FAQ on the content of the new General Terms and Conditions (GTC) for Indirect Purchasing, status 02/2017

1. **What has been changed in the new GTC (status 02/2017) in comparison to the old version (status 09/2015)?**
   For ensuring of an overarching basic protection of BMW Data and Information security the General Terms and Conditions (GTC) for Indirect Purchasing have been extended by two more sections, section 15 "Data to BMW Rights" and section 16 "Information Security".
   Furthermore, to establish uniformity, we have adjusted section 17 "Confidentiality" to the standard Confidentiality Agreement. The Confidentiality Agreement is in use about a year. Because it is two-sided formulated and provides confidentiality obligations for both parties, it is an adjustment also in your favor as a supplier.
   Besides, we added some small adjustments, like new definitions in section 1, the inclusion of additional compliance obligations (section 2.5 and 3.2) and the principle that the supplier in general shall not have claims to partial acceptance (section 5.4) or the rewording of section 9.4 about guarantees.

2. **Why are sections 15 and 16 so detailed?**
   Unfortunately legal regulations about rights to data as well as rights and obligations referring data within the contractual relationship have been missing so far. Therefore we had to include many details such as definitions and examples in the clauses, which regulate all use cases.

3. **What does "customary industry standards" (section 16.1) mean?**
   The customary industry standard for information security requirements in the automotive industry is the VDA (Verband der deutschen Automobilindustrie e.V.) ISA questionnaire (Information Security Assessment) as amended.
   The term "customary industry standards" in name takes the circumstances of the respective industry into account, it does not put unrealistic demands on you as the supplier but ensures a basic protection for BMW.
   To avoid a short-term new adaption of the section because of new technical developments, the term is consciously not better defined. Since we do not demand this standard for all procurement volumes or suppliers, the ascertainment has not been included in the GTC.
   The examination under the VDA ISA questionnaire take place within the VDA model TISAX ("Trusted Information Security Assessment Exchange"); see explanations under question 5.

4. **What means state of art (section 16.2)?**
   "State of art" is a common legal term which is not universal and not conclusively defined. Due to the faster technical development compared to the legislation, it has proved to use the term "state of art" in laws instead of trying to find concrete technical requirements. What "state of art" at a specific date means, can be determined for example by an existing

national or international standard or by a successful in practice proven model for each area.[1]

5. **What means the VDA TISAX-Model?**
   The members of the VDA have developed the model "TISAX" („Trusted Information Security Assessment Exchange") together. It is used for definition and application of an industry wide standard for information security requirements and test procedures, with the aim to recognize information security examinations mutually from partners and to establish a uniform protection level. It is available for achievement of information security examination on 01/2017.
   The aim of the BMW Group is an area-wide application of the TISAX-Model in the supplier network to increase the level of the information security in cooperation with partners. In the future BMW will request a certification of an appropriate VDA information security examination by accredited auditors.
   Detailed information of the TISAX-Model can be found on www.tisax.org.

6. **What means malicious software (section 16.3)?**
   These are f.e. viruses, malware, ransomware and generally every software which can cause damages to BMW.

7. **Who has to bear to costs of an audit (section 16.6 b)?**
   Expenses of an audit initiated by BMW has to be borne by BMW. (Expenses for a TISAX-examination bears the supplier.)

8. **Have the regulations for the source code been changed?**
   The content of section 5.2 has not been changed, but it can be found under 3.10 now.
   It still requires that the supplier has to hand over the source code to BMW in case the supplier creates or adapts software during the service provision.
   Furthermore, section 2.7 has to be observed for the use of Open Source Software (hereinafter as "OSS conditions") under the BMW conditions, which also has not been changed. According to 13.4 the granted rights to the supplier also extend to the source code and its associated documentation.
   Additionally special regulations can also be found in the (release in March 2017) "IT STC" (f.e. for IT project services or the purchase of software).

9. **Have the regulations about IP rights and rights of use been changed?**
   No, section 13 only underwent editorial changes. It still regulates that the services for BMW have to be free of rights of third parties and the supplier commits himself to free BMW from any claims of protection and usage rights. Additionally all copyrighted rights, industrial property rights and similar property rights to the provided service will pass to BMW, unless agreed otherwise.

10. **Who can I contact if I have questions?**
    If you have any questions please don't hesitate to contact your responsible contact person in the relevant purchasing department or our contract management team at vertragsmanagement@bmw.de.

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