政策与规范

数据处理和安全协议

产品文档

腾讯云

数据处理和安全协议

最近更新时间：2024-11-04 17:17:15

如果本数据隐私和安全附录（简称“**DPSA**”）与服务条款（以及其中通过引用形式包含的任何文件或政策，DPSA 除外）（简称“**协议**”）之间发生任何冲突，将以本 DPSA 为准。

定义

除非另有规定，以下术语应具有下文规定的含义。本 DPSA 中使用但未作定义的术语应具有协议中规定的含义。
“**管理信息**”是指组织向腾讯云提供的用于设置和管理腾讯云所提供的组织账户和服务的个人信息，以及因组织使用腾讯云提供的服务而生成的任何个人信息；
“**内容**”是指组织使用腾讯云提供的服务提交、上传、传输或显示的任何数据，包括个人信息；
“**控制方**”是指独自或与一个或更多其他人共同控制个人数据的收集、持有、处理或使用的人，包括《加利福尼亚州消费者隐私法案》 (CCPA) 中定义的任何“企业”（如适用）；
“**控制方-处理方传输条款**”是指欧盟委员会于 2010 年 2 月 5 日颁布的第 C(2010) 593 号决议中规定的标准合同条款（控制方至处理方），如在下文 **(2) 控制方-处理方传输条款**中所述；
“**数据泄露**”是指腾讯因协议而处理的个人数据的任何滥用、干扰、丢失、未经授权访问、修改或披露；
“**数据保护法**”是指适用于任何个人数据的收集、存储、处理、传输、披露和使用并不时在相关情形下适用于人或活动的数据保护法律，包括（但不限于）美国隐私法、《指令》、《电子隐私指令》和《通用数据保护条例》；
“**数据主体**”应指 (1)《通用数据保护条例》中定义的“数据主体”；(2) CCPA 中定义的“消费者”；或 (3) 作为个人数据主体的任何其他个人；
“**《指令》**”是指欧洲议会和欧洲理事会于 1995 年 10 月 24 日颁布的关于与个人数据处理相关的个人保护和该等数据的自由传输的第 95/46/EC 号指令；
“**《电子隐私指令》**”是指欧洲议会和理事会于 2002 年 7 月 12 日颁布的关于电子通信行业中的个人数据处理和隐私权保护的第 2002/58/EC 号指令；“**EEA**”是指欧洲经济区；
“**欧盟个人数据**”是指位于欧洲经济区内的数据主体的个人数据；
“**《通用数据保护条例》**”是指欧洲议会和欧洲理事会于 2016 年 4 月 27 日颁布的关于与个人数据的处理相关的自然人保护和该等数据的自由传输的第 2016/679 号条例；
“**特定司法管辖区要求**”是指在某些司法管辖区内适用的特定个人数据处理要求，如在下文 **(1) 特定司法管辖区要求**中所述；
“**组织**”是指同意服务条款的实体。就本 DPSA（包括其附件）而言，如果与不是代表组织行事的个人签订协议，提及“组织”时应被视为提及该个人；
“**个人数据**”具有数据保护法中赋予该术语或其他类似术语的含义，腾讯根据本协议处理这些数据以提供服务；
“**处理**”是指对个人数据进行一项或多项操作，包括任何收集、使用、存储或披露，或相关数据保护法中另行定义的操作行为；
“**处理方**”是指代表一个或多个控制方处理个人数据的人，包括《加利福尼亚州消费者隐私法案》中定义的任何“服务

提供商”或“承包商”（如适用）；
“**分包处理方**”是指腾讯按照第 7.4 条不时指定的、代表腾讯处理个人数据的任何腾讯关联公司或第三方；
“**监管机构**”是指拥有关于数据保护法的有效管辖权的监管机构；
“**腾讯云**”是指向组织提供服务的实体，如在服务条款中规定；
“**腾讯云门户**”是指组织可在完成腾讯云注册后有权访问的客户门户；
“**腾讯云隐私政策**”是指隐私政策中所述且腾讯不时更新和通知组织的政策；
“**腾讯安全政策**”是指腾讯不时确定的适当、合理的技术和组织措施，以防止未经授权或意外访问、处理、删除、丢失或使用个人数据。这些措施将包括控制方-处理方传输条款中规定的措施（如适用）；
“**服务条款**”是指服务条款中所述的条款；以及
“**第三国**”是指欧洲经济区（“**EEA**”）的数据保护法范围之外的所有国家，但不包括经欧盟委员会不时认可的、能够为个人数据提供充分保护的国家。截至本协议之日，此类国家包括安道尔、阿根廷、加拿大、法罗群岛、根西岛、马恩岛、以色列、泽西岛、新西兰、瑞士和乌拉圭。
“**美国隐私法**”是指《加利福尼亚州消费者隐私法案》（经《加利福尼亚州隐私权法案》修订，下称“CCPA”）、《科罗拉多州隐私法案》、《康涅狄格州数据隐私法案》、《犹他州消费者隐私法案》和《弗吉尼亚州消费者数据保护法案》；

