Data Processing Agreement

This Data Processing Agreement is entered into by and between:
本《数据处理协议》由以下双方签订：

BMW China Automotive Trading Ltd.
宝马(中国)汽车贸易有限公司
Floor 28th, Tower B, Gateway Plaza, No.18 Xiaguangli, North Road of East 3rd Ring, Chaoyang District, Beijing, 100027
北京市朝阳区东三环北路霞光里 18 号佳程广场 B 座 28 层，100027

("NSC")
（"**宝马汽贸**"）

And
与

COMFORT INTERNATIONAL M.I.C.E. SERVICE CO., LTD.
康辉集团北京国际会议展览有限公司
Room 002, No. 1510, 12th floor, No. 13 Agricultural Exhibition Hall South Road, Chaoyang District, Beijing, PRC, 100025
中国北京市朝阳区农展馆南路 13 号 12 层 1510 内 002，100025

(the "**Authorized Party**" or "**Processor**")
（"**受托方**"）

Whereas
鉴于

NSC assigns Authorized Party with the processing of Personal Data on behalf of NSC.
宝马汽贸指定受托方代表其处理个人信息。

1. **Definition**
   定义

"**Applicable Laws**" means the *Cybersecurity Law of the People's Republic of China*, the *Data Security Law of the People's Republic of China*, the *Personal Information Protection Law*, the *Regulations on Automotive Data Security Management (for Trial Implementation)*and any other laws, regulations and standards that relate to the Data security and Personal Data protection.
"适用法律"指《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《汽车数据安全管理若干规定（试行）》以及与数据安全和个人信息保护相关的任何其他法律、法规和标准。

"**Data**" means any record of information in electronic or non-electronic form.
"数据"是指任何以电子或非电子形式记录的信息。

"**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed.
"个人信息泄露"是指违反安全规定，导致被传输、存储或以其他方式处理的个人信息意外或非法损毁、丢失、更改，或者未经授权披露或访问。

"**Personal Data**" or "**Personal Information**" means any kind of information related to an identified or identifiable natural person as electronically or otherwise recorded, excluding information that has been anonymized.
"个人数据"或**"个人信息"**是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理的信息。

"**Sensitive Personal Data**" or "**Sensitive Personal Information**" means Personal Data, once leaked or illegal used, will easily lead to infringement of the human dignity or harm to the personal or property safety of a natural person, including biometric recognition, religious belief, specific identify, medical and health, financial account, personal location tracking and other information of a natural person, as well as any personal information of a minor under the age of 14.
"敏感个人数据" 或 **"敏感个人信息"** 是指是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗

教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

"**Personal Data Subject**" or "**Personal Information Subject**", means the natural person identified by or associated with the Personal Data.
"个人数据主体"或**"个人信息主体"**是指被个人信息识别或与之相关的自然人。

"**PRC**" or "**China**" means the People's Republic of China and does not include Hong Kong SAR, Macau SAR and Taiwan for the sole purpose of the Agreement.
"中国"指中华人民共和国，仅为本《协议》之目的，不包括香港特别行政区、澳门特别行政区和中国台湾地区。

"**Collection**" means the act of acquiring control over Data, including automatic acquisition through voluntary provision by Personal Data Subjects, interaction with Personal Data Subjects or recording acts of Personal Data Subjects, and indirect acquisition of Personal Data and non-Personal Data through sharing, transferring, or gathering public information.
"收集"是指获取数据控制权的行为，包括通过个人信息主体自愿提供、与个人信息主体互动或记录个人信息主体的行为直接获取，以及通过共享、传输、收集公开信息间接获取个人信息和非个人信息。

"**Processing**" means any operation or set of operations which is performed on Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
"处理"是指对数据进行的任何一项或一组操作，无论是否通过自动方式，如收集、记录、组织、结构化、存储、改编或更改、检索、咨询、使用、通过传输、传播或以其他方式提供、校准或组合，限制、删除或销毁。

2. Subject-matter and Duration of the Agreement
协议的内容和期限

This Data Processing Agreement ("**Agreement**") sets the principles and general rules under which the Authorized Party shall provide services related to the Processing of Data to NSC.
本《数据处理协议》（"**《协议》**"）规定了受托方应向宝马汽贸提供数据处理相关服务的原则和一般规则。

The subject-matter and the duration of each service shall, according to different needs, be described in a detailed manner in **Annex 1 (Processing and Transmission of**

Personal Data). Annex 1 shall explicitly refer to this Agreement.
每项服务的目的和期限应根据不同的需要，在**附件 1（《个人信息的处理和传输》）**中详细列明。**附件 1** 应当适用本《协议》的规定。

Annex 1 shall contain the following:
附件 1 应包含以下内容：

- Detailed description and definition of tasks.
  处理任务的详细描述和定义
- Types of Personal Data Processed
  所处理个人信息的类型
- Categories of Personal Data Subjects
  个人信息主体的类别
- Purpose of Processing
  处理目的
- Method of Processing
  处理方式
- Duration of Processing
  处理期限
- Personal Data protective measures to be adopted by the Recipient
  接收方采取的个人信息保护措施
- NSC's rights to supervise and audit Recipient's Processing of Personal Data; and
  宝马汽贸监督和审计接收方处理个人信息的权利；以及
- Other rights and obligations of NSC and the Recipient respectively
  宝马汽贸与接收方其他权利与义务

This Agreement and the Annexes hereto form a part of the respective Purchase Contract or any other contract (if any) under which the Authorized Party provides IT services or other service related to the Processing of Data to NSC.
本《协议》及其附件构成宝马汽贸与受托方之间相应的《采购合同》或其他任何合同（如有）的一部分，根据该等合同，受托方向宝马汽贸提供 IT 服务或与数据处理相关的其他服务。

The Agreement becomes effective as of the date of execution and is valid for an indefinite period . The Agreement may be terminated in writing by either party with a three-month prior notice, or upon termination of all Purchase Contract or any other contract concluded between the parties, whichever comes earlier.
本《协议》自签署之日起生效，并持续有效。本协议的终止可以通过任何一方提前三个月发出书面通知，或当双方签订的所有采购合同或其他任何合同终止时终止（以较早者为准）。

In the event of a conflict between this Agreement and the Purchase Contract or any other contract, the provisions of this Agreement shall prevail if and to the extent the provisions relate to the Processing of Personal Data and other Data. The provisions of **Annex 1** shall prevail in the event of any inconsistencies between this Agreement and the provisions of **Annex 1**.
如果本《协议》与采购合同或其他任何合同之间存在冲突，则在与个人信息和其他数据处理相关的范围内，应以本《协议》的规定为准。如果本《协议》与**附件 1** 的规定存在任何不一致之处，应以**附件 1** 的规定为准。

Any change of the activities in **Annex 1** requires the prior written consent of NSC and is subject to compliance with the special requirements set out in Applicable Laws, such as consent from Personal Data Subjects and security assessment for Data cross border transmission. The specific circumstances involving cross-border transmission of Data and written consent of NSC shall be implemented in accordance with **Annex 1** .
对**附件 1** 中列明的情况的任何变更都需要获得宝马汽贸的事先书面同意，并且必须遵守适用法律所规定的特殊要求，例如个人信息主体的同意和数据跨境传输安全评估。涉及数据跨境传输和宝马汽贸书面同意的具体情况应按照**附件 1** 执行。

3. Technical and Organizational Measures
技术和制度措施

Within its area of responsibility, the Authorized Party shall organise the internal organisation in such a manner that the Processing will meet the special requirements of Data protection. The measures to be taken are measures of Data security and measures that guarantee a level of protection appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems.
在其职责范围内，受托方应设立相关内部机构，使处理活动满足数据保护的特殊要求，所采取的措施包括数据安全措施，以及与风险相符的保证系统保密性、完整性、可用性和恢复能力的措施。

The Authorized Party shall take appropriate technical and organizational measures to ensure a level of security appropriate to the risk, especially to protect Data against any breach. The security measures adopted by the Authorized Party shall include but are not limited to the following and those listed in **Annex TOM**:
受托方应采取适当的技术和组织架构安排，以确保与风险相适应的安全水平，尤其是保护数据免受任何破坏。受托方采取的安全措施应包括但不限于以下以及**附件 TOM** 中列出的措施：

a) formulating internal security management system and operating procedures, determining the persons in charge of cybersecurity, data security and Personal Information protection and implementing responsibility for cybersecurity protection,

Personal Information protection as well as data security;
制定内部安全管理制度和操作规程，确定网络安全、数据安全和个人信息保护负责人，落实网络安全保护、个人信息保护和数据安全责任；

b) adopting the technical measures for preventing computer virus and the activities endangering cybersecurity such as cyberspace attack and cyberspace intrusion;
采取技术措施防范计算机病毒和网络攻击、网络入侵等危害网络安全的活动；

c) adopting the technical measures for monitoring and recording cyberspace operation status and the cybersecurity incidents and keeping relevant cyberspace logs for at least 6 months in accordance with relevant provisions;
按照有关规定，采取技术措施监测和记录网络空间运行状态和网络安全事件，并将相关网络空间日志保存至少 6 个月；

d) adopting the measures such as Data classification as well as backup and encryption of Personal Information and other important Data;
采取数据分类，个人信息和其他重要数据备份加密等措施；

e) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
确保处理系统和服务持续的保密性、完整性、可用性和恢复能力；

f) the ability to restore the availability and access to Data, and eliminate the negative impact in a timely manner in the event of a physical or technical incident;
能够恢复数据的可用性和访问，并在发生物理或技术事故时及时消除负面影响；

g) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing;
定期测试和评估确保处理安全的技术和制度措施的有效性的过程；

h) any other steps required by Applicable Laws.
法律所要求的任何其他措施。

The Authorized Party shall establish and document the implementation of the technical and organizational measures as stipulated in **Annex TOM** to the Agreement before starting to Process the Data and shall present the documentation to NSC for review.
在开始处理数据之前，受托方应制定并以书面形式记录**附件 TOM** 中规定的技术和制度措施的实施情况，并将相关文件提交给宝马汽贸审查。

To the extent agreed in **Annexes**, the Processing of Data in private premises or in the context of tele working is permitted. The Authorized Party assures and ensures that the provision of services or work in private premises or in the context of tele working complies with the specific measures and requirements under this article and Annex TOM.
在**附件**约定的范围内，允许在私人场所或远程工作环境中处理数据。受托方确保在私人场所或远程工作环境中提供的服务或工作符合本条款和**附件 TOM** 规定的具体措施和要求。

The technical and organizational measures are subject to technical progress and development and the Authorized Party shall, and NSC may require the Authorized Party

to, implement adequate and superior alternative measures in the course of the Agreement.
技术和制度措施应随着技术的进步和发展同步发展，受托方应当自行或者按照宝马汽贸的要求在协议期间采取充足且更优的替代措施。

