

Deine Reise in die Atlassian Cloud

– datenschutzkonform mit dem
5-Schritte-Flugplan



Stelle dir vor:



Dein Unternehmen möchte Geschäftsprozesse und Daten in die Cloud migrieren und dein Cloud-Projekt steht bereits kurz vor dem Go-Live. Irgendjemand stellt die Frage, ob es noch irgendetwas beim Datenschutz zu beachten gibt. Also soll der oder die Datenschutzbeauftragte noch schnell eingebunden werden: „Wir wollen nächste Woche die neue Cloud in Betrieb nehmen, müssen wir da noch etwas beim Datenschutz beachten?“ Welche Antwort würdest du an dieser Stelle vermuten?

Ohne Daten – ganz besonders ohne personenbezogene Daten – geht es heute in keinem Unternehmen mehr vorwärts. Unternehmen benötigen jederzeit Daten von Mitarbeitenden, Geschäftspartner*innen, Kunden und denjenigen, die noch Kunde werden sollen. Denn Geschäfte werden mit Menschen gemacht. Bereits an dieser Stelle kommt der Datenschutz ins Spiel: Ein umfangreiches gesetzliches Regelwerk, mit dem der Umgang mit personenbezogenen Daten festgelegt und reguliert werden soll.

Der Einsatz moderner IT bis hin zur hochspezialisierten Cloud-Lösung bringt überdies noch weitere Herausforderungen mit sich. Wie können hier Unternehmensdaten – egal ob personenbezogen oder nicht – angemessen geschützt werden? Umfangreiche IT-Strukturen vereinfachen und beschleunigen idealerweise die Geschäftsprozesse. Die wachsende Komplexität schränkt jedoch sowohl die Transparenz als auch die Kontrollmöglichkeiten ein. Transparenz und Kontrolle über personenbezogene Daten und deren Verwendung sind aber die grundlegenden Säulen des gesetzlichen Datenschutzes. Wie der Autor dieses Artikels einleitend bereits angedeutet hat, ist es nicht sinnvoll, erst am

Ende eines umfangreichen Projektes kurz den Datenschutz zu befragen und auf eine schnelle Absolution zu hoffen. Datenschutz kann erfolgreich umgesetzt werden, wenn seine Anforderungen – wie andere geschäftliche und IT-technische Anforderungen auch – von Anfang an beachtet werden. Diese Idee ist nicht neu und auch keine Erfindung eines Gesetzgebers. Das Stichwort – aus Zeiten lange vor der EU-Datenschutz-Grundverordnung (DS-GVO) – heißt „Privacy by Design“.

Wie ist es nun möglich, in einem Cloud-Projekt den Datenschutz frühzeitig und idealerweise bereits in der Design-Phase angemessen zu berücksichtigen?

Ein guter Start ist eine frühzeitige Einbindung der Personen, die sich im Unternehmen mit Datenschutz und ggf. auch mit Informationsschutz (-> Betriebs- und Geschäftsgeheimnisse) beschäftigen. Im Optimalfall findet bereits ein Austausch statt, wenn die ersten Ideen für den Einsatz einer Cloud diskutiert werden. Verfügt ein Unternehmen nicht über Cloud- und Technik-erfahrene Datenschutzbeauftragte, kann Seibert Media dabei helfen, diese Lücke zu schließen.

Zu Beginn stehen viele grundlegende Fragen im Raum. Ist das in deinem Projekt nicht der Fall? Dann hilft der*die Datenschützer*in, die richtigen Fragen zu stellen, zum Beispiel:

- Was soll mit dem Einsatz einer Cloud-Lösung erreicht werden (Ziele)?
- Welche Geschäftsprozesse sind betroffen?
- Welche Daten sollen in der Cloud gespeichert und genutzt werden?
- Wo genau werden die Daten gespeichert (inkl. eventueller Backups)?
- Von wem und woher stammen diese Daten?
- Wer sind die beteiligten Unternehmen (Cloudanbieter, Integrationspartner, ggf. weitere Gesellschaften der eigenen Unternehmensgruppe usw.)?
- Welche IT-Produkte und Technologien sollen zum Einsatz kommen?
- Welche Schnittstellen sind geplant?

Verfügt das Unternehmen bereits über ein aktives Datenschutz-Management-System (DSMS) und geeignete Dokumentationen zur Verarbeitung von personenbezogenen Daten, werden einige dieser Fragen schnell zu beantworten sein. Besonders die bereits im Verzeichnis der Verarbeitungstätigkeiten (die gesetzlich vorgeschriebene Datenschutzdokumentation gem. Art. 30 DS-GVO) dokumentierten Informationen sind hier eine wichtige Grundlage. Ist Datenschutz aber noch ein neues Thema für das Unternehmen, ist nun ein geeigneter Moment, um auch außerhalb des Cloud-Projekts für die notwendige Transparenz und rechtliche Compliance zu sorgen.

