AppGallery Connect数据处理附录

最后更新日期：2022年7月11日

接受如下所述条款的客户（简称“客户”）及《华为开发者服务协议》中所指的华为公司（二者统称“双方”或单独称为“一方”或“该方”）已签署服务协议（简称“协议”），约定由华为向客户提供AppGallery Connect（AGC）服务（服务清单详见《AppGallery Connect 协议包》。该服务清单明确提及本《AppGallery Connect数据处理附录》。本《AppGallery Connect数据处理附录》将不定期修订。）

本《AppGallery Connect数据处理附录》（简称“数据处理附录”或“DPA”）签署人，不论以何种方式签署或接受本DPA，声明和保证其经过合法授权、具备签署本DPA的法律行为能力、能够代表该方签署本DPA并确保本DPA经其签署后对该方产生法律效力。

本DPA自生效日期（详见下文）开始生效并取代双方在此之前签订的任何数据处理及安全条款。

1. 简介

本DPA反映了双方协议中就华为向客户提供所需的AGC服务过程中涉及的客户数据处理及安全保障条款。

本DPA仅对客户完成签署的客户华为帐号有效。如果客户拥有多个华为帐号，则需为每个帐号单独签署DPA。

本DPA作为协议的补充内容，在此情况下适用于协议双方：华为在向客户提供AGC服务的过程中，作为数据处理者代表客户处理其个人数据。

本DPA仅对注册了华为帐号的自然人/法人实体有效和产生法律效力、仅对向各个华为帐号直接提供的AGC服务有效和产生法律效力。

如果协议的任何附带文档、附录、附件或附表与协议发生冲突，则各个文档之间的服从优先级按以下顺序，编号数字大的文档优先于编号数字小的文档：

（1）协议；

（2）DPA；

（3）标准合同条款（如存在个人数据转移的情况，则《附件2》包含其所有附件）；

（4）数据传输协议（附件3）。

2. 定义

2.1 在本DPA中使用但未在本DPA中进行定义的术语与其在协议中的定义一致。在本DPA中，除非另有规定：

华为帐号与《华为开发者服务协议》中的华为帐号含义相同。

“附加产品”：指华为或第三方提供的产品、服务或应用。这些产品：（a）并非AGC服务的组成部分；和（b）可在AGC服务的用户界面中使用或者可以与AGC服务集成。

“关联公司”的含义与协议中的定义一致。如果协议中未进行定义，则指直接或间接对某实体进行控制、受其控制或处于共同控制的任何实体或其它实体。“控制”指一方直接或间接持有受控方或共同控制方百分之三十（30%）及以上的董事会成员（或其他管理层）的表决权股份或其它证券。

“适用法律法规”：指任何给定时间适用于客户个人数据处理的隐私或数据保护法律、法规及规定，例如GDPR以及任何取代前者的法律和法规（如适用）。

“客户数据”：指客户或客户的最终用户通过华为帐号使用服务而提供的个人数据。

“客户的最终用户”：指使用客户服务的用户（例如，使用客户应用的用户）。

“客户个人数据”：指客户数据中包含的个人数据。

“生效日期”：指客户或协议双方接受或签署本DPA的日期。

“EEA”：指着欧洲经济区。

“GDPR”：指《通用数据保护条例》，即2016年4月27日由欧洲议会及理事会通过的关于保护自然人个人数据处理及个人数据自由流动的第679号条例。GDPR取代了《数据保护指令》95/46/EC。

“华为第三方审计师”：指由华为指定的、具备相关资质的、独立的第三方审计师，届时其身份由华为向客户披露。

“ISO 27001认证”：指对所审计服务开展的ISO/IEC 27001:2013认证或同等级别的认证。

“邮件通知地址”： 指客户在AGC中指定的电子邮箱地址，用于接收华为发送的特定通知。

“个人数据泄露”： 指违反安全规定，导致华为系统中保存的客户数据或由华为处理的客户数据遭到意外或非法破坏、丢失、篡改、非法泄露或访问的情况。“个人数据泄露”不包括第5.7款中描述的安全事件。

“安全措施”： 包含第4.1.1款中的定义。

“安全文档”： 指华为按照第4.4.1款要求提供的所有证书。

“服务”包含《华为开发者服务协议》中定义的“按照客户在华为开发者联盟平台上签署的各种协议，由华为向客户提供的所有服务”。

“子数据处理者”： 指经由本DPA授权，获得客户数据的逻辑访问权限并对客户数据进行处理，以提供部分服务的第三方。

“服务期限”： 指从生效日期到华为停止提供服务的期限，包括适用情况下的任何服务暂停期以及协议终结后华为继续提供服务的过渡期。

“第三国”： 既不属于欧洲经济区也未被欧盟委员会根据GDPR第45条规定的机制认可为能够提供充分数据保护的国家和/或地区。

“欧盟标准合同条款”： EU Standard Contractual Clauses（EU SCC），即欧盟委员会根据欧洲议会和欧洲理事会第2016/679号条例（欧盟），于2021年6月4日宣布了2021/914号决定，并根据该决定发布了关于向第三国传输个人数据的合同条款。所述合同条款即为“标准合同条款”。

2.2　本DPA中使用的“个人数据”、“数据主体”、“数据处理”、“数据控制者”、“数据处理者”、“监管机构”等术语含义与适用法律法规里的定义相同。条款2.1里的术语定义与适用法律法规不一致的，以适用法律法规的定义为准。

3. 角色、数据处理范围和一般义务

3.1 双方确认并同意：

3.1.1　依据本DPA开展的个人数据处理活动中，根据适用法律法规规定，客户应视为数据控制者而华为视为数据处理者。

3.1.2　各方承诺遵守其在适用法律法规下的义务。各方仅负责履行其适用法律法规规定的义务。在双方之间，客户应对个人数据的准确性、质量和合法性以及客户获取个人数据的方式承担全部责任。

3.1.3 数据处理者应仅在本DPA范围内和/或按照协议向客户提供AGC服务的必要情形下对个人数据进行处理。

3.1.4 华为对客户的个人数据进行处理，目的是为了向客户提供AGC服务。除此之外，华为不得以其他目的使用客户的个人数据。

3.1.5 协议和本DPA应视为客户对华为处理其个人数据的指令要求。客户如要求华为执行协议和/或本DPA范围之外的其它指令要求（如有），需由客户及华为事先通过书面协议进行约定，包括华为执行这些额外指令要求产生的额外费用及客户的应付款。如果华为拒不执行客户对本DPA或协议指令进行的合理变更或在本DPA或协议范围之外新增的合理指令要求，客户有权终止本DPA和协议。