协议范围

本附录仅在您签署关于腾讯云提供的服务的服务条款后适用。本附录适用于属于内容的个人数据的处理。属于管理信息的个人数据将按照隐私政策进行处理，本附录应不适用于管理信息的处理。

个人数据处理授权

1. 双方确认，在履行协议下的义务的过程中，腾讯可能会作为提供腾讯云的一部分，因组织存储、访问和处理内容而处理相关个人数据。本 DPSA 旨在规定双方关于该处理的各自义务。
2. 各方向另一方保证，其将遵守因个人数据而适用于其的所有数据保护法。

控制方和处理方

腾讯和组织确认，就个人数据而言，组织是控制方，而腾讯是处理方。

服务区域

1. 在第 5.2 条的约束下，如果组织根据协议选择了服务区域，腾讯将仅在该服务区域内处理个人数据。

2. 组织确认并同意，出于运营、监管或其他原因，腾讯可能需要不时更改处理地点，前提是，在除组织首选服务区域外的地点进行任何个人数据处理都将视为协议规定的“重大变更”。
3. 组织确认并同意，服务条款中所列的腾讯签约实体可能不是保管或控制客户数据（包括个人数据）的实体，因此，该等数据可能在所选的服务区域存储和处理。如果组织提供不要求选择服务区域的信息，例如帐户相关信息，腾讯可能在任何地点处理和存储该等信息。

腾讯的义务

1. 如果腾讯代表组织处理个人数据，腾讯将：
a. 仅为开展服务之有限、特定目的，而按照组织的书面指示（其中应包括本 DPSA 的条款和通过组织的管理控制台提供的任何指示）和腾讯安全政策处理个　　人数据，并在无法遵守本 DPSA 或其任何条款时立即通知组织；
b. 归还或（按照组织的书面要求）安全销毁其持有的所有个人数据（包括所有备份副本），除非适用法律禁止其这样做；
c. 得知下述情况后，立即通知组织：
旨在获得或访问任何个人数据的任何法院命令或其他法律程序或任何监管机构、监管部门、官员或任何政府当局、部门或机构提出的任何请求或要求，除非适用法律禁止发出此通知；
数据泄露；
与数据保护法下的腾讯义务相关的任何重大投诉、通信或要求；以及
从组织收到关于个人数据的任何指示，并且腾讯自行判定这些指示可能违反有关司法管辖区的任何适用法律，包括任何数据保护法；
d. 确保个人数据只能由腾讯雇佣的正式授权人员访问，以及在第 8 条的约束下，只能由经正式授权且为履行腾讯在协议下的义务而需要访问个人数据的腾讯分包处理方和该等分包处理方的人员访问。
e. 确保腾讯雇佣并正式授权处理个人数据的人员承诺进行保密或负有适当的法定保密义务，并根据处理性质，确保该等个人遵守本 DPSA 下的相同数据保护义务和组织指示；
f. 遵守任何适用的特定司法管辖区要求；以及
g. 如果有关司法管辖区的法律要求，腾讯将：
在切实可行的情况下，采取适当的技术和组织安全措施，以便合理协助组织履行其义务，包括在相关司法管辖区内适当和适用的下列措施：(i) 对个人数据进行假名化或去标识化处理；(ii) 确保处理系统和服务维持机密性、完整性、可用性和韧性；(iii) 在发生物理或技术事件时，及时恢复个人数据的可用性和访问；以及 (iv) 定期测试、评价和评估技术与组织措施的有效性，以确保处理的安全性；
根据处理性质，在切实可行的情况下，通过采取适当的技术与组织措施，协助组织履行其义务，响应数据主体提出的行使数据保护法中所规定数据主体权利的请求；
协助组织确保遵守下述义务：(i) 采取适当的技术和组织安全措施；(ii) 在相关数据保护法要求进行通知和报告的情况下，向监管机构、相关数据主体或相应数据保护法要求的其他个人通知（如要求）数据泄露；和 (iii) 执行数据保护影响评估，并且如有要求，事先咨询监管机构；以及
在获悉腾讯根据或因为本 DPSA 处理的个人数据被不当、未经授权或非法访问、使用或披露后，立即以书面形式通知组织。腾讯应有义务向组织提供所有合理必要的信息，以便组织遵守数据保护法规定的义务。