Hier findest du eine Checklist zur Bestandsaufnahme zum Datenschutz in unserer Infothek zum Download.



Häufig stehen zu Beginn noch nicht alle Informationen zur Verfügung. Das soll aber nicht daran hindern, eine frühzeitige (Teil-)Bestandsaufnahme zu starten und die verfügbaren Informationen zu bewerten. Hierbei sind sowohl die Auswirkungen auf als auch die Anforderungen aus dem Datenschutz zu ermitteln.

Abhängig von den betroffenen Daten und den damit verbundenen Rahmenbedingungen kann dies recht unterschiedlich ausfallen. Die nachfolgenden Fragestellungen zeigen beispielhaft, um welche Themen es hier geht:

- Welche Daten dürfen bzw. dürfen nicht in der Cloud gespeichert werden?
- Müssen ergänzende rechtliche Rahmenbedingungen geschaffen werden, um die Nutzung der Cloud zu ermöglichen?
- Welche zusätzlichen Maßnahmen zur Datensicherheit sind in der Cloud erforderlich und welche werden bereits vom Cloudanbieter sichergestellt?
- Welche Garantien bietet der Cloudanbieter zum Schutz der Daten und sind diese ausreichend?
- Sind bestimmte Risikobewertungen und ggf. zugehörige Maßnahmen erforderlich?
- Wie werden auch beim Cloudeinsatz die Informationspflichten gem. Art. 12-14 DSGVO erfüllt?
- Wie können in der Cloud die gesetzlich vorgesehenen Betroffenenrechte, beispielsweise das Recht auf Auskunft und das Recht auf Datenlöschung, umgesetzt werden?



An dieser Stelle scheiden sich die Geister. Während bei manchen Unternehmen die Einführung eines Wikis als Fortschritt gefeiert wird, geben sich andere noch längst nicht nur mit einem schriftlichen „Statement of Work“ und einem 30-seitigen Grobkonzept zufrieden. Wie viel Konzeption und Dokumentation sind tatsächlich notwendig?

Allein aus Sicht des Datenschutzes lässt sich sagen: Planung und Dokumentation sind erforderlich. Das Gesetz verlangt an verschiedenen Stellen qualitative Gütekriterien (z. B. der „Stand der Technik“ in Art. 32, Abs. 1 DS-GVO) und verpflichtet Unternehmen dazu, die Einhaltung der gesetzlichen Vorgaben zum Datenschutz nachzuweisen (Art. 5, Abs. 2 DS-GVO, „Rechenschaftspflicht“). Für die Umsetzung eines Cloud-Projektes, das diese Vorgaben erfüllen soll, ist somit das eine oder andere Konzept, das die Umsetzung der nunmehr ermittelten Datenschutzanforderungen sicherstellt, erforderlich.

Neben Konzepten, die für eine sichere IT obligatorisch sind (Backup, Virenschutz, Change- und Patchmanagement usw.), legt der Datenschutz nahezu immer besonderen Wert auf diese Bereiche:

Das Berechtigungskonzept

Wie wird strukturell (Rollen, Rechte) und prozessual (Prozess von der Beantragung über die Freigabe bis zur Vergabe) sichergestellt, dass nur die befugten Personen Zugriff auf die Cloud haben? Dabei sollen nur die unbedingt erforderlichen Berechtigungen zugewiesen und solche, die nicht mehr benötigt werden, zeitnah wieder entzogen werden.

Das Löschkonzept

Dem Gesetz nach müssen personenbezogene Daten gelöscht werden, wenn diese für den ursprünglichen Zweck, zu dem sie gespeichert wurden, nicht mehr benötigt werden. Dabei sind eventuelle gesetzliche Pflichten zur Aufbewahrung mit zu berücksichtigen. In einem Löschkonzept werden die umfangreichen Anforderungen des Unternehmens an die Aufbewahrung und Löschung von Daten gesammelt und die rechtskonforme Berücksichtigung im eigenen Unternehmen festgelegt. Den Weg zur Erstellung eines Löschkonzeptes beschreibt die DIN 66398.