Any material changes by the Authorized Party to the technical and organizational measures agreed in this Agreement shall be agreed upon by NSC. Any such changes shall be documented in writing and become a part of the Agreement; **Annex TOM** will be amended respectively by the Authorized Party.
受托方对本《协议》规定的技术和组织架构安排所做的任何实质变更均应由宝马汽贸同意。任何此类变更应以书面形式记录，并成为《协议》的一部分；**附件 TOM** 将由受托方据此进行修订。

No special agreement is required if these changes lead to an improvement to the level of Data protection that was previously a part of this Agreement in the context of commissioned Data Processing and if NSC is informed about these changes, provided however, such changes will not alter the purpose and method of data processing; when the documentation of these changes is supplied to NSC the changes will automatically become a part of the Agreement and the **Annex TOM** must be adapted accordingly by the Authorized Party.
在委托数据处理的情况下，如果这些变更导致本《协议》规定的数据保护水平的提高，并且受托方向宝马汽贸进行报告，则无需另行签订协议，但前提是此类变更不会改变数据处理的目的和方式；当受托方向宝马汽贸提供这些变更的文件时，变更将自动成为《协议》的一部分，受托方应相应调整**附件 TOM**。

The Authorized Party shall in accordance with the requirements of the Applicable Laws implement the classified cybersecurity and data security system, and conduct assessment or filing with the public security organ as required by the laws, regulations and national standards.
受托方应按照法律的要求实施网络安全等级保护和数据安全制度，并按照法律、法规和国家标准的要求向公安机关进行评估或备案。

4. Correction, Deletion and Restriction of Data, Personal Data Subject Requests
更正、删除和限制数据，个人信息主体的请求

The Authorized Party may not on its own authority correct, delete or restrict the Data processed on behalf of NSC, but only on documented instructions from NSC. Insofar as a Personal Data Subject contacts the Authorized Party directly concerning a correction, deletion or restriction of Processing, the Authorized Party shall refer the request of the Personal Data Subject to NSC to the extent possible according to the information provided by the Personal Data Subject. The Authorized Party shall forward such request to NSC at the following e-mail address as [fiona.xu@bmw.com], without undue delay.

受托方不得自行更正、删除或限制其受宝马汽贸委托而处理的数据，而只能根据宝马汽贸提供的书面指示进行。如果个人信息主体就更正、删除或限制处理直接联系受托方，受托方应根据个人信息主体提供的信息，尽可能将个人信息主体的请求提交给宝马汽贸。受托方应将此类请求转发至以下电子邮件地址【fiona.xu@bmw.com】，不得无故延迟。

5. Other Responsibilities of the Authorized Party
受托方的其他职责

In addition to complying with the provisions of this Agreement and its obligations according to Applicable Laws, the Authorized Party has the following responsibilities:
除遵守本《协议》和法律规定的义务外，受托方还应承担以下义务：

- Written appointment - where stipulated by law - of a Cybersecurity Officer, a Data Security Officer and a Personal Information Protection Officer if required by laws. The Authorized Party will name the Cybersecurity Officer, the Data Security Officer and the Personal Information Protection Officer in each agreed **Annex**. Changes in the Cybersecurity Officer, the Data Security Officer and the Personal Information Protection Officer 's contact details shall be supplied to NSC.
  以书面形式任命法律规定的网络安全负责人、数据安全负责人和个人信息保护负责人。受托方将在每个拟定的**附件**中指定网络安全负责人、数据安全负责人和个人信息保护负责人。网络安全负责人、数据安全负责人和个人信息保护负责人联系方式的变更应告知宝马汽贸。
- The Authorized Party shall limit access to Data to its directors, officers or employees to whom the grant of access is absolutely necessary for the Authorized Party's performance of this Agreement. Without NSC's prior written consent, the Authorized Party shall not allow persons outside of the Authorized Party 's organization (including but not limited to agents, contractors and external counsel) to access Data, regardless of whether such persons are within the meaning of permitted sub-commissions in this Agreement.
  受托方应将访问数据的权限限于为履行本《协议》所必要的受托方的董事、高级管理人员或员工。未经宝马汽贸事先书面同意，受托方不得允许外部人员（包括但不限于代理、承包商和外部顾问）访问数据，无论该等外部人员是否符合本《协议》有关再委托的规定。
- The Authorized Party shall maintain confidentiality when Processing Data on behalf of NSC. The Authorized Party shall entrust only such employees with the Processing of Data who have been bound to confidentiality and shall take all reasonable steps (e.g. trainings and instructions) to ensure that any person entrusted with the fulfilment of this Agreement or who could otherwise have access to the Data complies with the obligations under Applicable Laws as well as the provisions under this Agreement, such as instructions and purpose limitation.
  对于受宝马汽贸委托处理的数据，受托方应予以保密。受托方应仅委托受保密义务约

束的员工处理数据，并应采取一切合理措施（如培训和指示）确保受委托履行本协议的任何人或以其他方式可以访问数据的任何人遵守法律规定以及本《协议》规定的义务，如指示和目的限制。

- The implementation and maintenance of all technical and organizational measures required for the respective order according to Applicable Laws in addition to the measures specified in **Annex TOM** to the Agreement.
  除**附件 TOM** 中规定的措施外，根据法律实施和维持各个订单所需的所有技术和制度措施。
- Immediate notification to NSC of any activities and measures caused or imposed by third parties on the Data, including but not limited to monitoring activities undertaken by a supervisory authority.
  立即向宝马汽贸报告第三方导致或施加的活动和措施，包括但不限于监管机构开展的监管活动。
- Monitoring and documentation by way of regular reviews of the performance and execution of the specific order by the Authorized Party (job control).
  受托方应定期审查其对具体订单的执行情况，并进行记录（作业控制）。
- Provision of evidence to NSC of the technical and organizational measures taken in addition to **Annex TOM**. For this purpose, the Authorized Party may present up-to-date attestations, reports or extracts thereof from independent bodies (e.g. external auditors, internal audit, the Cybersecurity Officer, the Data Protection Officer, the Personal Information Protection Officer, the IT security department or quality auditors) or suitable certification by way of an IT security or Data protection audit.
  向宝马汽贸提供在**附件 TOM** 额外采取的技术和制度措施的证据。为此，受托方可提供独立机构（如外部审计师、内部审计、网络安全负责人、数据安全负责人、个人信息保护负责人、IT 安全部门或质量审计师）的最新证明、报告或摘录，或 IT 安全或数据保护审计的相应证明。
- Provision of reasonable assistance to NSC in fulfilling its accountability and documentation obligations.
  为宝马汽贸履行其责任和文件记录义务提供合理协助。
- Provision of assistance by appropriate technical and organizational measures to NSC in fulfilling its obligation to respond to requests for exercising the Personal Data Subject's rights under Applicable Laws.
  通过适当的技术和制度措施向宝马汽贸提供协助，以协助宝马汽贸履行法律规定的响应个人信息主体请求的义务。
- Provision of assistance to NSC in ensuring compliance with the obligations under Applicable Laws, taking into account the nature of Processing and the information available to the Authorized Party
  根据处理的性质和受托方可获得的信息，协助宝马汽贸履行适用法律规定的合规义务。

6. Sub-commissions
再委托

The commissioning of sub-contractors requires the prior specific written authorisation of NSC(see **Annex 1** for specific). Where NSC grants such sub-commission, the Authorized Party shall set out the contractual agreements with the sub-contractor(s), in writing or electronically, in such a way that they reflect the Data protection provisions agreed upon between NSC and the Authorized Party, including but not limited to technical and organizational security measures. Where a sub-contractor is involved, the agreement between the Authorized Party and the sub-contractor shall confer to NSC the right to monitor and control the sub-contractor in accordance with this Agreement and as required under the Applicable Laws. The commissioning and the passing on of the Data by the Authorized Party to the sub-contractor is only permitted provided that all requirements for sub-commission have been met.
再委托需要宝马汽贸的事先书面授权（具体要求见**附件 1**）。如果宝马汽贸授权再委托，则受托方应以书面或电子方式与次受托人订立协议，并确保其中包含宝马汽贸与受托方之间商定的数据保护条款，包括但不限于技术和组织架构安排措施。如果涉及再委托，则应根据本协议和法律的要求，受托方和次受托人之间的协议应当授予宝马汽贸监督和控制次受托人的权利。只有在次受托人满足所有再委托要求的情况下，受托方才可将数据委托和提供给次受托人。

Upon request, the Authorized Party shall provide NSC with information on the substance of the Agreement and the implementation of the Data protection obligations within the sub-contract relationship, where necessary by inspecting the relevant contract documents. Authorized Party is entitled to redact such parts of relevant contract documents which are irrelevant for the control purposes of this Agreement (e.g. financial conditions).
根据要求，受托方应通过检查相关合同文件，向宝马汽贸提供有关《协议》实质内容的信息以及再委托合同关系中数据保护义务履行情况的信息。受托方有权编辑与本《协议》处理目的无关的部分（如财务状况）。

Sub-commissions referred to in this provision do not include ancillary services ordered by the Authorized Party from third parties to assist in the performance of the commission, provided that such ancillary services do not in any way allow or grant access to third parties to any Data. These may be e.g. telecommunications services, maintenance and user support, cleaning, auditing or the disposal of data media. However, sub-commissions of document/data media disposal must be announced to NSC if the core activity of the commissioned Processing involves the disposal of documents/data media. To safeguard the protection and security of the NSC's Data, even where ancillary services are taken from third parties, the Authorized Party shall nevertheless conclude adequate and lawful contractual agreements and undertake monitoring activities.
本条款中提及的再委托不包括受托方为协助履行委托义务而从第三方采购的辅助服务，前提是该等辅助服务中第三方不应有权以任何形式访问宝马汽贸的数据，例如电信服务、用户维护和用户支持，数据媒介的清洗、审计、清除。但是，如果委托处理的核心活动涉及

文件/数据媒介的处理，则处理该等文件/数据媒介必须向宝马汽贸通知。为保障宝马汽贸的数据安全，即使从第三方采购辅助服务，受托方仍应签订充分、合法的协议，并进行审查。

7. Accountability of the Authorized Party, Monitoring Rights of NSC
受托方的义务，宝马汽贸的检查权

The Authorized Party undertakes to give NSC upon request in a timely manner such information as is required to meet the NSC's control obligation relating to the Processing of Data, and make the necessary documentation available.
受托方承诺根据要求及时向宝马汽贸提供满足宝马汽贸与数据处理相关的控制义务所需的信息，并提供必要的文件。

The NSC or a third party mandated by the NSC ("Mandated Auditor") may carry out audits including inspections on the Authorized Party's business premises before the start of the Processing and in regular intervals thereafter in order to verify compliance of the technical and organizational measures implemented by the Authorized Party. The regular audits, including inspections, are agreed as follows:
宝马汽贸或宝马汽贸授权的第三方（"授权审计师"）可在开始处理之前和开始处理之后定期对受托方的营业场所进行审计（包括检查），以验证受托方实施的技术和制度措施的合规性。定期审计（包括检查）协议如下：

