数据受托处理附录

您(以下亦称「**客户**」或「**个人信息处理者**」或「**委托方**」）使用**北京泛睿达科技有限公司(包括其关联企业，下称 FRD 或「个人信息受托处理者」)**提供之服务时，可能涉及您所控制的个人信息之处理。在此情形下，您为个人信息处理者，FRD 为您的「个人信息受托处理者」。为满足《中华人民共和国个人信息保护法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》及相关个人信息保护法律法规的要求，并确保个人信息主体的权利得到保护，明确个人信息处理者和个人信息受托处理者的义务和责任，双方经协商一致，特签订本「**数据受托处理附录**」（包含一般条款、附录 A 及附录 B，以下合称为「**本附录**」），以便共同遵守。

一般条款

1. 总览

本附录内容说明双方当事人之权利及义务，包括于所应适用之隐私法律、信息安全，以及与客户数据（定义参后述）有关之个人信息处理及信息安全义务。本附录自「附录生效日」（定义参后述）生效，在适用的前提下并取代先前主合约中适用于客户数据中的个人信息处理之条款。本附录所使用之专用语以本附录中所赋予之定义为准。

2 定义

2.1 于本附录中:

2.1.1 「**附录生效日**」指(a) 主合约生效时；(b) FRD 开始处理个人信息时；(c) 双方当事人另行同意之日期，三者以较早发生日期为准。主合约指您为使用 FRD 提供之服务而同意或签署具有法律拘束力的合约，且 FRD 依该合约以个人信息受托处理者的角色为您处理个人信息。

2.1.2 「**所应适用之隐私法律**」是指数据处理活动涉及国家或地区的适用的关于个人信息保护与网络安全的法律、法规、规章、规范性文件及其他具有强制约束力的规范或指令及其不断修订、更新的版本；为本协议之目的，适用法律为中华人民共和国法律，包括但不限于《中华人民共和国个人信息保护法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》等。

2.1.3 「**客户数据**」指客户利用服务时所提供或使 FRD 得以接触之一切数据、服务之用户因使用该服务所提供之数据或该服务向用户收集之数据。

2.1.4 「**客户个人信息**」指客户数据中之个人信息，个人信息包括客户持有的他人的个人信息及所应适用之隐私法律中所定义之个人信息或敏感个人信息。

2.1.5 「**个人信息处理者**」是指在个人信息处理活动中自主决定处理目的、处理方式，应依法履行个人信息处理相关义务并对个人信息处理活动负责的组织和个人，为免疑义，在本附录约定的委托处理关系项下，委托方，即客户，为个人信息处理者。

2.1.6 「**个人信息受托处理者**」是指按照个人信息处理者的指示处理个人信息，不决定处理目的、处理方式的组织或个人，在本附录项下 FRD 为个人信息受托处理者。

2.1.7 「**个人信息处理**」, 是指个人信息处理者对个人信息所采取的包括但不限于收集、存储、使用、加工、传输、提供、公开、删除等处理活动。

2.1.8 「**个人信息主体**」，是指个人信息所标识或者关联的自然人。

2.1.9 「**个人信息安全事件**」指 FRD 之信息安全发生事故所导致存放于 FRD 运营或控制之系统中之客户个人信息未经授权的访问以及个人信息泄露、篡改、丢失。

2.1.10 「**通知电子邮件地址**」指您于主合约中所指定之电子邮件地址，或您以书面指定用于接收 FRD 发送之特定通知之电子邮件地址。

2.1.11 「**分包处理者**」指为个人信息受托处理者提供服务，代表个人信息受托处理者处理客户数据的任何 FRD 关联企业或第三方。

2.1.12 「**监管机关**」指中华人民共和国个人信息保护法第六章所定义之履行个人信息保护职责的部门。

2.1.13 「**服务期间**」指自本附录生效日至 FRD 完成服务之提供时止，包含 (若可适用) 任何服务中止期间、及终止后 FRD 为移转、归还、销毁所储存之个人信息之目的仍继续提供个人信息处理服务之期

间。

2.2 本协议中其他未定义术语的含义与《中华人民共和国个人信息保护法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》等法律法规所规定的含义相同。如相关法律法规中未明确定义有关概念的，双方同意，本协议范围内可参照适用《信息安全技术 个人信息安全规范》（GB/T 35273-2020）中的定义。