2. 如果腾讯认为组织的指示违反了数据保护法，其应通知组织。

组织的义务

1. 组织向腾讯陈述、保证并承诺，在整个期限内：
a. 个人数据已经并将按照数据保护法收集；
b. 组织向腾讯作出的所有指示均符合数据保护法；和
c. 向腾讯传输个人数据、腾讯按照组织的指示处理个人数据（如果腾讯作为该等个人数据的数据处理方）或接收和使用个人数据（如果腾讯作为该等个人数据的数据控制方）以及根据本 DPSA 的规定处理和使用个人数据均已获得相关数据主体同意（如果法律要求）并以其他方式被数据保护法所允许。
2. 组织同意，在腾讯要求时，将向腾讯赔偿由于组织直接或间接违反本条规定而导致腾讯遭受或发生的所有索赔、责任、成本、费用、损失或损害（包括附带损失、利润损失和声誉损失以及所有利息、罚金、法律和其他专业成本和费用），确保腾讯免受其损害。
3. 如果腾讯面临因违反与根据本 DPSA 处理的个人数据相关的数据保护法而引起或与之相关的实际或潜在索赔，组织将立即提供腾讯合理要求且与该索赔的辩护相关的所有材料和信息。
4. 如果组织得知与协议相关的任何实际或疑似数据泄露，组织应：
a. 在 30 天内采取合理的措施进行评估，以确定数据泄露根据数据保护法是否应通知，并立即以书面形式向腾讯通知评估结果；
b. 如果组织通知腾讯其认为根据数据保护法应当通知该数据泄露，则：
组织应编制数据保护法要求的与任何数据泄露相关的通知声明（简称“通知声明”）草稿，并在向有关数据保护监管机构、数据主体或任何其他个人披露之前，向腾讯提供通知声明草稿以供其审批。
腾讯应以书面形式向组织通知：
腾讯合理要求对通知声明草稿进行的任何更改，并且组织应在通知声明草稿中包含所有这些变更；或
腾讯批准通知声明草稿；和
腾讯批准通知声明草稿后，组织必须向有关数据保护监管机构、数据主体和数据保护法要求的任何其他个人提供经批准的通知声明；和
未经腾讯事先书面同意，不得发布关于任何疑似或实际数据泄露的任何公开声明或披露，而且必须确保其关联公司及其各自人员不这样做。

分包处理方的指定

1. 腾讯可授权任何分包处理方代表其处理个人数据，前提是，如果数据保护法要求，腾讯应与分包处理方签订书面协议，其中应包含基本上与本 DPSA 中所包含之条款相同的条款。组织特此向腾讯授予一般书面权限，以允许在遵守本第 8 条要求的前提下雇佣在腾讯云第三方处列出的分包处理方。
2. 如果腾讯处理个人数据时须遵守的数据保护法要求发送通知，则腾讯应通过电子邮件（和腾讯云门户）向组织通知涉及分包处理方增加或更换的任何预期变更。在此情况下，组织将在收到通知之日起十四 (14) 日内批准或拒绝此

类变更。如果组织未做出回应，则应被视为已接受分包处理方。如果组织拒绝更换分包处理方，腾讯可在向组织发出书面通知后终止协议且立即生效。
3. 如果腾讯雇佣分包处理方代表组织执行特定处理活动，并且该分包处理方未能履行其数据保护义务，腾讯仍将根据数据保护法完全对组织负责，履行该分包处理方的义务。

模块

如果您使用特定功能（见各相关模块中的定义），以下模块应适用并通过引用形式纳入本 DPSA。
1.移动推送 TPNS。
2.手游安全。
3.Web 应用防火墙。
4.游戏多媒体引擎。
5.DDoS 防护。
6.人脸识别。
7.媒体直播。
8.媒体包装。
9.对象存储。
10.云原生数据库 TDSQL-C。
11.弹性微服务。
12.时序数据库 CTSDB。
13.私有域解析 Private DNS。
14.数据库审计。
15.云数据库 Tendis。
16.数据库管理中心。
17.微瓴物联网类操作系统。
18.事件总线。
19.轻量应用服务器。
20.即时通信 IM。
21.边缘计算机器。
22.T-Sec-数据安全中心。
23.腾讯云 TI 平台。
24.云数据仓库。
25.漏洞扫描服务。
26.物联网通信。
27.代码托管。
28.项目管理。
29.测试管理。

