BMW GROUP

FAQ zu den Inhalten der neuen Allgemeinen Vertragsbedingungen im indirekten Einkauf (AVB), Stand 02/2017

1. **Was hat sich in den neuen AVB (Stand 02/2017) im Vergleich zur Vorversion (Stand 09/2015) verändert?**
   Um einen übergreifenden Basisschutz von BMW Daten und in Sachen Informationssicherheit zu gewährleisten, wurden die Allgemeinen Vertragsbedingungen (AVB) des indirekten Einkaufs um zwei Klauseln angereichert: 15. „Rechte an BMW Daten“ und 16. „Informationssicherheit“.
   Außerdem haben wir die Geheimhaltungsklausel 17. an die BMW Standard Geheimhaltungsvereinbarung angeglichen, um Einheitlichkeit zu schaffen. Diese ist seit gut einem Jahr im Einsatz. Da sie zweiseitig formuliert ist und Geheimhaltungspflichten für beide Parteien vorsieht, ist dies eine Anpassung auch zu Ihren Gunsten als Lieferant.
   Daneben haben wir kleinere Anpassungen vorgenommen, wie neue Begriffsbestimmungen in Klausel 1, die Aufnahme weiterer Compliance Verpflichtungen (Klausel 2.5 und 3.2) und des Grundsatzes, dass kein Anspruch auf Teilabnahmen besteht (Klausel 5.4) oder die Umformulierung der Klausel 9.4 zu den Bürgschaften.

2. **Warum sind die neuen Klausel 15 und 16 so ausführlich?**
   Leider fehlt es bisher an gesetzlichen Regelungen zu Rechten an Daten sowie Rechten und Pflichten mit Daten in Vertragsverhältnissen. Wir mussten daher viele Details, wie Definitionen und Beispiele, in die Klauseln aufnehmen, die alle Anwendungsfälle regeln und erfassen.

3. **Was heißt industrieüblicher Standard (Klausel 16.1)?**
   Der industrieübliche Standard für Informationssicherheitsanforderungen in der Automobilindustrie ist der VDA (Verband der deutschen Automobilindustrie e.V.) ISA Fragenkatalog (Information Security Assessment) in der jeweils gültigen Version. Da der industrieübliche Standard dem Namen nach die Gegebenheiten der jeweiligen Industrie berücksichtigt, stellt er keine überzogenen Forderungen an Sie als Lieferanten, sondern sichert BMW einen Basisschutz. Um zu vermeiden, dass kurzfristig eine erneute Anpassung der Klauseln notwendig wird, ist der Begriff bewusst nicht konkreter definiert worden.
   Die Prüfung nach dem VDA ISA Fragenkatalog erfolgt im Rahmen des VDA Modells TISAX („Trusted Information Security Assessment Exchange“); siehe Erläuterungen Frage 5.

4. **Was heißt Stand der Technik (Klausel 16.2)?**
   „Stand der Technik“ ist ein gängiger juristischer Begriff, der nicht allgemeingültig und abschließend definiert ist. Da die technische Entwicklung schneller ist als die Gesetzgebung, hat es sich bewährt, in Gesetzen den Begriff „Stand der Technik“ zu verwenden, statt zu versuchen, konkrete technische Anforderungen festzulegen. Was zu einem bestimmten Zeitpunkt „Stand der Technik“ ist, lässt sich zum Beispiel anhand existierender nationaler oder internationaler Standards oder anhand erfolgreich in der Praxis erprobter Vorbilder für den jeweiligen Bereich ermitteln.[1]

[1] https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/IT-SiG/Neuregelungen_KRITIS/B3S/b3s_node.html

5. Was ist das VDA TISAX-Modell?

Die Mitglieder des VDA (Verband der deutschen Automobilindustrie e.V.) haben gemeinsam das Modell „TISAX“ entwickelt („Trusted Information Security Assessment Exchange“). Es dient der Definition und Anwendung eines brancheneinheitlichen Standards für Informationssicherheitsanforderungen/ -prüfverfahren, mit dem Ziel, gegenseitig Informationssicherheitsprüfungen von Partnern anzuerkennen und ein einheitliches Sicherheitsniveau zu etablieren. Es steht ab 01/2017 für die Erlangung von Informationssicherheitstestierungen zur Verfügung.

Auch die BMW Group strebt eine flächendeckende Anwendung des TISAX-Modells im Lieferantennetzwerk an, um das Informationssicherheitsniveau in der Zusammenarbeit mit Partnern zu erhöhen. So wird BMW künftig von ihren Lieferanten den Nachweis einer angemessenen VDA-Informationssicherheitstestierung durch akkreditierte TISAX-Prüfdienstleister voraussetzen.

Detaillierte Informationen zum TISAX-Modell stehen unter www.tisax.org zur Verfügung.

6. Was ist schadenstiftende Software (Klausel 16.3)?

Hierbei handelt es sich um z.B. Viren, Malware, Ransomware und generell jede Software, die Schaden bei BMW anrichten kann.

7. Wer hat die Kosten eines Audits zu tragen (Klausel 16.6 b)?

Kosten für ein von BMW veranlasstes Audit trägt BMW. Die Kosten für eine TISAX-Testierung trägt der Lieferant.

8. Haben sich die Regelungen zum Quellcode von Software verändert?

Inhaltlich hat sich Klausel 5.2 nicht verändert, ist aber nun unter Klausel 3.10 zu finden. Sie regelt weiterhin, dass der Lieferant den Quellcode für den Fall an BMW übergeben muss, dass er im Rahmen der Leistungserbringung Software erstellt oder anpasst. Weiterhin ist Klausel 2.7 zu den BMW Bedingungen für den Einsatz von Open Source Software“ (nachfolgend „OSS Bedingungen“) zu beachten, die sich inhaltlich ebenfalls nicht verändert hat. Laut Klausel 13.3 erstrecken sich vom Lieferant eingeräumte Rechte auch den Quellcode und die dazugehörige Dokumentation.
Spezielle Regelungen dazu finden sich außerdem in den (demnächst erscheinenden) „IT BVB“ (z.B. für IT-Projektleistungen oder den Kauf von Software).

9. Haben sich die Regelungen zu Schutz- und Nutzungsrechten verändert?

Nein, die Klausel 13. hat nur redaktionelle Änderungen zugunsten der Übersichtlichkeit erfahren. Die darin erhaltenen Regelungen zu Rechten an dem für BMW zu erbringenden Leistungsergebnis bleiben von den neuen AVB Inhalten, insbesondere Klausel 15 „Rechte an BMW Daten“, unberührt.

10. An wen kann ich mich mit Fragen wenden?

Falls Sie Fragen zu den neuen AVB haben, wenden Sie sich bitte an Ihren zuständigen Ansprechpartner im indirekten Einkauf oder an unser Vertragsmanagement unter vertragsmanagement@bmw.de.