- The frequency of audits, including inspections, is based on the particularities of the specific order. Audits, including inspections, shall generally not take place more than once a calendar year, unless NSC is of the opinion that the Authorized Party or one of its sub-contractors is in breach of this Agreement or of Applicable Laws, or otherwise required by Applicable Laws.
  审计（包括检查）频率取决于具体指令的特殊性。定期进行的审计（包括检查），每年不得超过一次，除非宝马汽贸认为受托方或次受托人违反本《协议》或法律规定，或法律另有要求。
- For this purpose, the Authorized Party shall, upon request, provide NSC with evidence of the implementation of the technical and organizational measures pursuant to this Agreement and Applicable Laws.
  为此，受托方应根据要求向宝马汽贸提供根据本《协议》和法律规定实施技术和制度措施的证据。
- In case of on-site inspections carried out by NSC or by a Mandated Auditor, such audits or inspections are undertaken during the Authorized Party's regular business hours causing minimal disruption to the Authorized Party's business, which are ordinarily to be announced at least 2 (two) weeks in advance. If the Authorized Party violates its contractual obligations under this Agreement, or violates Applicable Laws, or if any law stipulates a shorter time period, the pre-notification time is

reduced to 24 (twenty four) hours. The Authorized Party undertakes to assist NSC in the execution of the inspections in the best possible way.
如果由宝马汽贸或其授权的审计人员进行现场检查，则此类审计或检查应在受托方的正常营业时间内进行，通常应至少提前 2（两）周通知，以对受托方的业务造成最小干扰。如果受托方违反其在本《协议》项下的合同义务，或违反所适用的法律，或违反任何法律规定的更短的期限，则提前通知的时间将缩短为 24（二十四）小时。受托方承诺以最佳方式协助宝马汽贸执行检查。

There will be no reimbursement of expenses by NSC which incurred to the Authorized Party due to the control visits to verify compliance to the agreed level of Data protection. NSC shall bear the costs of the Mandated Auditor unless such audit or inspection is the result of a Data protection incident for which the Authorized Party is responsible.
宝马汽贸不会对受托方为验证是否符合约定的数据保护水平而进行访问控制所产生的费用进行补偿。宝马汽贸应承担其授权的审计人员的费用，除非此类审计或检查是由可归责于受托方的数据安全事件造成的。

8. Notification of Infringements by the Authorized Party
受托方的侵权通知

The Authorized Party and NSC shall immediately notify each other where errors, irregularities or suspected infringements of provisions relating to the protection of Data occur. The parties agree to take all reasonable measures in order to remedy eventual infringements immediately.
如果出现错误、违规或涉嫌违反与数据保护相关的规定，受托方和宝马汽贸应立即通知对方。双方同意采取一切合理措施，以便立即补救侵权行为。

The Authorized Party shall notify NSC in all cases where the Authorized Party or persons employed by Authorized Party infringe provisions relating to the protection of Data belonging to the NSC or any other stipulations set out in the Agreement.
如果受托方或其雇佣的人员违反了与保护宝马汽贸数据有关的规定或本协议规定的任何其他规定，则受托方应通知宝马汽贸。

After the Authorized Party becoming aware of a Data Breach, the Authorized Party shall therefore notify NSC immediately, in any event within a maximum time frame of 48 (forty-eight) hours or any statutory time limit prescribed by Applicable Laws on NSC to notify a Data Breach, whichever is shorter, regardless of the origin of the Data Breach. In the event of necessary notification, the Authorized Party shall also provide NSC with the information including the nature of the Data Breach, the categories and approximate numbers of Data Subjects concerned, the categories and approximate numbers of Data records concerned, the name and contact details of Authorized Party's Cybersecurity Officer, Data Security Officer or Personal Information Protection Officer, from whom

more information may be obtained, the estimated risk and the likely consequences of the Data Breach, and any other information NSC may reasonably request relating to the Data Breach as necessary for NSC to fulfil its obligations under Applicable Laws to notify the authorities and Data Subjects, provided that this information does not belong solely to the area of responsibility of NSC. This notification obligations also apply to serious operational faults or where there is any suspicion of an infringement of provisions relating to the protection of Data or other irregularities in the handling of Data belonging to NSC. Upon consultation of NSC, the Authorized Party shall take appropriate measures to secure the Data and limit any possible detrimental effect on the Personal Data Subjects. Where obligations are imposed on NSC for report or notify the competent government authorities or Personal Data Subjects under the Applicable Laws, the Authorized Party shall assist in meeting them.
在任何情况下，无论数据因何种原因泄露，受托方意识到数据泄露后，应在不得超过 48（四十八）小时，或者法律要求的宝马汽贸报告数据泄露事件的适用法定期限内(以较短者为准)，立即通知宝马汽贸。在必要通知的情况下，受托方应向宝马汽贸提供数据泄露的性质、相关数据主体的类别和大致数量、相关数据记录的类别和大致数量，受托方的网络安全负责人、数据安全负责人或个人信息保护负责人的姓名和联系方式（以从该等人士处获得更多信息）、预估的风险以及数据泄露的可能后果，任何其他宝马汽贸合理要求的与数据泄露相关的信息，以使宝马汽贸履行法律规定的通知监管机关和数据主体的义务，前提是该信息不是完全属于宝马汽贸的责任范围。此通知义务也适用于严重的操作事故，或在处理属于宝马汽贸的数据时，疑似存在违反数据保护规定或其他违规行为的情况。经与宝马汽贸协商，受托方应采取适当措施保护数据，并限制对个人信息主体可能产生的任何不利影响。如果宝马汽贸有义务根据法律报告或通知监管机关或个人信息主体，则受托方应协助宝马汽贸履行该等义务。

9. Authority of NSC to Issue Instructions
宝马汽贸的指示权

The Authorized Party is at all times bound by the NSC's instructions relating to the execution of the Agreement and the Processing of Data belonging to NSC. NSC retains a general right of instruction as to the nature, scope and method of Data Processing, which may be supplemented with individual instructions. The Authorized Party shall Process Data solely pursuant to the processing scope and method instructed by NSC.
受托方始终受限于宝马汽贸有关本《协议》执行和处理宝马汽贸的数据的相关指示。宝马汽贸保留关于数据处理的性质、范围和方式的一般指示权，也可通过单独的指示进行补充。受托方应当完全按照宝马汽贸指示的处理范围和方法处理数据。

The Authorized Party may only pass on information including Data of NSC to third parties or to Personal Data Subject with the prior written consent of NSC.
受托方只能在获得宝马汽贸事先书面同意的情况下，将包括宝马汽贸数据在内的信息提供给第三方或个人信息主体。

The Authorized Party must not use the Data for any other purpose than the execution of the specific order and is particularly forbidden to disclose the Data to third parties. If the Authorized Party is legally obligated to disclose any Data, the Authorized Party will immediately inform NSC, unless that law prohibits such information on important grounds of public interest.
受托方不得将数据用于执行特定订单以外的任何其他目的，尤其禁止向第三方披露数据。如果法律要求受托方披露任何数据，受托方将立即通知宝马汽贸，除非法律出于公共利益等重大理由禁止此类通知。

No copies or duplicates of Data may be produced without the knowledge of NSC. This does not apply to backup copies, to the readout of log files etc. where these are required to assure proper Data Processing and the execution of the specific order under the condition that the content of the Data remains unchanged and the Processing does not interfere with NSC's interests.
在宝马汽贸不知情的情况下，不得制作任何数据的副本。本条规定不适用于备份副本、日志文件的读取等。在数据内容保持不变且处理不会干扰宝马汽贸利益的情况下，需要这些副本确保正确的数据处理和特定订单的执行。

The Authorized Party shall inform NSC immediately and prior to any Processing if the Authorized Party believes that an instruction of NSC constitutes an infringement of legal Data protection provisions, provided that such notification by the Authorized Party is accompanied by an explanation of the legal grounds of the Authorized Party's suspicion of infringement. The Authorized Party may then postpone the execution of the relevant instruction until it is confirmed or changed by NSC.
如果受托方认为宝马汽贸的指示违反法律要求的数据保护条款，受托方应在遵照指示进行处理之前立即通知宝马汽贸，且该等通知应当包括受托方怀疑的相关指示违法的法律依据。此后，受托方可以推迟相关指示的执行，直到宝马汽贸确认或更改相关指示。

10. Deletion of Data and Return of Data Media
删除数据并返还数据媒介

Upon (i) the expiration, termination or rescission of this Agreement, or (ii) completion of the contractual work or (iii) when requested by NSC, the Authorized Party shall return to NSC all Data of the Authorized Party, documents in its possession and all work products and Data produced in connection with the Agreement, or delete them in compliance with Applicable Laws with the prior consent of NSC. At the request of NSC, the Authorized Party shall provide the deletion log.
在本《协议》(i) 到期、终止或废除，(ii)规定的工作完成后，或(iii)当宝马汽贸要求时，受托方应将宝马汽贸的所有数据、其拥有的文件以及与本《协议》相关的所有工作成果和数据返还给宝马汽贸，或在征得宝马汽贸事先同意的情况下，根据法律将其删除。应宝马汽

贸的要求，受托方应提供删除日志。

Documentation intended as proof of proper Data Processing shall be kept by the Authorized Party beyond the end of the Agreement in accordance with relevant retention periods. The Authorized Party shall, upon request of NSC, hand such documentation over to the Authorized Party after expiry of the Agreement.
在协议到期后，受托方应按照相关的保留期限保存旨在证明数据处理符合协议约定的证明。受托方应根据宝马汽贸的要求，在本《协议》到期后将此类文件移交给宝马汽贸。

11. Liability
责任

The parties are liable for damages that the Personal Data Subject may suffer as a result of an illegal or incorrect Processing or use of Data in the course of the execution of the Agreement, constituting an infringement of the provisions set out in the Applicable Laws. Further legal claims shall remain unaffected.
双方在执行本协议过程中非法或不当处理或使用数据，违反法律规定的，双方应承担个人信息主体可能提起的损害赔偿责任，且不影响双方进一步的法律索赔。

The parties shall reasonably assist each other in a defense against unjustified claims.
双方应合理协助对方对不正当索赔进行抗辩。

Where NSC is liable to a Personal Data Subject as a result of the Authorized Party's breach of this Agreement, the Authorized Party shall defend NSC at the Authorized Party's cost (provided that NSC shall be given control over the Authorized Party's actions in any such legal proceedings) and shall indemnify and hold NSC harmless of all losses, damages, liabilities, claims, costs and expenses (including, but not limited to, court costs, reasonable attorneys' fees and litigation expenses) arising from the Authorized Party's breach of this Agreement.
如果宝马汽贸因受托方违反本《协议》而对个人信息主体承担责任，受托方应以其费用为宝马汽贸进行抗辩（前提是在任何此类法律程序中，宝马汽贸对受托方的行为有控制权），并应赔偿宝马汽贸，使其免受所有因受托方违反本《协议》造成的损失、损害、责任、索赔、成本和费用（包括但不限于合理的律师费和诉讼费用）。

12. Final Provisions
最终协议

With conclusion of this Agreement all existing (framework) agreements regarding a commissioned Processing of Data shall be replaced. Subject matter and description of an individual service commissioned (see examples set out in **Annexes** for details) shall remain unaffected for the term of the respective service.

