BKS GmbH

Datenschutzrechtliche Risikoeinschätzung hinsichtlich des Helpdesks von Jira Service Management (Atlassian)

datenschutz süd GmbH
20.06.2023

datenschutz süd

Inhaltsverzeichnis

1. Einleitung

Die BKS GmbH (im Folgenden: BKS) stellt seinen Kunden im Rahmen des Produkts BKS Ixalo|Key und der dazugehörigen App einen Helpdesk von Jira Service Management (Atlassian) zur Verfügung. BKS bietet seinen Kunden mithin den Service an Fehler- oder Problemsituationen im Rahmen eines Tickets bei BKS zu platzieren. Atlassian nutzt für seine Dienste die Infrastruktur von AWS. Seitens BKS ist angedacht die Möglichkeit seitens Atlassian, die grundsätzliche Datenspeicherung in der EU zu belassen, wahrzunehmen. Mit Atlassian wurde zudem ein Data Processing Addendum (DPA) abgeschlossen. Atlassian hat seine technischen und organisatorischen Maßnahmen nach den internationalen Standards ISO 27001 ausgerichtet.

Atlassian beauftragt Unterauftragsverarbeiter, die teilweise ihren Sitz außerhalb der EU/des EWR haben, mit der Durchführung begrenzter Aktivitäten. Atlassian schließt mit seinen Subdienstleistern EU Standardvertragsklauseln (SCC) ab.

Laut Atlassian kann ein Datentransfer in ein Land, welches außerhalb der EU liegt, bei der Nutzung von Jira Service Management für die aufgeführten Produktdaten nicht vermieden werden:

- Customer accounts,
- Product analytics,
- Data used by Halp.

Für alle anderen Produktdaten für die Nutzung von Jira Service Managemnet, wie

- All attachments,
- Comments,
- In-product notification data,
- Knowledge base category data (if integrated with Confluence),
- Asset object data and schema configuration data,
- Jira issues, request types, and field content (including system and custom fields),
- Jira search data ,
- Project configuration data (including workflows and custom field configuration),
- Queue data,
- Configuration management databases (CMDB) used for the external asset platform,
- SLA configuration data,
- Any incident management features powered by Opsgenie,

besteht die Möglichkeit die Datenspeicherung in der EU zu belassen. Dies wird für die hiesige datenschutzrechtliche Risikoeinschätzung vorausgesetzt.

Auf Basis der nachfolgenden von Atlassian zur Verfügung gestellten Unterlagen hat BKS die vorliegende Risikoeinschätzung hinsichtlich der Nutzung des Helpdesks von Jira Service Management erstellt.

https://www.atlassian.com/legal/data-transfer-impact-assessment

https://www.atlassian.com/trust/privacy/country/europe-and-gdpr

https://www.atlassian.com/trust/compliance/resources/gdpr

https://www.atlassian.com/de/trust/privacy/transparency-report

https://www.atlassian.com/trust/privacy/guidelines-for-law-enforcement

2. Datenschutzrechtliche Risiken

2.1. Relevante US-Gesetze

Laut Atlassian sind folgende Kategorien von US-Gesetzen bezüglich des staatlichen Zugriffs auf personenbezogene Daten relevant:

FISA 702, Executive Order 12333, CLOUD-Akt

FISA Section 702 („FISA 702“) – erlaubt es US-Regierungsbehörden, die Offenlegung von Informationen über Nicht-US-Personen, die sich außerhalb der USA befinden, zum Zwecke der Sammlung ausländischer Geheimdienstinformationen zu erzwingen. Diese Informationssammlung muss vom Foreign Intelligence Surveillance Court in Washington, DC, genehmigt werden. In den Anwendungsbereich fallende Anbieter, die FISA 702 unterliegen, sind Anbieter von elektronischen Kommunikationsdiensten („ECSP“) im Sinne von 50 USC § 1881(b)(4), die Remote-Computing-Dienstanbieter („RCSP“) umfassen können, wie unter 18 USC definiert § 2510 und 18 USC § 2711.

Executive Order 12333 ("EO 12333") - ermächtigt Geheimdienste (wie die US National Security Agency) zur Überwachung außerhalb der USA. Insbesondere erteilt es den US-Geheimdiensten die Befugnis, ausländische "Signal Intelligence"-Informationen zu sammeln, bei denen es sich um Informationen handelt, die aus Kommunikationen und anderen Daten gesammelt werden, die über Funk, Kabel und andere elektromagnetische Mittel übertragen oder zugänglich sind. Dies kann den Zugriff auf Unterwasserkabel beinhalten, die Internetdaten auf dem Weg in die USA transportieren. EO 12333 verlässt sich nicht auf die erzwungene Unterstützung von Dienstanbietern, sondern scheint sich stattdessen auf die Ausnutzung von Schwachstellen in der Telekommunikationsinfrastruktur zu verlassen.