3 有效期间

无论所应适用之主合约是否终止或届期，本附录将持续有效，直至本附录所示之服务期间届至时自动终止。

4 个人信息处理者的义务

4.1 个人信息处理者在此陈述、保证、承诺如下：

4.1.1 个人信息系按照相关法律法规进行收集、使用等处理；委托处理的个人信息范围仅限于实现处理目的所需的最小范围。

4.1.2 向 FRD 作出的所有指示均符合相关法律法规规定。

4.1.3 个人信息处理者应积极响应个人信息主体基于知情权、决定权、查阅权、复制权、更正权、补充权、删除权、可携带权等权利提出的请求。

4.2 在 FRD 要求时，将向 FRD 赔偿由于个人信息处理者直接或间接违反第 4 条规定而导致 FRD 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 FRD 免受其损害。

4.3 如果 FRD 面临因违反与个人信息相关的法律法规而引起或与之相关的，由个人信息主体向 FRD 提出的实际或潜在索赔，个人信息处理者将立即提供 FRD 合理要求的，且与该索赔的辩护相关的所有材料和信息。

4.4 如果本附录项下处理的个人信息发生了任何实际或疑似个人信息安全事件，个人信息处理者将：

4.4.1 及时采取适当补救措施，以减轻对个人信息主体造成的不利影响；

4.4.2 记录并留存所有与个人信息安全事件有关的事实及其影响，包括

采取的所有补救措施；

4.4.3 相关法律法规要求通知个人信息主体或相关监管机构的，由个人信息处理者承担通知义务。

4.5 若客户发现客户个人信息不正确或过时，客户应负责以符合合约所指服务之方式，依所应适用之隐私法律规定更正或删除该等数据。

5 个人信息处理受托人的义务

5.1 FRD 应：

5.1.1 遵守所应适用之隐私法律以处理客户个人信息。

5.1.2 FRD 仅得依据客户的书面指示之目的（参**附录 A**）内进行个人信息的处理及利用，不得超出约定的处理目的、处理方式等处理个人信息，除非取得个人信息处理者的事先同意。

5.1.3 处理个人信息的范围仅限于实现受托处理目的所需的最小范围。

5.1.4 存储个人信息的期限为实现处理目的所必要的最短时间；存储期限届满后，个人信息受托处理者应及时返还、删除其根据本附录所接收到的个人信息。法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的除外。

5.2 FRD 按照以下方式保障个人信息处理安全：

5.2.1 FRD 会依**附录 B** 所述执行并维持符合行业通行水准的技术、组织及实体措施（称「**数据安全措施**」），以确保个人信息的安全，包括防止个人信息遭到意外或非法破坏、丢失、篡改、未经授权提供或访问。数据安全措施包含有助于确保持续保密性、完整性及可用性之措施。FRD 有权随时更新数据安全措施，前提是这些更新不会大幅降低服务的安全性。在评估适当的安全等级时，双方应适切考虑技术水准、执行成本、数据处理的本质、范围、情境及目的、及所涉及之数据主体的风险。若数据处理涉及敏感个人信息，FRD 将会采取特定的限制措施及/或额外的安全措施。

5.2.2 确保授权处理个人信息的人员履行适当的保密义务，并建立最小授权的访问控制策略，采取合理措施确保任何可能会存取、接触

或处理控制者个人信息的处理者之人（包括员工或分包处理者）的可靠性，在任何情况下，应确保存取、接触或处理控制者个人信息的第三人仅能访问出于职责所需的最小必要的个人信息，且仅具备完成职责所需的最少的数据操作权限。

5.3 于服务期间内，FRD 将以符合主合约所指服务之方式，使客户得接触客户数据，客户得指示 FRD 对客户数据进行下列活动：查阅、复制、转移、补充。

5.4 若 FRD 认为客户对于个人信息处理的指示违反所应适用之法令者，应于合理期间内或至少于处理该个人信息前，以书面方式主动告知客户。

5.5 FRD 将维持必要的数据处理记录，记录可用于协助证明 FRD 对个人信息处理者已尽到主合约及本附录项下人信息受托处理者之义务。

6 个人信息安全事件

6.1 FRD 于知悉个人信息安全事件后将实时通知客户，并实时采取合理步骤（包括调查、确认风险影响程度及执行事件应变处理等）以降低危害并保全客户个人信息之安全性。个人信息处理者亦得与个人信息受托处理者共同合作采取合理的商业努力进行事件的调查，以消除或填补个人信息安全事件的危害。

6.2 FRD 于知悉个人信息安全事件时，应尽合理努力提供客户充足的信息，使其能通知个人信息主体或监管机构（包括第 6.3 条之内容），并满足其所应适用之隐私法律下之义务。

6.3 FRD 就个人信息安全事件之通知内容包含：（1）发生或可能发生个人信息泄漏、窜改、丢失的讯息种类、原因和可能造成的危害；（2）FRD 采取的补救措施和个人可以采取的减轻危害措施；（3）FRD 的联系方式。

6.4 FRD 没有义务评估客户数据及客户个人信息，以满足特定法律规定关于识别信息之要求。

6.5 FRD 依第 6.1 条就个人信息安全事件发出通知或提出反馈，不得被解释为 FRD 承认其对个人信息安全事件有疏失或负有责任。

7 个人信息主体权利行使

7.1 若 FRD 收到关于客户个人信息之个人信息主体权利行使请求时，FRD 将提供合理之技术与组织方式协助客户处理个人信息主体权利行使请求，在此情形下，FRD 将:

7.1.1 实时告知客户该个人信息主体权利行使请求之情形;

7.1.2 FRD 不会径向个人信息主体作出响应，法律、法规另有规定的除外;

8 数据披露与传输

8.1 为符合中华人民共和国相关法律要求，FRD 原则上将仅在中国境内处理客户数据，不会将客户数据进行跨境传输。

8.2 如客户确要将其委托 FRD 处理的个人信息进行跨境传输的，客户应当遵守所适用之隐私法律规定，取得个人信息主体的单独同意，并作为个人信息处理者与境外接收方签订合同，或采用其他合法合规的跨境传输机制后，指示 FRD 进行跨境传输。

8.3 当 FRD 收到具法律拘束力的个人信息披露请求时（例如法律调查），将于合理期间内告知客户该请求、时限及相关程序。

8.4 当 FRD 收到传输个人信息的要求，而该要求不具法律拘束力者，FRD 应拒绝该要求；于进行任何个人信息传输前，FRD 将事先咨询客户。

8.5 FRD 遵循第 9.2 条及第 9.3 条之程序后若进行个人信息传输，应记录向第三方传输个人信息之行为，包含以传输个人信息范围、传输对象、传输时间，并将该记录发送给客户。

9 分包处理者

9.1 客户授权并同意 FRD 使用列于**附录 A** 之分包处理者。

9.2 FRD 分包处理者如有增加或更换时，FRD 至少会在分包处理者开始处理客户数据及客户个人信息前 30 日，向客户通知 FRD 预期使用、新增、更换的分包处理者 (包含分包处理者之名称、所在地、及分包处理者将从事之活动)，客户有权提出反对。

9.3 自本附录生效起，客户明确授权 FRD 得使用 FRD 之关系企业作为分包处理者。关系企业指得是 FRD 以及在您所在国家收集和处理您个人信息的 FRD 关联方。

9.4 当 FRD 使用任何分包处理者时，应及时向个人信息处理者披露，且 FRD 会：

9.4.1 和分包处理者按照法律法规要求订立对个人信息保护力度不低于本附录约定的水平。

9.4.2 要求分包处理者仅会在执行数据委托处理义务之范围内依所应适用之合约规定（包含本附录）接触及使用客户数据。

9.4.3 确保分包处理者须履行本附录所述之数据保护义务，且 FRD 对本附录项下的数据处理义务及分包处理者之所有行为及疏失负责。

10 违约责任

10.1 双方应就其因违反本附录而给对方造成的任何损害向另一方承担赔偿责任。

10.2 双方同意，如果一方（"**赔偿方**"）因另一方（"**被追偿方**"）对违反本附录的行为对个人信息主体承担赔偿责任的，则赔偿方有权向被追偿方追偿。

10.3 本附录约定的赔偿金额、追偿金额应包括因违约方给守约方造成的一切损失，包括守约方进行与本附录/个人信息主体有关的起诉/应诉、申请仲裁/被申请仲裁、执行/被申请执行或采取其他措施等维护本合同项下守约方权利而产生的费用（包括但不限于诉讼费、仲裁费、财产保全费、财产保全担保费或保险费、执行费、律师费、公证费、公告费、评估费、鉴定费、拍卖费、税费、差旅费、电讯费、办案费等）。

11 法律适用及争议解决

11.1 本附录的订立、效力、执行和解释均应适用中华人民共和国法律。

11.2 个人信息处理者和个人信息受托处理者对于双方因本附录产生的纠纷以及任何一方因先行赔偿个人信息主体损害赔偿责任而向另一方的追偿，应由双方协商解决；协商解决不成的，任何一方可以依法向个人信息受托处理者所在地的有管辖权的人民法院提起诉讼。

12 通知条款

12.1 依本附录所发送之通知（包含个人信息安全事件之通知），应寄送至

FRD 之个人信息保护小组，电子邮件地址为：data@viverse.cn。

13 其他

13.1 本附录与主合约之其他部份约定间有冲突或不一致者，以本附录约定为准。

13.2 除非另有说明，附录中提及“本附录”者，指向的是本附录的一般条款下之内容。

13.3 本附录经双方正式签署后成立并立即生效。

附录 A 个人信息处理事项与个人信息安全事件通报

FRD 依主合约约定范围代客户处理客户个人信息，其处理目的、期限、方式、种类、保护措施及个人信息安全事件通报程序等事项，约定如下：

一、FRD 个人信息处理事项

(一) 处理个人信息之目的：

基于为客户提供主合约服务内容之目的，以个人信息受托处理者之角色，代客户处理客户个人信息。

处理个人信息的期限：

FRD 处理客户个人信息之期限应依客户之书面指示、或至主合约终止或解除后 FRD 为移转、归还、销毁所储存之个人信息之目的仍继续提供个人信息处理服务之期间届至时为止（两者以较早发生为准）。法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的除外。

