

数据处理条款

订立双方：

客户（下称“**数据控制者**”）

与

HCL America, Inc.（下称“**数据处理者**”）。

双方特此约定以下内容：

1. 这些数据处理条款的标的事项

- 1.1. 这些数据处理条款只适用于处理受欧盟数据保护法ⁱ管辖的个人数据[在双方就[提供服务]达成的[日期]生效的协议范围内]（“服务”）（下称“协议”），并且特此以引用方式纳入协议，并受协议管辖。
- 1.2. “欧盟数据保护法”一词指 2016 年 4 月 27 日欧洲议会和理事会的条例 (EU) 2016/679，用于保护自然人在处理个人数据和自由移动这些数据方面的权利，并撤销指令 95/46/EC（下称“《通用数据保护条例》”）。

ⁱ 虽然此处假定有一个欧盟模型，但是根据提供服务时所在的地点，可能会适用其他法律。

- 1.3. “处理”、“个人数据”、“数据控制者”和“处理者”等术语应具有欧盟数据保护法赋予它们的含义。
- 1.4. 如果数据处理器将在履行与数据控制者签订的协议期间，将代表数据控制者处理受欧盟数据保护法约束的个人数据，则应适用这份数据保护协议的条款。附录 2 概述了个人数据的类别、数据主体类别及处理个人数据的目的。

2. 数据控制者和数据处理器

- 2.1. 数据控制者将决定数据处理器访问或处理个人数据的范围、目的和方式。数据处理器只会按照数据控制者的书面指令处理个人数据。
- 2.2. 除为了遵守数据处理器必须履行的法律义务外，数据处理器将只会以对提供服务来说合适的方式并且只在这种合适的范围内，按照数据控制者的书面指示处理个人数据。在这种情况下，数据处理器应在处理前将该法律义务通知数据控制者，除非该法律明确禁止向数据控制者提供此类信息。如果数据处理器认为指示违反本条例，其应当及时通知数据控制者。
- 2.3. 双方已签订协议，以便为了附件 22 所述的目的，受益于处理器在保护和处理个人数据方面的专业知识。应允许数据处理器执行自己的方向，选择和使用它认为为达到这些目的所必需的手段，但需要符合这些数据处理条款的要求。

- 2.4. 数据控制者保证，其拥有所有必要的权利，将个人数据提供给数据处理者，以便为了相关服务而处理数据。在适用的数据保护法律要求的范围内，数据控制者有责任确保取得任何必要的主体同意进行此类处理，并确保保存关于此类同意的记录。如果此类同意被数据主体撤销，数据控制者有责任将撤销的事实通知数据处理者，而数据处理者亦有责任执行任何有关进一步处理该等个人数据的数据控制者的指示。

3. 保密性

- 3.1. 在不影响双方之间任何现有合同安排的情况下，数据处理者应将所有个人数据视为严格保密，并将此类个人数据的保密性告知其所有从事处理此类个人数据的雇员、代理和/或获批准的子处理者。数据处理者应确保所有上述人员或各方已签署适当的保密协议，或以其他方式受保密义务约束，或者负有适当的法定保密义务。

4. 安全性^{ii, iii}

- 4.1. 考虑到目前的技术水平、实施成本以及处理的性质、范围、背景和目的，还有自然人的权利和自由面临的拥有各种可能性和严重程度的风险，在不损害双方商定的任何其他安全标准的情况下，数据控制者和数据处理者应实施适当的技术和组织措施，以确保与风险相适应的个人数据处理安全级别。这些措施应酌情包括：

ii GDPR 第 32(3) 条：遵守第 40 条所述的获批准的行为准则，或遵守第 42 条所述的获批准的认证机制，这可以作为一种元素，借此证明符合本条款第 1 款规定的要求。