3.1.6 除非适用法律要求华为采取其他方式来处理客户的个人数据，华为将严格遵循第3.1.5款中的指令要求。如出现适用法律要求采取其他处理方式的，华为将在数据处理前通过邮件通知地址知会客户（除非适用法律以保护公共利益为由，禁止华为向客户发出邮件）。

3.1.7 为向客户提供AGC服务，华为将遵从适用法律法规以及其他可适用于华为的法律对客户的个人数据进行处理。

3.2 在不影响第3.1.1款效力的前提下，当客户作为数据处理者、华为作为子数据处理者时，客户向华为保证其有关客户个人数据的指令和行为，包括将华为指定为子数据处理者，经过数据控制者合法授权。

3.3 如果客户要求华为遵守其他不适用于华为处理客户个人数据的隐私或数据保护法律法规，华为有权自行决定（i）当遵从客户要求的数据保护法律或法规超出了合理的费用范围，可拒绝此客户要求；或（ii）当遵从客户要求的数据保护法律或法规在合理的费用范围内，经华为确定费用并经客户支付后，华为可遵从该客户要求。

3.4 如果客户使用附加产品，服务可允许该附加产品根据实际情况访问客户个人数据，以实现该附加产品与服务之间的互联互通。需要说明的是，本DPA不适用于任何客户使用的附加产品中的个人数据的处理，包括该附加产品传入和传出的个人数据。

4. 数据安全

4.1 华为的数据安全措施、控制机制及协助

4.1.1 华为的数据安全措施

依据通用行业标准，华为从物理、技术和组织层面实施恰当的安全措施来保护客户数据在整个生命周期内的安全，避免数据泄露、损坏或丢失并确保客户数据的保密

性、完整性和可用性。这些安全措施包括但不限于对通信和存储进行加密、控制对数据中心的访问、最小化授权和记录个人数据系统的访问情况。安全措施详情请参阅附件1。为及时应对新安全威胁和漏洞，华为应不定期更新安全措施，以确保服务的总体安全。

4.1.2 华为员工及子数据处理者对安全措施的遵从

华为将采取恰当措施、根据其员工、分包商及子数据处理者的职责范围，确保其对安全措施的遵从，包括确保所有获得授权后对客户个人数据进行处理的人员忠实履行其对客户个人数据的保密承诺或依法承担相应的客户个人数据保密义务。

4.1.3 其他数据安全控制机制

作为安全控制机制之一，华为将定期对AGC的安全措施开展内部或独立的第三方测试，以验证AGC安全措施的效用并持续更新相关安全证书。

4.1.4 华为提供的数据安全协助

客户同意华为（基于客户个人数据处理的性质、华为可获得的相关信息及避免该信息泄露做出的限制，如保密性要求）以下述方式协助其履行在个人数据安全、个人数据泄露方面的职责，包括适用法律法规对客户职责的适用规定，包括GDPR第32款至34款（含）（如适用）：

a) 依据第4.1.1款（“华为的数据安全措施”）实施和维护数据安全措施；

b) 遵从第5款（“个人数据泄露”）的要求；及

c) 依据第4.4.1款（“安全文档评审”）要求，向客户提供安全文档以及相关协议包括本DPA要求的信息。

4.2 客户的安全职责及安全评估

4.2.1 客户的安全职责

客户同意，在不影响华为依据第4.1款（“华为的数据安全措施、控制机制及协助”）及第5款（“个人数据泄露”）履行义务的条件下：

a) 客户仅对其使用服务的行为负责，包括：

i. 恰当地使用业务，确保客户数据相关的风险受对应层级安全措施的控制；

ii. 确保账户认证凭证、客户访问服务所使用的系统和设备安全；

iii. 按需备份客户数据；及

b) 华为无义务保护由客户自行决定向华为及其子数据处理者系统（如，离线或线下存储设备）储存或传输的客户数据副本的安全。

4.2.2 客户安全评估

4.2.2.1 客户仅负责评审安全文档并从自身角度评估服务、安全措施、其它安全控制机制和华为在第4款（“数据安全”）下的承诺是否满足客户需求，包括该客户根据适用法律法规应遵从的相关安全义务。

4.2.2.2 客户承认并同意（基于当前最先进的安全技术、实施成本及客户个人数据处理的性质、范围、上下文和目的以及对个人产生的风险等因素考虑），华为实施和维护的安全措施（详见第4.1.1款（“华为的数据安全措施”）能够针对客户数据相关风险给予对应层级的安全保护。

4.3 安全认证和报告

为确保安全措施持续有效，华为应开展如下活动：

4.3.1 华为将通过独立的外部审计对其安全措施的充分性进行验证。

4.3.2 审计：（i）依据ISO 27001标准或其他同等标准；（ii）定期开展；且（iii）由华为选择的第三方独立审计师完成，审计费用由华为承担。

4.3.3 审计的输出包括（a）相关证书（安全文档）；及（b）审计报告。该审计报告作为华为保密信息处理。

4.4 遵从性评审和审计

4.4.1 安全文档评审

除本DPA要求的信息之外，应客户要求且如果双方已经签署适用的保密协议（NDA），华为将向客户提供安全文档以及其它华为认为能够证明其如实履行本DPA下义务的必要文档。

4.4.2 客户的审计权

若客户按照第4.4.1款对华为安全文档开展的评审不足以验证华为对本DPA所负义务的履行情况，则：

a) 华为将允许客户或由客户指定的独立审计师开展审计（包括检验），以按照第4.4.3款（“其它评审和审计条款”）来验证华为对本DPA下所负义务的履行情

况。华为将按照第4.3款（“安全认证和报告”）和第4.4款（“遵从性评审和审计”）的要求充分支持此类审计。

b) 如果客户已经签署了第8款（“数据存储位置和传输”）中介绍的标准合同条款，华为将在不影响监管机构在此标准合同条款下的任何审计权的情况下，允许客户或由客户指定的独立审计师按照第4.4.3款（“其它评审和审计条款”）开展标准合同条款中规定的审计。

4.4.3 其它评审和审计条款

4.4.3.1 如果客户希望开展第4.4.1款和第4.4.2款中提及的评审或审计，必须向华为提交书面申请。

4.4.3.2 收到第4.4.3.1款要求的书面申请后，华为和客户将共同商议并确定合理的评审/审计开始日期、范围和时长以及适用于第4.4.2款下审计的安全及保密性控制机制。

4.4.3.3 审计将仅针对用于验证华为对本DPA的遵从所需的材料开展，不包含任何华为依据合同要求进行保密的材料。

4.4.3.4 针对按照第4.4.2款开展的审计，华为可（依据产生的合理费用）向客户收取相关费用。这种情况下，华为将在审计开展前向客户提供相关费用的详情以及费用计算依据。客户负责向其指定的审计师支付此类审计费用。