30.持续集成。
31.制品库。
32.持续部署。
33.消息队列 TDMQ。
34.全栈式风控引擎。
35.边缘安全加速平台 EO。
36.人脸核身。
37.Prometheus 监控服务。
38.自动化助手。
39.云点播。
40.移动解析 HTTPDNS。
41.腾讯特效SDK。
42.语音合成。
43.语音识别。
44.云直播。
45.实时音视频。
46.前端性能监控。
47.账号风控平台。
48.应用云渲染。
49.文字识别。
50.验证码。
51.机器翻译。
52.视频内容安全。
53.音频内容安全。
54.图片内容安全。
55.文本内容安全。
56.数据湖计算。
57.腾讯微卡。
58.云防火墙。
59.短视频 SDK。
60.密钥管理系统。
61.腾讯云数据连接器。
62.低代码互动课堂。
63.容器安全服务。
64.云拨测。
65.日志服务。
66.互动白板。
67.堡垒机。

68.主机安全。
69.控制中心。
70.云点播-混合云版。
71.智能音乐平台。
72.腾讯云数据仓库 TCHouse-D。
73.腾讯云小程序平台。
74.人脸融合。
75.数据安全审计。

特定司法管辖区要求

欧洲

1. 腾讯同意，其不会在第三国处理欧盟个人数据，除非腾讯遵守控制方-处理方传输条款中规定的数据输入方义务。
2. 如果控制方-处理方传输条款与本 DPSA 其余部分之间有任何冲突，则就任何欧盟个人数据而言，将以控制方-处理方传输条款为准。
3. 就控制方-处理方传输条款而言，将适用以下附加规定：
a. 双方同意遵守控制方-处理方传输条款，不需要做任何修改；
b. 组织和腾讯的名称与地址将被视为纳入控制方-处理方传输条款并用于履行控制方-处理方传输条款；
c. 组织是控制方-处理方传输条款中定义的数据输出方，腾讯或腾讯的相应关联公司是控制方-处理方传输条款中定义的数据输入方；并且
d. 各方签署本 DPSA 将被视为签署控制方-处理方传输条款中所包含条款。
4. 如果任何司法管辖区的法律或监管程序要求，双方将作为单独文件签署或重新签署控制方-处理方传输条款中所包含的条款，该单独文件中应规定以可能要求的方式拟进行的个人数据传输。

韩国

1. 如果腾讯安全政策不足以遵守韩国隐私法律和法规下的适用要求，腾讯将不时采取额外措施来遵守该等要求（如适用于个人数据的国外接收人），包括下列法律法规：
a. 促进信息与通信网络利用和信息保护法（简称“**ICT 网络法案**”）第 28 和 63 条；
b. 根据 ICT 网络法颁布的执行令第 15 和 67 条；
c. 个人信息保护技术和管理措施指南（由韩国通信委员会发布）；
d. 个人信息保护法（“**PIPA**”）第 29 条；
e. 根据 PIPA 颁布的执行令第 30 条；以及
f. 个人信息安全保护措施指南（由行政安全部发布），以及上述法规的不时修订和/或补充。
2. 腾讯将：
a. 仅为了执行委托的工作且在该工作的范围内使用个人数据；
b. 同意接受组织对腾讯处理个人数据进行的培训和监督；以及
c. 同意接受有关监管机构的监督和审查。

3. 对于因违反腾讯在本 DPSA 或适用法律下的义务而造成的一切损害、责任、成本和费用，腾讯将向组织及任何相关数据主体进行赔偿。

美国隐私法

1. 在适用的美国隐私法要求的范围内，经提出或发出合理的书面要求或通知：

a. 组织可采取合理、适当的措施确保腾讯使用个人数据的方式符合组织在适用的美国隐私法项下的义务；

b. 如组织合理认为腾讯使用个人数据的行为违反了适用的美国隐私法，组织可采取合理、适当的措施制止和补救该等未经授权的使用；

c. 腾讯应向组织提供腾讯掌握的、为证明腾讯遵守其在美国隐私法项下的义务而所需的信息。

d. 腾讯应允许组织或组织的指定审计师就腾讯遵守其在适用的美国隐私法项下的义务的情况进行合理的年度评估并予以配合，相关费用由组织承担，且只有在双方就评估范围达成一致意见后方可进行评估。或者，腾讯可安排合格的独立审计师评估腾讯为支持其履行在适用的美国隐私法项下的义务而实施的政策以及技术和组织措施，审计师应采用适当且公认的控制标准或框架和评估程序进行该等评估。一经合理要求，腾讯应向组织提供相关评估报告。