Atlassian könnte nach eigenen Angaben, wie die meisten in den USA ansässigen SaaS-Unternehmen, technisch gesehen FISA 702 unterliegen. Atlassian verarbeitet jedoch keine personenbezogenen Daten, die für US-Geheimdienste von Interesse sein könnten.

Darüber hinaus ist es nach eigenen Angaben unwahrscheinlich, dass Atlassian Gegenstand von vorgelagerten Überwachungsanordnungen gemäß FISA 702 und der Art von Anordnungen ist, die hauptsächlich in der Schrems II-Entscheidung behandelt und als problematisch angesehen wurde. Atlassian stellt keine Internet-Backbone-Dienste bereit, sondern überträgt nur Datenverkehr, an dem seine eigenen Kunden

beteiligt sind. Bisher hat die US-Regierung FISA 702-Upstream-Aufträge nur auf Marktanbieter ausgelegt und angewandt, die Datenverkehr über ihr Internet-Backbone fließen lassen und Datenverkehr für Dritte (d. h. Telekommunikationsanbieter) übertragen.

Executive Order 12333 enthält keine Genehmigung, private Unternehmen (wie Atlassian) zu zwingen, personenbezogene Daten an US-Behörden weiterzugeben, und FISA 702 verlangt, dass ein unabhängiges Gericht eine bestimmte Art der Erfassung ausländischer Geheimdienstdaten genehmigt, die im Allgemeinen nichts mit kommerziellen Informationen zu tun hat. Für den Fall, dass US-Geheimdienste an der Art von Daten interessiert sind, die Atlassian verarbeitet, würden Schutzmaßnahmen wie das Erfordernis der Genehmigung durch ein unabhängiges Gericht und die Anforderungen an die Notwendigkeit und Verhältnismäßigkeit die Daten vor übermäßiger Überwachung schützen.

Nach Angaben von Atlassian erlaubt der CLOUD Act der US-Regierung nur den Zugriff auf Daten in strafrechtlichen Ermittlungen, nachdem ein von einem unabhängigen Gericht genehmigter Haftbefehl auf der Grundlage der wahrscheinlichen Ursache einer bestimmten Straftat eingeholt wurde.

2.2. Praktische Erfahrung von Atlassian im Umgang mit behördlichen Zugriffsanfragen

Atlassian veröffentlicht einen jährlichen Transparenzbericht mit Informationen über behördliche Anfragen zum Zugriff auf Daten.

https://www.atlassian.com/de/trust/privacy/transparency-report

Obwohl Atlassian technisch möglicherweise den in Schrems II genannten Überwachungsgesetzen unterliegt, war Atlassian nach eigenen Angaben bisher nicht Gegenstand von den vorgenannten behördlichen Anfragen.

3. Getroffene Maßnahmen zur Einhaltung des EU-Schutzniveaus

Für die sichere Nutzung von Jira Service Management werden durch Atlassian verschiedene Maßnahmen ergriffen, die die Übermittlungsinstrumente ergänzen, um die Einhaltung des EU-Schutzniveaus für personenbezogene Daten zu gewährleisten.

Wenn personenbezogene Kundendaten, die aus Europa stammen, zwischen Unternehmen der Atlassian-Gruppe oder von Atlassian an Unterauftragsverarbeiter von Drittanbietern übertragen werden, schließt Atlassian SCCs mit diesen Parteien ab. Dieses ist im Einklang mit den Richtlinien des European Data Protection Board (edpb) als Transfer-Instrument gem. Art. 46 DSGVO grundsätzlich geeignet, einen Datentransfer in die USA bzw. in Drittländer zu legitimieren[1]. Durch den Vertrag mit den Unterauftragsverarbeitern stellt Atlassian sicher, dass die Unterauftragsverarbeiter nur insoweit auf die Daten des Kunden zugreifen, als dies zur Durchführung ihrer begrenzten Tätigkeiten erforderlich ist.

[1] https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

Atlassian ist gemäß den SCCs verpflichtet, seine Kunden zu benachrichtigen, falls eine Regierungsbehörde einen Antrag auf Zugriff auf personenbezogene Kundendaten stellt. Für den Fall, dass es Atlassian gesetzlich untersagt ist, eine solche Offenlegung vorzunehmen, ist Atlassian vertraglich verpflichtet, dieses Verbot anzufechten und einen Verzicht zu beantragen. Gemäß den SCCs ist Atlassian verpflichtet, die Rechtmäßigkeit von Zugriffsanfragen von Regierungsbehörden zu überprüfen und solche Anfragen anzufechten, wenn sie als rechtswidrig erachtet werden.