4.4.3.5 华为可通过书面形式，拒绝采用客户指定的审计师来开展第4.4.2款中的审计，条件是：华为有充分的理由证明此审计师不具备相关资质或独立性，是华为的竞争对手、或其他明显不合适的情况。这种情况下，客户需指定其它审计师或自行开展审计。

5. 个人数据泄露

5.1 根据适用法律法规，华为应在发现个人数据泄露后立即通知客户，不得延误。根据获取的信息，华为应向客户发出包含如下内容的通知：

a) 个人数据泄露的性质，（条件允许的情况下）包括涉及的数据主体类型和大致数量；

b) 华为数据保护官或其他接口人的姓名及联系方式，以方便客户获取更多相关信息；

c) 个人数据泄露可能导致的后果；

d) 为解决个人数据泄露问题已经采取的措施，包括减轻不利影响的恰当措施。

5.2 如果上述信息无法随通知提供，应在获取到这些信息后立即发给客户。

5.3 华为将立即采取必要、恰当的措施对个人数据泄露情况进行调查、减轻影响、修复问题并向客户提供协助，确保客户能够履行其在数据保护立法下的个人数据泄露相关义务。

5.4 此类数据泄露事故通知应发至邮件通知地址或由华为自行决定直接沟通（例如，通过电话或面对面会议）。客户仅负责确保通知邮件通知地址最新、有效。

5.5 华为不会为了识别特定法律要求的信息而对客户数据的内容进行评估。在不影响华为履行第6款（“向数据控制者提供协助”）下所负义务的情况下，客户仅负责遵从适用其自身的事故通知法和履行数据事故相关的第三方通知义务。

5.6 华为根据第6款（“向数据控制者提供协助”）发出的通知或采取的响应措施不应解释为华为承认相关数据事故是华为的过错或责任。

5.7 客户同意，不将无效的安全事故纳入第5款（“个人数据泄露”）范畴。无效的安全事故指未导致客户数据或华为用于存储客户数据的任何设备或设施被非法访问的事故，包括但不限于通过Ping或其他广播攻击防火墙或边缘服务器、端口扫描、登录尝试、DoS攻击、包嗅探（或通过其他方式非法访问流量数据但未能访问数据头部之外的其它内容）进行非法访问但未能成功的事故或类似事故。

6. 向数据控制者提供协助

6.1 根据适用法律法规要求以及数据处理的性质和可获得的信息，华为应就如下事宜向客户提供合理支持：

6.1.1 确保遵从数据控制者根据适用法律法规应承担的义务；

6.1.2 向数据控制者提供所有合理、必要的信息，证明对适用法律法规的遵从；

6.1.3 如适用，开展GDPR第35和36款规定的必要的数据保护影响评估和事先咨询；

6.1.4 提供协议，包括本DPA要求的信息。

6.2 如果客户要求提供且华为按第6.1款要求提供的协助不属于AGC服务，也不是华为的相关日常活动，则华为可向客户收取此协助产生的合理费用。

6.3 华为应按照适用法律法规要求保留其代表客户开展的所有类别的数据处理活动记录。同样，如有要求，客户应通过开发者联盟网站的管理中心向华为提供相应信息，并保证所有信息的准确性。

6.3.1 如适用，数据处理记录应包含GDPR第30.2款要求的信息。

6.3.2 应要求，华为应向监管机构提供这些信息。

6.3.3 华为应保留电子版的数据处理记录。

7. 数据主体权利

7.1　根据适用法律法规要求，华为按照如下条款7.2至7.4向客户提供与AGC服务功能一致的技术能力，协助客户履行对数据主体请求承担的义务。客户将获权访问AGC，从而获取这些能力。

7.2　华为应在不违背AGC服务功能的情况下允许客户在服务期限内删除客户数据。客户使用删除能力删除客户数据后，将无法恢复这些数据。华为将遵从客户的删除指令和适用法律，尽快在30天内将客户数据从华为系统中移除，除非华为遵循的任何适用法律或法规要求华为以更长的期限去保留这些数据。

7.3　在服务期限内，华为与数据主体不产生直接关系且应在收到客户个人数据相关的数据主体请求后，通过合理的方式通知数据主体首先联系客户。客户将负责响应此类数据主体请求，包括根据情况使用AGC服务提供的功能来响应此类请求。

7.4 华为应尽力配合客户、协助客户就此类请求、投诉、指令或其他第7.1款中提及的文书采取相关行动。在合理的范围内，基于数据处理的性质、华为可获得的信息、行业实践和费用，华为将实施恰当的技术和组织措施，向数据控制者提供所需的合作与协助。如果华为认为客户要求的协助超出了上述合作与协助的范畴，华为可向客户收取合理费用。

8. 数据存储位置和传输

8.1　华为应将客户数据保存在与客户沟通达成一致的数据中心，不得保存在其它位置。客户个人数据位于由客户选择的业务区域决定的数据中心内，除非华为在《**数据处理信息**》的“数据存储位置选择例外情况”章节中明确定义了不同的解决方案。点击**AppGallery Connect数据中心**即可获得相关数据中心信息。

8.2　受提供AGC服务的华为实体所处的场所位置、客户场所位置或客户数据主体的位置影响，华为开展的数据处理活动可能受华为与客户达成一致的《标准合同条款》或《数据传输协议》管辖。欧盟根据各方的角色制定了不同的标准合同条款。第8.2条列出了这些角色组合及其法律后果。

8.2.1　如果客户和/或由华为提供的AG　Connect服务，按照《华为开发者服务协议》第15.2条应遵从GDPR，且华为卷入了第三国成立的子数据处理者或子数据处理者在第三国处理个人数据：

- 华为应按照需要，与在第三国成立的子数据处理者执行《模块三：数据处理者向数据处理者转移数据》。在该角色组合中，客户不是《标准合同条款》的签约方。

- 在这种情况下，根据条款1和《附录1：标准合同条款》，华为的子数据处理者应作为“数据进口方”，华为应作为“数据出口方”。

8.2.2 如果客户在第三国成立，并按照《华为开发者服务协议》第15.2条与华为签订此DPA，则双方同意：

- 双方执行此DPA，即视为双方已执行标准合同条款的《模块四：数据处理者向数据控制者转移数据》（附件2）；

- 根据条款1和《附录1：标准合同条款》，华为应作为“数据出口方”，客户应作为“数据进口方”；

- 在《标准合同条款》的第7条里，双方选择包含“对接条款”；

- 在《标准合同条款》的第11条里，双方并未选择任择申诉机制；

- 在《标准合同条款》的第17条里，双方选择“选项1”，管辖法律应为爱尔兰法律；

- 在《标准合同条款》的第18条里，双方选择解决与标准合同条款相关的争议的适用法院为在都柏林具有管辖权的爱尔兰法院；

- 标准合同条款的《附录I》B部分所需的信息记录在文件后面；以及

- 主管监督机构为爱尔兰数据保护委员会（Irish Data Protection Commission）。

8.2.3 在GDPR不适用于数据处理的角色组合中，华为和客户都应遵守《附件3》。

8.3 在不影响第9.2条的前提下，应适用法律要求，华为可将该法律要求知会到客户后开展数据传输，除非出于重要的公共利益考虑，该法律禁止华为知会客户。

8.4 如果按照第8.2条或第9.2条的数据传输，应适用法律法规要求，需要获得相关机构的审批，客户应在数据传输前获得所述审批。客户及华为同意，在相关机构要求或适用法律法规要求的前提下，在相关机构留存和/或提交（如适用）一份协议副本。