Die Informationspflichten

Die Säulen des Datenschutzes sind „Transparenz“ und „Kontrolle“ für die betroffenen Personen. Auch bei Nutzung einer Cloudlösung sind die vom Gesetzgeber vorgeschriebenen Informations- und Transparenzpflichten zu erfüllen. Bei einem Umstieg in die Cloud müssen ggf. die bereits bestehenden Rechtstexte („Informationen zur Verarbeitung der personenbezogenen Daten“, „Datenschutzerklärung“, „Privacy Notices“ o. ä.) aktualisiert werden. Die Herausforderung ist hier die Beschaffung der Detailinformationen, die in solchen Informationstexten enthalten sein müssen.

Die Betroffenenrechte

„Kontrolle“ erhalten die betroffenen Personen über die im Gesetz festgelegten Betroffenenrechte. Unternehmen sind verpflichtet, die Erfüllung dieser Rechte zu gewährleisten. Wahlweise muss, entweder in einem separaten Konzept oder als Bestandteil anderer Konzepte innerhalb des Cloud-Projekts, garantiert werden, dass eine Umsetzung dieser Rechte auch in der Cloud praktisch funktioniert. Beispiel: Ein*e Bewerber*in, dessen*deren Bewerbungsunterlagen in der Cloud gespeichert sind, wünscht nach einer Absage die Löschung seiner*ihrer Bewerbungsdaten. Die Daten werden nun gelöscht – aber entfernt der Cloudanbieter diese Daten tatsächlich aus seiner Cloud-Infrastruktur, inkl. aller Backups – und bis wann? Sein Problem? Nein – vor dem Gesetz ist das Unternehmen, das die Cloud nutzt, dafür verantwortlich. In der Praxis lässt sich das lösen, aber es erfordert eine konzeptionelle Betrachtung.



Was bedeuten Umsetzung und Go-Live aus Sicht des Datenschutzes? Alle wesentlichen – vor allem die rechtlichen – Stolpersteine sind beseitigt oder soweit bekannt, dass man noch daran vorbeikommt. Datenschutzverträge werden finalisiert, benötigte Rechtstexte (Datenschutzerklärung & Co.) werden geschrieben, Mitarbeitende werden bei Bedarf geschult und die Datenschutzerklärungen aktualisiert.

Die meisten Anforderungen aus dem Datenschutz sind aber bereits in die IT-Konzepte und -Prozesse eingeflossen. Diese sind nun datenschutzkonform gestaltet und stellen eine angemessene Umsetzung des Datenschutzes sicher. Im Cloud-Projekt ist der Datenschutz ein Baustein von vielen. Diesen Baustein spontan eine Woche vor dem Go-Live einzubauen (siehe die Einleitung zu diesem Beitrag) ist praktisch nicht möglich. Ja, Datenschutz erfordert zusätzliche Ressourcen, vor allem in der Planungs- und Konzeptionsphase. In vielen Fällen kostet das aber deutlich weniger, als den Datenschutz nicht zu beachten oder zu versuchen, ihn nachträglich zu implementieren.

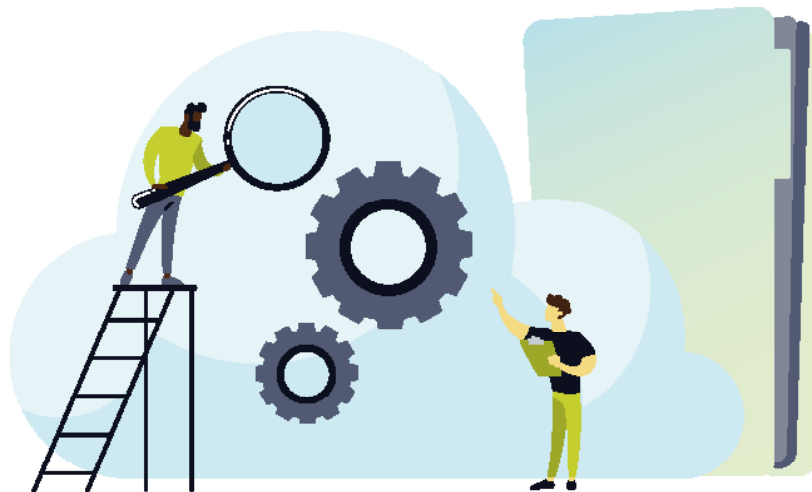


Es ist nicht immer beliebt, aber es gehört zum Stand der Technik, in der IT angemessen zu testen. Das ist im Datenschutz nicht anders. Betreibt ein Unternehmen ohnehin aktiv Qualitätssicherung, dann ist die Ergänzung weiterer Testfälle und Prüfungen für den Datenschutz keine große Herausforderung mehr.