2. 考虑到数据处理的背景，双方应采取适当的技术和组织措施，以保证与风险相适应的安全水平，并在双方之间明确划分实施该等措施的责任。在适用的美国隐私法要求的范围内，腾讯应提供与该等法律要求的力度同等的隐私保护。

3. 禁止腾讯做出以下任何行为：

a. 出售和共享个人数据；

b. 为开展服务之特定目的以外的任何目的保留、使用或披露个人数据；

c. 在腾讯与组织的直接业务关系范围外保留、使用或披露个人数据；

d. 将从组织处或代表组织收到的个人数据与可能从腾讯与个人数据所涉及的个人单独互动过程中或从任何其他来源收集的任何个人数据合并，但美国隐私法允许的除外。就本美国隐私法条款而言，“出售”和“共享”及其他类似措辞应具有美国隐私法中规定的含义。

澳门

1. 在将腾讯指定为处理方以及指定分包处理方（在本协议允许的范围和程度内）时，组织应通知当地数据保护办公室 (GPDP - Gabinete para a Protecção de Dados Pessoais)。

2. 腾讯有权合理要求组织提供符合相关澳门数据保护法下的指示的证据，包括上面第 1 节规定的通知。

3. 在处理敏感数据时（如《澳门数据保护 法》（第 8/2005 号法）第 7 条所定义），组织应以书面形式明确通知腾讯，并确保遵守《澳门数据保护法》下针对该等数据处理规定的特定要求。

控制方-处理方传输条款

就关于将个人数据传输到无法提供充分数据保护的第三国处理方第 95/46/EC 号指令第 26(2) 条而言：

数据输出组织的名称：这是指签订协议的组织或个人（如果与不是代表组织行事的个人签订协议）。

（简称“**数据输出方**”）

与

数据输入组织的名称：服务条款第 1.2 节规定的签约实体。

（简称“**数据输入方**”）

单独称为“**一方**”；合称为“**双方**”，
已就以下合同条款（简称“**《合同条款》**”）达成一致，以在数据输出方将附件 1 所述的个人数据传输给数据输入方的过程中充分保障个人隐私及基本权利和自由。

定义

就《合同条款》而言：
a. “个人数据”、“特殊类别的数据”、“处理/正在处理”、“控制方”、“处理方”、“数据主体”和“监管机构”将具有欧洲议会和欧洲理事会于 1995 年 10 月 24 日针对个人数据的处理和该等数据的自由传输而颁布的旨在保护个人数据的第 95/46/EC 号指令赋予的含义；
b. “数据输出方”是指传输个人数据的控制方；
c. “数据输入方”是指同意从数据输出方接收个人数据以在传输后代表数据输出方并根据数据输出方的指示和《合同条款》中的规定处理此类数据的处理方，并且该处理方不受第三国体制的约束，可确保提供第 95/46/EC 号指令第 25(1) 条中规定的充分保护；
d. “分包处理方”是指数据输入方或数据输入方的任何其他分包处理方聘用的任何处理方，该处理方同意从数据输入方或数据输入方的任何其他分包处理方接收个人数据，以在传输后代表数据输出方并根据数据输出方的指示和《合同条款》中的规定以及书面分包合同的条款对此类数据执行处理活动；
e. “适用数据保护法”是指在数据输出方成立地点所在的成员国境内，适用于数据控制方的、保护与处理个人数据相关的个人基本权利和自由（特别是个人隐私权）的法律；
f. “技术和组织安全措施”是指用于保护个人数据的措施，通过这些措施，可以防止个人数据遭到意外或非法破坏或意外丢失、修改、未经授权的披露或访问（特别是在处理活动涉及到通过网络传输数据时）以及所有其他非法形式的处理活动。