9. 子数据处理者

9.1 华为将雇佣子数据处理者进行数据处理活动。应适用法律法规要求，华为将要求子数据处理者实施数据保护义务，尤其是与实施恰当的技术和组织措施相关的义务。这些义务绝大部分与本DPA要求相同。客户特此向华为进行一般性授权，允许华为雇佣子数据处理者。华为应通过AGC或其他恰当的方式向客户提供子数据处理者的雇佣关系变化或替换信息。客户可以访问Aspiegel SE的子数据处理者清单，**华为服务（香港）有限公司的子数据处理者清单**以及华为软件技术有限公司的**子数据处理者清单**以获悉相关子数据处理者信息。客户将被视为已于生效日期接受所述清单中的所有子数据处理者。

9.2 客户特此授权华为，在以下情况下，以客户名义，代表客户与子数据处理者签订包含附件3《数据传输协议》的数据处理协议：

- 按照第9.1条雇佣的子数据处理者在客户和/或华为所在国范围之外成立或处理客户数据，且适用法律法规要求签订《数据传输协议》；且

- 如上文规定，适用法律法规不要求签订相关标准合同条款。华为应在《数据传输协议》中明确表示其行为代表客户。客户应考虑第8.4条。

9.3 客户有权于知晓新的子数据处理者后的14天内于该网页（https://developer.huawei.com/consumer/cn/support/feedback）向华为发出书面通知，阐明合理原因并拒绝采用该子数据处理者。如果华为不顾客户按照第9.3款提出的反对，仍然决定雇佣该子数据处理者，则客户有权终结协议。

9.4 如果华为使用子数据处理者，则华为应根据适用法律法规，仍然全权对客户负责，确保客户在本DPA下的义务得以履行。

10. 违约责任

10.1 如果一方直接违反其在本DPA下的承诺，则该方对另一方遭受的损失负责，但必须遵守协议中的责任限制和责任排除规定。

10.2 如果客户并未违反本DPA，华为应保护客户免受任何因华为违反其在本DPA下的数据保护承诺而导致第三方对客户发起的任何索赔或法律程序（包括合理的律师费）。华为有权主导对此索赔或法律程序的调查并应自费雇佣律师处理该索赔或法律程序、进行抗辩。

10.3 不论本DPA中其它条款作出何种规定，在不与标准合同条款矛盾的前提下，一方不对另一方的下述事宜负责：

a) 利润损失；

b) 业务损失；

c) 收入损失；

d) 商誉损失或其他类似损失；

e) 预期节余；

f) 使用损失；

g) 任何惩罚性的、其它间接或连带损失或损害。

11. 对本DPA进行变更

11.1 华为可不定期对本DPA中引用的URL及该URL所指的内容进行变更。

11.2 满足如下条件，则华为可对本DPA实施变更：

a) 变更已明确经本DPA同意，包括第11.1款中提及的变更；

b) 法人实体的名称或形式发生变化；

c) 按要求遵循适用法律、法规、由政府监管方或机构发布的法庭令或指令；或

d) 变更不会导致：（I）服务的总体安全性下降；（ii）华为按照第3.1款（“华为对客户指令的遵从”）开展客户数据处理的范围扩大或约束范围缩小；（iii）经华为判断，对客户在本DPA下的权利有实质性的负面影响。

11.3 如果华为因第11.2（c）或（d）款的原因需要对本DPA进行变更，则华为应通过下述任一方式，在变更生效前的30天内（或按适用法律、法规、由政府监管方或机构发布的法庭令或指令要求的周期），向客户发出通知：（a）向邮件通知地址发送电子邮件；或(b)通过AGC向客户发出通知。如果客户拒绝此类变更，则客户可在收到华为变更通知的90天内于该网页（https://developer.huawei.com/consumer/cn/support/feedback）向华为发送书面通知终止协议。

12. 服务期限与终止

12.1 本DPA于生效日期生效，直至协议终结或届满。不论协议终结或届满规定为何，本DPA将持续有效，直至华为按照第12.2款删除所有客户数据后方能自动失效。

12.2 华为应在本DPA终结或届满时，按照适用法律法规要求从华为系统删除所有客户数据（包括已有的数据副本）。华为将遵从该删除指令，尽快在30天内将客户数据从华为系统中移除，除非适用的法律法规要求华为保留这些数据。

12.3　客户承认并同意，由客户负责在协议到期或本DPA终结前将其希望保留的客户数据导入到自己的系统中。

附件1：数据安全措施

自生效日期起，华为将实施和维护本附件1中确定的安全措施：华为可对这些安全措施不定期更新或修改，但前提是此类更新或修改不会导致AGC服务的总体安全性下降。

1. 数据中心和网络安全

华为采用第三方数据中心。这些数据中心分散于选定区域内的不同地理位置，其云服务供应商必须具备充分的安全措施。

2. 数据

（a）数据存储和隔离

华为在第三方服务器中的多租户环境内存储数据。数据和文件系统架构在多个位于不同地理位置的数据中心之间重用。华为对客户数据采取逻辑隔离。

（b）磁盘报废和擦除策略

存储了数据的磁盘可能出现性能问题、错误或硬件失效，因此需要报废（“报废的磁盘”）每个报废的磁盘都应交由数据中心操作员对其实施一系列数据销毁操作。

3. 访问控制

3.1 客户的数据访问

客户的管理员必须通过集中认证系统的双因子认证方能管理服务。

3.2 内部数据访问策略

华为采用集成在LDAP系统的集中访问管理系统来控制人员对生产服务器的访问且仅向获得授权的少部分人提供基于角色的访问权限。

华为使用唯一的用户ID、强健的密码、双因子认证和受控的访问清单，从最大程度上降低非法使用账号的可能性。访问权限的授予或修改基于：授权人员的职责、开展授权任务所需的职责要求以及“按需”原则。

