KANTAR

如果该译文的含义与英文版本之间有任何差异，则以英文版本为准

条款和条件（本服务的购买）

1. **定义**

1.1. 在本协议中，下列词语具有以下含义：

1.1.1. “**协议**”是指订购单及本条款共同构成之文书。

1.1.2. **“附属公司”** 是指直接或间接通过一个或多个中介机构控制或受其控制或处于共同控制之下的任何实体，并且在客户不时以 Kantar 的身份进行交易的情况下，但不包括 Europanel。

1.1.3. “**机密信息**” 是指涉及客户和/或 Kantar 集团任何董事、高级职员、雇员、预算、价格、定货簿、方法、问卷账目、财务、母公司、子公司、客户数据及其顾客和客户的任何信息。

1.1.4. “**控制**” 应具有以下含义：

直接或间接拥有指导该实体管理或政策的权力，无论是通过拥有投票权证券、与投票权有关的合同或其他方式，或

直接或间接拥有超过百分之五十 (50%) 的已发行投票权证券或该实体的其他所有权权益。

1.1.5. “**客户**”是指订购单载明的 Kantar 附属公司。

1.1.6. “**客户数据**”是指由客户或其顾客或者代表客户或其顾客向供应商提供的或者供应商依据本协议需要生成、处理、储存或传输的任何数据 （包括任何与员工、客户/顾客或客户或其顾客之供应商相关的个人数据）、文件、文本、图画、图表、规格、图像（连同由上述内容构成的任何数据库）。

1.1.7. “**数据保护法规**”是指 GDPR、《欧洲隐私与电子通讯指令》(European Privacy and Electronic Communications Directive)（该等法规可不时修订）和在任何国家或地区执行上述指令的任何法规。

1.1.8. “**交付成果**”是指将作为本服务的一部分进行供应的所有产品、商品、设备和材料。

1.1.9. “**收费**”是指订购单上载明的应由客户支付的总金额。

1.1.10. “**GDPR**”是指欧洲议会和理事会于 2016 年 4 月 27 日颁布的针对个人数据处理当中的自然人保护和针对个人数据自由流动的欧盟第 2016/679 号法规，该法规废止了“95/46/EC 号指令”（《一般数据保护条例》(General Data Protection Regulation)）。

1.1.11. “**知识产权**”是指当前或日后可能存在于世界任何地方的所有专利、发明权、版权及相关权利、著作人格权、数据库权利、半导体拓扑图权利、实用新型、设计权、商标、服务标志、商号、域名、商誉中的权利、未披露信息或机密信息中的权利以及其他类似或同等权利或保护形式。

1.1.12. “**个人数据**”的定义详见附表 3。

1.1.13. “**订购单**”是指本条款和条件所附之采购订单，或参照采购订单编号的任何其他书面通信，以及适用本条款和条件的采购订单。

1.1.14. “**本服务**”是指订购单载明的服务， 或者在任何其他书面通信中提及的订购单编号所指明的服务。

1.1.15. “**供应商**”是指订购单中确定的实体。

1.1.16. “**供应商人员**” 是指被要求履行本服务的所有人员。

1.1.17. “**供应商政策**” 是指适用于 The Kantar Group Limited. 及其直接或间接拥有的子公司之供应商的所有政策或行为准则，该等政策或行为准则由客户不时向供应商告知或者在客户运营的任何外联网上不时向供 应商提供（可根据要求提供），包括但不限于作为附表 1 附于本协议之后的《Kantar 业务行为准则》以及任何适用的 Kantar 反贿赂政策。

2. **本服务**

2.1.1 本条款和条件适用于本服务。

2.1.2 本服务开始履行，即视为订购单已被接受。供应商应于订购单载明的日期开始提供本服务。供应商应根据客户不时提出的请求、供应商政策、最佳行业实践以及本协议的条款向客户提供本服务。本服务的履行时间是关键所在。

2.1.3 供应商保证每位供应商人员：

(a) 遵守不时更新的供应商政策；

(b) 受过适当培训，有资格提供本服务；

(c) 已根据客户发出的具体指示进行适当筛选，没有任何犯罪记录；以及

(d) 有权在提供本服务的地区工作。

2.1.4 供应商作出以下持续有效的保证、承诺和陈述：

(a) 其完全有能力和权限来签订本协议以及履行本协议项下的义务；

(b) 其遵守所有适用的法律、法规和行为守则；

(c) 在履行本协议项下义务的过程中，不会实施对客户或其顾客的声誉产生或可能产生严重负面影响的任何作为或不作为；以及

(d) 交付成果完整、准确、不侵权，全面符合本协议的规定。

3. **收费**

3.1. 只有在本服务履行完毕，且达到令客户合理满意的情况下，供应商才有权向客户开具发票。

3.2. 客户应在其下一个付款期（即收到注明正确订购单编号的有效发票当月月末之后六十 (60) 天后的某一日期之后的期间）支付本服务的收费。如果客户系代表其顾客从供应商处获取本服务，则只有在客户收到其顾客的付款后，客户才有义务向供应商付款。收费不含销售税或类似税款。如法律有相关要求，客户有权对收费进行扣除或扣缴。

3.3. 若无异议的金额逾期未付款，供应商可对该逾期金额收取利息，利率按英格兰银行每年的基本利率再加 2% 执行。

4. **终止**

4.1. 客户可随时按以下方式全部或部分 （按比例扣减收费）终止本协议：

4.1.1. 为方便起见，提前三十 (30) 天书面通知供应商；或者

4.1.2. 如果供应商实质性违反本协议，且在客户通知其纠正违约行为后 14 天内仍未予以纠正，则客户可立即终止本协议；或者

4.1.3. 如果已经下达订单或通过决议终止供应商或者如果发出对供应商进行清算的命令或通过相关决议，或者对供应商的任何资产指定接收人或破产管理人，或者出现法院或债权人有权指定接收人或管理人的情形，或者法院作出清算或接管命令，或者供应商与其债权人作出相关安排，则客户可立即终止本协议；或者