Atlassian befolgt die eigene Richtlinie für Anfragen von Strafverfolgungsbehörden bei der Beantwortung von behördlichen Anfragen nach Daten.

https://www.atlassian.com/trust/privacy/guidelines-for-law-enforcement

Um Daten von Atlassian zu erhalten, müssen Strafverfolgungsbeamte rechtliche Schritte einleiten, wie z. B. eine Vorladung, ein Gerichtsbeschluss oder ein Haftbefehl.

https://www.atlassian.com/trust/privacy/country/europe-and-gdpr

https://www.atlassian.com/trust/compliance/resources/gdpr

Alle Kundendaten in Atlassian Cloud-Produkten werden bei der Übertragung über öffentliche Netzwerke mithilfe von TLS 1.2 (oder aktueller) mit Perfect Forward Secrecy (PFS) verschlüsselt, um sie vor einer unautorisierten Veröffentlichung oder Modifikation zu schützen. Die Implementierung von TLS setzt die Verwendung starker Chiffren und Schlüssellängen voraus, sofern diese vom Browser unterstützt werden.

Datenlaufwerke auf Servern, auf denen Kundendaten und Anhänge in Jira Software Cloud, Jira Service Management Cloud, Jira Work Management, Bitbucket Cloud, Confluence Cloud, Statuspage, Opsgenie und Trello gespeichert sind, verwenden im Ruhezustand die AES-256-Verschlüsselung nach Branchenstandard.

Atlassian nutzt den AWS Key Management Service (KMS) für das Schlüsselmanagement. Der Verschlüsselungs-, Entschlüsselungs- und Schlüsselmanagementprozess wird im Rahmen interner Prüfprozesse bei AWS regelmäßig untersucht und verifiziert.

4. Fazit

Angesichts der in diesem Dokument enthaltenen Informationen, einschließlich der praktischen Erfahrungen von Atlassian im Umgang mit behördlichen Anfragen und der technischen, vertraglichen und organisatorischen Maßnahmen, die Atlassian zum Schutz der personenbezogenen Daten seiner Kunden ergriffen hat, ist Atlassian der Ansicht, dass die Risiken, die mit der Übermittlung und Verarbeitung europäischer personenbezogener Daten in die USA verbunden sind, Atlassian nicht bei der Erfüllung der Verpflichtungen gemäß den SCCs beeinträchtigt oder den Schutz der Rechte natürlicher Personen beeinträchtigt.

Aus Sicht von BKS sind die von Atlassian beschriebenen Maßnahmen unter Berücksichtigung der konkreten Umstände der Übermittlung als ausreichend anzusehen. Hierbei ist zu beachten, dass von einem Drittstaatentransfer allenfalls Anfragen für den technischen Support betroffen sind. Hierbei kann sogar der Ticketschreiber mitentscheiden, welche Daten über das Ticketsystem verarbeitet werden.

Aufgrund der Zugriffsmöglichkeiten seitens der Behörden in den USA verbleiben jedoch hinsichtlich des Ticketsystems gewisse datenschutzrechtliche Risiken, die sich derzeit nicht gänzlich ausschließen lassen. Allerdings gab es in der Vergangenheit laut Angaben von Atlassian bislang keine behördlichen Anfragen, welche auf die Offenlegung von personenbezogenen Daten abzielten, die Atlassian als Auftragsverarbeiter verarbeitet. Darüber hinaus ist die Wahrscheinlichkeit, dass die personenbezogenen Daten der Atlassian-Kunden für die US-Geheimdienste von Interesse sind, eher gering. Denn die US-Regierung hat in einem „White Paper“ im September 2020 klargestellt, dass Unternehmen, die gewöhnliche kommerzielle Produkte oder Dienstleistungen anbieten und deren Datentransfers gewöhnliche kommerzielle Informationen betreffen, keinen Grund zu der Annahme haben, dass US-Geheimdienste versuchen würden, diese Daten zu sammeln. Die Dienste, welche Atlassian als Auftragsverarbeiter anbietet, stellen gerade solche kommerziellen Dienste dar.

Dementsprechend kann unter Berücksichtigung der konkreten Umstände der Übermittlung und der getroffenen Schutzmaßnahmen ein angemessenes Datenschutzniveau mit Einschränkungen angenommen werden.