4. 人员安全

华为人员必须遵从公司关于保密、职业道德、恰当使用资源和职业化方面的规范。华为将在法律允许的范围内，按照适用的劳动法律和法规对华为人员开展恰当的背景调查。

华为人员必须执行保密协议并确认知悉和遵从华为的保密及隐私保护策略。华为人员将接受安全培训和定期评估，以了解其安全及隐私保护策略的掌握情况。此外，华为应定期向华为人员发送全球最新的安全新闻，以帮助其提升安全意识。处理客户数据的华为人员必须完成适用其角色的其它要求（如，华为网络安全认证）。未经授权，华为人员不得处理客户数据。

附件2：标准合同条款

模块四：数据处理者向数据控制者转移数据

第一节

第1条

目的和范围

(a) 这些标准合同条款的目的是确保遵守欧洲议会和理事会2016年4月27日关于在个人数据处理中对自然人的保护以及此类数据的自由流动的欧盟第2016/679号条例（《一般数据保护条例》）的要求，用于将个人数据转移到第三国。

(b) 缔约方：

(i) 附录I.A中所列的转移个人数据的自然人或法人、公共机构、机关或其他机构（“实体”），以下称为“数据输出方”；以及

(ii) 附录I.A中所列的直接或通过其他实体（本条款缔约方）间接从数据输出方接收个人数据的第三国实体，以下称为“数据输入方”。

均已同意这些标准合同条款（“条款”）。

(c) 本条款适用于附录I.B中规定的个人数据转移。

(d) 本条款的各个附录是本条款的组成部分。

第2条

条款的效力和不变性

(a) 本条款规定了适当的保护措施，包括根据欧盟第2016/679号条例第46条第1款和第46条第2款（c）项中关于可执行的数据主体权利和有效的法律救济措施，以及欧盟第2016/679号条例第28条第7款中关于从控制者向处理者和/或从处理者向处理者转移数据、标准合同条款等，前提是除非选择适当的模块或附录中的信息有所增加或更新，否则不得修改这些保护措施。这并不妨碍各方将本条款中规定的标准合同条款纳入更广泛的合同中，和/或在此基础上增设其他条款或额外保护措施，前提是这些内容不直接或间接与标准合同条款冲突，也不损害数据主体的基本权利和自由。

(b) 本条款不影响数据输出方根据欧盟第2016/679号条例承担的义务。

第3条

第三方受益人

(a) 数据主体可以作为第三方受益人向数据输出方和/或数据输入方发起并实施本条款，但以下情况除外：

(i) 第1条、第2条、第3条、第6条、第7条；

(ii) 第8.1条（b）款和第8.3条（b）款；

(iii) N/A

(iv) N/A

(v) 第13条；

(vi) 第15.1条（c）款、（d）款和（e）款；

(vii) 第16条（e）款；

(viii) 第18条-模块一、模块二和模块三：第18条（a）款和（b）款；模块四：第18条。

(b) （a）款并不妨碍欧盟第2016/679号条例规定的数据主体权利。

第4条

解释

(a) 如果本条款中使用了已在欧盟第2016/679号条例中定义的术语，这些术语的含义与该条例保持一致。

(b) 本条款应根据欧盟第2016/679号条例的规定进行阅读和解释。

(c) 本条款的解释不得与欧盟第2016/679号条例规定的权利和义务相抵触。

第5条

位阶

如果本条款在达成或订立时与合同各方已存在的相关协议的条款存在矛盾之处，以本条款为准。

第6条

关于转移的说明

附录I.B中具体说明了转移的详细信息，尤其是转移的个人数据的类型以及转移的目的。

第7条

对接条款

(a) 非本条款缔约方的实体可在各方同意的情况下，通过完成附录并签署附录I.A，随时作为数据输出方或数据输入方加入本条款。

(b) 一旦完成附录并签署附录I.A，加入实体应被视为本条款的缔约方，并按照附录I.A中的规定，具有数据输出方或数据输入方的权利和义务。

(c) 在成为缔约方之前，加入实体不具有任何本条款规定的权利和义务。

第二节：各方义务

第8条

数据保护措施

数据输出方保证其已尽合理努力确定数据输入方能够通过实施适当的技术和组织措施履行本条款规定的义务。

1.2 **指示**

(a) 数据输出方应仅基于作为其控制者的数据输入方的书面指示处理个人数据。

(b) 如果数据输出方无法遵守这些指示，包括如果这些指示违反了欧盟第2016/679号条例或其他欧盟或成员国数据保护法律，则数据输出方应立即通知数据输入方。

(c) 数据输入方应避免采取任何可能阻止数据输出方履行其欧盟第2016/679号条例下的义务的行动，包括子处理者处理或与主管监管机构合作的情形。

(d) 在终止提供处理服务后，数据输出方应根据数据输入方的选择，删除其代表数据输入方处理的所有个人数据，并向数据输入方证明此类数据已删除，或将所有其代表数据输入方处理的个人数据返还给数据输入方并删除已有副本。

2.2 **处理安全**

(a) 缔约方应实施适当的技术和组织措施以确保数据的安全（包括在传输过程中的安全），并防止导致意外或非法破坏、丢失、篡改、未经授权披露或访问（“个人数据泄露”）。在评估安全级别是否适当时，他们应适当考虑最新技术、实施成本、个人数据的性质、处理的性质、范围、背景和目的以及数据处理给数据主体带来的风险，尤其要考虑在可以实现处理目的的情况下，进行加密或假名化处理（包括在传输过程中）。

(b) 数据输出方应协助数据输入方根据（a）款的规定确保数据的适当安全。如果数据输出方根据本条款处理的个人数据发生泄露，数据输出方应在知悉数据泄露后立即通知数据输入方，并协助数据输入方处理泄露事件。

(c) 数据输出方应确保授权处理个人数据的人员已承诺保密或承担适当的法定保密义务。

3.2 **记录与合规**

(a) **缔约方应能够证明其遵守本条款的规定。**

(b) **数据输出方应向数据输入方提供所有必要的信息，以证明他们遵守了本条款中规定的义务，以满足审计要求。**

第9条

子处理者的使用

不涉及。

第10条

数据主体权利

缔约方应相互协助，根据适用于数据输入方的本地法律或欧盟第2016/679号条例响应数据主体关于欧盟境内数据输出方的数据处理相关的问询和请求。

第11条

补偿

(a) 数据输入方应以透明、易获取的形式，通过个人通知或在其网站，告知数据主体授权处理申诉的联系人。数据输入方应及时处理数据主体的任何申诉。

第12条

赔偿责任

(a) 缔约方应就其因违反本条款而给其他各方造成的任何损害进行赔偿。

(b) 缔约方应就其因违反本条款下的第三方受益人权利而给数据主体造成的任何物质或非物质损害，对数据主体承担赔偿责任，数据主体有权获得赔偿。这不影响数据输出方根据欧盟第2016/679号条例承担的赔偿责任。