4.1.4. 如果供应商无力支付到期债务，则客户可立即终止本协议。

4.2. 本协议或本服务的任何部分到期或终止时，供应商将向客户交付所有机密信息，并联络客户和/或第三方以确保顺利交接。

4.3. 本协议到期或终止，不影响截至终止之日已产生的任何权利，亦不影响以明示或默示方式规定在协议终止后仍然有效的任何条款。

5. **审计**

5.1 在本协议有效期内及之后的 6 年内， 供应商应按照公认的会计原则和文件留存原则在其主要营业地保留与本服务相关的真实且准确的书面账户和记录（包括但不限于工时表、索赔记录、发票、费用、贷项通知单），且应允许客户和/或其顾客或客户授权代表在发出合理书面通知的前提下检查该等记录，以评估本协议（包括但不限于第 10 条规定的限制）是否得到遵守。如果经审计， 客户发现存在任何与本服务相关的超额支付现象或任何违反本协议条款的其他事项，供应商应立即自担费用纠正该等不符合规定的事项，并向客户完整退回任何超额支付的款项和相关审计的费用。

6. **责任与赔偿**

6.1. 本协议的任何内容均不得排除或限制任何一方就以下索赔所承担的责任：

6.1.1. 因该方过失造成死亡或人身伤害；或

6.1.2. 该方的任何欺诈行为（包括虚假声明）；或

6.1.3. 不得通过合法方式予以限制或排除的相关责任；或

6.1.4. 根据本协议由供应商向客户提供的任何赔偿；或

6.1.5. 供应商违反第 8 至第 10 条（含第 8 条和第 10 条）或 第 12.1 条；或

6.1.6. 供应商故意或有意违约。

6.2. 在遵守第 6.1 条的前提下，客户不对任何间接、特殊性或继起性损失承担责任，亦不对任何利润损失 （无论是直接的还是间接的）、商誉损失、业务损失、收入损失或预期结余损失承担责任。

6.3. 如果供应商因以下事项，使客户招致和/或遭受任何损失、成本、负债、损害、费用、索赔和诉讼，供应商应向客户作出赔偿：

6.3.1. 违反本协议；或

6.3.2. 在提供本服务期间造成客户财产损失或损坏；或

6.3.3. 供应商、供应商人员和/或分包商或与本协议相关的供应商雇员的任何过失或疏忽； 或

6.3.4. 有人声称交付成果和/或本服务的使用侵犯任何第三方的知识产权。

6.4. 在遵守第 6.1 条和第 6.2 条的前提下，客户承担的由本协议引起或与之相关的全部责任（无论是基于合同还是侵权，包括过失或其他过错）累计不得超过责任事件发生之日的过往十二 (12) 个月内客户根据本协议向供应商支付或应付之收费的总金额。

6.5. 在遵守第 6.1 条和第 6.2 条的前提下，客户承担的由本协议引起或与之相关的全部责任（无论是基于合同还是侵权，包括过失或其他过错）累计不得超过 每起索赔 10,000,000 英镑（一千万英镑）。

7. **保险**

7.1. 供应商应就其在本协议项下的义务和责任向声誉良好的第三方保险人购买保险，投保内容如下：

7.1.1. 公共责任险：每起事故最低保额 1,000,000 英镑，且在相关保险期内不设限；

7.1.2. 雇员责任险：每起事故最低保额 5,000,000 英镑，且在相关保险期内不设限；

7.1.3. 专业损害赔偿责任险：每起事故最低保额 1,000,000 英镑，且在相关保险期内不设限；

7.2. 各保险单应将客户列为额外被保险人，并应包含向责任主要承担者赔偿的条款。各保险单不得进行损害分摊，且客户还可获得任何其他附加保险。客户不负责免赔额，且该免赔额不得低于 50,000 英镑。

7.3. 供应商应购买客户不时合理要求购买的其他保险。

8. **数据保护**

8.1. 如果本服务的提供要求供应商代表客户处理个人数据，供应商将：

8.1.1. 遵守数据保护法规；

8.1.2. 仅依据作为数据控制人的客户的指示行事；

8.1.3. 遵守附表 2 （信息安全附录）；

8.1.4. 遵守附表 3 （数据保护：GDPR）

8.2. 如果因客户未能遵守数据保护法规、本第 8 条以及附表 3 条款，致使客户遭受或招致任何损失、负债、索赔、费用、损害及成本，供应商应向客户作出赔偿。

8.3. 供应商应遵守 GDPR 要求的涉及任何要求处理个人数据的本服务的具体条款（如附表 3 所载）。

8.4. 供应商保证会制定适当措施，该等措施会包含 ISO/IEC 27001 信息安全标准或不时替代该标准的具有同等意义的任何其他标准。

9. **知识产权**

9.1. 在遵守第 9.2 条的前提下，客户拥有交付成果中的知识产权；交付成果中的所有知识产权一经创建，即由供应商不可撤销且无条件地转让给客户（供应商保证客户会获得完整的所有权）。供应商应（并应确保供应商人员）以有利于客户的方式完全且不可撤销地放弃与该等交付成果相关的著作人格权（若有）。

9.2. 本协议的任何内容均不旨在影响供应商在本服务中使用或独立开发的材料之所有权，亦不旨在影响供应商在履行本服务过程中使用的（但并非由供应商开发的）一般方法、工具、技术或流程（统称为“供应商已有材料”）。如果供应商已有材料（或其中一部分）被纳入交付成果，或者需要该等材料来使用或开发本服务，则供应商特此授予客户一项永久性、在全球有效、不可撤销、非排他、免特许权使用费的许可，允许客户使用供应商已有材料，以便客户获得本服务的全部利益。

9.3. 供应商保证并陈述，其已获得所有依据本协议授予或转让的知识产权之转让权或许可权，且相关转让或许可事项的授予行为和条款不侵犯任何第三方的知识产权。

9.4. 供应商不得因本协议而获得客户拥有的或任何第三方向客户许可的任何知识产权之任何权利、所有权或利益，且供应商确认所有该等知识产权归客户和/或其许可人所有。

10. **不得贿赂**

10.1. 供应商应遵守《海外反腐败法》（《美国法典》第 15 章第 § 78dd-2 节）(Foreign Corrupt Practices Act, 15 U.S.C. §78dd-2)（简称“《海外反腐败法》”） 及 2010 年英国《反贿赂法》(UK Bribery Act 2010)（简称“《反贿赂法》”），并确保其集团公司、合作方及上述各方之董事、雇员、代理人和中介或为客户开展服务的任何相关方（以上各方均简称“关联人士”）遵守该等法律。

10.2. 供应商不得（且应促使各关联人士不得）违背己方的法定职责，直接或间接要求、同意收取或接受经济利益或其他利益，或诱使各方施加其影响力来影响其所做的行为或决定（包括以不恰当的方式履行职责） 或为客户获取或保留业务。如果供应商获悉任何违反《海外反腐败