签订本协议后，应替换所有关于委托处理数据的现有（框架）协议。委托服务的目的和描述（详见**附件**中的示例）在各自服务期限内不受影响。

All changes to the Agreement shall be in written form.
本协议的所有变更均应以书面形式进行。

If any provision of the Agreement is held to be or become invalid or incomplete as a whole or in parts, the validity and enforceability of the remaining provisions will not in any way be affected or impaired. In such an event the parties undertake to mutually replace such provision with a valid provision which best serves the economic purpose and the will of the parties.
如果本《协议》的任何条款整体或部分被认定为无效或不完整，则剩余条款的有效性和可执行性将不会以任何方式受到影响或损害。在这种情况下，双方承诺以最符合双方经济目的和意愿的有效条款替换该条款。

The Authorized Party appoints the following contact person for the performance of the Agreement:
受托方任命以下联系人负责本《协议》的履行：

[仲岚，总监
Lan Zhong, Account director]

Any changes concerning the person or the responsibility of these contact persons shall immediately be notified to the other party.
有关联系人或联系人责任的任何变更应立即通知另一方。

This Agreement and any dispute or claim arising out of or in connection with or is subject to this Agreement shall be governed by the laws of the People's Republic of China. Jurisdiction for disputes deriving from the Agreement or related to the execution of the Agreement is the people's court in the place where NSC domiciles.
本《协议》以及由本《协议》引起的、与本《协议》有关的或受本《协议》约束的任何争议或索赔均受中华人民共和国法律管辖。因本《协议》产生的或与执行本《协议》有关的争议，由宝马汽贸住所地的人民法院管辖。

Annex 1, and Annex TOM constitute a part of the Agreement.
附件 1 和**附件《技术和制度措施》**构成本《协议》的一部分。

NSC
宝马汽贸

Signature:
签字:

[Li Yao, Head of Data Governance, date]
[李尧，数据治理总监，时间]

Signature:
签字:

[Tonya Tan, Vice President Sales, BMW China Automotive Trading Ltd., date]
[谭莹莹，销售副总裁，宝马（中国）汽车贸易有限公司，时间]

Optional Signature:
可选签字:

[Yan Liang, Senior Manager of BMW Luxury Class, date]
[梁岩，BMW 大型豪华车高级经理，时间]

Authorized Party
受托方

Signature:
签字:

[Jingjing Qian, Deputy General Manager, date]
[钱晶晶，常务副总经理，时间]

Signature:
签字:

[Lan Zhong, Account Director, date]
[仲岚，总监，时间]

Annex 1 (Processing and Transmission of Personal Data)
附件 1 (个人信息的处理和传输)

Authorized Party 受托方:	[COMFORT INTERNATIONAL M.I.C.E. SERVICE CO., LTD. 康辉集团北京国际会议展览有限公司]
BMW Supplier number of the Authorized Party 受托方宝马汽贸供应商号码:	[4063697]
Assignment 工作任务:	[To arrange trip itineraries for the clients. 为客户规划行程。]
Date of assignment 工作任务日期:	[6/5/2024]
Date of Data Processing Agreement 数据处理协议签署日期:	[5/28/2024]

Where stipulated by law the Authorized Party has appointed [Lan Zhong, zhonglan@cct.cn] as Personal Information Protection Officer. Any change in the Personal Information Protection Officer's contact details shall be supplied to the NSC.
Referring to the Purchase Contract and to the framework Data Processing Agreement listed upon, the parties agree on [the following service related to and/or including the Processing of Personal Data to be provided by the Authorized Party.
根据法律，受托方任命[仲岚, zhonglan@cct.cn]作为个人信息保护负责人。个人信息保护负责人的联系方式的任何变更应向宝马汽贸提供。
根据采购合同以及以上数据处理协议，各方同意受托方会提供相关的服务及/或包含个人信息处理。

1. Subject-matter and duration of the service
主题和服务期间

The subject-matter of the service is the performance of the following tasks by the Authorized Party 主题为受托方提供以下服务，

[1. Contact and communicate with ~250 clients to confirm participation;
2. Arrange VIP tours to Universal Studios Beijing for ~250 groups of clients;
3. Timely respond to clients' requests/questions/needs/concerns before, during and after the trip;
4. Collect and evaluate customer satisfaction.
1. 联系并确认~250 名客户是否参与；
2. 为~250 名客户规划并安排北京环球影城 VIP 之旅的行程；

3. 及时回应并解决客户在行程前、中、后期的需求和问题；
4. 收集客户满意度]

The duration of this Agreement is agreed as follows 协议的期间为以下: [starting on 6/5/2024, and automatically expired at the expiration of the Purchase Contract or when the tasks are fully executed. 开始于 2024 年 6 月 5 日，在采购合同或当任务完全履行完后自动到期].

2. Details of the substance of the service
具体服务实质细节

Scope, nature and purpose of the proposed Collection, Processing and/or use of Personal Data
范围、性质及收集、处理及/或是应用个人信息的目的

[Name and phone number will be processed for the authorized party to contact and communicate with the clients.
客户的姓名和电话将会被提供，受托方将根据以上信息联系客户。].

Personal Data shall be processed and used exclusively within the territory of China. Any transfer of Personal Data to a third country requires the prior written consent of NSC and is subject to compliance with the special requirements set out in Applicable Laws.
NSC will provide the Authorized Party with the following Personal Data related to the Personal Data Subjects.
个人信息应仅在中国领域处理和使用。任何向第三方国家传输的个人信息需要宝马汽贸的事先书面同意，且受制于适用法律的特别规定。
宝马汽贸应向受托方提供跟数据主体有关的以下个人信息。

A. **Categories of customer data not collected from vehicles:** [note: depending upon the actual situation of Data Processing, please delete the sub-category if the "personal basic information and identity information" of a customer is not involved.] [注：根据数据处理的实际情况，如果不涉及客户的"个人基本信息和身份信息"，请删除子类别。]
不从车机收集的客户数据：

☒ Basic information of a customer (e.g. name, date of birth, gender, ethnic, nationality, family relations, telephone, email)
☒客户的基本信息（例如姓名、出生日期、性别、民族、国籍、家庭关系、电话、电子邮件）

☐ Identity information of a customer (e.g. identification card, certificate of military officer, passport, driving license, social security card, work and residence permit)
☐客户身份信息（例如身份证、军官证、护照、驾驶证、社会保障卡、工作证和居住证）

Behavior: it is helpful to give insight into a customer's daily transactions and patterns. It contains:
行为：有利于深入了解客户的日常交易模式，包括：

☐ Customer transaction data (e.g. sales history, payments, refunds, premiums, indemnities)

☐ 客户交易数据（例如销售历史、付款、退款、保费、赔偿）

☐ Customer interaction data (e.g. user behavior (website visits, click tracking, call records), response data (to surveys), complaints, feedback)

☐ 客户互动数据（例如用户行为（网站访问、点击跟踪、通话记录）、回复数据（调查）、投诉、反馈）

☐ Location data (e.g. position data (GPS), movement profiles)

☐ 位置数据（例如位置数据（GPS）、行动侧写）

☐ Financial data (e.g. income, expenses, credit rating)

☐ 财务数据（例如收入、支出、信用评级）

☐ Others: [Please complement]

☐ 其他：[请补充]

Identifier: it helps to distinctly identify a customer in different data sets. It contains:

标识：有利于在不同的数据集中清楚地识别客户，包括：

☒ Contact data (e.g. name, address, tel. number, email)

☒ 联系方式（例如姓名、地址、电话号码、电子邮件）

☐ Contract data (e.g. customer ID, services)

☐ 合同数据（例如客户 ID、服务）

☐ Account data (e.g. bank details, tax identification number, social media accounts, VIN, vehicle plate)

☐ 账户数据（例如银行详细信息、税务识别号、社交媒体账户、VIN、车牌）

☐ Others: [Please complement]

☐ 其他：[请补充]

Personality: it helps to give insight into a person's character traits. It contains:

个性数据：有利于观察个人性格特征，包括：

☐ Lifestyle (customer's interests, taste, hobbies and preferences)

☐ 生活方式（客户的兴趣、品味、爱好和偏好）

☐ Criminal offenses (e.g. criminal actions, administrative offenses data)

☐ 刑事犯罪（例如刑事诉讼、行政违法数据）

☐ Others: [Please complement]

☐其他：[请补充]

Socio-demographics statistics: it describes a customer's background and contains:

社会人口统计：描述客户的背景，包括：

☐ Biological data (e.g. health information)

☐ 生物数据（如健康信息）

☐ Resume data (e.g. education, profession)

☐ 简历数据（例如教育、职业）

☐ Others: [Please complement]

☐ 其他：[请补充]

Categories of Sensitive Personal Data

敏感个人信息的类别

☐ **Personal property information:** bank account, authentication information (password), deposit information (including amount of deposit, payment and receipt record), real estate information, credit history, personal credit information, transaction and consumption record, account statement record, as well as virtual property information such as virtual currency, virtual transaction, game-based redeem code, etc.

☐**个人财产信息：**银行账户、认证信息（密码）、存款信息（包括存款金额、付款和收款记录）、房地产信息、信用历史记录、个人信用信息、交易和消费记录、账户对账单记录，以及虚拟货币、虚拟交易、基于游戏的兑换代码等虚拟财产信息。

☐ **Personal biometric information:** personal gene, fingerprint, voiceprint, palmprint, auricle, iris, facial recognition features, etc.

☐**个人生物特征信息：**个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等。

☐ **Personal identity information:** identification card, certificate of military officer, passport, driving license, work permit, social security card, residence permit, etc.

☐ **个人身份信息：**身份证、军官证、护照、驾驶证、工作证、社会保障卡、居留证等。

☐ Others: sexual orientation, marital history, religion, undisclosed record of criminal offenses, correspondence and content, contact list, list of good friends, list of groups, whereabouts track record, webpage browsing record, lodging information, precise geo-positioning information, etc.

☐其他：性取向、婚姻史、宗教、未披露的犯罪记录、通信和内容、联系人列表、好友列表、群组列表、行踪记录、网页浏览记录、住宿信息、精确定位信息等。

Personal Data Subject

个人信息主体

☐ Applicants.

☐ 应聘者。

☐ Children under 14.

☐ 14 周岁以下儿童。

☐ Children under 16.

☐ 16 周岁以下儿童。

☒ Customers (including leads or prospects).

☒ 客户（包括潜在客户）。

☐ Employees.

☐ 员工。

☐ Employees of business partners (e.g. authorized dealers, IT provider, Corporate Customer, etc.).

