlägig, s. 4.2 Input-Management).

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-Sicherheitskonzepts	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

Mit Schreiben vom 5.9.2014 hat die DSZ den Antrag der Pix Software GmbH auf Reduktion des Prüfkontingents in Höhe von 24 Std. bewilligt.

4. 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. Prüfhandlung: Dokumentensichtung, Interview, Vor-Ort-Prüfung der RZ, 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	
Die Herstellung ist sowohl allgemein beschrieben wie auch intern insbesondere über Konzepte, Prozessbeschreibungen, Arbeitsanweisungen und Checklisten festgelegt. Die virtuellen Maschinen werden in einem Rechenzentrum der Firma myLoc managed IT AG betrieben. Als Backup steht ein zweites Rechenzentrum der Firma Portunity GmbH zur Verfügung. Beide Rechenzentren werden im Rahmen eines „Housings“ genutzt. Bei der Vor-Ort-Prüfung in beiden Rechenzentren im Rahmen des Audits wurde	

festgestellt, dass beide Dienstleister keinen Zutritt zu den Racks mit den Servern und Storages und keinen Zugang zu den Komponenten sowie keinen Zugriff auf Daten haben. An der Leistungserbringung sind darüber hinaus keine weiteren Dienstleister beteiligt.
Der Hersteller Atlassian hat standardmäßig keinen Zugriff auf die Installationen. Kunden können Atlassian in eigener Verantwortung einen Zugriff bspw. über Fernwartungsprogramme gewähren.

Prüfhandlung:

Dokumentensichtung, Interview, Vor-Ort-Prüfung der RZ, Demonstration / Prüfung einzelner Prozesse Vor-Ort

4.1.2. Herstellung

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.2 Input-Management	Nicht einschlägig
Prüfmethode / Prüfhandlung	
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. Ein Input-Management gehört deshalb nicht zum Leistungsumfang.	

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.3 Auftragsmanagement	Im Rahmen des Auftragsmanagements sind Verbindlichkeit, Handlungssicherheit und aktueller Status für jeden Auftrag bei allen Beteiligten jederzeit sichergestellt. Prozesse zur Steuerung und Kontrolle von Unterauftragnehmern sind eingeführt.
Prüfmethode / Prüfhandlung	
Im Rahmen des Auftragsmanagements sind Verbindlichkeit, Handlungssicherheit und aktueller Status für jeden Auftrag bei allen Beteiligten jederzeit sicher zu stellen. 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. Weiterhin liegen insbesondere Dokumentationen vor zu • Maßnahmen und Abläufe zur Auftragsbearbeitung • Beschreibungen der Rollen und Schnittstellen zwischen Auftragnehmer und Auftraggeber und ihren Aufgaben und Weisungsbefugnissen • Beschreibungen der Änderungsprotokollierung während der Auftragsbearbeitung Auch wenn zurzeit keine Unterauftragnehmer im Sinne des § 11 BDSG zur Auftragsdurchführung eingesetzt werden, sind die erforderlichen Steuerungs- und Kontroll-Prozesse für Unterauftragsverhältnisse eingeführt und ihr Einsatz in Prozessen und Konzepten berücksichtigt. , s. insbesondere:	

- Auftragsmanagement
- Prozess Genehmigung Unterauftragnehmer
- Prozess Kontrolle von Unterauftragnehmern
- Prozess Neue Unterauftragnehmer

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.

Prüfhandlung:

Dokumentensichtung, Interview, Vor-Ort-Prüfung

Im Rahmen der Vor-Ort-Prüfung wurden insbesondere folgende Aspekte untersucht:

- Ticket System: Anlage von Kunden, Dokumentation von Weisungen, Umsetzung von Weisungen
- Prozess „Instanz einrichten“
- Konfiguration von Zugängen
- Rollenkonzept
- Prozessbeauftragung

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

Werden Datenweitergaben vom Auftragnehmer zum Auftraggeber als Teil der Leistungserbringung definiert, kann durch dieses Modul die Datenschutzkonformität der entsprechenden Prozesse geprüft werden.

Aufgrund der Art der Dienstleistung (Hosting) obliegt die Verantwortung für die Datenübertragung allein dem Auftraggeber. Lediglich hinsichtlich der möglichen sicheren Anbindung besteht die Möglichkeit der Mitwirkung des Auftragnehmers.