法》、《反贿赂法》或本第 10 条的行为，应立即以书面形式通知客户。

11. **客户及顾客材料**

11.1. 向供应商提供的用于履行本服务的客户或其顾客之任何财产的所有权，归客户或其顾客所有（根据适用情况确定）。

11.2. 客户或其顾客有权在任何时候从供应商处重新取回客户或其顾客的财产，但须在合理范围内提前通知。

11.3. 供应商应保障其持有的客户或其顾客的任何财产处于安全状态，未经客户及其顾客书面同意，不得处置或放弃持有该等财产，但为履行本服务而另有要求的除外。

11.4. 供应商特此放弃其对客户或其顾客之任何财产可能拥有的任何留置权或其他权利，并保障该等财产免于遭受任何留置及其他权利负担。

11.5. 供应商应仅在履行本服务的相关事项中使用客户或其顾客的财产。

12. **反现代奴役法**

12.1. 供应商保证，供应商及其高级职员、雇员、代理人或分包商均：

12.1.1 未作出违反 2015 年《反现代奴役法》(Modern Slavery Act 2015) 的违法行为（“反现代奴役法违法行为”）；

12.1.2 未被告知其因反现代奴役法违法行为的指控而接受调查，或依据 2015 年 《反现代奴役法》而遭到起诉；

12.1.3 未知悉其供应链中出现因反现代奴役法违法行为的指控而接受调查或依据 2015 年《反现代奴役法》而遭到起诉的任何情形； 12.1.4 供应商应遵守 2015 年《反现代奴役法》；

12.1.5 如果供应商知悉或有理由相信其或其任 何高级职员、雇员、代理人或分包商违反或可能违反本第 12 条项下的任何供应商义务，供应商应立即以书面形式通知客户。

13. **一般条款**

13.1. 在本协议有效期内及之后 5 年内， 供应商应为所有机密信息保密，不得使用该等机密信息或将其披露给任何第三方，除非为履行本服务而确有必要使用或披露机密信息或法律作出相关要求。

13.2. 未经另一方事先书面同意，任何一方不得让与、分包或以任何方式转让其在本协议项下的任何权利或义务，但客户可将其权利转让给 The Kantar Group Ltd. 的任何（直接或间接拥有的）子公司。

13.3. 本协议各条款均可分割，且与其他条款不同。某具体条款无效或不可执行，不影响本协议其他条款。

13.4. 一方未行使或延迟行使本协议、普通法或衡平法提供的权利或救济，不构成该方放弃该权利或救济，亦不构成放弃任何其他权利或救济。

13.5. 本协议的任何内容均不得视为就协议双方建立或暗示建立任何合伙关系或代理关系。

13.6. 本协议构成双方就双方所处理事项所达成的全部协议和谅解，并替代双方先前就该等事项所达成的任何协议。本协议只有经客户与供应商以书面形式协定，方可修订。

13.7. 非本协议的协议方均不享有 1999 年《合同（第三方权利）法案》(Contracts (Rights of Third Parties) Act 1999) 项下的任何权利。

13.8. 本协议要求发出的任何通知均应采用书面形式，且只有通过以下方式发送到订购单上的对方地址，方可视为有效送达：专人递送、一等邮件或特快专递。

13.9. 本协议及任何非合同义务应由英国法律管辖，双方同意将任何争议提交给英国法院，且英国法院对该等争议具有非专属管辖权。

.

KANTAR

附表 1: KANTAR 业务行为准则

Kantar 及其公司在全世界许多市场、国家和地区运营。在任何情况下，我们都尊重相关的全国性法律及任何其他具有国际影响力的法律，如英国《反贿赂法》、美国《海外反腐败法》和英国《反现代奴役法》（如适用） 以及行业行为准则。我们承诺在所有业务层面中均依道德规范行事，并保持最高标准的诚实与正直。

我们期望并要求我们所有业务伙伴（包括供应商）做出同样的道德承诺，因此我们要求您确认同意我们的业务行为准则（见第一纵列），该准则已为非 Kantar 实体作出必要修订（见第二纵列）。

我们期望我们所有供应商均采用适当的制度来促进遵守这些标准并实施监控，以及遵守当地法律和适用的国际法律。

我们期望我们的供应商展现他们对本准则所述原则的承诺，并拥有持续的风险管理流程，以便识别与其运营相关的环境、健康和安全及劳工实践和道德方面的风险。

供应商应当鼓励员工上报疑虑事件，且无需惧怕威胁或报复。供应商应当按要求采取适当行动。

供应商应当为其自身供应链制定与本准则相类似的标准。

Kantar 的准则	**Kantar 对供应商的期望**
我们作为 Kantar 集团（简称“**集团**”）各公司的高级职员和员工，均认识到我们对所有利益相关方（包括股东、客户、员工和供应商）负有重要义务，他们对我们的成功至关重要；	您确认您认可我们的义务，不会作出有损于这些义务的行为。
与我们业务有关的信息应清楚、准确地传达，不得采用歧视的方式，且须符合当地法规。	您确认您将以所述方式对待有关 Kantar 集团的信息。
我们基于资历和价值来挑选和提拔人才，不因种族、宗教、出生国、肤色、性别、性取向、性别认同或表达、年龄或残疾与否来加以歧视或作为考虑因素。	您确认您在您的组织中也制定同样的政策。
我们相信工作场所应当安全、文明，就业必须自由选择；我们不会容忍任何类型的性骚扰、歧视或攻击性行为，这些行为包括通过言语或行动对个人进行持续的贬损、展示或传播具有冒犯性的材料，或者在 Kantar 或客户经营场址使用或持有武器。	您确认您在您的组织和您的供应链中也制定同样的政策，且您将以所述方式尊重我们的工作场所和人员。 需要特别指出的是： • 就业必须自由选择；不得使用强迫劳动或抵债性劳动或任何其他形式的现代奴役； • 不得强迫工人提交护照或政府签发的身份作为就业条件； • 不得使用童工； • 支付给工人的报酬必须符合所有适用的工资