☐ 业务合作伙伴（如授权经销商、IT 供应商、公司客户等）的员工。

☐ Others: [Please complement]
☐ 其他：[请补充]

3. Specific technical and organizational measures as an amendment to Annex TOM to the Data Processing Agreement
作为《数据处理协议》附件《技术和制度措施》修正案的具体技术和制度措施

☒ No specific technical and organizational measures.
☒没有具体的技术和制度措施。
☐ Following specific technical and organizational measures (please complement):
☐ 以下具体技术和制度措施（请补充）：
[Please complement company name and address. If it is necessary for the Processor to take additional security measures for this specific agreement which go be-yond the technical and organizational measures agreed in the frame contract, these measures should be listed here.]
[请补充公司名称和地址。如果受托方需要为特定协议采取额外的安全措施，这些措施将在框架合同中约定的技术和制度措施中列出。]

If an adequate level of data protection can be guaranteed by the Processor, the Controller grants permission for the employees appointed by the Processor to this contract for mobile work and remote access. If this cannot be guaranteed, the Processor must take other adequate measures.]
如果受托方能够保证充分的数据保护水平，则数据处理者将授权受托方根据本合同任命的员工流动工作和远程访问的许可。如果无法保证，受托方必须采取其他适当措施。]

☒ The Processing of Personal Data in private premises or in the context of tele working is permitted.
☒ 允许在私人场所或远程工作环境中处理个人信息。

4. Sub-commissions
再委托

The Controller grants its approval to the commissioning of the following sub-contractors pursuant to section 6 of the Data Processing Agreement. After signing of this Agreement, if the Processer commissions any sub-contractor without prior written consent of the Controller, the Processer shall assume the secure data liability caused by the sub-contractor to the Controller.
数据处理者根据《数据处理协议》第 6 节授权再委托。签署本协议后，如果受托方未经数据处理者事先书面同意，则受托方应承担次受托人对数据处理者造成的数据安全责任。在受托方再委托前，需要对本节进行修改。任何未在本节中列出的再委托应被视为受托方违反本《协议》，受托方应当对数据处理者由此承担的任何损害和赔偿责任负责。

☒ No sub-contractors
☒ 无次受托人
☐ Sub-contractors within China:
☐ 中国境内的次受托人：
[Please complement company name and address]
[请补充公司名称和地址]
☐ Sub-contractors outside of China:
☐ 中国境外的次受托人：
[Please complement company name and address]
[请补充公司名称和地址]

5. Monitoring rights of NSC
宝马汽贸的检查权

The regular control visits pursuant to section 7 of the Data Processing Agreement, notwithstanding NSC's right to unscheduled control visits in the case of e.g. suspected incidents or non-compliance with the technical or organizational measures, are agreed upon as follows: Before start of Data Processing and subsequently on a regular basis latest of three years.
根据《数据处理协议》第 7 节进行的定期控制访问，尽管宝马汽贸有权在疑似安全事件或（受托方或次受托人）未遵守技术或制度措施的情况下进行非计划控制访问，但协议如下：在数据开始处理之前，以及其后最迟三年定期进行。

6. Cross-border Transmission and Processing of Personal Data
个人信息的跨境传输和处理

Upon the request of NSC or as required by the Authorized Party, processing of any Data if involving transmission to a third country outside of China or allowing remote accessing by a third party outside of China, such data processing activities shall obtain NSC's written approval in advance, or if such request is originally from NSC, such request shall be documented in writing. Any additional costs if such transmission is not requested by NSC shall be borne by the Authorized Party if not included in the Purchasing Contract. The Authorized Party shall prepare relevant documents/go through required procedures or to assist NSC in doing so as required under the Applicable Laws for cross-border data transmission.
如应宝马汽贸要求或受托方需要，数据的处理涉及到传输至中国以外或允许中国以外的第三方远程访问，该等数据处理行为应获得宝马汽贸的事先书面批准，如果该等数据处理行为来源于宝马汽贸的需求，应将该等需求书面记载。任何非由宝马汽贸需求带来的额外成本，如果没有在采购合同明确的情况下应由受托方承担。受托方应按照适用法律的要求准备相关文件/完成相应程序或协助宝马汽贸进行前述事项。

7. Contact person 联系人

The parties appoint the following contact persons for the execution of individual order:
各方任命下面的人作为具体订单的执行人

On behalf of the **NSC:** [Fiona Xu, C5-CN-9]
代表宝马汽贸：[徐静怡，C5-CN-9]

On behalf of the **Authorized Party:** [Lan Zhong, Account Director]
代表受托方：[仲岚，总监]

Any changes with regard to one of the persons mentioned or their responsibility shall immediately be communicated to the other party.
任何对以上人员的调整或者她/他们职责的调整应立刻通知另一方。

NSC
宝马汽贸

Signature:
签字:

[Li Yao, Head of Data Governance, date]
[李尧，数据治理总监，时间]

Signature:
签字:

[Tonya Tan, Vice President Sales, BMW China Automotive Trading Ltd., date]
[谭莹莹，销售副总裁，宝马（中国）汽车贸易有限公司，时间]

Optional Signature:
可选签字:

[Yan Liang, Senior Manager of BMW Luxury Class, date]
[梁岩，BMW 大型豪华车高级经理，时间]

Authorized Party
受托方

Signature:
签字:

[Jingjing Qian, Deputy General Manager, date]
[钱晶晶，常务副总经理，时间]

Signature:
签字:

[Lan Zhong, Account Director, date]
[仲岚，总监，时间]

Annex TOM
附件 TOM
Technical and Organizational Measures (TOM)
技术及制度措施

1. Measures
措施

This section describes measures that are taken to ensure that the internal organization meets the specific requirements of privacy protection.
本节描述确保组织内部满足隐私保护具体要求应采取的措施。

- A group wide process enforces a Personal Information impact assessment by the Data Privacy Protection Officer for every project or application that will process Personal Data. Personal Information impact assessment results should be stored for at least 3 (three) years.
  建立集团范围内的程序，确保由数据隐私保护负责人对每一个将处理个人数据的项目或应用进行个人信息安全影响评估，且该记录应保存至少三年。
- Special processing rules for processing personal information of minors under the age of 14.
  处理不满十四周岁未成年人个人信息的，制定专门的个人信息处理规则。
- A network of qualified data privacy protection officers that supports the intra-group Data Processing and ensures the conformity to Applicable Laws. (Defining and executing intra group data processing agreements).
  建立由适格的数据隐私保护负责人组成的网络，支持集团内部的数据处理并确保符合适用法律(界定和执行集团内部的数据处理协议)。
- A network of IT and information security officers that supports the IT Risk, Security, Compliance and Quality Management division.
  建立由IT和信息安全负责人组成的网络，为IT风险、安全、合规和质量管理部门提供支持。
- Audit management by IT, Internal Auditing and Public Accountant ensures the compliance with the policies, instructions, regulations and legal requirements by performing audits on a regular basis.
  由IT、内部审计部门以及外部会计师进行定期进行审计，确保遵守政策、指示、法律法规要求。
- Throughout the Authorized Party a consistent segregation of functions is obligatory.
  在受托方的集团范围内，确保职能分离的一致性。
- A central repository of policies, IT security guidelines, instructions, regulations and processes ensures a consistent regulatory base for all Authorized Party employees and is accessible to any employee.
  将政策、IT安全指南、指令、法规和流程文件集中存储，确保所有受托方员工适用一致的监管要求，并且任何员工均可访问。
- Separation of duties should be clearly assigned and documented.

明确界定、分配职责的分工，并以书面形式记录。

- All employees processing Personal Data are obligated when taking up their duties to maintain confidentiality. The obligation of confidentiality continues after their employment ends.
  所有处理个人数据的员工在就职时均有保密义务，并在其劳动关系结束后继续履行保密义务。
- All employees processing Personal Data have to take the Data protection training. Exam results and percentage of people trained are documented and reviewed regularly.
  所有处理个人数据的员工均必须参加数据保护培训。应当对考试结果和受训人员的百分比予以记录并定期审查。
- Executives and project managers assume responsibility for ensuring that their employees receive regular qualification training in information protection and Data privacy protection. Internal administrators are required to orient them-selves with the web-based training in Data privacy protection. Administrators from external companies must be instructed by their employers and must be familiar with Data privacy protection as well.
  管理人员及项目经理有责任确保员工定期接受信息安全和数据隐私保护方面的资格培训。内部管理员应参加数据隐私保护方面的网络培训。外部管理员必须遵循雇主的指示并具备数据隐私保护知识。
- Executives and project managers assume responsibility to incorporate the Data Processing Agreements in processing Personal Data if needed by Applicable Laws or internal regulations.
  (如适用法律或内部规定要求) 管理人员及项目经理有责任在处理个人数据时签订数据处理协议。
- The external Partner is [required / preferred] to have the ISO/IEC 27001 certification.
  外部合作伙伴【必须/建议】获得ISO/IEC 27001认证。

2. Measures for physical access control
物理访问控制措施

This section describes measures that are taken to prevent unauthorized persons from gaining access to Data Processing systems for Processing or using Personal Data.
本节描述为防止未授权人员进入数据处理系统处理或使用个人数据应采取的措施。

- Physical access to the company premises/buildings is controlled with badge readers and turnstiles. Security guards and gate keepers ensure access control remains operational, even if technical equipment or systems fail.
  公司场所/建筑的物理访问应设置入口检查装置（出入卡阅读器）。即使技术设备或系统出现故障，保安和门卫也会确保访问控制保持正常运行。
- Monitoring of break-in-attempts and automatic locking of user accounts upon several erroneous login attempts.

检测未经授权的访问尝试，并在多次错误的登录尝试后自动锁定用户账户。

- Video surveillance cameras and access system log files ensure the traceability in case of an unauthorized access.
  保存视频监控摄像文件和门禁系统日志文件，确保在发生未经授权访问时的可追溯性。
- Differentiated security zones are defined in a central system.
  在中央系统中划分不同的安全区。
- Access rights are controlled in a central system and are granted by a full-time responsible person based on the minimum principle and an expected validity interval. The responsible person is obliged to keep this information up to date.
  访问权限由中央系统控制，并由全职负责人根据最小原则和预期的有效间隔授予。该负责人有义务使上述信息保持最新状态。
- Special (color coded) identification badges are provided to visitors, invited guests and third-party employees.
  为来访者、被邀请的客人和第三方雇员提供特殊（颜色编码）的身份证件。
- The visitor's Personal Data is recorded in a software system and the retention of their personal identification is maintained at the reception area.
  访客的个人数据应记录在软件系统中，并在接待处保存他们的个人身份资料。
- All employees and visitors are required to visibly display their identification badges. Identification badges may not be given to another person.
  所有员工和访客都被要求主动地展示他们的身份识别证件。身份识别证件不得交由他人使用。
- In special security zones hosts are responsible for visitors and visitors must be accompanied at all times. Special security measures must also be implemented in areas where special protection is only needed "from time to time". The rules for employees include the following obligations to
  在特定的安全区域，由接待者对来访者负责并全程陪同。在特定时间段实行特别保护的区域也必须采取特殊安全措施。对雇员的规定应包括以下义务
  - Always advise the responsible member of staff if you are expecting visitors.
    在等待访客时，应告知负责的工作人员。
  - Not allow anyone without the necessary authority to follow close behind them through any doors.
    不允许未获得授权的人跟随在他们身后通过门禁。
  - Assure that objects requiring a high level of confidentiality, integrity or availability must be kept out of the way of visitors or unauthorized personnel.
    确保要求高度机密性、完整性或可用性的物品必须远离访客或未经授权的人员。
- In special security zones access is granted on a per person basis nobody else is allowed to enter. Employees may apply to their direct superiors or the person responsible for the zone, who grants access rights where justified. They are obliged to ensure that their authorization cannot be abused.
  在特定的安全区域，访问权按人次计算，其他未授权人员不得进入。雇员可以向他们的直接上级或该区域负责人提出申请，由他们在合理的情况下授予访问权。他们有义

