世纪互联

世纪互联在线服务
数据保护补充协议

最后更新日期：2022 年 1 月 15 日

这些承诺自 2022年 1 月 15 日起对世纪互联具有约束力。

**目录**

[简介 3](#_Toc92899585)

[适用的 DPA 条款与更新 3](#_Toc92899586)

[电子通知 3](#_Toc92899587)

[早期版本 3](#_Toc92899588)

[定义 4](#_Toc92899589)

[一般条款 5](#_Toc92899590)

[遵守法律 5](#_Toc92899591)

[数据保护条款 5](#_Toc92899592)

[范围 5](#_Toc92899593)

[数据处理的性质；所有权 5](#_Toc92899594)

[所处理数据的披露 6](#_Toc92899595)

[个人数据的处理 6](#_Toc92899596)

[数据安全性 7](#_Toc92899597)

[安全事件通知 8](#_Toc92899598)

[数据位置 8](#_Toc92899599)

[数据保留和删除 8](#_Toc92899600)

[处理方保密承诺 8](#_Toc92899601)

[关于使用子处理方的通知和控制 8](#_Toc92899602)

[敏感个人数据 9](#_Toc92899603)

[如何联系世纪互联 9](#_Toc92899604)

[附录 A – 安全措施 10](#_Toc92899605)

[附录 B – 数据主体和个人数据的类别 12](#_Toc92899606)

[附录 C – 额外保护措施附录 14](#_Toc92899607)

[附件 1 – 2010标准合同条款（处理方） 15](#_Toc92899608)

[附件 2 – 欧盟通用数据保护条例条款 19](#_Toc92899609)

简介

双方同意，本世纪互联在线服务数据保护补充协议（“DPA”）规定了双方与在线服务涉及的客户数据及个人数据的处理活动和安全性相关的义务。本 DPA 以引用的形式纳入在线服务条款（或使用权利的后续位置）中。客户使用非世纪互联产品的活动受单独的条款（包括不同的隐私和安全条款）的约束。

如果本 DPA 条款与世纪互联客户协议的任何其他条款之间存在任何冲突或不一致，则以本 DPA 为准。本 DPA 条款将取代世纪互联隐私声明中的任何冲突条款，这些隐私声明中的冲突条款原本适用于此处定义的客户数据或个人数据的处理。在此说明，当2010标准合同条款适用时，[附件 1](#Attachment1) 中的2010标准合同条款（如果适用的话）优先于本 DPA 条款中的任何其他条款，这与2010标准合同条款的第 10 条一致。

世纪互联在本 DPA 中向签有世纪互联客户协议的所有客户作出承诺。对于客户而言，这些承诺对世纪互联具有约束力，无需考虑 (1) 适用于任何给定在线服务订购的使用权利，或 (2) 任何引用 OST 的其他协议。

适用的 DPA 条款与更新

**更新限制**

客户续订或新订购某个在线服务时，当时的 DPA 条款将会适用，且该 DPA 条款在该在线服务的订购期内不会更改。

**新功能、补充程序或相关软件**

尽管已规定上述更新限制，世纪互联推出新的功能、补充程序或相关软件（即以前的订购不包含的内容）后，世纪互联可以为客户对这些新的功能、补充程序或相关软件的使用而提供适用的条款或相应更新 DPA。如果这些条款中包含对 DPA 条款的任何实质性不利变更，世纪互联将为客户提供选择使用新的功能、补充程序或相关软件的机会，且不会影响客户对普遍可用的在线服务的现有功能的使用。如果公司不使用新功能、补充程序或相关软件，则相应的新条款将不会适用。

**政府规定和要求**

尽管已规定上述更新限制，如果有任何现行或未来的法律、政府要求或义务，(1) 要求世纪互联遵守那些通常不适用于境内的业务运营的任何法规或要求；(2) 给世纪互联继续不加修改地提供产品带来困难；和/或 (3) 导致世纪互联认为本DPA条款或在线服务可能与任何此类法律、要求或义务发生冲突，则世纪互联可以修改或终止在线服务。

电子通知

世纪互联可能会通过电子方式向客户提供关于在线服务的信息和通知，包括通过电子邮件、在线服务门户或世纪互联指定的网站。通知自世纪互联发出之日起生效。

早期版本

DPA 条款提供适用于当前可用的在线服务的条款。如需 DPA 条款的早期版本，客户可以参阅<https://www.21vbluecloud.com/ostpt/>，或联系其经销商或世纪互联客户经理。

定义

本 DPA 中使用但未定义的所有术语将与世纪互联客户协议中的同一术语含义相同。在本 DPA 中会使用以下术语（定义如下）：

“客户数据”指客户通过使用在线服务向世纪互联提供或以客户的名义提供的所有数据，包括所有文本、声音、视频或图像文件以及软件。

“中国法律法规”是指适用于本DPA的中华人民共和国的法律和法规，包括但不限于《网络安全法》《数据安全法》《个人信息保护法》（即下文定义的“《个保法》”）及其任何更新。

“数据保护要求”指中国法律法规、GDPR、当地 EU/EEA 数据保护法律和任何适用的法律法规，以及与以下两方面相关的其他法律要求：(a) 隐私和数据安全；(b) 任何个人数据的使用、收集、保留、存储、保护、披露、传输、处置及其他处理。

“DPA 条款”是指 DPA 中的条款以及使用权利中任何特定在线服务的条款，这些条款专门针对特定在线服务（或在线服务功能）补充或修改 DPA 中的隐私和安全条款。如果 DPA 与此类特定在线服务条款之间存在任何冲突或不一致，则对于适用的在线服务（或在线服务的功能）而言，应以特定在线服务条款为准。

“GDPR”指欧洲议会和欧盟理事会 2016 年 4 月 27 日颁布的，关于在处理个人数据时对自然人的保护、此类数据的自由移动以及废除指令 95/46/EC 的法规 (EU) 2016/679（一般数据保护条例）。

“当地 EU/EEA 数据保护法律”指实施 GDPR 的任何附属法律和法规。

“GDPR 条款”指[附件2](#Attachment2) 中的条款，根据这些条款，世纪互联会按照 GDPR 第 28 条的要求，就其个人数据处理活动作出具有约束力的承诺。