	法； • 工作周数不得超过当地法律规定的最大值； • 不得对工人做出不人道的对待，包括性骚扰、性虐待、体罚、身体胁迫或言语虐待； • Kantar 希望其供应商为所有工人创造和培养安全的工作条件； • 必须尽可能避免工人接触物理性危害，如无法避免，则必须加以控制； • 供应商必须有适当的程序来处理可能对工人有影响的紧急情况；以及 • 必须建立管理、跟踪和报告职业伤害和疾病的系统。
我们不会容忍使用、持有或传播非法药品的行为，亦不会容忍我们的人员在药品或酒精的影响下参加工作。	您确认您在您的组织中也制定同样的政策，且您将以所述方式尊重我们的工作场所和人员。
我们会对所有涉及集团业务或其客户的信息保密。特别需要指出的是，我们明确禁止“内幕交易”，不得将机密信息用于为个人谋利。	您确认您同意我们就我们的信息所制定的政策。
我们承诺按照国家法律和行业准则保护消费者、客户和雇员的数据。	您确认您在您的组织中作出同样的承诺，以同样方式对待来自我们业务或与我们业务或业务伙伴相关的所有信息。
我们创造的作品不会故意包含有违社会公序良俗的陈述、暗示或图像，而且我们会对我们的作品对少数族群的影响进行适当考量，无论该少数族群是否按种族、宗教、出生国、肤色、性别、性取向、性别认同或表达、年龄或残疾等进行划分。	在适用情况下，您确认您在您的工作中也秉持相同的标准。
我们不会从事那些有意或旨在误导他人的工作，包括与社会、环境和人权相关的事项。	在适用情况下，您确认您在您的工作中也秉持相同的标准。
在接受工作前，我们会考虑相关客户或工作是否会损害集团的声誉。这包括与参与侵犯人权活动的客户有联系而造成的声誉受损。	这仅涉及 Kantar 集团成员。

我们不会为了给个人或家庭谋利而直接或间接地参与任何与集团内部公司形成竞争或与我们在该公司的义务产生冲突的活动。	这仅涉及 Kantar 集团成员。
我们不会向任何第三方贿赂、提议向其贿赂或向其索贿（无论是现金还是其他形式的贿赂），该等第三方包括但不限于政府官员、客户、经纪人或上述各方的代表。我们将通过培训、沟通和以身作则方式共同确保所有员工了解该政策。	这直接适用于您。
我们不会为个人利益接受来自供应商、潜在供应商或其他第三方的超出象征性价值的商品或服务。	这直接适用于您。
我们不会在我们的业务中产生任何个人或家庭利益冲突，亦不会与我们的供应商或与我们进行业务往来的其他第三方产生这种利益冲突。	您应该在您的组织中制定同样的政策。
未经 Kantar 董事会事先书面批准，不得向政治人物、政党或行动委员会进行任何企业捐赠，包括低于市场价格提供服务或物品。	您应该就此类捐赠（连同合适的授权程序）制定您的政策。
我们将通过以下方式继续努力为社会和环境做出积极贡献：维持高标准的营销道德；在我们的业务、供应链和客户工作中遵守人权；尊重环境；支持社区组织；支持雇员个人发展；以及在我们的供应链中管控重大的可持续发展风险。关于我们对上述领域的承诺，我们的可持续发展政策和人权政策声明有更详尽的描述。	您应该在您的组织中制定同样的政策。需要特别指出的是： • 供应商必须遵守英国《反现代奴役法》； • 供应商必须取得所有相关的环境授权（包括针对废弃物和排放物的授权）； 供应商必须通过回收利用、重新使用和替换材料等手段，在其设施和流程中实施保护措施，力争杜绝污染。

我们确认，我们遵守为我们的组织修订的《Kantar 业务行为准则》。如果我们发现任何违规行为，特别是向您的组织或任何其他第三方行贿或提供不适当的礼物或服务，或涉及可能直接或通过关联损害 Kantar 声誉的其他事项，我们将立即通知您。

签名：

姓名：

职务：

组织：

日期：

附表 2: 信息安全附录

1. **序言**

本安全要求附表（简称"**本附表**"）制定了针对供应商信息安全的基本要求，以确保客户机密信息及客户之顾客的机密信息的机密性、可用性及完整性。供应商应在履行本服务项下之服务的过程中遵守这些要求。

2. **术语**

2.1. 在本附表中，下列词语（无论是首字母大写还是全部小写）具有如下相应含义。首字母大写但未在本附表进行定义的词语的含义与其在本协议中的含义相同。

2.2. 承包人是指储存、处理、操作或能够访问任何客户机密信息或客户之顾客机密信息的分包商、独立承包人、服务提供商或供应商代理人。

2.3.

客户敏感信息是指包含个人数据[电子邮件、姓名等]、健康信息、财务信息或投资控股信息的任何客户机密信息和客户之顾客机密信息。

2.4. 加密是指将数据从原始格式（明码文本）转换为乱数格式（密码文本）的可逆变换，该变换机制用来保护信息的机密性、完整性和/或真实性。加密需要一种加密算法以及一个或多个加密密钥。

2.5. 储存是指储存、存档、备份和/或类似行为。

3. **安全核查**

3.1. 在供应商处理、存储或通过其他方式有权访问客户机密信息和客户之顾客机密信息的整个期间，应允许客户每年现场审查供应商的安全计划。供应商将及时安排在双方同意的日期进行该安全审查（但在任何情况下均不得晚于收到客户安全审查要求后三十 (30) 天内）。

3.2. 在合理必要的范围内，供应商应让客户查阅供应商的政策、流程和其他相关文件以及询问供应商的人员，以便该审查顺利进行。 供应商应于审查完成后三十 (30) 天内向客户提交一份纠正计划， 然后根据双方同意的纠正时间表及时纠正各个问题。

4. **具体安全要求**

4.1. 安全政策

供应商应以书面形式制定一系列范围广泛的安全政策和流程，且应至少涉及以下方面：

4.1.1. 供应商对信息安全的承诺；

4.1.2. 信息分类、标识和处理，而且涉及信息处理的政策和流程必须载明信息传输、储存和销毁的容许方法，且该等方法的防护程度不得低于《客户供应商信息保护指南》（见下文）中规定的方法；