务确保其授权不会被滥用。

- All users of mobile devices and teleworkers must take the necessary precautions to prevent potential theft:
  所有移动设备的使用者和远程工作人员必须采取必要的预防措施，以防止潜在的盗窃行为。
  - Notebooks must be secured by means of a cable lock or locked away in cabinets.
    笔记本必须用电缆锁固定或锁在柜子里。
  - On flights a mobile device must be carried in the hand luggage.
    乘坐飞机时，移动设备必须放在手提行李中。
  - In a vehicle it must be locked in the luggage compartment when one leaves the vehicle.
    乘坐汽车时，若离开车辆，必须将移动设备锁在行李箱中。
  - In hotels a mobile device must be locked away in a safe or cabinet, if possible, or secured using the cable lock.
    在酒店里，（如果可能的话）移动设备必须锁在保险箱或柜子里，或用电缆锁固定。
  - In public areas a mobile device must not be left unattended.
    在公共场所，移动设备不得无人看管。
  - The loss of a mobile device must be reported to the security headquarters or the investigation services without delay.
    移动设备的丢失必须立即报告给安全总部或调查部门。
  - Physical network connecting points in the Authorized Party's areas which are not located inside a protected area shall be protected from unauthorized access.
    受托方区域的物理网络连接点，（如不在保护区域内）应受到特别保护以防止未经授权的访问。

2.1 Measures for logical access control
逻辑访问控制措施

This section describes measures that are taken to prevent Data Processing systems from being used without authorization.
本节描述为防止数据处理系统被擅自使用应采取的措施。

- Authorized access to IT systems is guaranteed by an application. Access to all server resources is granted and withdrawn within the application.
  对IT系统的授权访问由应用程序控制。对所有服务器资源的访问权限均由该应用程序授予或撤销。
- Usage of anonymous IDs (i.e. root, administrator) is not permitted. Systems are configured in such a way that the privileges required for system administration can be assigned to particular roles or groups. Measures are implemented to detect unauthorized access attempts.

不允许使用匿名的ID（即超级用户，管理员）。配置系统时，应将系统管理所需的权限分配给特定的角色或组。采取措施检测未经授权的访问尝试。

- No shared usage of IDs is allowed. Personal user accounts must be only used by the owners themselves. It is for-bidden to use the personal user account of another person.
  不允许共享ID。个人用户账户必须仅由所有者本人使用，严禁使用他人的个人用户账户。
- An internal approval process for important operations (e.g. batch modification, copy and downloading) regarding Personal Data.
  对有关个人数据的重要操作（如批量修改、复制和下载）实行内部审批程序。
- One unique identification number / id per person is used.
  每个人使用一个唯一的识别号码/ID
- Access rights to IT resources are granted on the basis of roles following the minimum principle, an expected validity interval and must be kept up to date.
  IT资源的访问权限是基于角色授予的，遵循最小原则和预期的有效期间隔，并且必须保持最新状态。
  - Access rights (authorization) are withdrawn promptly when they are no longer needed.
    不再需要访问权限(授权)时应立即撤销。
  - Access rights to Sensitive Personal Data are granted only for a specific purpose and sufficient necessity.
    对敏感个人数据的访问权限只应在具有特定的目的和充分的必要性时授予。
  - External personnel are granted access rights only for a limited period (no longer than one year). These access rights are revoked automatically at the end of the limited period.
    外部人员只能获得有限期限(不超过一年)的访问权，并且该等访问权限将在有限期限结束时自动撤销。
  - Access rights are checked at least once a year.
    访问权限至少每年审查一次。
- A policy specifies the structure, expiry, assignment, and use of passwords. For example:
  通过政策规定密码的结构、期限、分配和使用。例如：
  - Password rules are technically enforced to assure minimum length and complexity. The password must be at least eight characters long. The technically feasible character set (letters, numbers, special characters) must be fully utilized.
    在技术上强制执行密码规则，以确保最小长度和复杂性。密码长度必须至少为8个字符，必须包含数字、字母、特殊字符。必须充分利用技术上可行的字符集(字母、数字、特殊字符)。
  - Passwords are changed at regular intervals and passwords that have already been used may not be used again immediately.

密码需定期更换，已经使用过的密码不得立即再次使用。

- Passwords must be kept secret. They may not be divulged to others. If there is any suspicion that pass-word input has been observed, a new password must be assigned without delay.
  密码必须保密，不得泄露给其他人。如果怀疑密码可能泄露，必须立即分配一个新的密码。
- User ID will be automatically locked in case of unsuccessful attempts to enter the correct password.
  在尝试输入密码失败的情形下，用户ID将被自动锁定。

- A general password resetting process is implemented and supported by an application. Information concerning past password resets is made available to the user.
  通过应用程序实现并支持密码重置过程。有关密码重置的历史应告知用户。
  - Passwords may only be changed by the owner himself. A password may only be reset by the user himself or by an authorized body.
    密码只能由所有者本人修改。密码只能由用户本人或授权机构重置。
  - Initial or reset passwords assigned by authorized central bodies shall be changed without delay.
    由授权中央机构分配的初始密码或重置密码应立即更改。
- PC or laptop screens must always be locked during periods of absence and laptops must be secured with security cables or locked inside cabinets. Mobile devices must use password-protected screen-lock mechanism if present, which is activated automatically after a few minutes of inactivity.
  个人电脑或笔记本电脑的屏幕在离开期间必须保持锁定，笔记本电脑必须用安全电缆固定或锁在柜子里。移动设备必须使用有密码保护的屏幕锁定机制（如有），该机制在设备闲置若干分钟后自动激活。
- Wireless communications are always encrypted. Notebooks are equipped with VPN clients, personal firewalls and hard disk encryption.
  无线通信应保持加密。笔记本电脑应配备VPN客户端、个人防火墙和硬盘加密。
- All data transferred over public networks is encrypted via Secure Sockets Layer (SSL) and HTTPS/Transport Layer Security (TLS).
  所有通过公共网络传输的数据都通过安全套接字层（SSL）和HTTPS/传输层安全协议（TLS）进行加密。
- Connecting external hardware to the Authorized Party's intranet is not allowed.
  不得将外部硬件连接到委托方的内部网络。
  - Externally commissioned security checks, such as penetration tests, may be executed as an exception to the rule above. In the course of such security checks, a partner connects external hardware to the Authorized Party's intranet for a previously agreed period. Notice of the security checks must be given to Operational Security.
    作为上述规则的例外，可委托第三方进行安全检查，如渗透测试。在安全检查过程中，第三方合作伙伴可将外部硬件连接到受托方的内网，并在事先约定的时间

内进行检查，但必须将安全检查的通知提交给运营安全部。

- Authentication information and strictly confidential information are encrypted for transmission and storage.
  应对认证信息和需严格保密的信息进行加密，以便传输和存储。
  - The standards approved by NSC must be used for encryption. The currently released hard disk encryption software is installed and activated on notebooks.
    加密必须使用经宝马汽贸批准的标准进行。应当在笔记本电脑上安装并激活最新版本的硬盘加密软件。
  - Finally Secure, MS Bitlocker, PGP or the recently released version of ZIP may be used for encryption.
    可使用Finally Secure, MS Bitlocker, PGP或最近发布的ZIP等软件进行加密。
  - If files are encrypted with a version of ZIP, the password must be communicated to the recipient by a different means (e.g. by telephone, text message). The password must not be sent by e-mail.
    如果文件是通过ZIP加密的，密码必须通过不同的方式（例如，通过电话、短信）发送给收件人。密码不得通过电子邮件发送。
  - Passwords will not be displayed by applications or systems while they are being entered and are stored in encrypted or hashed form by the application or system during use. This is ensured by providing a centralized standard authentication solution.
    通过提供集中式标准身份验证解决方案来确保密码在输入时不会由应用程序或系统显示，并在使用过程中由应用程序或系统以加密或散列的形式存储。可以通过提供集中的标准身份验证解决方案进进行。
- The systems and processes described are regularly reviewed and checked independently to verify the efficacy of the implemented measures.
  所述的系统和程序会被定期审查和独立检查，以验证所实施措施的有效性。
  Information objects with special protection and actual risk exposure are secured with two factor authentication. Criteria for actual risk exposure are for example:
  受特殊保护和具有实际暴露风险的信息应采用双因素身份验证进行保护。判断实际暴露风险的标准如下：
  - Incidents in the past resulting from fraudulent use of user IDs,
    过去因欺诈性使用用户ID而发生过事故。
  - Personal advantages for the potential initiator of the damage,
    潜在的攻击者具有有利条件。
  - Little knowhow needed in order to gain access to the information and subsequently put it on the market,
    可以轻易地获取信息并随后利用其获利。
  - Access from insecure locations.
    从不安全的地点进行访问。
- A policy, operational plans and procedures shall be implemented for tele working activities.