“个人数据”指与已确定身份或可确定身份的自然人相关的任何信息。可确定身份的自然人指能够直接或间接地通过身份标识（例如，姓名、身份证号、位置数据、在线身份标识）或特定于该自然人身体、生理、基因、心理、经济、文化或社会身份的一个或多个因素确定其身份的人。

“《个保法》”指2021年11月1日起生效的《中华人民共和国个人信息保护法》。

“2010标准合同条款”指适用于将个人数据传输至在无法确保提供充分的数据保护的第三方国家/地区设立的处理方之事宜的标准数据保护条款（详见 2010 年 2 月 5 日欧盟委员会决议 2010/87/EC 批准的 GDPR 第 46 条）。2010标准合同条款位于[附件 1](#Attachment1) 中。

“2021标准合同条款”指适用于将个人数据传输至在无法确保提供充分的数据保护的第三方国家/地区设立的处理方相关事宜的标准数据保护条款（处理方到处理方模式，详见2021年6月4日欧盟委员会决议2021/914/EC批准的GDPR第46条）。

“子处理方”指世纪互联所使用的负责处理客户数据和个人数据的其他处理方，如 GDPR 第 28 条所述。

本 DPA 中使用但未定义的术语（例如“个人数据违规”、“处理”、“控制方”、“处理方”、“概况分析”、“个人数据”和“数据主体”）将沿用 GDPR 第 4 条所定义的含义，而无论 GDPR 是否适用。术语“数据导入者”和“数据导出者”具有标准合同条款中规定的含义。

一般条款

遵守法律

世纪互联将遵守适用于在线服务的提供的所有法律和法规，包括安全违规行为通知法和数据保护要求。但是，世纪互联没有责任遵守任何适用于客户或客户的行业但通常不适用于信息技术服务提供商的法律或法规。世纪互联无权决定客户数据是否包含受任何特定法律或法规约束的信息。所有安全事件均受下面的安全事件通知条款约束。

客户必须遵守与其使用在线服务相关的所有适用法律和法规，包括与生物数据、通信保密和数据保护要求相关的法律。客户应负责确定在线服务是否适合用于存储和处理受特定法律或法规约束的信息，且有责任以符合客户的法律和监管义务的方式使用在线服务。客户负责响应第三方就客户对在线服务的使用提出的任何要求，如要求根据中国法律法规或其他适用法律删除内容。

数据保护条款

本部分 DPA 包括以下小节：

* 范围
* 数据处理的性质；所有权
* 所处理数据的披露
* 个人数据的处理
* 数据安全性
* 安全事件通知
* 数据位置
* 数据保留和删除
* 处理方保密承诺
* 关于使用子处理方的通知和控制
* 生物特征数据
* 如何联系世纪互联
* 附录 A – 安全措施
* 附录B – 数据主体和个人数据的类别
* 附录C – 额外保护措施附录

范围

本 DPA 条款适用于所有在线服务，但 OST 附件 1（或使用权利的后续位置）中明确规定排除的任何在线服务除外，这些在线服务受适用的在线服务特定条款中引用的隐私和安全条款的约束。

在此说明，本DPA条款仅适用于在世纪互联和世纪互联的子处理方所控制的环境中的数据处理。这包括通过在线服务发送至世纪互联的数据，但不包括留存在客户场所或任何客户选定的第三方操作环境中的数据。

与在线服务通常采用的隐私和安全措施相比，预览版采用的此类措施可能会减少或有所不同。除非另有规定，否则客户不应使用预览版来处理具有法律或法规遵从性要求的个人数据或其他数据。本 DPA 中的以下条款对预览版不适用：个人数据的处理和数据安全性。

数据处理的性质；所有权

世纪互联将仅根据客户记录在案的指令，遵守下述限制，并出于以下目的使用或以其他方式处理客户数据和个人数据：(a) 根据客户的书面指示为客户提供在线服务；(b) 为向客户提供在线服务而进行的相关经营活动。在双方之间，客户保有对客户数据的所有权利、所有权和权益。除了本节中客户授予世纪互联的权利之外，世纪互联未获得有关客户数据的任何权利。本段不影响世纪互联向客户许可的软件或服务中包含的世纪互联的权利。

**处理数据以便为客户提供在线服务**

就本 DPA 而言，“提供”在线服务包括：

* 交付客户及其用户所许可、配置和使用的功能，包括提供个性化用户体验；
* 故障排除（预防、检测和修复问题）；以及
* 持续改进（安装最新更新，以及对用户生产力、可靠性、效力、质量和安全性进行改进）。

提供在线服务时，世纪互联不会出于以下目的使用或以其他方式处理客户数据或个人数据：(a) 用户画像、(b) 广告或类似商业目的，或者 (c) 旨在创建新功能、服务或产品或出于任何其他目的的市场调研，除非此类使用或处理符合客户记录在案的指令。

**为经营活动而进行处理**

就本 DPA 而言，“经营活动”包含以下各项，每项均作为向客户提供在线服务的一个相关事项：(1) 帐单和帐户管理；(2) 报酬（例如计算员工佣金和合作伙伴奖励）；(3) 内部报告和业务建模（例如，预测、收入、产能规划、产品战略）；(4) 打击可能影响世纪互联或世纪互联产品的欺诈、网络犯罪或网络攻击；(5) 改进可访问性、隐私或能效等核心功能；以及 (6) 财务报告和履行法律义务（遵守下文概述的所处理数据的披露限制）。

在为经营活动而进行处理数据时，世纪互联将遵守数据最小化原则且不会出于以下目的使用或以其他方式处理客户数据或个人数据：(a) 用户画像，(b) 广告或类似商业目的，或 (c) 任何本节规定目的之外的其他目的。

所处理数据的披露

世纪互联将不会披露或允许任何人访问所处理的数据，除非：(1) 客户指示；(2) 本 DPA 规定；或者 (3) 法律要求。就本节而言，“所处理数据”指：(a) 客户数据；(b) 个人数据；以及 (c) 世纪互联根据世纪互联客户协议处理的与在线服务相关的、属于客户保密信息的任何其他数据。所有对该等数据的处理都应遵守世纪互联在世纪互联客户协议中的保密义务。

除非法律要求，否则世纪互联不会向执法部门披露或允许其访问所处理数据。如果执法部门要求世纪互联提供所处理数据，世纪互联将建议执法部门直接与客户联系，由客户向其提供相关数据。如果世纪互联被强制要求向执法部门披露或允许其访问所处理数据，世纪互联将立即通知客户并提供要求的副本，除非法律禁止这样做。