4.1.3. 供应商资产的可接受使用范围，包括电脑系统、网络和消息传送；

4.1.4. 信息安全事故管理，包括数据泄露通知和证据收集程序；

4.1.5. 最终用户、管理员和系统的密码格式、内容和使用的认证规则；

4.1.6. 访问控制，包括定期检查访问权；

4.1.7. 对违反该等政策和流程的人员采取的惩戒性措施；以及

4.1.8. 按照与本第 4 节规定的相关要求相一致的方式来对待本第 4 节剩余部分所述的主题内容。

如果供应商的政策有任何根本性变化，应在 30 天内通知 Kantar。

4.2. 供应商信息安全计划的责任。供应商应承担信息安全责任，指定员工维护供应商的信息安全计划及实施信息安全和信息风险管理。

4.3. 供应商信息安全计划的审计、审核和监控。供应商应定期监控和审核其信息安全计划， 以确保存在适当的安全保障来限制客户机密信息和客户之顾客机密信息所面临的风险。

4.4. 资产和信息管理。供应商应：

4.4.1. 对其处理或储存的所有客户机密信息和客户之顾客机密信息保存一份详细清单；

4.4.2. 对其在执行本协议项下的活动中使用的物理计算和软件资产保存一份详细清单；

4.4.3. 在操作、处理和储存客户机密信息和客户之顾客机密信息时，遵循《客户供应商信息保护指南》（见下文）。

4.5. 物理和环境安全

供应商应：

4.5.1. 仅允许获得授权的供应商人员进入供应商储存、访问或处理客户机密信息和客户之顾客机密信息的区域。

4.5.2. 对基础设施系统执行合理范围内的最佳实践，包括灭火、冷却、电力、应急系统和雇员安全。

4.5.3. 对储存、访问或处理客户机密信息和客户之顾客机密信息的所有区域实施进入权控制，且该控制程度与上述信息的敏感度相一致。

4.5.4. 定期对储存、访问或处理客户机密信息和客户之顾客机密信息的区域实施监控

4.6. 雇员相关事项

供应商应：

4.6.1. 对每位供应商人员实施刑事背景调查（包括在法律允许的情况下对有权限访问客户机密信息和客户之顾客机密信息的承包商进行调查，但适用法律作出限制或禁止的除外）； 该背景调查必须在允许上述人员访问上述机密信息之前执行，且供应商不得允许任何背景调查不过关的人员访问上述机密信息；

4.6.2. 培训新人员（包括承包人），使其了解如何在可接受的范围内使用和处理供应商的机密信息及受供应商委托的其他公司的机密信息（如客户机密信息和客户之顾客机密信息）；

4.6.3. 为其人员（包括承包人）提供安全及数据隐私教育和培训，并对完成此类教育课程的人员进行记录；以及

4.6.4. 执行正式用户注册和注销流程，用来授予及取消供应商信息系统和服务的访问权；如任何供应商人员（包括承包人）被终止聘用，则供应商应尽快（但在任何情况下均不得晚于取消聘用后的两 (2) 个工作日内）取消该等人员对客户机密信息和客户之顾客机密信息的访问权限。

4.7. 通信与运营

供应商应：

4.7.1. 定期进行备份，以便在约定的恢复时间内恢复对客户的服务（如果双方未约定具体恢复时间，则在商业上合理的时间内恢复服务）；

4.7.2. 按照《客户供应商信息保护指南》（见下文）对包含客户机密信息和客户之顾客机密信息的所有备份媒介进行加密；

4.7.3. 未经客户事先书面同意，不得在供应商经营场址之外的地方储存或复制客户机密信息和客户之顾客机密信息；

4.7.4. 未经客户事先书面同意，不得将客户机密信息和客户之顾客机密信息传输、转让或提供给任何第三方，亦不得向任何第三方提供上述机密信息的访问权限；

4.7.5. 如果客户批准上述第 4.7.3. 款和第 4.7.4. 款所述的活动，则供应商应就以下内容保留一份详细清单：储存或复制客户机密信息和客户之顾客机密信息的第三方和/或供应商经营场址以外的地方；接收上述机密信息或获得上述机密信息访问权的第三方；储存、复制、提供上述机密信息或提供其访问权限的目的；上述机密信息传输或以其他方式提供给上述第三方的方式；向上述第三方传输或以其他方式提供上述机密信息时所使用的传输和加密/保护方法或协议（若适用）；传输或以其他方式提供给

上述第三方的上述机密信息的描述；批准相关安排的客户雇员的姓名；以及获得该批准的日期；

4.7.6. 删除或销毁客户机密信息和客户之顾客机密信息时，采用符合或超过美国国防部《安全数据处理标准》(Department of Defense Standard for Secure Data Sanitization) (DOD 5220.22M) 的数据销毁程序。客户提出书面要求时，供应商应立即删除或销毁任何或所有客户机密信息和客户之顾客机密信息；

4.7.7. 在传输或运送客户机密信息和客户之顾客机密信息时，遵循《客户供应商信息保护指南》（见下文），包括有关加密的规定；

4.7.8. 对储存客户机密信息和客户之顾客机密信息的所有移动设备或供应商人员用于访问任何上述机密信息的所有笔记本电脑使用硬盘驱动器加密，且该加密应符合《客户供应商信息保护指南》（见下文）；

4.7.9. 在传输、访问、处理或储存客户机密信息和客户之顾客机密信息的供应商服务器和/或最终用户平台上保持最新的恶意软件检测及预防；

4.7.10. 使用防火墙、杀毒软件、反恶意软件、入侵检测系统和其他在商业上合理的防护技术来维持加固的互联网防御边界和安全基础设施；以及

4.7.11. 定期对传输、访问、处理或储存客户机密信息和客户之顾客机密信息的所有供应商系统实施补丁管理和系统维护。

4.8. 访问控制

供应商应：

4.8.1. 对用户认证执行最佳实践；如果使用密码来认证那些访问客户机密信息和客户之顾客机密信息的个人或自动化流程，则该密码须符合针对密码使用、创建、储存和保护的当前最佳实践。（请参阅下文的《客户供应商信息保护指南》）。

4.8.2. 确保用户 ID 仅供个人使用，不与他人共享，并在用户与供应商终止关系后 48 小时内移除；

4.8.3. 基于以下内容来分配访问权限：客户机密信息和客户之顾客机密信息的敏感性、个人的工作要求、个人对上述具体机密信息的“须知”程度；

4.8.4. 至少每年核查供应商人员（包括承包人）的访问权限，以确保“须知”限制保持最新状态；

4.8.5. 定期核查用户进入那些存放客户机密信息和客户之顾客机密信息的供应商设施的报告；以及

4.8.6. 不得将客户机密信息和客户之顾客机密信息以不安全的方式且在无人看管的情况下放置在供应商设施中的桌面、打印机或其他地方。

4.9. 应用程序开发；漏洞扫描及渗透测试

供应商应：

4.9.1. 实施安全的开发方法，且该方法在整个开发生命周期中纳入安全措施；

4.9.2. 开发和实施安全编码标准；

4.9.3. 使用自动化扫描工具对所有外向型应用程序及由供应商（或承包人）开发并交付给客户的任何软件执行安全编码检查；

4.9.4. 至少每季度对接收、访问、处理或储存客户机密信息和客户之顾客机密信息的所有外向型应用程序执行漏洞扫描；一经客户要求，供应商应书面确认其已成功执行该等漏洞扫描；