传输的具体内容

传输的具体内容，特别是特殊类别的个人数据，将在适用时在附件 1 中进行说明，该内容构成《合同条款》不可缺少的一部分。

第三方受益人条款

1. 数据主体可以作为第三方受益人对数据输出方强制执行本条、第 4(b) 至 4(i) 条、第 5(a) 至 5(e) 和 5(g) 至 5(j) 条、第 6.1 和 6.2 条、第 7 条、第 8.2 条以及第 9 至 12 条。
2. 如果数据输出方在事实上已不存在或被取消法律资格，数据主体可对数据输入方强制执行本条、第 5(a) 至 5(e) 和 5(g) 条、第 6 条、第 7 条、第 8.2 条以及第 9 至 12 条，除非任何继任实体根据合同或法律规定承担数据输出方的全部法律义务，并据此接管数据输出方的权利和义务，在此情况下，数据主体可对此类实体强制执行上述条款。
3. 如果数据输出方和数据输入方在事实上均已不存在、被取消法律资格或丧失偿债能力，数据主体可对分包处理方强制执行本条、第 5(a) 至 5(e) 和 5(g) 条、第 6 条、第 7 条、第 8.2 条以及第 9 至 12 条，除非任何继任实体根据合同或法律规定承担数据输出方的全部法律义务，并据此接管数据输出方的权利和义务，在此情况下，数据主体可对此类实体强制执行上述条款。分包处理方所应承担的此类第三方责任仅限于其独自根据《合同条款》执行的处理操作。

4. 在数据主体明确希望且国内法律许可的情况下，数据主体可指定某一团体或其他机构作为其代表，双方对此无任何异议。

数据输出方的义务

数据输出方同意并保证：

a. 个人数据的处理（包括数据传输本身）已经遵守并将继续遵守适用数据保护法的相关规定（并已在适用时通知了数据输出方所在成员国的相关机构），且不违反该国的其他相关规定；

b. 其已要求并在整个个人数据处理服务存续期间要求数据输入方仅代表数据输出方且根据适用数据保护法以及《合同条款》对所传输的个人数据进行处理；

c. 数据输入方将提供充分的保证以实施本协议附件 2 规定的技术和组织安全措施；

d. 其已对适用数据保护法的要求进行评估，确认所采取的安全措施合理适当，可以防止个人数据遭到意外或非法破坏或者意外丢失、修改、未经授权的披露或访问（特别是在处理活动涉及到通过网络传输数据时）以及所有其他非法形式的处理活动，且此类措施就现有技术水平和实施成本而言，可确保达到防范数据处理以及要保护的数据特征所产生的风险所需的适当安全级别；

e. 确保遵守相关安全措施；

f. 如果传输涉及特殊数据类别，在数据传输之前已经或在数据传输之后将尽快通知数据主体，说明此类数据可能传输到无法提供第 95/46/EC 号指令规定的充分保护的第三国；

g. 如果数据输出方决定继续传输或暂停数据传输，则根据第 5(b) 条和第 8.3 条的规定，将从数据输入方或任何分包处理方收到的通知转交给数据保护监管机构；

h. 经数据主体要求，向其提供《合同条款》的一份副本（附件 2 除外）、一份安全措施摘要说明以及一份有关任何分包处理服务的合同副本（此合同须根据《合同条款》订立），除非《合同条款》或此类合同含有商业信息，在此情况下，可移除此类商业信息；

i. 如果需进行分包处理，分包处理方应根据第 11 条执行处理活动，并为个人数据以及数据主体的权利提供至少与《合同条款》针对数据输入方规定的保护级别同等的保护；

j. 确保遵守第 4(a) 至 4(i) 条的要求。

数据输入方的义务

数据输入方同意并保证：

a. 仅代表数据输出方并按照数据输出方的指示以及《合同条款》的规定处理个人数据。如果出于任何原因无法遵守此规定，则数据输入方同意，就其无法遵守此规定的情况立即通知数据输出方，在这种情况下，数据输出方有权暂停数据传输和/或终止合同；

b. 如果其无理由认为适用法律妨碍其遵守数据输出方的指示以及履行其合同义务，且在适用法律发生变更时，可能对《合同条款》下的保证和义务造成实质性不利影响，则其应在知悉此类情况后及时将此类变更通知数据输出方，在这种情况下，数据输出方有权暂停数据传输和/或终止合同；