收到任何其他第三方对所处理数据的请求后，世纪互联应立即通知客户，除非法律禁止这样做。世纪互联会拒绝相关请求，但法律另有要求的除外。如果请求有效，世纪互联会尝试安排第三方直接从客户处请求数据。

世纪互联不会向任何第三方提供以下各项：(a) 对所处理数据的直接、间接、全部或自由访问权限；(b) 用于保护所处理数据安全的平台加密密钥或破解此类加密的能力；或 (c) 对所处理数据的访问权限（如果世纪互联意识到相关数据将被用于第三方的请求中所述内容以外的目的）。

为支持上述条款，世纪互联可能会向第三方提供客户的基本联系信息。

个人数据的处理

所有由世纪互联处理的与提供在线服务相关的个人数据都是作为 (a) 客户数据或 (b) 由世纪互联产生、衍生或收集的数据（包括因客户使用基于服务的功能而发送给世纪互联的数据）的一部分获得的。客户通过使用在线服务向世纪互联提供的或以客户的名义提供的个人数据也属于客户数据。假名标识符可能包含在世纪互联为提供在线服务而处理的数据中，也属于个人数据。假名化或去标识化但不匿名的任何个人数据，或从个人数据衍生的个人数据同样属于个人数据。

双方还同意本小节中的以下条款：

**客户和世纪互联的角色和责任**

*受GDPR约束的处理*

如果世纪互联是受 GDPR 约束的个人数据的处理方或子处理方，则该处理活动受[附件 2](#Attachment3) 中 GDPR 条款的约束，并且：

客户和世纪互联同意，客户是个人数据的控制方，而世纪互联是此类数据的处理方，但以下情况除外：(a) 当客户充当个人数据处理方时，世纪互联是子处理方；或 (b) 特定在线服务的条款或本 DPA 中另有规定的情况。当世纪互联充当个人数据的处理方或子处理方时，只能依照记录在案的客户指令来处理个人数据。客户同意，其世纪互联客户协议（包括 DPA 条款和任何适用的更新）连同产品文档以及客户使用和配置在线服务中相关功能的活动，系客户就个人数据的处理向世纪互联作出的完整的记录在案的指令。任何附加或替代的说明必须依照修订客户的世纪互联客户协议的流程得到各方同意。在 GDPR 适用且客户是处理方的情况下，客户向世纪互联保证，客户的指令（包括指派世纪互联作为处理方或子处理方）已获得相关控制方的授权。

如果世纪互联在为向客户提供在线服务的相关经营活动中须使用或以其他方式处理受GDPR约束的个人数据，则世纪互联将遵守 GDPR 针对此类使用规定的独立数据控制方应尽的义务。世纪互联为经营活动而处理此类数据时，应接受 GDPR 针对数据“控制方”规定的额外责任，以便：(a) 在 GDPR 规定的范围内，遵守监管要求；(b) 为客户提供更高的透明度，并确认世纪互联在进行此类处理时应承担的责任。世纪互联使用保护措施保护正在处理的客户数据和个人数据，包括本 DPA 中指明以及 GDPR 第 6(4) 条中所述的措施。关于本段规定的个人数据处理，世纪互联作出“额外保护措施”附录中的承诺，条件是：(i) 出于经营活动而传输的任何个人数据（如“额外保护措施”附录中所述）被视为“相关披露”；(ii) “额外保护措施”附录中的承诺适用于此类个人数据。

*受《个保法》约束的处理*

客户和世纪互联同意，客户是《个保法》下个人数据的“个人信息处理者”（在《个保法》下的用词，相当于GDPR中的控制方），而世纪互联是此类数据的受托处理者（如《个保法》所界定），但以下情况除外： (a) 当客户充当个人数据的受托处理者时，世纪互联是其子处理方；或 (b) 特定在线服务的条款或本DPA中另有规定的情况。当世纪互联充当个人数据的受托处理者或子处理方时，世纪互联只能依照记录在案的客户指令来处理个人数据。客户同意，其世纪互联客户协议（包括DPA条款和任何适用的更新）连同产品文档以及客户使用和配置在线服务中相关功能的活动，系客户就处理个人数据向世纪互联作出的完整的记录在案的指令。任何附加或替代的说明必须依照修订客户的世纪互联客户协议的流程得到各方同意。在《个保法》适用且客户系受托处理者的情况下，客户向世纪互联保证，客户的指令（包括指派世纪互联为受托处理者或子处理方）已获得相关“个人信息处理者”的授权。

如果世纪互联在为向客户提供在线服务的相关经营活动中须使用或以其他方式处理受《个保法》约束的个人数据，在客户和世纪互联之间，世纪互联将遵守《个保法》针对此类使用规定的独立“个人信息处理者”应尽的义务，而客户有责任从《个保法》规定的相关数据主体处获得所有必要的同意，以便向世纪互联提供此类个人数据（为经营活动之目的，世纪互联可能将这些个人数据传输至中国境外的第三方）。为与其业务运营有关的处理而言，世纪互联接受《个保法》就数据的“个人信息处理者”规定的额外责任，以：(a) 在《个保法》规定的范围内，遵守监管要求； (b) 为客户提供更高的透明度，并确认世纪互联在进行此类处理时应承担的责任。世纪互联使用保护措施保护正在处理的客户数据和个人数据，包括本DPA中指明以及《个保法》中所述的措施。

**处理详细信息**

双方确认并同意：

* **主题事项。**处理活动的主题事项仅限于本 DPA 的上述“数据处理的性质；所有权”一节、 GDPR 及《个保法》范围内的个人数据。
* **处理活动的持续时间。**处理活动的持续时间应遵照客户指令和 DPA 条款。
* **处理活动的性质和目的。**处理活动的性质和目的应为依照客户的世纪互联客户协议提供在线服务，以及保证为向客户提供在线服务时的相关经营活动（详见本 DPA 的上述“数据处理的性质；所有权”一节）。
* **数据类别。**世纪互联在提供在线服务时处理的个人数据类型包括：(i) 客户选择包含在客户数据中的个人数据；以及 (ii) 《个保法》第4条定义的或GDPR 第 4 条明确规定的（视情况而言）可能由世纪互联产生、衍生或收集的数据，包括因客户使用基于服务的功能而发送给世纪互联的数据。对于客户选择包含在客户数据中的个人数据的类型，可以是客户根据 GDPR 第 30 条作为控制方所维护记录中指明的个人数据的任何类别，包括附录B中规定的个人数据的类别。
* **数据主体。**数据主体的类别为客户的代表和最终用户（如员工、承包商、合作方和客户），可能包括客户根据 GDPR 第 30 条作为控制方所维护记录中指明的数据主体的任何其他类别，包括附录B中规定的数据主体的类别。