4.9.5. 使用外部第三方安全测试公司至少每年对接收、访问、处理或储存客户机密信息的所有外向型应用程序执行侵入测试；该等侵入测试应由客户批准的供应商之测试供应方执行；一经客户要求，供应商应书面确认其已成功执行该等侵入测试；针对在由供应商或代表供应商执行的侵入测试中发现的所有实质性问题，供应商应于三十 (30) 天内予以纠正，若该等问题无法在三十 (30) 天内予以纠正，则须在供应商与客户共同约定的时间内予以纠正；

4.10. 承包人

供应商应：

4.10.1. 采取合理措施来选择和维持承包人，该等承包人须有能力根据适用法律和法规采取安全措施、以不低于本协议（包括本附表）要求的保护级别来保护客户机密信息和客户之顾客机密信息，且供应商应与各承包人签订书面合同，通过合同方式要求各承包人执行和维持该等安全措施。

4.10.2. 未经客户事先书面同意，不得向任何承包人提供任何客户机密信息和客户之顾客机密信息，亦不得允许任何承包人访问、处理、储存、查看或以其他方式接触上述机密信息；

4.10.3. 就任何承包人的所有行为及不作为向客户承担责任，包括承包人未能遵守本协议（包括本附表）之规定的情形；

4.10.4. 定期对各承包人实施核查，包括核查承包人的信息安全政策和实践。

5. 信息安全事件管理

供应商应：

5.1.1. 制定、测试和维持信息安全漏洞响应流程，且该流程应包括：证据保存；通知及配合执法部门、政府部门和类似机构（根据适用情况）；以及执行取证分析；

5.1.2. 以书面形式向客户通知任何涉及客户机密信息和客户之顾客机密信息的信息安全漏洞（包括任何实际或疑似未经授权访问上述机密信息的情形），或者发生于或涉及承包人的系统、硬件、设备、装置或经营场址的电脑的安全事件，或者以其他方式涉及供应商人员的安全事件；供应商应就任何该等事件及时发出通知，但在任何情况下均不得晚于供应商最初获悉该事件之日起的二十四 (24) 小时内。 此后，供应商应定期向客户更新有关该事件的调查及缓和情况。供应商应允许客户或其指定人员全面参与该调查。供应商应承担由任何相关方引起的与该等事件有关的所有费用，包括但不限于通知受影响的数据主体、取证调查、数据主体的信用监控以及其他补救和法律工作；以及

5.1.3. 针对各起事件，供应商应在其结束该事件后十 (10) 天内向客户提供最终书面通知，该通知应包含有关该事件根源、已采取的行动、防止未来发生类似事件的计划等详细信息。

6. **业务连续性管理**

供应商应：

6.1.1. 制定和维持全面的业务连续性计划（“BCP”），说明在出现计划外事件时所采取的恢复技术和业务运营的措施；

6.1.2. 行使其唯一且绝对的决定权，以其认为合适的方式至少每年测试或核查其业务连续性计划。

7. **合规**

供应商应：

7.1.1. 遵守《客户供应商信息保护指南》（见下文）；

7.1.2. 制定并维持双方约定的针对记录留存和数据销毁的政策和实践，且该等政策和实践适用于客户机密信息和客户之顾客机密信息以及供应商在本协议项下的活动中生成的或与该等活动相关的任何其他信息；

7.1.3. 制定道德准则，并要求雇员每年进行复习和确认（除非法律禁止相关行为）。

8. **后续风险管理措施**

8.1. 如果客户对供应商和/或供应商的一个或多个设施（或供应商之承包人的设施，根据具体情况确定）在之前已执行了安全审查，而且经过此类安全审查，客户发现了相关问题，则供应商应：

8.1.1. 在合理范围内配合客户，及时制定双发同意的风险管理计划以补救相关疑虑事项（前提是供应商尚未予以补救），以及

8.1.2. 在风险管理计划规定的相应日期前执行风险管理计划所述的行动。

8.2. 最近一次安全审查的风险管理计划如下所述，或者，如果以下计划为空白，则应在双方制定并同意的另一份文件中做出规定。

风险管理计划		
关注程度	行动计划	日期
高		
中		
低		

9. **身份盗窃**

如果供应商处理、操作或有权限访问个人信息，且如果在供应商履行本协议相关活动过程中，供应商的雇员发现任何与该个人信息有关的相关人员潜在身份盗窃事件，供应商应立即通知客户。

10. **更新**

客户可在提前三十 (30) 天书面通知供应商的情况下，随时更新此信息安全附录。如果供应商认为其无法遵守更新内容，供应商应在该三十 (30) 天内以书面形式说明其无法遵守的具体条款。 在此情况下，客户保留终止向客户提供任何或所有服务或项目的权利，且无需对该终止行为承担责任或遭到处罚。

附件 1

客户供应商信息保护指南

客户信息分类和操作矩阵表

概述了在传输（或运送）、储存或销毁客户机密信息和客户之顾客机密信息（包括客户敏感信息）时的有关具体要求。

信息分类	范例	传输	储存	销毁
除客户敏感信息外的客户机密信息和客户之顾客机密信息	商业策略和计划；审计报告；预发布营销信息；客户专属软件；技术规格或架构	电子格式：通过公共网络传输或通过可移动媒介或装置或其他电子媒介在供应商经营场址以外的地方运送时进行加密； 打印件：通过带追踪编号的快递（包括隔夜配送服务）或挂号邮件发送。	仅限获授权的人员获得访问权；每季度执行访问权审核。最好加密储存。	电子格式：采用 DOD 5220.22M 或同等流程。 打印件： 用碎纸机撕毁
客户敏感信息	个人信息（包括姓名、电子邮件、电话、邮寄地址、社会保险号或账号） 个人财务信息） 个人健康信息	如上	仅限获授权的人员获得访问权；每季度执行访问权审核。要求加密储存。	如上