c. 其在处理所传输的个人数据之前已实施附件 2 规定的技术和组织安全措施；

d. 如果出现下列情形，其将立即将相关事宜通知数据输出方：

执法机构提出任何具有法律约束力的个人数据披露要求，除非另有禁止规定（例如根据刑法，为保护执法调查的机密性而禁止此类披露）；

任何意外或非经授权访问，以及
数据主体直接提出任何要求，但此类要求并得到回应，经另行授权做出回应的情况除外；
e. 如果数据输出方就数据输入方处理所传输的个人数据进行查询，及时对此类查询进行合理处理，并遵守监管机构就处理所传输的数据提出的建议；
f. 经数据输出方要求，提交其数据处理设施，用以对《合同条款》规定的处理活动进行审计，此类审计将由数据输出方或数据输出方选定的检查机构实施，此类检查机构需由独立成员组成、拥有必要的专业资质并受保密义务约束，必要时，还需获得监管机构的认可；
g. 如果数据主体无法从数据输出方获得《合同条款》或任何现有分包处理合同的副本，则经数据主体要求，为数据主体提供此类副本，除非《合同条款》或合同包含商业信息，在这种情况下，可移除此类商业信息，在提供此类副本时，不应包含附件 2，该附件将替换为一份安全措施摘要说明；
h. 如果需进行分包处理，则其已事先通知数据输出方并获得数据输出方的书面同意；
i. 分包处理方应根据第 11 条提供数据处理服务；
j. 及时将根据《合同条款》订立的任何分包处理方协议副本发送给数据输出方。

责任

1. 双方同意，如果任何一方或分包处理方以任何方式违反第 3 条或第 11 条中规定的义务，致使任何数据主体遭受损失，则该数据主体有权从数据输出方处获得补偿，以弥补其遭受的损失。
2. 如果数据输入方或其分包处理方不履行其在第 3 条或第 11 条项下的义务，而数据主体因数据输出方在事实上已不存在、被取消法律资格或丧失偿债能力而无法根据第 6.1 条向数据输出方提出索赔要求，则数据输入方同意，数据主体可将数据输入方视为数据输出方，并向数据输入方发起索赔，除非任何继任实体已根据合同或法律规定承担数据输出方的全部法律义务，在这种情况下，数据主体可对此类实体强制行使其权利。数据输入方不得因分包处理方不履行其义务来逃避自身责任。
3. 如果分包处理方未履行其在第 3 条或第 11 条项下的义务，而数据主体因数据输出方和数据输入方在事实上均已不存在、被取消法律资格或丧失偿债能力而无法根据第 6.1 条和第 6.2 条向数据输出方或数据输入方提出索赔要求，则分包处理方同意，数据主体可将数据分包处理方视为数据输出方或数据输入方，并就数据分包处理方独自根据《合同条款》进行的处理操作向数据分包处理方发起索赔，除非任何继任实体已根据合同或法律规定承担数据输出方或数据输入方的全部法律义务，在这种情况下，数据主体可对此类实体强制行使其权利。分包处理方的责任将仅限于其独自根据《合同条款》进行的处理操作。

调解与司法管辖

1. 数据输入方同意，如果数据主体向其申索第三方受益人权利和/或根据《合同条款》对所遭受的损失提出补偿，数据输入方应接受数据主体的决定：
a. 将此类争议转交给独立个人或监管机构（如适用）进行调解；
b. 将此类争议转交给数据输出方所在成员国的法院。
2. 双方同意，数据主体所做的选择不会影响其根据国内或国际法律的其他条款规定寻求补救的实体性或程序性权利。

与监管机构合作

1. 如果监管机构要求备案一份本协议的副本，或者适用数据保护法要求进行此类备案，则数据输出方同意进行此类备案。
2. 双方同意，监管机构有权对数据输入方及其任何分包处理方进行审计，且此类审计的范围与条件与根据适用数据保护法对数据输出方进行的审计相同。
3. 如果存在任何适用于数据输入方或其任何分包处理方且阻止根据第 8.2 条对数据输入方或其任何分包处理方执行审计的法律，则数据输入方应及时通知数据输出方。在此类情况下，数据输出方将有权采取第 5(b) 条中规定的措施。