**数据主体权利；协助完成请求**

世纪互联将通过与在线服务的功能和世纪互联所担任的处理方角色相一致的方式，向客户提供数据主体的个人数据，并使客户能够满足数据主体的请求，令其能够行使《个保法》或 GDPR （视情况而言）赋予他们的权利。如果世纪互联收到客户的数据主体发出的要求行使《个保法》或 GDPR 赋予的一项或多项与由世纪互联充当数据处理方或子处理方的在线服务相关的权利的请求，则世纪互联应让数据主体直接向客户提出请求。客户应负责回应任何此类请求，包括在必要时使用在线服务的功能进行回应。世纪互联应满足客户的合理请求，协助客户响应此类数据主体请求。

**处理活动的记录**

如果 GDPR 或《个保法》要求世纪互联收集和维护与客户有关的某些信息的记录，客户将应要求将此类信息提供给世纪互联，并保持其准确和最新。如果 GDPR 或《个保法》要求，世纪互联可将任何此类信息提供给监管机关。

数据安全性

**安全实践和策略**

世纪互联将实施并维持适当的技术和组织措施来保护客户数据和个人数据，防止传输、存储或以其他方式处理的个人数据遭到意外或非法破坏、丢失、更改、未经授权的披露或访问。世纪互联安全策略会规定这些措施。世纪互联将向客户提供该策略，以及客户合理要求获取的有关世纪互联安全实践和策略的其他信息。

此外，这些措施应符合 ISO 27001、ISO 27002 和 ISO 27018 中规定的要求。客户可以获得针对上述要求的安全控制措施的说明。每项核心在线服务均实施和维持附录 A 中规定的安全措施，以保护客户数据。

世纪互联可随时添加行业或政府标准。世纪互联将不会删除 ISO 27001、ISO 27002、ISO 27018，除非该标准或框架不再在行业中使用并且已被后续标准或框架（如果有）取代。

**数据加密**

默认情况下，在客户和世纪互联之间的公共网络上或世纪互联数据中心之间传输的客户数据（包括其中涉及的任何个人数据）是经过加密的。

世纪互联也会对在线服务中静态存储的客户数据加密。在客户或代表客户的第三方可以基于在线服务而构建应用程序的情况下（例如某些 Azure 服务），客户可以自行决定使用世纪互联提供的功能或客户从第三方获得的功能对存储在这类应用程序中的数据进行加密。

**数据访问**

世纪互联采用最低访问权限机制来控制对客户数据（包括其中涉及的任何个人数据）的访问。世纪互联实施基于角色的访问控制，以确保对服务运营所需的客户数据的访问出于合理目的，并受到管理层的监督和批准。对于核心在线服务，世纪互联坚持实施附录A“安全措施”表中所述的访问控制机制，且世纪互联人员不能长期访问客户数据，任何所需的访问均为限时的。

**客户责任**

客户需自行负责独立确定在线服务的技术和组织措施是否符合客户的要求，包括其在适用的数据保护要求下的任何安全义务。客户承认并同意，（考虑到技术现状、实施成本以及个人数据处理活动的性质、范围、情境和目的及对个人的风险）世纪互联实施和维持的安全实践和政策能够提供与个人数据相关的风险相适应的安全级别。客户负责针对客户提供或控制的组件（例如通过 Microsoft Intune 登记的设备或 Microsoft Azure 客户虚拟机或应用程序中的组件）实施和维持隐私保护及安全措施。

**合规性审计**

世纪互联将通过下列方式，对其在处理客户数据和个人数据的过程中使用的计算机、计算环境和物理数据中心的安全性进行审计：

* 在标准或框架规定进行审计的情况下，每年至少发起一次此类控制标准或框架的审计。
* 每次审计将根据每个适用的控制标准或框架的监管或认证机构的标准和规则执行。
* 每次审计将由合格、独立的第三方安全审计人员执行，这些人员由世纪互联选择并支付相关费用。

每次审计均会生成审计报告（以下简称“世纪互联审计报告”）。如果客户要求，世纪互联会向客户提供各份世纪互联审计报告。世纪互联审计报告将受世纪互联和审计人员的保密和分发限制的约束。

如果2010标准合同条款适用，则本节是2010标准合同条款中的条款 5 的第 f 段和条款 12 的第 2 段的附加内容。DPA 本节中的任何内容均不会更改2010标准合同条款或 GDPR 条款的内容，也不会影响任何监管机关或数据主体在2010标准合同条款或数据保护要求下享有的权利。

安全事件通知

如果世纪互联意识到存在导致意外或非法地破坏、丢失、更改、在未经授权情况下披露或访问世纪互联处理的客户数据或个人数据的违反安全性规定的活动（以下均简称“安全事件”），世纪互联应立即 (1) 向客户通知安全事件；(2) 调查安全事件并向客户提供有关安全事件的详细信息；并 (3) 采取合理措施减缓影响并最大限度地减少安全事件导致的损坏，且不得出现不当延误。

安全事件通知将通过世纪互联选择的任何方式（包括电子邮件）发送给客户的一个或多个管理员。客户须自行负责确保其管理员维护每个适用的在线服务门户上的联系信息的准确性。客户须自行负责遵守适用于客户的事件通知法下的义务，并履行与任何安全事件相关的任何第三方通知义务。

世纪互联应采取合理的措施协助客户履行 GDPR 第 33 条、《个保法》和其他适用法律和法规的规定的将此类安全事件通知相关监督机构和数据主体的客户义务。

世纪互联根据本节规定通知或响应安全事件不表示世纪互联承认与安全事件有关的任何过错或责任。

如有任何可能的帐户或身份验证凭据的误用或任何与在线服务有关的安全事件，客户必须立刻通知 世纪互联。

数据位置

世纪互联将客户数据仅存储在中国。

世纪互联不会控制或限制客户或其最终用户访问或迁移客户数据的地区。如果客户通过允许中国境外的任何人士访问其客户数据（包括该等客户数据中包含的个人数据）来传输其任何客户数据，或将该等客户数据转移出境，客户应遵守适用的数据保护要求（包括中国法律法规）的所有规定。