加密

以下内容是客户当前的首选加密算法及当前可接受的其他加密算法。供应商在加密客户机密信息和客户之顾客机密信息时，应使用其中一种首选加密算法，除非在合理范围内该算法不可行，在此情况下，供应商在加密上述机密信息时，应使用其中一种可接受的其他加密算法。

首选加密算法		
目的	**算法**	**最短秘钥长度（比特）**
秘钥交换	RSA Diffie-Hellman 算法	首选 2048，若无法做到，则 1024
数据保护	CBC 模式中的 AES CBC EDE3 模式中的 3DES	首选 256，若无法做到，则 128 168
散列	SHA-256	不适用
HMAC	HMAC SHA-256	256
数字签名	RSA (SHA-256) DSA (SHA-256)	首选 2048，若无法做到，则 1024

可接受的其他加密算法		
目的	**算法**	**最短秘钥长度（比特）**
数据保护	CTR 模式中的 AES RC4 CBC 模式中的 RC5 CBC 模式中的 Blowfish CBC 模式中的 CAST-128 CBC 模式中的 IDEA	首选 2048，若无法做到，则 128

散列	首选 SHA-2，若无法做到，则 SHA-1 绝不应采用 MD5，除非是从技术上讲需要例外处理的情况。	不适用
HMAC	首选 HMAC SHA-2，若无法做到，则 SHA-1 绝不应采用 MD5，除非是从技术上讲需要例外处理的情况。	160 128
数字签名	ECC (SHA-256, SHA-2) RSA（首选 SHA-2，若无法做到，则 SHA-1）， DSA（首选 SHA-2，若无法做到，则 SHA-1）	至少 160 首选 2048，若无法做到，则 1024

基于密码的认证指南

供应商（或承包人）管理或控制的所有密码应符合以下准则：

地区	指南
最短密码长度	8 个字符
密码复杂程度	选择 4 种字符类型（小写字母、小写字母、数字、特殊字符）中的 2 种，不可以与个人或流程产生简单关联，不可以在字典中查到，不可以代表某种模式。强烈建议使用含 3 种字符类型（共 4 种）的密码
密码最长使用期	最多 90 天
最短密码历史	1 天
传输中的保护	强制要求。密码必须在传输中加密。
储存中的保护	强制要求。密码必须使用经批准的散列算法（见上表）进行散列。

KANTAR

附表 3

数据保护

1. **定义**

1.1. 在本附表 3 中，

未在本协议进行定义的词语的含义与其在 GDPR 中的含义相同。

1.1.1. 范围内个人数据是指供应商在提供本服务或履行本协议项下其他义务的过程中处理的任何个人数据；

1.1.2. 数据保障措施是指管理、技术和物理方面的保障措施，且该等措施保护范围内个人数据的完整性和安全性免受威胁或损害，以及保护范围内个人数据免受未经授权或意外的破坏、丢失、改变或使用及免受未经授权的访问，且该等措施符合最佳行业实践；

1.1.3. 示范条款是指欧盟委员会 2010 年 2 月 5 日的决定 (2010/87/EU) 所批准的标准合同条款，该决定是针对向在第三国创建之处理器传输个人数据的标准合同条款（但排除欧盟委员会在该决定中指定为具有可选性的任何合同条款），且该等条款可由欧盟委员会不时予以修订或替换；

1.1.4. **“分处理商”**是指供应商指定的代表客户处理与本协议有关的范围内个人数据的任何第三方；

1.1.5. 术语“**控制者”、“数据主体”、“成员国”、“个人数据”、“处理”、“处理商”和“监管机构”**应具有与 GDPR 中相同的含义，其同源术语应据此进行解释；提及将数据从任何国家或地区传输出去包括但不限于从该国家或地区之外的地方远程访问该数据的情形；

1.1.6. 提及本协议第 2.1.4. 条中的适用法律仅限于供应商须遵守的欧盟法律或成员国法律，且仅限于这些条款适用于范围内个人数据的情形（即处理该等数据须符合欧盟法律或成员国法律）。

2. **义务**

2.1. 供应商和客户均应始终遵守所有数据保护法规和与本协议相关的所有适用供应商政策所规定的相关义务。

2.2. 除提供本协议项下的本服务和履行本协议项下的其他义务外，供应商无权使用或以其他方式处理任何范围内个人数据。

2.3. 双方的作用。双方承认并同意，对于范围内个人数据的处理，客户是控制者，供应商是处理商，并且只能根据以下第 2.8.4. 节中的要求聘用分处理商。

2.4. 供应商应：

2.4.1. 仅根据客户的书面指示处理范围内个人数据；

2.4.2. 在获悉任何范围内个人数据存在任何错误或不准确之处时，立即通知客户；

2.4.3. 对于供应商、任何分处理商或任何供应商人员持有或控制的范围内个人数据的任何副本而言，当该等副本不再需要用于履行供应商在本协议项下的义务时，供应商应确保将其永久性销毁，但客户以书面形式另行指示或数据保护法规另有要求的除外；

2.4.4. 确保只有下述供应商人员能使用范围内个人数据：(i) 在供应商履行本协议项下义务的过程中，需要访问该数据以开展工作的供应商人员；(ii) 在数据的处理、看管和操作方面，受过关于数据保护法规要求的适当培训的供应商人员；以及 (iii) 负有关于范围内个人数据的合同保密义务或法定保密义务的供应商人员；以及

2.4.5. 在遵守第 2.15.. 条的前提下，在客户提出合理要求时，配合客户，向客户提供协助和信息以及签署所有相关文件，以协助客户遵守任何数据保护法规所要求的涉及任何范围内个人数据的义务，

2.4.6. 此外，供应商还应配合和遵守任何监管机构作出的涉及上述数据的指令或决定，且须在各情形中在所需时间内协助客户，以满足监管机构所施加的任何时间限制。

2.5. 就范围内个人数据（该数据的处理须符合欧盟或成员国法律）而言，供应商：

2.5.1. 不得（且应确保任何分处理商不得）将该等数据从任何国家或地区传输出去，亦不得要求任何客户进行该等传输，但以下情形除外：

2.5.2. 该数据传输在欧洲经济区成员国之间进行；

2.5.3.