应实施针对远程工作活动的政策、操作计划和程序。

- All teleworkers use two factor authentication to access the corporate network.
  所有远程工作者应使用双因素身份验证访问公司网络。
- When using mobile devices to access the Authorized Party's intranet or public networks (Internet), the access protection standards must be applied. Existing mechanisms must not be deactivated in particular.
  当使用移动设备访问受托方的内部网络或公共网络（互联网）时，必须在现有保护机制的基础上适用访问保护标准。特别是不得使现有机制失效。
- Where mobile devices are examined by officials at state borders without presence of the user, they must be rein-stalled by IT Support before being connected to the Authorized Party's intranet again.
  如果移动设备在用户不在场的情况下被海关官员检查，它们必须由IT部门进行重安装后，方能再次连接到受托方的内部网络。

2.2 Measures for Data access control
数据访问控制措施

This section describes measures that are taken to ensure that persons authorized to use a data processing system, have access only to those Data they are authorized to access, and that Personal Data cannot be read, copied, altered or removed without authorization during Processing, use and after recording.
本节描述为确保被授权使用数据处理系统的人员仅访问其被授权访问的数据应采取的措施，以及确保在处理、使用和记录期间未经授权不能读取、复制、更改或删除个人数据。

- Authorized access to IT systems is guaranteed by an application.
  由应用程序确保对IT系统的授权访问。
- Documented permission management and history is mandatory for IT systems working with Personal Data.
  对于处理个人数据的IT系统，必须确保文件化的权限管理和历史记录。
- Separated permission approval and permission granting is mandatory for IT systems working with Personal Data.
  对于处理个人数据的IT系统，必须确保单独的许可审批和许可授予。
  - Access to information with protection needs will be approved by the designated manager or disciplinary superior. The approver must be in a position to determine whether access is needed or not.
    对有保护需求的信息的访问将由指定的经理或上级批准。审批者必须确定访问是否必要。
  - Access to information with special protection needs will be approved according to the "four-eye" principle. The approval must include verification of the need for access.
    对有特殊保护需求的信息的访问将根据＂四眼原则＂进行批准。审批必须包括对访问需求的核实。

- Access rights for IT resources are granted on the basis of roles following the "need to know" principles and an expected validity interval. They are kept up to date.
  IT资源的访问权限是基于角色授予的，遵循"需知原则"和预期的有效期间隔，并且必须保持最新状态。
  - Access rights (authorization) are withdrawn promptly when they are no longer needed.
    不再需要访问权限(授权)时应立即撤销。
  - External personnel are granted access rights only for a limited period (no longer than one year). These access rights are revoked automatically at the end of the limited period.
    外部人员只能获得有限期限(不超过一年)的访问权，并且该等访问权限将在有限期限结束时自动撤销。
  - Access rights are checked at least once a year.
    访问权限至少每年审查一次。
- Function separation (testing, deploy and production environment) is mandatory for program development.
  对于程序开发，必须执行强制性的功能分离（测试、部署和生产环境）。
- Administration tasks with high privilege levels are separated from other tasks by using different user IDs.
  使用不同的用户ID将高权限级别的管理任务与其他任务分开。
  - IT systems are administered by authorized personnel.
    IT系统由授权人员管理。
  - The number of administrators is restricted to an absolute minimum. Administrator access rights are granted within the framework of personal accounts.
    管理员的人数应限制在最低限度。管理员访问权限在个人帐户框架内授予。
- Data access options available to administrators are reduced to an absolute minimum, and such Data access is logged.
  管理员可用的数据访问权限应限制在最低限度，并记录此类数据访问。

2.3 Measures for disclosure control
披露控制措施

This section describes measures that are taken to ensure that Personal Data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred Personal Data using data transmission facilities.
本节描述为确保个人数据在电子传输或运输过程中，或在被记录到数据存储介质上时，不能未经授权读取、复制、更改或删除，并确定和检查哪些机构将使用数据传输设施传输个人数据应采取的措施。

- Wireless communications are always be encrypted.
  无线通信应保持加密。

- Encryption in accordance with the current standard of NSC is used for all wireless networks without exception.
  所有无线网络均使用符合宝马汽贸标准的加密技术。

- Appropriate methods are taken to de-identify Personal Data (as far as possible) in the event of disclosure.
  在披露个人数据时，（尽可能的）采取适当的方法进行去标识化。
- Authentication information and strictly confidential information is encrypted for transmission and storage.
  应对认证信息和需严格保密的信息进行加密，以便传输和存储。
  - The standards approved by NSC must be used for encryption. The currently released hard disk encryption software must be installed and activated on notebooks.
    加密必须使用宝马汽贸批准的标准进行。应当在笔记本电脑上安装并激活当前发布的硬盘加密软件。
  - Finally Secure, MS Bitlocker, PGP or the recently released version of ZIP may be used for encryption.
    使用Finally Secure, MS Bitlocker, PGP或最近发布的ZIP等软件进行加密。
  - If files are encrypted with a version of ZIP, the password must be communicated to the recipient by a different means (e.g. by telephone, text message). The password must not be sent by e-mail.
    如果文件是通过ZIP加密的，密码必须通过不同的方式（例如，通过电话、短信）发送给收件人。密码不得通过电子邮件发送。
- Appropriate erasure methods must be taken to ensure that data (and its copy) is irreversibly deleted or destroyed.
  必须采取适当的删除方法，确保数据（及其副本）被不可逆转地删除或销毁。
- When decommissioning an IT system, the local programs and Data are erased in an appropriate manner. This includes a secure deletion and destruction of storage media.
  当IT系统停止使用时，以适当的方式删除本地程序和数据，包括安全删除和销毁存储介质。
  - If the information on a data medium cannot be deleted for technical reasons, other appropriate measures must be taken to ensure that confidential information / Personal Data and the data media on which it is stored are properly destroyed.
    如果由于技术原因不能删除数据介质上的信息，则必须采取其他适当的措施，以确保保密信息/个人数据和存储它的数据介质被适当销毁。
- Authorization for the Data transfer/transport is granted following the need-to-know principle.
  数据传输的授权按照“需知原则”进行。
- The security mechanisms offered by portable devices must always be used. This includes encryption of laptops and mobile storage devices like USB sticks.
  必须始终使用便携式设备提供的安全机制，包括对笔记本电脑和U盘等移动存储设备

进行加密。

- Mobile data media must always be locked away when the user is absent.
  当用户不在场时，移动数据介质必须始终被锁起来。
- Any Data that is no longer required must be deleted from the data medium before leaving the premises.
  任何不再需要的数据必须在离开办公场所前从数据介质中删除。
- When being moved to new premises, mobile data media containing information with a special protection need must be kept in secure containers (e.g. lockable security boxes).
  当被转移到新的办公场所时，涉及需特别保护信息的移动数据介质必须保存在安全的容器中（例如，可上锁的安全盒）。
- When a mobile data carrier or mobile device has been used at a potentially risky location and there are plans to use it again, the data carrier must be erased reliably and the mobile device must be reinstalled.
  当移动数据载体或移动设备已在潜在风险地点使用，并计划再次使用时，必须可靠地擦除数据载体并重新安装移动设备。
- Mobile data carriers may only be used for company purposes if they have been procured by the Authorized Party.
  移动数据载体只能用于公司的目的，如果该等载体是由受托方采购。

- Communication with mobile users and remote premises uses VPN technology.
  与移动用户和远程场所的通信应使用VPN技术。
  - Transparent connections between potentially risky locations and the Authorized Party's network are not permitted.
    不允许在潜在风险地点和受托方的网络之间进行透明连接。
  - Secure access (personal firewall, VPN etc.) with advanced access facilities may be granted to selected employees by central departments.
    具有高级访问控制功能的安全设施（个人防火墙、VPN等）可由中央系统授予选定的员工。
  - Each secure access facility is assigned to a designated person and the number of such employees must be kept to an absolute minimum.
    每个安全访问设施都分配给一名指定人员，这类员工的数量必须保持在最低限度。
- Confidential and sensitive documents (including Personal Data) have to be destroyed securely on the spot, if they are no longer needed.
  保密和敏感文件（包括个人数据）如果不再需要，必须当场安全地销毁。
  - If systems are taken off the premises for repair, all of the data media in the system is removed before-hand or all information concerning the company is reliably deleted.
    如果系统被带离现场进行维修，应当事先移除系统中的所有数据介质，或者可靠地删除有关公司的所有信息。
  - Shredding machine is available for destroying sensitive and confidential documents.
    碎纸机可用于销毁敏感和保密文件。

- Fire safe and lockable cabinet is available for confidential / legal documents.
  防火保险箱可用于存放保密/法律文件。

- The exchange of Data via connections with cooperative and equity joint ventures is explicitly approved by the responsible executive and where ever applicable from the data privacy department as well.
  在与合作企业或合资企业交换数据时，应由负责的高级管理人员明确批准，（在适用的情况下）应由数据隐私部门批准。

2.4 Measures for input control
输入控制措施

This section describes measures that are taken to ensure that it is possible after the fact to check and ascertain whether Personal Data have been entered into, altered or removed from Data Processing systems and if so, by whom.
本节描述为确保能够在事后检查和确定个人数据是否被(以及被何者)输入、更改或从数据处理系统中删除应采取的措施。

- Authorized access to IT systems is guaranteed by an application.
  由应用程序确保对IT系统的授权访问。
- Documented permission management and history is mandatory for IT systems working with Personal Data.
  对于处理个人数据的IT系统，必须确保文件化的权限管理和历史记录。
- Access rights for IT resources are granted on the basis of roles following the need-to-know principle and an expected validity interval and must be kept up to date.
  IT资源的访问权限是基于角色授予的，遵循“需知原则”和预期的有效期间隔，并且必须保持最新状态。
  - Access rights (authorization) must be withdrawn promptly when they are no longer needed.
    不再需要访问权限(授权)时应立即撤销。
  - External personnel are granted access rights only for a limited period (no longer than one year). These access rights are revoked automatically at the end of the limited period.
    外部人员只能获得有限期限(不超过一年)的访问权，并且该等访问权限将在有限期限结束时自动撤销。
  - Access rights are checked at least once a year.
    访问权限至少每年审查一次。
- All developed applications log operations and procedures that are relevant to security (e.g. entry, modification and deletion of data).
  所有开发的应用程序都会记录与安全有关的操作和程序（例如，数据的输入、修改和删除）。
  - Security-related administrative and operating activities are always logged for no less than 6 months.

与安全相关的管理和操作活动始终被记录，保存时间不少于6个月。

- Security-related operations are recorded in the form of log files and kept available for an appropriate length of time (no less than 6 months) so that they can be used as part of an incident investigation if necessary.
  与安全相关的操作以日志文件的形式记录，并在适当的时间内（不少于6个月）保存，以便在必要时作为事件调查的证据。

- System and application managers are responsible for ensuring that suitable measures are taken to prevent corruption and unauthorized access to log Data.
  系统和应用程序管理员负责确保采取适当的措施，防止日志数据的损坏和未经授权的访问。
- Log analysis tools are implemented to detect unusual or suspicious operating activities.
  部署日志分析工具用于检测异常或可疑的操作活动。
- All developed applications include plausibility checks during Data input and output.
  所有开发的应用程序均包括数据输入和输出过程中的置信度检查。
- Archiving and deletion of documents and Data is defined mandatorily describing responsibilities, procedures and retention times.
  对文件、数据的归档和删除进行强制性规定，界定责任、程序和保留时间。
- A procedural instruction defines mandatory rules for the archiving and deletion of documents and Data.
  建立程序性指令，规定文件、数据归档和删除的强制性规则。

2.5 Measures for job control
作业控制措施

This section describes measures that are taken to ensure that Personal Data processed are processed strictly in compliance with the Data NSC's instructions.
本节描述为确保所处理的个人数据严格按照宝马汽贸的指示进行处理应采取的措施。

- A centralized contract management with periodic SLA reviews is in place.
  建立集中化的合同管理，并定期进行SLA审查。
- Assignments to service providers are not approved before the required legal documents (Data Privacy Agreements on Processing of Personal Data, appropriate technical and organizational measures of the provider) are in place.
  在指定服务供应商前，应确保已提交所需的法律文件（关于处理个人数据的数据隐私协议、供应商的适当技术和制度措施）。
- The use of public internet services for transaction, Processing and saving of company information is generally not allowed. Exceptions require individual legal and privacy impact assessments.
  一般情形下，不允许使用公共互联网进行交易、处理和保存公司信息。例外情形下，需进行单独的法律和隐私影响评估。
- All employees Processing Personal Data are obligated to maintain confidentiality

immediately when taking up their duties. The obligation of confidentiality continues after their employment ends.
所有处理个人数据的员工在就职时均有义务保守秘密，并在其劳动关系结束后继续履行保密义务。