数据保留和删除

在客户订购期限内，客户可随时访问、提取和删除存储在每项在线服务中的客户数据。

除免费试用外，在客户的订购期满或终止后，世纪互联会将仍然存储在在线服务中的客户数据在功能受限制的帐户中保留九十 (90) 天，以便客户提取这些数据。为期九十 (90) 天的保留期限结束后，世纪互联将禁用客户的帐户并在接下来的九十 (90) 天内删除存储于在线服务内的客户数据和个人数据，除非本 DPA 授权世纪互联予以保留。

在线服务可能不支持客户提供的软件的保留或提取。对于依照本节之规定删除客户数据或个人数据的活动，世纪互联不承担任何责任。

处理方保密承诺

世纪互联将确保其负责处理客户数据和个人数据的人员 (i) 仅依照客户指令或本 DPA 规定处理此类数据；且 (ii) 有义务维护此类数据的机密性和安全性，即便在任务结束之后仍是如此。世纪互联应依照适用的数据保护要求和行业标准，定期为具有客户数据和个人数据访问权限的世纪互联员工提供强制性数据隐私和安全培训与教育。

关于使用子处理方的通知和控制

世纪互联可能会聘用子处理方来代表世纪互联提供某些有限或辅助服务。在有限的情况下，当需要排除故障和改进客户支持事件或解决技术问题时，世纪互联可能会授权位于中国境外的子处理方根据适用的法律法规访问客户数据。世纪互联将监督此类访问，并在问题解决后根据适用的法律法规终止此类访问。客户同意世纪互联聘用这些第三方和世纪互联关联公司作为子处理方。**如果标准合同条款、 GDPR 条款或《个保法》要求征得此类同意，上述授权将构成客户对“世纪互联分包对客户数据和个人数据处理工作”的事先书面同意。**

世纪互联应负责保证其子处理方履行本 DPA 中规定的世纪互联的义务。世纪互联会在世纪互联网站上提供有关子处理方的信息。在聘请任何子处理方时，世纪互联将通过书面合同确保子处理方仅会出于交付世纪互联委托其提供的服务之目的而访问和使用客户数据或个人数据，并禁止其将客户数据或个人数据用于任何其他目的。世纪互联应确保子处理方受相应书面协议的约束，且此类协议须要求子处理方至少提供本 DPA 要求世纪互联提供的数据保护级别，包括所处理数据的披露限制。世纪互联同意监督子处理方，以确保履行这些合同义务。

世纪互联可不时聘请新的子处理方。在向任何新的子处理方提供对客户数据或个人数据的访问权限之前，世纪互联将至少提前十四 (14) 天（通过更新网站并为客户提供获取该更新通知的机制）将此新的子处理方告知客户。然而，对于核心在线业务，在向任何新的子处理方提供对客户数据的访问权限之前，世纪互联将至少提前六 (6) 个月（通过更新网站并为客户提供获取该更新通知的机制）将此新的子处理方告知客户。如果世纪互联指定新的子处理方负责新的将处理客户数据或个人数据的在线服务，世纪互联将在提供在线服务之前通知客户。

如果客户不认可新的子处理方，则可以终止对受影响在线服务的任何订购，而不会受到处罚，但前提是应在相关通知期结束之前提供含有不认可的理由解释的书面终止通知。如果受影响的在线服务是套件（或单独购买的服务）的一部分，则任何终止在线服务的行为也将适用于整个套件。终止后，世纪互联将从后续客户账单或客户经销商账单中删除对已终止在线服务的任何订购的付款义务。

敏感个人数据

“敏感个人数据”，又称“敏感个人信息”，具有《个保法》第28条规定的含义，也具有其他数据保护要求中同等术语的含义（如适用）。在此说明，敏感个人数据可能包括但不限于GDPR第4条规定的“生物识别数据”，以及其他数据保护要求中的相应术语（如适用）。如果客户使用在线服务处理敏感个人数据，客户应负责：(i) 向数据主体提供通知，包括关于该等处理的必要性及对其利益的潜在影响的通知；(ii) 征得数据主体的单独同意（若客户依赖于同意作为处理敏感个人数据的合法基础）；以及 (iii) 根据适用数据保护要求的合理要求，采取必要措施保护敏感个人数据。世纪互联将依照客户书面指示（如上文“客户和世纪互联的角色和责任”一节所述）处理该等敏感个人数据，并根据本 DPA 下的数据安全和保护条款保护该等敏感个人数据。

如何联系世纪互联

如果客户认为世纪互联未遵守其隐私或安全承诺，可以联系客户支持，网址为 https://www.azure.cn/zh-cn/support/contact/，或致函世纪互联，世纪互联的邮寄地址为：

**世纪互联云合规部**

上海蓝云网络科技有限公司（“世纪互联”）

中国北京市朝阳区酒仙桥6号电子城国际电子总部6号楼 12-13层 邮编：100015

附录 A – 安全措施

对于核心在线服务中的客户数据，世纪互联已经实施并将维持以下安全措施，这些措施连同本 DPA（包括 GDPR 条款）中的安全承诺是世纪互联在此类数据安全性方面的唯一责任。