(二) 处理个人信息的种类：

個資當事人姓名、帳號及密碼、通訊紀錄和內容、電子郵件、手機號碼

(三) 处理个人信息的方式：

包括收集、储存、使用、加工、传输、公開、提供等，但应严格限制在为履行主合约义务之必要范围。

(四) FRD 使用之分包处理者清單：

编号	分包处理者	处理方式
1	Photon	音讯处理传输
2	Microsoft	语音消息文字转换
3	AWS	存储用户传输档案
4	Agora	提供串流服务

5	IPDATA	分析 IP 位置
6	杭州网易智企科技有限公司	利用 AI 监测违法违规的内容
7	神策网络科技(北京)有限公司	分析 VIVERSE 的服务性能等

分包处理者另有变更或增加者，FRD 将另已邮件通知客户。

(五) **数据安全责任与保护措施：**

FRD 数据安全责任与保护措施，请参本附录第 5.2 条及附录 B 等相关约定。

(六) **个人信息保护影响评估：**

主合约服务期间内，FRD 将依应适用之隐私法律规定进行个人信息保护影响评估，影响评估报告和处理情况应至少保存三年。

二、个人信息安全事件通报程序

(一) 发生个人信息安全事件时，FRD 应执行个人信息安全事件通报程序，个人信息安全事件之通报程序，请参附录第 6 条。根据《中华人民共和国个人信息保护法》（下简称「**《个保法》**」），客户作为个人信息处理者，应通知「履行个人信息保护职责的部门」(下称「**中国大陆监管机关**」）和个人信息主体，通知应包括下列事项：

1. 发生或可能发生个人信息泄漏、窜改、丢失的讯息种类、原因和可能造成的危害；
2. 个人信息处理者采取的补救措施和个人可以采取的减轻危害措施；
3. 个人信息处理者的联系方式。

(二) FRD 作为个人信息受托处理者，应依客户之书面指示协助客户履行《个保法》规定之义务（包括通知中国大陆监管机构或依中国大陆监管机构之要求将个人信息安全事件通知个人信息主体）。

附录 B 数据安全措施

自附件生效日起，在适用的情况下，FRD 将执行并维持附录 B 中所应适用之数据安全措施。

数据处理活动

1. 若 FRD 有权限接触个人信息：

- FRD 使用合理的控制措施以防止对个人信息之非法接触;

2. 若 FRD 传输个人信息：

- FRD 将透过安全传输通讯协议传输个人资料;

3. 若 FRD 储存个人信息：

- FRD 将销毁所有已无使用需要的纸本文件，并保存销毁此类文件之纪录;
- 为储存及分享个人信息之目的而维持一个安全空间;
- 通过记录每个人的身份，以确保只有参与和资料输出者合作的特定项目之个人得有权限接触数据处理者的安全空间，且当该个人之劳动关系终止、或当该个人不再需要拥有接触个人信息之权限时，FRD 即会终止该个人之接触权限。

除了前述安全措施的说明外，我们会尽最大努力保障服务的连贯性和安全性，

我们实施了相应的隐私与安全措施。该措施包括以下内容：

1. 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：(1) 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 (2) 对于异常行为检测机制。

2. 网络安全：我们实施相应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：对 FRD 的数据中心实施相应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，以尽力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。

我们的服务是按照现有技术和条件所能达到的「现状」提供的，但不能随时预见和防范法律、技术以及其他风险，在法律允许的范围内，如因下列不可抗力或意外事件无法正常提供服务的，我们不承担任何法律责任：

1. **不可抗力，即双方所不能预见、并且它的发生及其后果是不能克服和不能避免的客观情况，包括但不限于如下情形：(1)自然灾害如洪水、冰雹、海啸、台风、旱灾、火灾；(2)社会因素如罢工、暴乱、战争及所适用的政策、法律、法规导致不能履行；**

2. **因电力供应故障、通讯网络故障等公共服务因素；**

3. **因黑客攻击、病毒、您自身软硬件设备异常等非 FRD 独立责任；**

4. **经提前公告或通知的，我们在短时间内的系统维护（包括但不限于排除故障、**

系统升级、系统扩容、服务器迁移)。