**关于“数据安全和个人数据保护要求”的补充声明**

1. 乙方应遵守所有适用法律，包括但不限于与个人信息隐私和数据安全相关的所有适用法律，并实施适当的保护措施来保护数据，包括制定内部管理流程和操作制度、对个人信息实行分类管理、采取加密或去标识化等安全技术措施,谨慎程度不低于业界认可的做法（如ISO 27001/27002、中国全国信息安全标准化技术委员会发布的相关国家标准、以及其他业内信息安全标准），并确保所有该等保护措施（包括处理数据的方式）符合本协议的条款及所有适用的隐私规则，以防止对项目中涉及的任何个人信息的未授权处理或非法处理，并保护任何此类个人信息免遭意外丢失，损坏或破坏。
2. 乙方应采取必要地管理、技术和物理保护措施，防止（a）合理可预见的对数据的安全性、保密性和完整性造成的内部和外部风险；以及（b）任何安全事件或安全漏洞。乙方将定期评估、测试及监督信息安全计划的主要控制、系统及程序的有效性。
3. 乙方应严格依照国家有关保护个人信息的相关法律、法规、政策的规定存储和处理因其履行本协议而可以接触到的、或以其他方式获得的个人信息。收集、使用信息主体的个人信息应当遵循合法、正当、最小必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围并经信息主体的明示同意。乙方应确保将因本项目收集和处理的个人信息存储在境内。
4. 乙方不应在任何笔记本电脑、平板电脑、闪存盘、手机或其他移动设备上长期存储数据。
5. 乙方应确保所有的数据在使用、静止和传输过程中都受到AES 256 位或更高的加密技术（或可能成为行业标准的更高的加密技术）的保护。此外，所有储存在数据库、服务器、备份媒介或其他形式的非移动设备上的数据都会受到保护，不论是使用加密、逻辑访问控制或其他可靠的保护措施（包括OWASP认可的密码散列功能或其他行业标准或同等措施），以防止所有可合理预期的数据泄露。
6. 乙方应当定期对可能处理本项目个人信息的相关人员进行安全教育和培训，并要求该等人员遵守保密义务且不得向任何第三方转移、披露或泄露任何个人信息。
7. 乙方应确保相关网站、小程序和其他运营平台的运营符合相关法律、法规的规定，包括但不限于《网络安全法》、《数据安全法》及《个人信息保护法》，并应确保运营主体已根据相关法律、法规的规定取得从事其经营活动所需的所有批准、同意、授权或法律法规要求履行的任何其他义务。
8. 应要求，甲方或甲方的第三方可以随时对乙方环境中与所处理的数据和/或所提供的服务相关的控制进行合理必要的评估、审核、检查或审查，确认是否符合本协议、本声明和任何适用的隐私规则。乙方将充分配合该等评估，允许甲方或甲方的代理人接触或获得（a）知情人士，（b）物理场所，（c）文件，（d）基础设施，及（e）处理数据的应用软件。
9. 乙方得知有证据可让乙方合理推断存在或发生安全事件或安全漏洞后，应尽快且在任何情况下不迟于二十四（24）小时将实际或疑似安全事件或安全漏洞通知甲方：（a）通过电子邮件通知甲方，并附上已读确认，发送至Asthma-Data@Gird.cn，主题中包含“安全事件”或“安全漏洞”（视情况而定）字样，并抄送乙方在甲方的主要业务联系人；并（b）依照本协议的通知条款。乙方应在通知中说明其是否有理由相信需要安全事件或安全漏洞个人信息。同时，乙方也应立即采取措施，对安全事件或安全漏洞进行补救，费用由乙方承担。对于甲方在应对和/或减轻安全事件或安全漏洞造成的损害方面发生的实际费用，乙方将补偿给甲方。
10. 除适用的隐私规则可能严格要求的以外，如果没有事先获得甲方的事先书面同意，乙方不会将任何安全事件或安全漏洞通知任何第三方或政府机构。在不限制前述规定的前提下，乙方也同意尽一切合理的努力，并在自行承担全部成本费用的情况下，依照法律、法规、国标的要求，及时对前述安全事件做出响应，并及时修复相关安全漏洞。
11. 所有因乙方违反法律法规及本协议约定导致甲方及相关的信息主体所遭受的任何成本、罚款、索赔、费用，由乙方自行承担。项目完成或本协议期限届满或终止后，任何纸质的文件将由乙方交由甲方保留。