| 领域 | 惯例 |
| --- | --- |
| 信息安全组织 | **安全责任方**。世纪互联已任命一位或多位安全官负责协调和监控安全规则及程序。**安全角色和责任**。能够访问客户数据的世纪互联人员必须遵守保密义务。**风险管理程序**。在处理客户数据或启动在线服务之前，世纪互联已执行风险评估。在安全文档失效之后，世纪互联将根据相应保留要求来保留其安全文档。 |
| 资产管理 | **资产清单**。世纪互联维护存储客户数据的所有介质的清单。只有获得书面访问授权的世纪互联人员方可访问此类介质清单。**资产处理**- 世纪互联对客户数据进行分类，以帮助标识此类数据，并允许对访问进行适当限制。- 世纪互联对打印客户数据实施限制，并制定了处置包含客户数据的打印材料的程序。* 在将客户数据存储在便携式设备上、远程访问客户数据或在世纪互联设施外部处理客户数据之前，世纪互联人员必须获得世纪互联授权。
 |
| 人力资源安全 | **安全培训**。世纪互联向其员工通告有关安全程序及其相应角色的事宜。世纪互联还向其员工通告违反安全规则和程序可能带来的后果。世纪互联在培训中将只使用匿名数据。 |
| 物理和环境安全 | **出入设施**。世纪互联只允许已确认身份的授权人员出入处理客户数据的信息系统所在的设施。**访问组件**。世纪互联维护包含客户数据的介质的收发记录，包括介质类型、授权发送人/接收人、日期和时间、介质数量、所含客户数据类型。**防止中断**。世纪互联使用各种行业标准系统，防止由于电源故障或线路干扰导致数据丢失。**组件报废处置**。不再需要客户数据时，世纪互联将使用行业标准流程来删除该数据。 |
| 通信和运营管理 | **运营策略**。世纪互联维护安全文档，此类文档描述世纪互联的安全措施和相关程序，以及能够访问客户数据的世纪互联人员的责任。**数据恢复程序**- 世纪互联长期维护客户数据的多份副本，以便能够从该副本恢复客户数据，但备份频率不得低于每周一次（除非在该时段内没有更新任何客户数据）。- 世纪互联将客户数据副本和数据恢复程序保存在不同于处理客户数据的主要计算机设备所在位置的地方。- 世纪互联制定特定程序来监管对客户数据副本的访问。- 世纪互联至少每十二个月对数据恢复程序审核一次。- 世纪互联记录数据恢复工作，包括负责人员、所恢复数据的描述，以及在适用的情况下，在数据恢复过程中必须手动输入哪些数据（如果有）。**恶意软件**。世纪互联实施了反恶意软件控制，帮助防止恶意软件获得对客户数据的未授权访问权限，包括来自公共网络的恶意软件。**跨界数据**- 世纪互联会加密或允许客户加密通过公共网络传输的客户数据。- 世纪互联限制对从其设施取出的介质上的客户数据的访问。**活动记录**。世纪互联会记录或允许客户记录信息系统的访问和使用情况，包含客户数据、注册访问 ID、时间、授予或拒绝的授权以及相关活动。 |
| 访问控制 | **访问策略**。世纪互联维护能够访问客户数据的人员的安全权限记录。**访问授权**- 世纪互联将维护并更新有权访问包含客户数据的世纪互联系统的相关人员的记录。- 对于已有一段时间（不超过六 (6) 个月）未使用的身份验证凭据，世纪互联将予以停用。- 世纪互联将指定可以授权、更改或取消数据和资源的访问权限的人员。- 世纪互联确保如果有多个人员具有访问客户数据所在系统的权限，则每个人都具有单独的标识符/登录名。**最小权限**- 仅允许技术支持人员在需要时访问客户数据。- 世纪互联只允许需要访问客户数据才能履行其工作职能的人员访问客户数据。**完整性和保密性**- 世纪互联指示世纪互联人员在离开世纪互联控制的场所或在计算机无人照看时禁用管理会话。- 世纪互联以一种在生效期间确保不会泄密的方式来存储密码。**身份验证**- 世纪互联使用行业标准做法来确定试图访问信息系统的用户的身份，并对他们进行身份验证。- 如果身份验证机制是基于密码的，则世纪互联要求该密码必须定期更新。- 如果身份验证机制是基于密码的，则世纪互联要求该密码长度至少为八个字符。- 世纪互联确保不将已停用或过期的标识符授予其他人员。- 世纪互联将监控或允许客户监控使用无效密码反复尝试访问信息系统的行为。- 世纪互联维护行业标准程序，以停用已被破坏或无意中泄露的密码。- 世纪互联使用行业标准密码保护做法，包括在分配或分发密码时和存储期间保持密码的机密性和完整性的做法。**网络设计**。世纪互联采取控制措施，避免人员获取对未授权他们访问的客户数据的访问权限。 |
| 信息安全事件管理 | **事件响应流程**- 世纪互联维护安全违规行为的记录，包括违规行为的描述、时间、违规行为的后果、报告者名称、接收违规报告的人员，以及恢复数据的程序。- 对于属于安全事件的每次安全违规，世纪互联应在 72 小时内发出通知（见上文中“安全事件通知”一节的规定），任何情况下均不得无正当理由拖延。- 世纪互联会跟踪或允许客户跟踪客户数据的披露情况，包括披露的具体数据、披露对象和披露时间。**服务监控**。世纪互联安全人员至少每六个月验证一次日志，如果需要将会提议修正措施。 |
| 业务连续性管理 | - 世纪互联维护处理客户数据的世纪互联信息系统所在的设施的应急计划。- 世纪互联的冗余存储及其恢复数据的程序旨在尝试按照客户数据丢失或破坏之前的原始或上次复制的状态来重建数据。 |

附录 B – 数据主体和个人数据的类别

**数据主体：**数据主体包括客户的代表和最终用户，包括客户的员工、承包商、合作者和顾客。数据主体还可以包括尝试与世纪互联提供的在线服务的用户进行通信或向其传输个人信息的个人。世纪互联确认，根据客户对在线服务的使用情况，客户可以选择在个人数据中包含以下任何数据主体类型的个人数据：

* 客户的（当前、以前或准）员工、承包商和临时员工；
* 上述人员的家属；
* 客户的合作方/联系人（自然人）或者法律实体合作方/联系人的员工、承包商或临时员工（当前、以前或准员工）；
* 用户（例如，顾客、客户、患者、访客等）以及作为客户服务用户的其他数据主体；
* 与客户的员工进行积极协作、交流或以其他方式互动，和/或使用客户提供的应用程序和网站等通信工具的合作伙伴、利益相关方或个人；
* 被动地与客户互动的利益相关方或个人（例如，因为他们是调查研究的主体，或在与客户的往来文档或通信中被提及）；
* 未成年人；或者
* 拥有专业特权的专业人员（例如，医生、律师、公证人、宗教工作者，等等）。