Insofern muss sichergestellt werden können, dass eine Weitergabe von Daten zum Auftraggeber oder an eine dritte Stelle hinsichtlich Vertraulichkeit und Integrität sicher ist und ausschließlich von hierfür autorisierten Personen durchgeführt werden kann.

Die diesbezüglichen technischen Möglichkeiten der verschlüsselten Übertragung stellt der Auftragnehmer zur Verfügung. Die Rollen und Berechtigungen sind von ihm im Hinblick auf das Hosting der VM hinreichend und angemessen dokumentiert und implementiert.

Die Verantwortung für die Rechteverwaltung der gehosteten Applikation liegt beim Auftraggeber selbst. Allerdings muss er darauf achten, dass er den einrichtenden Administrator des Auftragnehmers nach Übernahme der Berechtigungsverwaltung deaktiviert. Hierauf weist der Auftragnehmer aber auch deutlichst hin.

Prüfhandlung:

Dokumentensichtung, Interview, Vor-Ort-Prüfung insbesondere zu:

- Ticket System

- Prozess „Instanz einrichten“
- Rollenkonzept
- Abgrenzung Pix Admin zu Kunden Admin
- Konfiguration von Zugängen
- Zugriffe auf die Kundeninstanz: Administrator, Support, Kunden Admin
- Verschlüsselte Datenübertragung

4.1.3. Datenschutzkonzept

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.5 Datenschutzkonzept	Pix hat ein angemessenes Datenschutzkonzepts für die angebotene Leistung „Hosting“ auf der Basis des DATENSCHUTZSTANDARDS DS-BVD-GDD-01 dokumentiert und implementiert. Soweit insbesondere Schnittstellen zu schaffen, Verantwortlichkeiten zu regeln und Prozesse zu implementieren sind, ist dies auf Auftragnehmerseite hinreichend geschehen.

Prüfmethode / Prüfhandlung

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. Von daher liegt die Verantwortung insbesondere im Bereich der

- Eingabekontrolle
- Prozessbeschreibung Auskunft
- Prozessbeschreibung Berichtigung
- Prozessbeschreibung Sperrung
- Prozessbeschreibung Löschung

überwiegend beim Auftraggeber. Soweit insbesondere Schnittstellen zu schaffen, Verantwortlichkeiten zu regeln und Prozesse zu implementieren sind, ist dies auf Auftragnehmerseite geschehen. Dies gilt auch für die Prozesse mit weiterreichender Verantwortung des Auftragnehmers wie:

- Protokollkonzept
- Trennungsgebot
- Auftragskontrolle
- Prozessbeschreibung Sicherheitsvorfall

Im Einzelnen wurden folgende Aspekte betrachtet:

Modul		Feststellung
4.5.1	Eingabekontrolle	erfüllt
4.5.2	Trennungsgebot	erfüllt
4.5.3	Auftragskontrolle	erfüllt

4.5.4	Prozessbeschreibung Auskunft	erfüllt
4.5.5	Prozessbeschreibung Berichtigung	erfüllt
4.5.6	Prozessbeschreibung Sperrung	erfüllt
4.5.7	Prozessbeschreibung Löschung	erfüllt
4.5.8	Prozessbeschreibung Sicherheitsvorfall	erfüllt

Prüfhandlung:

Dokumentensichtung, Interview sowie Vor-Ort-Prüfung.

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

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.

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 Verschlüsslungen reagiert.

Insofern werden die Schutzziele angemessen verwirklicht:

- Vertraulichkeit: Insbesondere durch physische Maßnahmen, Einsatz von Verschlüsselungstechnik, angemessene Rollen- und Berechtigungskonzepte sowie ein Protokollkonzept wird sichergestellt, dass nur vom Auftragnehmer oder Auftraggeber bevollmächtigte Personen Zugriff auf die Auftragsdaten haben. Die Administration der Berechtigungen zum Zugriff auf die Auftragsdaten liegt grundsätzlich nur beim Auftraggeber.
- Integrität: Die Administration der Berechtigungen zum Zugriff auf die Auftragsdaten liegt grundsätzlich nur beim Auftraggeber. So wird sichergestellt, dass nur vom Auftraggeber bevollmächtigte Personen Veränderungen an den Auftragsdaten vornehmen können.
- Verfügbarkeit: Die Auftragsdaten stehen dem Auftraggeber rechtzeitig und in dem mit ihm vereinbarten Umfang zur Verfügung.