- All employees Processing Personal Data take the training for Data protection (at least once a year). Exam results and percentage of people trained are documented and reviewed regularly.
  所有处理个人数据的员工均必须参加数据保护培训（至少每年一次）。应当记录考试结果和受训人员的百分比并定期审查。
- A thorough background checks on employees who have access rights to Sensitive Personal Data.
  对具有敏感个人数据访问权限的员工进行彻底的背景调查。
- Audit management by IT ensures the compliance with the policies, instructions, regulations and legal requirements by performing audits on a regular basis.
  由IT部门定期进行审计，确保符合政策、指示、法律法规要求。
- Relevant departments are in place to be responsible to detect, analyze and eliminate, where possible, new vulnerabilities to prevent intrusion of unauthorized third parties into the IT system.
  相关部门负责检测、分析和消除新的漏洞，以防止未经授权的第三方入侵IT系统。

2.6 Measures for availability control
可用性控制措施

This section describes measures that are taken to ensure that Personal Data are protected against accidental destruction or loss.
本节描述为确保个人数据不被意外破坏或丢失应采取的措施。

- IT operations offer a wide choice of service levels for multiple IT services defined in a catalogue of services ranging from "super critical" to "noncritical" using redundant and distributed services if required.
  IT运营部门为IT服务提供广泛的服务级别(从“非常关键”到“不关键”)选择，必要时，可使用冗余和分布式服务。
  - Data is stored on a central file server, wherever possible, as regular Data backup is then assured within the framework of routine IT operations.
    在可能的情况下，数据应存储在中央文件服务器上，从而在日常IT操作的框架内进行定期数据备份。
  - The operators of IT systems (application and infrastructure operation) are responsible for making regular backup copies of application and configuration Data. The actual frequency and organization (generation concept) of backup routines reflect the frequency with which the Data is changed.
    IT系统的操作员(应用程序和基础设施) 负责定期备份应用和配置数据。备份的实际频率可反映数据更改的频率。
  - The operators of IT systems (application and infrastructure operation) are

responsible for the recovery of Data.
IT系统的操作员（应用程序和基础设施）负责恢复数据。

- Data centers follow central guidelines for facility security and prevention of damages from fire or water.
  数据中心在设施安全和防火灾、水灾上遵循中央指导方针。
- Unbreakable power supplies, redundant power circuits and house lead-ins, independent power generators are provided in all Data centers.
  所有数据中心均配备不间断电源、冗余电源电路和室内引线，以及独立的发电机。
- All IT systems are scanned for vulnerabilities and misconfigurations (at least once a year).
  所有的IT系统均应进行漏洞和错误配置的扫描（至少每年一次）。
- Network firewalls and intrusion detection systems isolate different network zones assuring an adequate security level.
  部署网络防火墙和入侵检测系统隔离不同的网络区域，以确保充足的网络安全水平。
  - All network gateways through which network traffic enters or leaves the Authorized Party's intranet are protected.
    网络流量进出受托方内网的网络网关均受到保护。
  - The internal structure of the Authorized Party's intranet is concealed from the outside world (Internet).
    受托方内网的内部结构对外部世界（互联网）是不可见的。
  - Communications between partner networks that pass through the Authorized Party's intranet are tunneled.
    受托方内网与合作伙伴网络之间以隧道方式进行通信。
  - Transfer between public networks and the Authorized Party's intranet is protected by Network Access Points (NAPs).
    公共网络和受托方内网之间的传输受到网络接入点（NAPs）保护。
  - Inside, there are demilitarizes zones (DMZ) which have different security classifications.
    内部设有非军事区（DMZ），它们有不同的安全级别。
- Industry standard anti-malware software is used on all endpoints with protection against ransomware and other exploits.
  所有终端均使用符合行业标准的反恶意软件，以防止勒索软件和其他漏洞。
- Access rights for network zones are granted on the basis of roles following the need-to-know principle and an expected validity interval and must be kept up to date.
  网络区域的访问权限是基于角色授予的，遵循“需知原则”和预期的有效期间隔，并且必须保持最新状态。
  - The authenticity of the accessing user's identity is verified for every attempt to access the Authorized Party's intranet or the IT systems within the Authorized Party's intranet.
    试图访问受托方内部网络或IT系统时，访问用户身份的真实性应得到验证。
  - Every IT system belonging to the Authorized Party, which is used to process Data that is not exclusively public, is equipped with an access management

system for users.
受托方的每个IT系统（如果用于处理不完全公开的数据），均配备了用户访问管理系统。

- All IT systems are equipped with permanent virus protection that checks for viruses every time a file is accessed and antivirus checks are carried out at all gateways to the Authorized Party's intranet for content transferred in un-encrypted form.
所有的IT系统均配备了永久性的病毒保护软件，在每次访问文件时均会检查病毒，并且在进入受托方内网的所有网关上对以未加密形式传输的内容进行防病毒检查。
  - Measures are taken to ensure that the IT systems are equipped with up- to-date antivirus software.
采取措施确保IT系统配备最新的防病毒软件。
  - Antivirus software is operated on a central basis.
反病毒软件在中央系统上运行。
- Continuous server performance monitoring assures a proactive capacity management.
持续监测服务器性能以确保主动的容量管理。
  - Provision is made for the permanent monitoring of required resources in order to ensure the needed availability and performance.
按照规定对所需资源进行长期监测，以确保所需的可用性和性能。
- Availability management and continuity management is defined and controlled by the strategic division of IT operations.
可用性管理和连续性管理由IT运营的战略部门定义和控制。
- High quality backup and recovery services are offered centrally using physical and virtual tape infrastructure. Backup media is encrypted and stored offsite in a secure, environmentally controlled location.
使用物理和虚拟磁带基础设施集中提供高质量的备份和恢复服务。备份介质被加密并存储在异地、受控制的安全环境。
- Adequate backup and recovery concepts are in place for any application.
任何应用程序均具备适当的备份和恢复策略。
- A contingency plan is in place for "special protection" services.
为需"特别保护"的服务制定应急计划。
- An effective Security Incident Handling process assures the detection of Security Incidents at an early stage and a precise reaction to Security Incidents.
制定有效的安全事件处理流程，确保在早期阶段发现安全事件，并对安全事件做出准确反应。
- An effective process for IT Crisis Management ensures a well-defined, optimum and timely reaction to disruptions in the areas of information or telecommunication technology.
制定有效的IT危机管理流程，确保对信息或通信中断做出明确、最佳和及时的反应。
  - For every IT unit an IT Crisis Manager and at least one deputy are appointed and provided with all of the authority required to perform the job.

为每个IT部门任命一名IT危机经理和至少一名副手，并授予其执行工作所需的所有权限。

- The roles within IT Crisis Management and their correlation with individual people are documented within the IT units.
  IT危机管理中的角色及相应负责的个人在IT部门中被记录。
- IT Crisis Management consists of processes which ensure
  IT危机管理包括以下过程，以确保
  - identification of IT crises
    识别IT危机
  - initiation of IT Crisis Management in the unit concerned and alerting the decision makers (IT Crisis Managers)
    有关单位启动IT危机管理，并提醒决策者（IT危机管理人员）
  - informing other, potentially affected units of the IT crisis
    向其他可能受影响的单位通报IT危机
  - reaching a decision on measures to overcome the IT crisis and issuing authorized instructions
    就解决IT危机的措施达成决定，并发布授权指令
  - escalation to the next high escalation level, if necessary, termination and de-escalation of the IT crisis, and post-processing and analyzing IT crises
    （如有必要）升级到下一个高的升级级别，终止和解除IT危机的升级，并对IT危机进行后期处理和分析
  - promptly report to the relevant departments and inform the affected individuals
    及时向有关部门报告并通知受影响的个人

- When the alert is given, the point of contact in the IT unit triggers Incident Management within its own unit automatically. This remains at this escalation level at least until such time as the IT crisis is de-escalated by the unit of NSC that gave the alert.
  当警报发出后，IT部门的联络点将自动执行其自身单元内的事件管理。并在发出警报的宝马汽贸相关单位将IT危机降级之前，一直保持在该级别。

2.7 Measures for separation control
分离控制措施

This section describes measures that are taken to ensure that Data collected for different purposes can be processed separately.

本节描述为确保出于不同目而收集的数据能够被单独处理应采取的措施。

- Access rights for IT resources are granted on the basis of roles following the need-to-know principle and an expected validity interval and must be kept up to date.
  IT资源的访问权限是基于角色授予的，遵循“需知原则”和预期的有效期间隔，并且必须保持最新状态。

  - Access rights (authorization) must be withdrawn promptly when they are no longer needed.
    访问权限(授权)在不再需要时应立即撤销。
  - External personnel are granted access rights only for a limited period (no longer than one year). These access rights are revoked automatically at the end of the limited period.
    外部人员只能获得有限期限(不超过一年)的访问权，并且该等访问权限将在有限期限结束时自动撤销。
  - Access rights are checked at least once a year.
    访问权限至少每年审查一次。
- Sensitive systems shall have a dedicated (isolated) computing environment.
  敏感系统应具有专门的（隔离的）计算环境。
- De-identified information and the information enabling the restoration of Personal Data shall store separately.
  去标识化信息和能够恢复个人数据的信息应单独存储。
- Biometric data and personal identification data shall be stored separately.
  生物识别数据和个人识别数据应单独存储。
- Administration tasks with high privilege levels are separated from other tasks by using different user IDs.
  使用不同的用户ID将高权限级别的管理任务与其他任务分开。
  - IT systems are administered only by authorized personnel.
    IT系统由授权人员管理。
  - The number of administrators is restricted to an absolute minimum. Administrator access rights are granted within the framework of personal accounts.
    管理员的人数应限制在最低限度。管理员访问权限在个人帐户框架内授予。
- Programming environment, test environment, integration and production are made available separately. This also applies to temporary development environments.
  编程环境、测试环境、临时开发环境以及集成和生产环境应进行分离。
- Physical or logical Data segmentation per function or client is ensured by specific measures. Data exchange between systems is restricted to interfaces defined and documented before implementation, which are part of the prior approval.
  通过具体措施确保每个功能或客户的数据保持物理或逻辑隔离。系统之间的数据交换仅限于事前定义和记录的接口，并作为事先批准的一部分。
- Status of data exchange interfaces are real-time monitored to prevent malicious data acquisition. Exchange of Personal Data between systems must be encrypted.
  对数据交换接口的状态进行实时监控，以防止恶意的数据获取。系统之间的个人数据交换必须进行加密。
- Personal Data must not be used other than for the purpose defined in the Data Privacy Agreements on Processing of Personal Data and the respective prior approval process.

个人数据不得用于数据隐私协议以及相应审批流程中定义的处理目的之外的其他用途。