**数据类别**：传输的包含在电子邮件或文档中的个人数据，以及在线服务环境中的其他电子数据。世纪互联确认，根据客户对在线服务的使用情况，客户可以选择在个人数据中包含以下任何类别的个人数据：

* 基本个人数据（例如出生地点、街道名称和门牌号（地址）、邮政编码、居住城市、居住国家/地区、手机号码、名字、姓氏、姓名的首字母、电子邮件地址、性别、出生日期），包括有关家庭成员和子女的基本个人数据；
* 身份验证数据（例如用户名、密码或 PIN 码、安全性问题、审计线索）；
* 联系人信息（例如地址、电子邮件、电话号码、社交媒体标识符；紧急联系人详细信息）；
* 唯一标识号和签名（例如社会保障号、银行帐号、护照和身份证号、驾照号码和车辆登记号码、IP 地址、员工编号、学号、门诊号、签名、采用跟踪 Cookie 或类似技术的唯一标识符）；
* 假名标识符；
* 财务和保险信息（例如保险号、银行帐户名称和帐号、信用卡名称和号码、发票号码、收入、保险类别、支付行为、信用状况）；
* 商业信息（例如购买历史记录、特别优惠、订购信息、付款历史记录）；
* 生物特征信息（例如 DNA、指纹和虹膜扫描）；
* 位置数据（例如小区标识、地理位置网络数据、开始呼叫/结束呼叫的位置。使用 WiFi 接入点获得的位置数据）；
* 照片、视频和音频；
* Internet 活动（例如浏览历史记录、搜索历史记录、阅读、看电视、听收音机活动）；
* 设备标识（例如 IMEI 号码、SIM 卡号、MAC 地址）；
* 概况分析（例如基于观察到的犯罪或反社会行为，或基于访问过的 URL、点击流、浏览日志、IP 地址、域、安装的应用程序的匿名配置文件，或基于营销偏好的配置文件）；
* 人力资源和招聘数据（例如就业状况声明、招聘信息（如履历、就业经历、教育经历详细信息）、工作和职位数据（包括工作时间、评估和工资）、工作许可详细信息、工作机会、雇用条款、税收详细信息、付款详细信息、保险详细信息以及位置和组织）；
* 教育数据（例如教育经历、当前教育、分数和成绩、获得的最高学位、学习障碍）；
* 公民和居住信息（例如公民身份、入籍状态、婚姻状况、国籍、移民身份、护照资料、居住详细信息或工作许可证）；
* 为执行维护公共利益或行使官方权力的任务而处理的信息；
* 特殊数据类别（例如种族或民族、政见、宗教或哲学信仰、工会成员资格、遗传数据、用于唯一识别自然人的生物数据、有关健康的数据、有关自然人的性生活或性取向的数据，或与刑事定罪或犯罪有关的数据）；或者
* 《个保法》第4条或GDPR 第 4 条规定的任何其他个人数据。

附录 C – 额外保护措施附录

上海蓝云网络科技有限公司（“世纪互联”）通过本DPA的额外保护措施附录（简称本“附录”）就世纪互联代表客户处理GDPR范围内的个人数据为客户提供额外保护措施，并为与客户个人数据相关的数据主体提供额外补救措施。

本附录是对本DPA的补充，是本DPA的一部分。

1. **质疑命令。**如果世纪互联从任何第三方收到命令，要求强制披露本DPA项下处理的任何个人数据，世纪互联应：
2. 尽一切合理的努力安排第三方直接从客户处请求数据；
3. 立即通知客户，除非提出要求的第三方所适用的法律禁止，如果禁止通知客户，则应尽一切合法努力获得免除该禁令的权利，以便尽快向客户传达更多信息；
4. 基于请求方法律方面的缺陷或与欧盟法律或适用成员国法律的任何相关冲突，尽一切合法努力对披露命令提出异议。

如果在采取上述a.至c.的步骤后，世纪互联仍然被强制披露个人数据，世纪互联将只披露为满足强制披露命令所需的最低规模的数据。

本节所说的合法努力不包括根据相关管辖权地的法律会导致民事或刑事处罚的行为，例如蔑视法庭。

1. **数据主体的赔偿。**根据第 3 节和第 4 节的规定，对于世纪互联因应非欧盟/欧洲经济区政府机构或执法机构的命令披露标准合同条款规定的个人数据（简称“相关披露”）而对数据主体造成的任何实质性或非实质性损害，世纪互联应对数据主体进行赔偿。尽管有上述规定，但如果数据主体已经从世纪互联或其他方面就同一损害获得了赔偿，那么世纪互联将无义务对数据主体作出本节中规定的赔偿。
2. **赔偿条件。**第 2 节规定赔偿的条件是数据主体确定世纪互联作出了以下行为并获得了世纪互联的确认：
3. 世纪互联进行了相关披露；
4. 非欧盟/欧洲经济区政府机构或执法机构基于相关披露对数据主体提起正式诉讼；
5. 相关披露直接导致数据主体遭受实质性或非实质性损害。

数据主体承担条件 a. 至 c. 的举证责任。

尽管有上述规定，但如果世纪互联确认相关披露未违反 GDPR 第 V 章规定的义务，则世纪互联没有义务按照第 2 节中的规定赔偿数据主体。

1. **损害范围。**第 2 节规定的赔偿仅限于 GDPR 中规定的实质性和非实质性损害，并且不包括后果性损害赔偿以及并非由于世纪互联违反 GDPR 造成的所有其他损害。
2. **权利的行使。**不论2010标准合同条款第 3 条或第 6 条有任何限制，数据主体都可以对世纪互联行使本附录授予数据主体的权利。数据主体只能以个人名义提出本附录中的索赔，索赔不得包含在集体、团体或代表诉讼中。本附录授予数据主体的权利是数据主体的个人权利，不得转让。
3. **变更通知。**除了标准合同条款的第 5(b) 条之外，世纪互联同意并保证，没有理由相信适用于其或其子处理方的法律（包括在任何通过其自身或通过子处理方将个人数据传输到的国家/地区）会阻止其履行从数据导出方处收到的指令及其在本附录、2010标准合同条款或2021标准合同条款下的义务，如果本法规的变更有可能对本附录或标准合同条款所提供的担保和义务产生重大不利影响，世纪互联将在知悉后立即将变更通知客户，在这种情况下，客户有权暂停数据传输和/或终止合同。
4. **终止。**如果欧洲委员会、主管成员国的监督机构或者欧盟或主管成员国的法庭批准了适用于本DPA项下处理的客户数据中的个人数据或其他个人数据的其他合法传输机制（如果这些机制仅适用于某些数据，则本附录将仅针对那些数据终止），并且不需要本附录中规定的额外保护措施，本附录将自动终止。