Es umfasst insbesondere eine:

- IT-Strukturanalyse,
- Risikoabschätzung (nach BSI-Grundschutz),
- die betrachteten Schadensszenarien in der Risikoabschätzung,
- Ableitung der Maßnahmen für IT-Systeme, Kommunikationsverbindungen und Räume.

Es definiert das angebotene Schutzniveau nach BSI-Grundschutz "normal".

Das vollständige IT-Sicherheitskonzept steht Auftragnehmern (auch in der "Vertragsphase) zur Verfügung.

Das IT-Sicherheitskonzept enthält ein Schulungskonzept zur IT-Sicherheit.

Das IT-Sicherheitskonzept regelt die Löschung oder Zerstörung defekter oder ausgemusterter Datenträger.

Im Einzelnen wurden folgende Aspekte betrachtet:

Modul		Feststellung
4.6.2.1	Erstellung und Verwendung des IT-Sicherheitskonzepts	erfüllt
4.6.2.2	Mindeststandard Gebäudesicherheit	erfüllt
4.6.2.3	Mindeststandard Zutrittsschutz	erfüllt
4.6.2.4	Mindeststandard Zugangsschutz	erfüllt
4.6.2.5	Mindeststandard Zugriffsschutz	erfüllt
4.6.2.6	Mindeststandard Verfügbarkeit	erfüllt
4.6.2.7	Mindeststandard Datenübertragung	erfüllt

Prüfhandlung:

Dokumentensichtung, Interview sowie Vor-Ort-Prüfung.

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

Pix hat ein Datenschutz-Managementsystem zur nachhaltigen Sicherstellung des Datenschutzes, so wie er im Datenschutzkonzept definiert worden ist, dokumentiert und eingeführt. Hierzu zählt insbesondere:

Die freiwillige, wirksame Bestellung eines Datenschutzbeauftragten (Bestellurkunde und Fachkunde sind dokumentiert).

Prozesse zur stichprobenartigen Kontrolle ausgewählte Prozesse und der angebotene Leistung im Hinblick auf ihre Datenschutzkonformität.

Prozesse zur Kontrolle von Unterauftragnehmern sind dokumentiert, werden aber nicht - vollständig - umgesetzt, da im Wirkbetrieb keine Unterauftragnehmer eingesetzt werden.

Die Prozesse zur Kontrolle von Unterauftragnehmern werden auf die Housing-Rechenzentren der Firma myLoc managed IT AG (Betrieb der VM) und der Firma Portunity GmbH (Backup, verschlüsselt),bei denen es sich nicht um Auftragnehmer im Sinne des § 11 BDSG handelt, entsprechend angewendet.[1]

Nachweise über nach dem Konzept vorgesehene Prüfungen liegen noch nicht vor, da die Prozesse erst seit kurzem implementiert sind.

Prüfhandlung:

[1] S. a. zu 4.1.1 Leistungsbeschreibung, 4.3 Auftragsmanagement

Dokumentensichtung, Interview sowie Vor-Ort-Prüfung.

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.8 IT-Sicherheitsmanagementsystem	Ein angemessenes IT-Sicherheitsmanagementsystem ist eingeführt und dokumentiert.
Prüfmethode / Prüfhandlung	
Pix hat ein IT-Sicherheits-Managementsystem dokumentiert und eingeführt. Hierzu liegt insbesondere eine Leitlinie zur IT-Sicherheit vor. Die Bestellung eines IT-Sicherheitsbeauftragten (Bestellung, Aufgaben / Befugnisse und Fachkunde) ist dokumentiert. Prozesse zur stichprobenartigen Kontrolle ausgewählter Prozesse und der angebotene Leistung im Hinblick auf IT-Sicherheitsmaßnahmen sind dokumentiert. Ein Prozess zur kontinuierlichen Verbesserung der IT-Sicherheit ist etabliert. Nachweise über nach dem Konzept vorgesehene Prüfungen liegen noch nicht vor, da die Prozesse erst seit kurzem implementiert sind. Prüfhandlung: Dokumentensichtung, Interview sowie Vor-Ort-Prüfung.	