iii 处理者可以通过分享认证来展示合规，

- (a) 采取措施以确保只能由获授权人士为本数据处理条款附录 2 所列的目的而查阅个人数据；
 - (b) 在评估适当的安全账户级别时，应特别考虑处理所带来的所有风险，例如意外或非法损毁、遗失或更改、未经授权或非法储存、处理、访问或披露个人数据；
 - (c) 个人数据的假名化和加密；
 - (d) 确保处理系统和服务的持续保密性、完整性、可用性和弹性的能力；
 - (e) 在发生物理或技术事故时，及时恢复个人数据可用性和访问权限的能力
 - (f) 定期测试、评估和评价用于确保处理个人数据安全性的技术及组织措施的有效性；
 - (g) 采取措施，在向数据控制者提供服务的系统内，识别个人数据处理方面的漏洞；
 - (h) 双方在附录 3 中商定的措施。
- 4.2. 数据处理者须始终就处理个人数据制定适当的书面安全政策，并在任何情况下均需概述第 4.1 条所述的措施。
- 4.3. 应数据控制者的要求，数据处理者应展示其根据此处第 4 条所采取的措施，以允许数据控制者对这些措施进行审计和测试。数据处理者有权获得数据控制者提供的至少 14 天提前通知，由数据控制者或由已经与数据控制者签订保密协议的第三方审计与个人数据相关的数据处理者的场所和操作。客户应自行承担与审计有关的一切费用和开支。除监管机构所进行的审计外，]进行的审计在任何日历年不得超过一次，而且必须在进行审计前至少提前 14 天发出书面通知。数据处理者应配合由数据控制者或其代表进行的此类审计。客户有权对供应商处理客户个人数据时使用的系统进行审计，以核实供应商在进行此类处理时是否遵守了其在本协议中的义务。任何审计均须符合下列条件：
- i 被指定进行审计的任何第三方不得与处理者或其任何关联公司存在竞争关系；
 - ii. 处理者无需授权任何第三方访问其任何系统、设施或场所，除非且直到该第三方已签订令处理者合理满意的保密协议；
 - iii. 审计范围应严格限于处理个人数据时使用的处理者系统（或处理者系统的部分）；

- iv. 在不限第 (c) 款的情况下，控制者或任何第三方均无权访问关于供应商的任何其他客户或供应商的内部成本或利润的任何数据或信息。

5. 安全改进

- 5.1. 各方承认，安全要求在不断变化，并且有效的安全需要经常评估以及定期改进过时的安全措施。因此，数据处理者将持续评估根据第 4 条实施的措施，并将加强、补充和改进这些措施，以保持符合第 4 条规定的要求。双方将真诚地协商执行适用的数据保护法或有管辖权的数据保护机构规定的具体更新的安全要求所需要的重大变更的费用（如果有的话）。
- 5.2. 如果由于不时修订适用的数据保护法而需要修订协议，以便向数据处理者执行数据控制者指令，以改进安全措施，则双方将真诚协商对本协议的修改。

6. 数据传输

- 6.1. 对于任何（计划的）永久性或临时性的个人数据传输到欧洲经济区以外的没有足够保护级别的国家的情况，数据处理者应将通知数据控制者，并且只有在获得数据控制者的授权后才应执行此类（计划的）传输。附录 4 提供了一份数据控制者在达成协议和这些数据处理条款后同意的传输清单。
- 6.2. 如果数据控制者或数据处理者依赖一个特定的法定机制来规范国际数据传输，但该机制随后被修改、撤销或在有管辖权的法院被裁定无效，那么数据控制者和数据处理者同意真诚合作，及时终止传输或寻求一个合适的替代机制，可以合法地支持传输。

7. 信息义务和事件管理

- 7.1. 当数据处理器意识到会影响处理作为服务协议主题的个人数据的事件时，它应当及时把有关事件通知数据控制者，应当始终配合数据控制者，并应当遵循关于此类事件的数据控制者的指令，从而使数据控制者能够对事件进行彻底调查，作出正确的回应，并就事件采取适当的进一步措施。
- 7.2. 第 7.1 条所使用的“事件”一词在任何情况下均应被理解为：
 - (a) 就使行欧盟数据保护法中的数据主体权利而提出的投诉或要求；
 - (b) 政府官员调查或没收个人数据，或有明确迹象显示该等调查或没收即将进行；
 - (c) 未经授权或意外地访问、处理、删除、遗失或以任何形式非法处理个人数据；
 - (d) 任何违反这些数据处理条款第 3 及 4 条包含的安全性及/或保密性规定的行为，导致意外或非法破坏、损失、变更、未经授权披露或访问个人数据，或者任何有关已发生或即将发生此类违约行为的迹象；
 - (e) 其中数据处理器认为，执行从数据控制者接收到的指示将违反数据控制者或数据处理器需要遵守的适用法律。
- 7.3. 数据处理器应始终具备书面程序，使其能够及时向数据控制者提供关于事件的回应。如果根据适用的欧盟数据保护法，事件有合理可能会需要数据控制者发出数据泄露通知，则数据处理器应执行其书面程序，使其能够在不迟于知晓该事件后 72 小时内通知数据控制者。