(c) 如有多方应对因违反本条款而给数据主体造成的任何损害负责，其应负连带责任，而数据主体有权针对其中任何一方向法院提出诉讼。

(d) 各方同意，如果一方根据（c）款的规定承担责任，它有权向另一方/其他各方就其对损害的责任进行相应索赔。

(e) 数据输入方不得援引处理者或子处理者的行为来逃避其本身的赔偿责任。

第13条

监管

不涉及。

第三节：公共机构访问数据的情况下的本地法律和义务

第14条

影响遵守本条款的本地法律和实践

（注：适用于欧盟处理者将从第三国控制者收到的个人数据与处理者在欧盟收集的个人数据合并的情况下。）

(a) 缔约方保证，其没有理由相信适用于数据输入方处理个人数据的第三方目的地国的法律和实践（包括任何披露个人数据的要求或授权公共机构访问的措施）会妨碍数据输入方履行本条款规定的义务。这基于以下理解：在本质上尊重基本权利和自由且不超出民主社会中为保障欧盟第2016/679号条例第23条第1款所列的任何目标的必要且相称的法律和实践，与本条款并不矛盾。

(b) 缔约方声明，在提供（a）款中的保证时，他们特别考虑了以下要素：

(i) 转移的具体情况，包括处理链的长度、所涉及参与者数量以及使用的传输渠道、打算进行的再转移、接收方的类型、处理目的、转移数据的类型和形式、转移发生的经济领域、转移数据的存储位置；

(ii) 鉴于转移的具体情况，第三方目的地国的法律和实践，包括需要向公共机构披露数据或授权这些机构访问的法律和实践，以及适用的限制和保护措施；

(iii) 为补充本条款下的保护措施而制定的任何相关合同、技术或组织保护措施，包括在传输中和在目的地国处理个人数据时采取的措**施。**

(c) 数据输入方保证在根据（b）款进行评估时，已尽最大努力为数据输出方提供了相关信息，并同意将继续与数据输出方合作以确保遵守本条款。

(d) 各方同意记录根据（b）款进行的评估，并按要求将其提供给主管监管机构。

(e) 数据输入方同意，在同意本条款后，并且在合同有效期内，如果有理由相信数据输入方正在或已经受到不符合（a）款要求的法律或实践的约束，则立即通知数据输出方，包括在第三国法律发生变化后或措施（如披露请求）表明在实践中适用了不符合（a）款要求的此类法律。

(f) 在根据（e）款发出通知之后，或者如果数据输出方有理由认为数据输入方不能继续履行本条款规定的义务，则数据输出方应立即确定适当的措施（例如，确保安全性和保密性的技术或组织措施），由数据输出方和/或数据输入方采取这些措施来解决这种情况。如果数据输出方认为无法确保适当的安全措施或者基于主管监管机构的指示，则应暂停数据转移。在这种情况下，只要涉及本条款规定的个人数据处理，数据输出方应有权终止合同。如果合同涉及两个以上的缔约方，除非各方另有约定，否则数据输出方只能对相关缔约方行使终止权。当根据本条款终止合同时，应适用第16条（d）款和（e）款。

第15条

公共机构访问数据的情况下数据输入方的义务

（注：适用于欧盟处理者将从第三国控制者收到的个人数据与处理者在欧盟收集的个人数据合并的情况下。）

1.2 **通知**

(a) 以下情况下，数据输入方同意及时通知数据输出方，并在可能的情况下及时通知数据主体（如有必要，在数据输出方的帮助下)；

(i) 收到公共机构（包括司法机构）根据目的地国法律发出的具有法律约束力的请求，要求其披露根据本条款转移的个人数据；此类通知应包括要求披露的个人数据的信息、提出请求的机构、请求的法律依据和提供的答复；或

(ii) 意识到公共机构根据目的地国的法律直接访问了根据本条款转移的个人数据；此类通知应包括输入方可获取的所有信息。

(b) 如果根据目的地国的法律，数据输入方被禁止通知数据输出方和/或数据主体，则数据输入方同意尽其最大的努力来获得对该禁令的豁免，以期尽快并尽可能多地传递信息。数据输入方同意记录其做出的最大努力，以便能够根据数据输出方的要求进行展示。

(c) 在目的地国法律允许的范围内，数据输入方同意在合同期限内定期向数据输出方提供与收到请求有关的尽可能多的信息（尤其是请求的数量、请求的数据类型、提出请求的机构、请求是否受到质疑以及此类质疑的结果等）。

(d) 数据输入方同意在合同期限内保存根据（a）至（c）款规定的信息，并按要求将其提供给主管监管机构。

(e) （a）至（c）款不妨碍数据输入方根据第14条（e）款和第16条规定的义务，在无法遵守本条款的情况下及时通知数据输出方。

2.2 **合法性和数据最小化审查**

(a) 数据输入方同意审查披露请求的合法性，特别是披露请求是否仍在提出请求的公共机构的权力范围内，如果经过仔细评估后得出结论认为，根据目的地国的法律、国际法规定的适用义务和国际礼让原则，有合理理由认为该请求是非法的，则对请求提出质疑。数据输入方应在同样的条件下寻求上诉的可能性。在对请求提出质疑时，数据输入方应寻求临时措施，以便在主管司法机构作出决定前暂停请求的效力。在根据适用的程序规则要求披露请求的个人数据之前，数据输入方不得进行披露。这些要求不妨碍第14条（e）款规定的数据输入方的义务。

(b) 数据输入方同意记录其法律评估以及对披露请求的任何质疑，并在目的地国法律允许的范围内，将记录提供给数据输出方。数据输入方还应按照请求将记录提供给主管监管机构。