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	
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. Hierzu liegen insbesondere dokumentiert vor: • Prozessbeschreibungen aller für die Auftragsbearbeitung notwendigen manuellen und technisch unterstützten Prozesse. Dies umfasst auch, dass die betrauten Personen mit den relevanten Prozessen vertraut sind. • Ein Prozess zur Weisungsbearbeitung sowie interne Changes (Change Management) • Prozesse zur Kontrolle der ordnungsgemäßen Bearbeitung • Der Nachweis über die Wirksamkeit des Auftragsmanagementsystems gegenüber den Auftraggebern über die Hinterlegung im "Kundenportal" der Pix, auf das jeder Auftraggeber ungehinderten Zugriff erhält Nachweise über nach dem Konzept vorgesehene Prüfungen liegen noch nicht vor, da die Prozesse erst seit kurzem implementiert sind. Prüfhandlung:	

Dokumentensichtung, Interview, Vor-Ort-Prüfung

4.2. Module in Abhängigkeit des Leistungsumfangs

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
5.1 Vertrag	Die Bewertung erfolgt summarisch ohne Rechtsprüfung: Der von Pix angebotene Mustervertrag zur Auftragsdatenverarbeitung ("ADV-Vereinbarung 1.5") 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.
Prüfmethode / Prüfhandlung	
Gemäß § 11 BDSG sind Aufträge zur Erhebung, Verarbeitung oder Nutzung schriftlich zu erteilen. Soweit der Auftragnehmer hierzu einen eigenen Mustervertrag vorhält, muss er den Anforderungen des § 11 BDSG entsprechen und insbesondere die Weisungen zu den technischen und organisatorischen Maßnahmen entsprechend der Anlage des § 9 BDSG in angemessener Weise beinhalten. Pix bietet einen eigenen Mustervertrag zur Auftragsdatenverarbeitung standardmäßig im Vertragsset zur Bestellung der Leistung an ("ADV-Vereinbarung 1.5"). Dieser bezieht sich insbesondere auf die • Umsetzung der Anforderungen der §§ 9 und 11 BDSG. • Regelungen zu vertraglichen Bindungen von Unterauftragnehmern (UAN) an die Weisungen des Auftraggebers (z. Zt. werden keine UAN in diesem Sinne eingesetzt). Prüfhandlung: Dokumentensichtung, Interview	

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
5.2 Beendigung der Leistungsbeziehung	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.
Prüfmethode / Prüfhandlung	
Für den Fall der Beendigung eines Auftrages sind klare Regelungen im Hinblick darauf, was mit den beim Auftraggeber vorhandenen Daten geschehen soll, in den Musterklauseln des Musterangebots "ADV Vereinbarung 1.5"	

vorgesehen. Hierzu besteht auch ein Prozess zur Auftragsbeendigung. Im Rahmen des Hostings obliegt es beim Auftragsende allein dem Auftraggeber, die Rückführung der Daten durchzuführen. Ein wirksamer Löschprozess der gehosteten Virtuellen Maschinen (VM) ist eingeführt und dokumentiert. Prüfhandlung: Dokumentensichtung, Interview

5. Audit Teilnehmer

Beteiligte Stellen / Unterauftragnehmer / Dienstleister / sonstige Dritte

Name / Adresse	Aufgabe bei der Leistungserbringung
RZ-Düsseldorf: myLoc managed IT AG am Gatherhof 44 40472 Düsseldorf	Housing der Racks für den Produktivbetrieb
RZ-Wuppertal: Portunity GmbH Gathe 117 42107 Wuppertal	Housing der Racks für das Backup der VM

6. 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 Erteilung des Zertifikats empfohlen.

Bemerkungen der DSZ Datenschutz Zertifizierungsgesellschaft mbH

Das Siegel wurde erteilt mit Schreiben vom 13.11.2014

Nummer des Zertifikats:
U-001

Gültigkeit des Zertifikats:
20.11.2016