客户作出书面指示，且该传输须符合客户规定的任何其他合理限制；以及

针对此类所拟议的数据类型之传输，供应商应在任何时候及时与客户签订协议（如果由分处理商传输或传输给分处理商，则应要求分处理商及时与供应商签订协议），且所签协议采用未经修订的示范条款，但应按照客户合理规定的方式或双方书面约定的其他形式来完成协议的签订。

2.6. 对于不适用第 2.5. 条规定的范围内个人数据（但其处理须符合任何数据保护法规，且该法规禁止或限制：

(a) 该范围内个人数据传输至任何国家或地区，或者

(b) 该范围内个人数据在任何国家或地区进行处理），

则供应商不得通过违反任何该等禁止或限制来传输或处理该范围内个人数据。

2.7. 供应商应：

2.7.1. 始终指定一名供应商人员（且以书面方式将该人员的身份告知客户的数据保护专员），该人员负责协助客户回答来自数据主体或任何监管机构的询问；

2.7.2. 确保第 2.7.1. 条所提及的供应商人员始终对该条款所述的问询作出及时且合理的回应，充分考虑数据保护法规对及时回应所作的相关要求；以及

2.7.3. 只有在相关客户作出书面指示时，方可对第 2.7.1. 条所述的任何询问采取相关行动。

2.8. 供应商：

2.8.1. 不得将任何范围内个人数据披露或传输给任何第三方，但以下情形除外：

2.8.2 依据客户书面指示以及第 2.5. 条所作的披露或传输；

2.8.3 数据保护法规或本协议的任何其他条款要求的情形；

2.8.4 就分处理商处理范围内个人数据而言：

(a) 应遵守本协议第 13.2. 条的规定（转让、分包）；

(b) 确保分处理商依据书面合同处理相关数据，且该分处理商承担的合同义务应与供应商根据本附表 3（数据保护：GDPR）承担的义务一致；

(c) 确保分处理商履行并遵守上述义务；以及

(d) 如果客户提出要求，供应商应确保分处理商与客户订立书面合同，且该分处理商承担的合同义务应与供应商根据本附表 3（数据保护：GDPR）承担的义务一致；

2.9. 供应商：

2.9.1. 应采纳、执行和维持数据保障措施，包括作为该数据保障措施之一部分的安全流程和实践，以保护范围内个人数据免遭未经授权或意外的访问或者破坏、丢失、修改、使用或泄露；

2.9.2. 向客户保证，供应商已制定了符合数据保护法规规定的供应商数据安全义务的书面安全政策、流程和实践；

2.9.3. 应在供应商提供本服务的各个设施以及针对处理范围内个人数据的任何及所有网络，维持和执行数据保障措施；以及

2.9.4. 应按照现行行业实践及客户的合理要求，不时审查和修改数据保障措施（且一经书面要求，应立即向客户提供该等修改的数据保障措施）。

2.10. 如果任何范围内个人数据遭到任何未经授权或意外的访问、使用或泄露，或者供应商有合理理由相信已发生该等访问、使用或泄露或存在发生该等访问、使用或泄露的风险（包括但不限于丢失任何存储或可能储存范围内个人数据的任何媒介、装置或设备，或无法明确定位该等媒介、装置或设备），供应商应：

2.10.1. 及时通知客户（但在任何情况下均须在二十四 (24) 小时内通知客户），并就该等访问、使用或泄露对客户的影响以及供应商已采取及即将采取的纠正行动提供合理的详细信息；

2.10.2. 在遵守第 2.15. 条的前提下，及时采取所有必要且合适的纠正行动，纠正造成该等访问、使用或泄露的根本原因；

2.10.3. 根据数据保护法规的要求采取有关该等访问、使用或泄露的任何行动，包括但不限于在客户提出要求时，向个人数据可能受到影响的数据主体发出通知，无论数据保护法规是否要求发出该通知均是如此；以及

2.10.4. 如果该等访问、使用或泄露使得数据主体的财务信息能够被获取，或可合理地认为存在身份盗窃或欺诈的风险，则供应商应在合理期限内（但不得少于一 (1) 年）向任何该等数据主体提供信用监控服务。

2.11. 除本协议规定的任何审计权利外，经客户要求并经客户合理决定，供应商还允许客户（自行或代表其客户）或客户指示的独立审计师审计和审查供应商和经批准的分处理商的信息安全计划、数据处理设施和数据保护合规计划，以验证是否符合本附表 3（数据保护：GDPR）、数据保护立法和客户或客户自身客户的义务（下称“数据保护和安全审计”）。

2.12. 此类数据保护和安全审计可包括旨在破坏供应商或经批准的分处理商的信息安全计划和相关安全措施的测试（包括安全渗透测试），且应在不少于提前 10 天发出书面通知的情况下进行。

2.13. 如果客户合理认为，数据保护和安全审计的结果发现供应商或经批准的分处理商所采取的安全措施存在缺陷，供应商应评估该缺陷，并在客户同意的时间范围内提供令客户满意的适合的解决方案。

2.14. 供应商承认，任何监管机构或其代理人可不时对供应商或任何经批准的分处理商进行审计，且任何此类审计不受到此类 2.11.、2.12.、2.13. 和 2.14. 条款中所述的任何限制的约束。

2.15. 客户：

2.15.1. 负责行使自身权利，在供应商代表客户处理个人数据时，指示供应商采取合理必要的措施，以便供应商履行其在本协议项下的义务；以及

2.15.2. 在数据保护法规允许的范围内，授权供应商代表客户向分处理商提供同等指示。

2.16. 供应商为遵守第 2.4. 条、第 2.10.2. 条、第 2.10.3. 条及第 2.10.4. 条所招致的费用应按照下述情况由相关方承担：

2.16.1. 如果因供应商、任何分处理商或任何供应商人员违反本协议，或者上述各方的任何过失、故意或欺诈行为或不作为，导致要求供应商采取相关行动，则相关费用应由供应商承担；以及

2.16.2. 在其他情况下，相关费用应由客户承担。

2.17. 应客户要求，供应商应在任何时候将客户作为唯一数据控制者且由供应商代表客户根据本协议处理的所有个人数据退还给客户和/或应客户要求从其系统中删除这些个人数据，供应商或其附属公司为遵守适用法律或法规要求而需要保留的任何备份副本除外，前提是根据本附表 3（数据保护）对此类副本加以保密和提供安全保护。

供应商代表签字

签名 _____

姓名 _____

职务 _____

供应商名称 _____

日期 _____