(c) 数据输入方同意基于对请求的合理解释，在响应披露请求时提供允许的最少的信息。

第四节：最终条款

第16条

违反条款和合同终止

(a) 无论出于何种原因，如果数据输入方无法遵守本条款，应立即通知数据输出方。

(b) 如果数据输入方违反或无法遵守本条款，数据输出方应暂停向数据输入方转移个人数据，直至再次确保遵守条款，或终止合同。这不影响第14条（f）款。

(c) 在以下情况下，只要涉及本条款规定的个人数据处理，数据输出方有权终止合同：

(i) 数据输出方已根据（b）款暂停向数据输入方转移个人数据，且在合理时间内（暂停转移一个月内），仍未恢复遵守本条款；

(ii) 数据输入方严重或持续违反本条款；或

(iii) 数据输入方未能遵守主管法院或监管机构针对其在本条款下的义务的具有约束力的决定。

在这种情况下，数据输出方应将违规情况通知主管监管机构。如果合同涉及两个以上的缔约方，除非各方另有约定，否则数据输出方只能对相关缔约方行使终止权。

(d) 欧盟数据输出方在根据（c）款终止合同前收集并转移的数据（包括其副本）应立即全部删除。数据输入方应向数据输出方证明数据已删除。在数据被删除或返还之前，数据输入方应继续确保遵守本条款。如果适用于数据输入方的本地法律禁止返还或删除所转移的个人数据，数据输入方保证其将继续确保遵守本条款，并仅在该本地法律所要求的范围和期限内对相关数据进行处理。

(e) 在以下情况下，任何一方均可撤销其受本条款约束的协议：（i）欧盟委员会根据欧盟第2016/679号条例第45条第3款通过的涉及本条款适用的个人数据转移的决定；或（ii）欧盟第2016/679号条例被融入了个人数据转移目的地国家的法律框架。这不影响欧盟第2016/679号条例所规定的与数据处理相关的其他义务。

第17条

管辖法律

本条款应由支持第三方受益人权利的国家的法律进行管辖。各方对此达成共识，应适用爱尔兰的法律。

第18条

法院和管辖权的选择

本条款引起的任何争议应由爱尔兰都柏林具有管辖权的法院以诉讼的方式解决。

附录I：

2. **缔约方名单**

数据输出方：

名称：Aspiegel SE

地址：Aspiegel SE的地址（3rd floor Mespil Court Mespil Road Ballsbridge, Dublin 4, D04 E516, Ireland

联系人姓名、职位和联系方式：Joerg Thomas, Director, DPO Office, dpo@huawei.com

与根据本条款转移的数据相关的活动：按照客户选择向客户提供AG Connect服务

签名和日期：……

角色：数据处理者

数据输入方：

名称：客户名称

地址：客户营业地址，如注册开发者帐号时登记的地址

联系人姓名、职位和联系方式：客户联络信息以及在AG Connect服务下以及注册开发者帐号时提供的相关信息，包括通知邮件地址

根据本条款与数据转移相关的活动：客户根据自己的选择使用AG Connect服务

签名和日期：……

角色：数据控制者

2. **转移说明**

其个人数据被转移的数据主体的类型

使用客户产品和服务的最终用户

被转移的个人数据类型

为了能向客户提供其使用的AG Connect服务而被华为处理的数据。针对不同AG Connect服务而处理的相关数据类型，请见【】。

转移的敏感数据（如适用）以及充分考虑到数据性质和所涉及的风险而实施的限制或保护措施

If applicable, as described in connection with the relevant AGC Service as listed here.

如适用，与【】列出的相关AG Connect服务的描述保持一致。

转移的频率

根据使用的AG Connect服务及具体特性，客户可能会持续访问或分享相关数据。更多信息，请见【】。

处理的性质

Data is processed by Huawei in order to provide the AGC Services used by Customer, as further described in relation to each AGC Service listed here.

如【】对各项AG Connect服务的描述，为了向客户提供AG Connect服务，华为需处理相关数据。

数据转移和进一步处理的目的

如【】对各项AG Connect服务的描述，数据转移和处理是为了提供AG Connect服务。

个人数据留存期限；如未定义留存期限，需说明用于确定留存期限的标准

根据数据进口方的隐私政策和数据留存惯例，并遵循适用的数据保护法律。

附件3：数据传输协议（数据处理者）

本协议仅在GDPR不适用时适用：

数据出口组织名称：AGC协议和本DPA定义的客户

（数据出口方）

以及

数据进口组织名称：

电话：_____

传真：_____

Email：_____；或

其他用于确认该组织身份的信息：

_____

（数据进口方）

以下涉及数据进口方或数据出口方时，简称“一方”，涉及数据进口方和数据出口方时，统称“双方”。

条款1 定义

为履行本DPA目的：

（a）适用法律法规指任何给定时间适用于客户个人数据处理的隐私或数据保护法律、法规及规定。

（b）客户数据指客户或客户的最终用户通过华为帐号使用服务而提供的个人数据。

（c）客户的最终用户指使用客户服务的用户（例如，使用客户应用的用户）。

（d）客户个人数据指客户数据包含的个人数据。

（e）本协议中使用的“个人数据”、“特殊数据类型”、“数据处理”、“数据控制者”、“数据处理者”、“数据主体”，“子处理者”，“监管机构”等术语含义与欧盟GDPR里的定义相同，除非适用数据保护法律另有规定；并且：

本DTA未进行定义的术语，应服从（i）本DTA所依附的数据处理协议（DPA）的术语定义，或（ii）适用法律法规的术语定义。

条款2 数据传输细节

数据传输细节（以及被覆盖的个人数据）详见《附录1》。

条款3 数据出口方义务

数据出口方同意并保证：

（a）个人数据处理，包括数据传输本身，已经按照且将一直按照适用法律法规的相关规定执行（并且，在适用情况下，数据出口方已经通知其登记成立国家的相关机构），包括按照适用法律法规要求，在传输个人数据之前获得数据主体同意，并向数据主体通知以下信息：

（i）数据进口方名称；

（ii）数据进口方联络信息；

（iii）个人数据传输类型；

（iv）个人数据传输目的；

（v）适用法律法规要求的其他任何信息。

（b）在评估了适用法律法规的要求之后，DPA第4条（数据安全性）和附件1（安全措施）中规定的技术和组织安全措施适用于保护个人数据免遭意外或非法破坏或意外损失、更改、未经授权的披露或访问，特别是在处理涉及通过网络传输数据的情况下，以及所有其他非法形式的数据处理。此外，考虑到现有最先进技术及其实施成本，这些措施可以确保一定程度的安全性，匹配数据处理所带来的风险和需要保护的数据的性质。

（c）在数据传输涉及特殊数据类型的情况下，数据主体在数据传输之前，已经被告知或同意根据适用法律法规将其数据传输到数据出口方登记成立的国家范围之外。

（d）数据出口方将按照监管机构要求，获得监管机构事先审批，并应适用法律法规要求，留存一份本DTA副本于监管机构。

（e）应适用法律法规要求，在一段特定的时间内对客户数据进行维护。

条款4 数据进口方义务

数据进口方同意并保证：

（a）仅按照数据出口方指示、本DTA（特别是附件1），以及适用法律、政府或监管机构要求，或根据法庭命令，代表数据出口方处理个人数据。在这种情况下，数据进口方应在履行相关法律要求或法庭命令之前尽快通知数据出口者。如果数据进口方出于任何原因无法遵从数据出口方指示或本DTA，数据进口方同意在无不当拖延的情况下通知数据出口方其无法遵从。在这种情况下，数据出口方有权中止个人数据传输，且双方应本着真诚合作的原则，协商确定任何必要且合理的措施，使数据进口方可以遵从出口方指示及本DTA。