Im Datenschutz sind daneben auch regelmäßige und anlasslose Prüfungen gefordert: „... Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit ...“ (Art. 32, Abs. 1 lit. d DS-GVO)

Unternehmen, die beispielsweise ein Qualitätsmanagement oder eine IT-Revision betreiben oder nach Standards wie der ISO 27001 zertifiziert sind, verfügen meist über alle wichtigen Voraussetzungen für regelmäßige Wirksamkeitskontrollen. Auch hier ist es größtenteils ausreichend, die bestehenden Prüfprozesse um die Prüfanforderungen im Datenschutz zu erweitern.

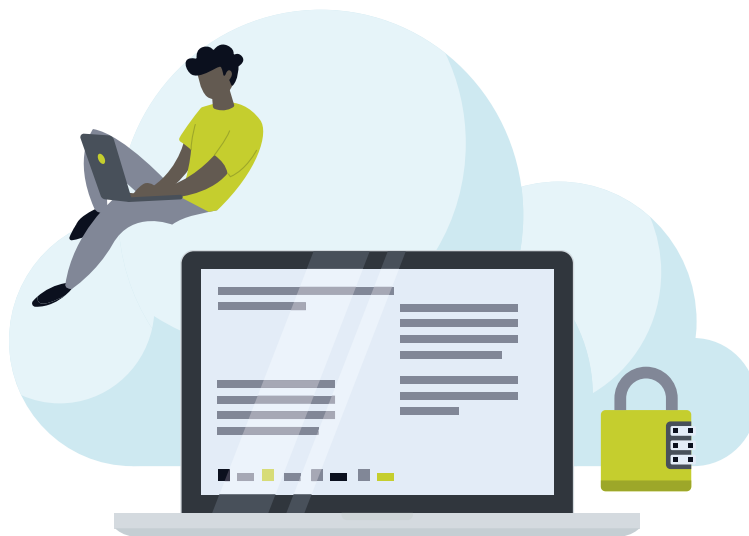
Kann ein Unternehmen das nicht leisten, können solche Prüfungen auch durch externe Dienstleister aus dem Daten- und Informationsschutz vorgenommen werden.





Hast du etwas gemerkt?

Bestandsaufnahme, Anforderungsmanagement, Konzeption, Umsetzung, Qualitätssicherung – das ist nichts Neues. Das ist der übliche, professionelle Weg zu einem erfolgreichen IT-Projekt. Der Datenschutz ist in diesem Zusammenhang vor allem eine Liste mit detaillierten Anforderungen, die frühzeitig berücksichtigt werden sollte. Mit diesem 5-Schritte-Flugplan hast du nun eine erste Handreichung, wie das funktionieren kann.



Die Inhalte für dieses Whitepaper sind in Zusammenarbeit mit unserem Datenschutzexperten Thomas Rosin entstanden.

Thomas Rosin hat sich auf Daten- und Informationsschutz spezialisiert. Neben seiner Tätigkeit als Datenschutzbeauftragter und Berater für Unternehmen lehrt er Datenschutz im Masterstudiengang Wirtschaftsinformatik an der Rheinischen Fachhochschule Köln.

Kontakt: info@thomasrosin.de

Web: www.thomasrosin.de



Noch Fragen?

Bei allen weiteren Fragen rund um die Atlassian Cloud wende dich gerne an uns. Als Atlassian Platinum Solution Partner mit Erfahrungen aus tausenden von Atlassian-Projekten beraten wir dich bei der Evaluation eines für dich optimalen Lizenzmodells, kümmern uns um sämtliche Fragen rund um dein Lizenz-Set-up und unterstützen dich bei allen Aspekten rund um die Skalierung deiner Atlassian-Produkte.

Termin vereinbaren

Exklusiver Lizenzverkauf

Bei uns erhältst du alle Lizenzen, die du für deine individuelle Atlassian-Lösung benötigst. Darüber hinaus profitierst du beim Kauf deiner Atlassian-Lizenzen über Seibert Media von vielen zusätzlichen Vorteilen.

Migration & Einführung

Wir helfen dir bei der Planung und Umsetzung der Daten- und Usermigration von Server oder Data Center zu Atlassian Cloud. Außerdem stehen wir dir bei der Betreuung der laufenden Prozesse zur Seite – bis hin zur Abrechnung.

Cloud Training & Workshops



Wir bieten umfangreiche Trainings und Workshops im Cloud-Umfeld. Vereinbare noch heute einen Termin mit einer* einem unserer erfahrenen Consultants.

Mail: atlassian-licensing@seibert-media.net

Telefon: +49 800 181 209 2

Website: seibert-media.net/atlassiancloud/



Platinum
Solution Partner