7.4. 根据此处第 7

条向数据控制者发出的任何通知，均应向数据控制者的雇员发出，其联系信息请参见本数据处理条款的附录 1，并且通知应包含：

- (a) 事件性质描述，包括在可能的情况下，相关数据主体类别及大致数目，以及相关个人数据记录的类别及大致数目；
- (b) 数据处理者的数据保护官或其他可提供更多信息的联系人姓名和联系方式；
- (c) 对事件可能造成的后果的描述；以及
- (d) 描述数据处理者为处理该事件而采取或拟采取的措施，包括在适当情况下为减轻其可能的不利影响而采取的措施。

8. 与子处理者签约

[数据控制者授权数据处理者将位于国家地点的子处理者用于附录 2 所述的与服务相关的活动

- 8.1. 数据处理者应确保子处理者受数据处理者在这些数据处理条款下同样的数据保护义务的约束。
- 8.2. 数据控制者可以要求数据处理者审计第三方子处理者，或者提供已进行审计的确认（或在可能的情况下，获取或协助客户获取关于第三方子处理者操作情况的第三方审计报告），以确保数据处理者按照本协议规定履行其义务。

9. 归还或销毁个人数据

- 9.1. 在本协议和本数据处理条款终止时，根据数据控制者的书面请求下，或者当满足了服务中商定的所有目的从而不再需要处理数据时，数据处理者须删除、销毁或将所有个人数据交回数据控制者，并销毁或归还任何现有副本。
- 9.2. 数据处理者构应当把协议和这些数据处理条款终止一事通知所有支持其处理个人数据的第三方，并且须确保所有此类第三方自行销毁此类个人数据，或将此类个人数据归还给数据控制者。

10. 协助数据控制者

- 10.1. 数据处理者应在可能的情况下，通过适当的技术和组织措施协助数据控制者，以履行数据控制者回应行使数据主体在 GDPR

下的权利的要求的义务。

- 10.2. 数据处理者应协助数据控制者确保履行第 4 条（安全性）规定的义务，并在考虑到处理的性质和数据可用信息的情况下，协助其与监管当局进行 GDPR 第 36 条要求的事先磋商。

10.3

数据处理者应向数据控制者提供所有必要的信息，以证明数据处理者遵守其义务，并允许和协助数据控制者或数据控制者授权的其他审计人员进行审计，包括检查。

11. 持续时间和终止

- 11.1. 这些数据处理条款应自适用协议的生效日起生效，其中该协议用于管理数据处理者向数据控制者提供的支持、维护和/或专业服务。
- 11.2. 协议和这些数据处理条款的终止或期满不免除数据处理者根据第 3 条承担的保密义务。
- 11.3. 数据处理者应处理个人数据，直至协议终止之日为止，除非数据控制者另有指示，或者直到根据数据控制者的指示归还或销毁个人数据。

12. 杂项

- 12.1. 如果这些数据处理条款的规定与服务协议的规定之间存在不一致，则以这些数据处理条款的规定为准。
- 12.2. 数据控制者不得不合理地拒绝或延迟同意就数据处理者为保护数据处理者免受相关附加风险而提出的对本附录的任何相应变更。如果数据控制者对本附录提出任何其他变更，而数据控制者合理地认为此类变更对满足任何数据保护法的要求来说是必要的，则双方应迅速讨论拟议的变更，并本着诚意进行谈判，以期就这些或其他变更达成协议并予以实施，从而在合理可行的情况下，尽快满足客户通知内确定的要求。
- 12.3. 如果数据处理者收到数据主体根据任何数据保护法律就其个人数据提出的要求，数据处理者应及时通知数据控制者；并且要确保签约的处理者不会提出要求，在这种情况下，除非根据客户或相关客户关联公司的书面指示，或者根据签约处理者所适用的法律的要求，而在这种情况下，数据处理者应在适用法律允许的范围内，在数据处理者回应请求之前，将此类法律要求通知数据控制者。

- 12.4. 这些数据处理条款受处理个人数据的相关会员国的法律的管辖。任何源自或涉及本数据处理条款的争议应只提交给处理个人数据的相关会员国的主管法院。
- 12.5. 双方同意按要求签署下列附录。

附录 1:

数据控制者的[数据保护官/合规官]的联系方式。

[联系方式]

数据处理者的[数据保护官/合规官]的联系方式。

[联系方式]

附录 2:

将在协议范围内处理的个人数据，以及处理这些数据的目的

附录 3:

安全措施

附录 4:

数据控制者授权进行的、向欧洲经济区以外没有适当保护级别的国家进行的数据传输：