（b）在数据出口方所在国家的适用法律法规要求下（并根据第11条），以与该国家适用法律法规相当的标准保护其接收的个人数据；应数据进口方要求，数据出口方应将其适用法律法规中规定的、超出了本DTA范围或双方签订的任何其他数据处理协议范围的义务告知数据进口方。

（c）遵守所在国或公司适用法律法规，例如数据传输相关的法律法规。

（d）没有理由证明适用于数据进口方的立法会阻止数据进口方履行数据出口方指示以及数据进口方在DTA项下的义务。此外，如果适用于数据进口方的立法发生变更，且可能会对数据进口方根据本DTA提供的担保和应履行的义务产生重大不利影响，数据进口方将在知悉后立即通知数据出口方。在这种情况下，数据出口方有权中止个人数据传输，且双方应本着真诚合作的原则，协商确定任何必要且合理的措施，使数据进口方可以遵从出口方指示及本DTA。

（e）数据进口方在处理被传输的个人数据之前已经实施DPA第4条（数据安全）和附件1（安全措施）所规定的技术和组织安全措施，从而防范未经授权或偶然的个人数据接入、收集、使用、披露、复制、修改、处理或销毁，或其他类似风险。

（f）数据进口方将在无不当拖延的情况下，向数据出口方及时通知以下信息：

（i）包括法律强制性要求在内的任何具有法律约束力的披露个人数据的请求，包括由执法机构提出的要求，除非另有禁令，例如根据刑法禁令维护执法调查的机密性。

（ii）任何实际的或疑似的数据损失、盗窃、损坏，以及偶然或未经授权的接入或处理。

（iii）直接从数据主体收到了请求。这种情况下，数据进口方不得响应此类请求，除非已获得相关授权或被要求进行相应。

（iv）收到的与处理个人数据有关的任何投诉，并遵守数据出口方与此有关的一切指示。

（g）及时妥善地处理数据出口方有关其处理有待传输的个人数据的所有查询，以提供合理的合作，并回应来自数据出口方国内相关监管机构或其他相关当局的问询，以及在处理数据传输方面遵守有关监管机构具有法律约束力的建议。

（h）应数据出口方或数据出口方所在国家有关当局的要求，提交其用于根据DTA处理个人数据的数据处理工具以供审核。

（i）如存在数据子处理过程，数据进口方将提前通知数据出口方并获得数据出口方同意。

（j）子处理者将根据第7部分进行数据处理。

条款5 责任

1. 子处理者违约，数据进口方也需要一并承担相应责任。

2. 双方同意，如有一方因另一方违反本DTA而承担责任（为免存疑，就数据进口方而言，数据进口方对子处理者的违约负责），后者应在其应承担的责任范围内，赔偿前者因此而产生的任何成本、收费、损害、费用及损失。所述赔偿取决于：

（a）数据出口方是否及时通知数据进口方索赔信息；且

（b）数据进口方是否获得合作机会，与数据出口方共同参与相关索赔辩护及解决。

条款6 管辖法律

本DTA应根据数据进口方所在国法律进行管辖。

条款7 子处理

数据出口方授权数据进口方卷入子处理者。数据进口方必须获得数据出口方同意，才能将其在本DTA项下的义务分包给子处理者，且必须与子处理者签订书面分包协议。该书面分包协议约定的子处理者义务必须与本DTA项下数据进口方所承担的义务相同。如果子处理者未能履行该书面协议项下的数据保护义务，数据进口方应就子处理者在本协议项下的义务履行对数据出口方承担全部责任。

数据进口方应向数据出口方提供一份卷入当前数据处理活动的子处理者清单。数据出口方应被视为已在生效日期接受了清单包含的所有子处理者。对于任何其他子处理者，数据出口方有权在知悉新的子处理者后的十四（14）天内书面通知数据进口方，以合理的理由拒绝引入新的子处理者。如果数据进口方在数据出口方的反对下仍选择使用新的子处理者，则数据出口方有权终止本DTA以及其他包含该DTA的协议。

为免存疑，如果数据进口方使用子处理者，数据进口方应根据适用法律法规，对其在本DTA项下的所有义务履行承担全部责任。

条款8 数据传输

数据出口方授权数据进口方，可将个人数据传输至数据进口方成立所在国境外，前提条件是该数据传输符合本DTA所有条款，尤其是第4(a)条，以及其他任何适用的法律法规。数据出口方和数据进口方签订的数据处理协议或其他任何协议应明确指出协议项下个人数据可被传输至哪些国家和领土范围。

条款9 个人数据处理服务终止后的义务

双方同意，在数据处理服务终止后，数据进口方及其子处理者应按照数据出口方指示，将所有传输的个人数据及其副本归还给数据出口方，或销毁所有此类数据，并向数据出口方提供销毁证明，法律规定数据进口方不得或无需返还或销毁部分或全部此类数据的情况除外。在这种情况下，数据进口方应保证其将会确保传输的个人数据的保密性，且不会在未来主动处理任何传输的个人数据。

条款10 协议副本

此DTA可以以任意数量的副本执行，每个副本在执行和交付时均应为该DTA原件，但所有副本共同构成一个相同的文档。本DTA签名框中的签名应被视为本DTA及其所有附件（以及它们各自的附件和附录）每一页的签名。

条款11 补充条款

数据出口方所在国适用法律要求比本DTA规定的要求更多或更高的情况下，所述适用法律将适用本DTA。

日期：

数据进口方： 数据出口方：

【签名】【签名】

附录1：数据传输描述

数据出口方

数据出口方：客户，即客户数据控制者。

数据进口方

数据进口方：华为，如AGC协议定义，华为将根据DPA代表客户处理客户数据；或华为在适用情况下卷入的子处理者。

数据主体

传输的个人数据涉及的数据主体类型（请明确）：客户最终用户

数据类型

传输的个人数据涉及的数据类型：客户最终用户的个人数据

特殊数据类型（如适用）

传输的个人数据将取决于以下基础数据处理活动（请明确）：

处理客户数据，从而提供客户通过AGC协议要求的AGC服务。

附录2：数据进口方实施的技术和组织安全措施描述

本附录构成条款的一部分，必须由各方填写并签署。

根据第3（b）条和第4（c）条描述数据进口方实施的技术和组织安全措施：具体措施详见DPA第4条（数据安全）和附件1（安全措施）。