管制法律

《合同条款》受数据输出方所在成员国的法律管辖。

合同变更

双方承诺不会变更或修改《合同条款》。此项承诺不妨碍双方在必要时就业务相关问题添加相应条款，但前提是，《合同条款》不会与该条款冲突。

分包处理

1. 未经数据输出方事先书面同意，数据输入方不得将其根据《合同条款》代表数据输出方执行的任何处理操作进行分包。如果数据输入方经数据输出方同意将其根据《合同条款》应承担的义务进行分包，则其必须与分包处理方签署书面协议，此类协议对分包处理方规定的义务应与数据输入方根据《合同条款》应承担的义务完全相同。如果分包处理方未能根据此类书面协议履行其数据保护义务，则数据输入方将承担对数据输出方的全部责任并根据此类协议履行分包处理方的义务。
2. 数据输入方与分包处理方之间事先订立的书面合同还应载列第 3 条中规定的第三方受益人条款，如果数据主体因数据输出方或数据输入方在事实上已不存在、被取消法律资格或丧失偿债能力而无法根据第 6.1 条向数据输出方或数据输入方提出赔偿要求，并且没有任何继任实体根据合同或法律规定承担数据输出方或数据输入方的全部法律义务，则应援引此类第三方受益人条款。分包处理方所应承担的此类第三方责任仅限于其独自根据《合同条款》执行的处理操作。
3. 第 11.1 条所提及协议中有关数据保护分包处理的规定将受数据输出方所在成员国的法律管辖。
4. 数据输出方将留存一份根据《合同条款》达成的分包处理协议的清单，数据输入方应按照第 5(j) 条的规定将此类协议通知数据输出方，此类协议将至少每年更新一次。该清单将提供给数据输出方的数据保护监管机构。

个人数据处理服务终止后的义务

1. 双方同意，在数据处理服务条款终止后，数据输入方和分包处理方将按照数据输出方选择的方式，将所有已传输的个人数据及其副本退还给数据输出方，或者销毁所有此类个人数据并向数据输出方证明此类数据已被销毁，除非法律禁止数据输入方退还或销毁全部或部分已传输的个人数据。在这种情况下，数据输入方应保证其能够确保已传输的个人数据的机密性，并且不会再主动处理此类已传输的个人数据。
2. 数据输入方和分包处理方应保证，如果数据输出方和/或监管机构提出要求，其将提交相应的数据处理设施，以供对第 12.1 条提及的措施进行审计。

附件 1

传输说明（控制方-处理方）

本附件构成《合同条款》的一部分，须由双方完善并签署。
成员国可根据本国规程完善或指明本附件应包含的任何其他必要信息。

数据输出方

数据输出方是协议中所述的组织，或在协议是由不是代表组织行事的个人签订的情况下，数据输出方为该个人。
数据输出方已委托数据输入方提供协议中所述的在线服务。

数据输入方

数据输入方是协议中所述的腾讯公司，一家领先的互联网增值服务提供商。数据输出方已委托数据输入方提供协议中所述的某些在线服务。

数据类别

传输的个人数据涉及以下类别的数据（请指明）：
数据输出方上传的内容，或数据输出方不时通知数据输入方的内容。

特殊数据类别

传输的个人数据涉及以下特殊类别的数据（请指明）：
数据输出方上传的内容，或数据输出方不时通知数据输入方的内容。

处理操作

传输的个人数据可能涉及以下基本处理活动（请指明）：
数据输入方将处理个人数据，以支持数据输出方执行的活动。具体而言，数据输入方按照数据输出方指示并代表数据输出方执行的处理活动包括：数据托管、数据备份、通信、数据分析、统计、分析、IT 系统管理、订单履行、支持服务、员工管理服务、处理订单付款、发送营销信息、推广和调查、操作、软件维护和托管、信息技术服务（包括桌面和网络管理）、系统监控、应用程序开发、归档、灾难管理和数据恢复。

附件 2

技术和组织安全措施

为了保护您的内容，我们实施了全面的隐私与安全计划。该计划包括以下内容：
1. **数据安全。**我们设计并实施了下列措施，以防止客户的数据遭到未经授权访问：
a. 数据分级分类标准；
b. 一系列物理、网络、系统和应用程序层面的身份验证和访问控制功能；和
c. 基于大数据的异常行为检测机制。
2. **网络安全。**我们实施严格的内部网络隔离规定，以通过物理和逻辑隔离实现内部网络（包括办公网络、开发网络、测试网络和生产网络）的访问控制和边界保护。
3. **物理和环境安全。**根据相关区域安全要求，对腾讯云的数据中心实施严格的基础设施和环境访问控制。根据数据中心人员类别及其各自的访问权限建立访问控制矩阵，以确保对数据中心人员的访问和操作进行有效的管控。

4. **事件管理。**实施主动和实时的服务监控，并结合快速响应和处理机制，以实现快速发现和处理安全事件。
5. **遵守标准。**我们遵守在我们的“合规中心”页面列出且不时更新的标准。