附件 1 – 2010标准合同条款（处理方）

客户签署世纪互联客户协议的同时会签署本附件 1，后者由世纪互联进行会签。如果世纪互联根据GDPR的要求而签署2021标准合同条款，则本附件1是对2021标准合同条款的补充。如果本附件1与2021标准合同条款（若由世纪互联签署）之间存在任何不一致，则应以根据适用法律为客户数据和个人数据提供适当的数据保护水平之目的而解决该等不一致问题。若选择不适用“标准合同条款”，客户须以书面通知的形式（根据世纪互联客户协议的条款）向世纪互联发送以下信息：

* 客户及其任何不适用“标准合同条款”的关联公司的法定全称；
* 若客户有多份世纪互联客户协议，其不适用标准合同条款所适用的具体世纪互联客户协议；以及
* 客户（或其关联公司）不适用“标准合同条款”的声明。

根据欧盟委员会 2010/87/EU（2010 年 2 月）的规定，在使用标准合同条款需要监管机构批准的国家/地区，标准合同条款无法用于从该国家/地区合法出口数据，除非客户获得了监管机构的批准。

2018 年 5 月 25 日起，在下面的标准合同条款中引用指令 95/46/EC 中的各个条款将被视为引用 GDPR 中相关及相应的条款。

依据有关将个人数据传输至位于第三方国家/地区（无法确保提供充分的数据保护）的处理方事宜的 95/46/EC 指令第 26(2) 条，客户（作为数据导出者）和世纪互联公司（作为签名出现在下方的数据导入者，单独使用时称为“各方”，合称“双方”）均同意以下合同条款（以下简称“条款”或“标准合同条款”），以便针对数据导出者将本附录 1 中指定的个人数据传输给数据导入者事宜，给予隐私保护以及个人的基本权利和自由方面的充分保护。

**条款 1：定义**

(a)“个人数据”、“特殊类别的数据”、“处理”、“控制方”、“处理方”、“数据主体”和“监督机构”沿用欧洲议会和欧盟理事会 1995 年 10 月 24 日关于涉及个人数据处理的个人保护以及此类数据自由流动的 95/46/EC 指令中的定义；

(b)“数据导出者”指传输个人数据的控制方；

(c)“数据导入者”指同意从数据导出者接收个人数据，以依照其指示和标准合同条款中的条款，在传输之后代表其自身对数据进行处理的处理方。该处理方不受 95/46/EC 指令第 25(1) 条所定义的确保充分保护的第三方国家/地区系统的约束；

(d) “子处理方”指由数据导入者或数据导入者的任何其他子处理方雇用的处理方，其同意从数据导入者或数据导入者的任何其他子处理方接收个人数据（专门用于处理数据传输之后、代表数据导出者进行的活动，并且依照其指示、条文中的条款和书面子合同中的条款）；

(e)“适用的数据保护法”指保护个人的基本权利和自由（特别是其关于处理个人数据的隐私权）的法律，适用于在其中建立数据导出者的成员国中的数据控制方；

(f)“技术和组织安全措施”指旨在保护个人数据免受意外或非法破坏，或者避免意外丢失、更改、未经授权的披露或访问（特别是数据处理涉及通过网络进行数据传输），以及所有其他非法形式的数据处理的措施。

**条款 2：转让详细信息**

有关转让的详细信息，特别是特殊类别的个人数据（如果适用），将在下面构成条款的组成部分的附录 1 中指定。

**条款 3：第三方受益人条款**

1.数据主体可以作为第三方受益人，对数据导出者实施本条款、条款 4(b) 至 (i)、条款 5(a) 至 (e)，以及 (g) 至 (j)、条款 6(1) 和 (2)、条款 7、条款 8(2) 和条款 9 至 12。

2.如果数据导出者事实上已消失或者在法律上已不复存在，数据主体可以对数据导入者实施本条款、条款 5(a) 至 (e) 和 (g)、条款 6、条款 7、条款 8(2) 和条款 9 至 12，除非任何后续实体已根据协议或依照现行法律承担数据导出者的全部法定义务，从而享有数据导出者的权利并承担其义务，在此情况下，数据主体可以对此类实体实施这些条款。

3.如果数据导出者和数据导入者事实上已消失、在法律上已不复存在或者已经破产，数据主体可以对子处理方实施本条款、条款 5(a) 至 (e) 和 (g)、条款 6、条款 7、条款 8(2) 和条款 9 至 12，除非任何后续实体已根据协议或依照现行法律承担数据导出者的全部法定义务，从而享有数据导出者的权利并承担其义务，在此情况下，数据主体可以对此类实体实施这些条款。子处理方的此类第三方责任应限于其根据条款的自有的处理操作。

4.如果数据主体明确表明此类意愿且国家/地区法律允许，双方不反对数据主体由关联公司或其他机构进行代表。

**条款 4：数据导出者的义务**

数据导出者同意并保证：

(a) 个人数据的处理（包括传输本身）已经并将继续根据适用的数据保护法的相关规定（在适用时已通知在其中建立数据导出者的成员国中的有关当局）执行，并且不违反与该成员国的相关规定。

(b) 其已指示并将在整个个人数据处理服务期间指示数据导入者仅代表数据导出者，且根据适用的数据保护法和条款来处理传输的个人数据；

(c) 数据导入者将提供关于下面的附录 2 中指定的技术和组织安全措施的充分保证；

(d) 在评估适用的数据保护法要求之后，安全措施是适当的，可以保护个人数据免受意外或非法破坏，或者避免意外丢失、更改、未经授权的披露或访问（特别是数据处理涉及通过网络进行数据传输），以及所有其他非法形式的数据处理，并且这些措施可以确保适当的安全级别来应对要保护的数据的处理及其性质所带来的风险，同时还考虑到技术现状以及实施这些措施的成本；

(e) 其将确保遵守这些安全措施；

(f) 如果传输涉及特殊类别的数据，数据主体已被通知，或者在传输之前（或在之后尽快）被通知其数据可传输至未根据 95/46/EC 指令中的定义提供充分保护的第三方国家/地区；

(g) 在数据导出者决定继续传输或取消暂停的情况下，将从数据导入者或任何子处理方接收到的通知转发给数据保护监督机构（依照条款 5(b) 和条款 8(3)；

(h) 根据请求向数据主体提供条款的副本（附录 2 除外）、安全措施的概述，以及须根据条款签订的任何子处理服务协议的副本，除非条款或合同包含商业信息，在此情况下，其可以删除此类商业信息；

(i) 在进行子处理时，处理活动须由子处理方根据条款 11 执行，并且应根据条款，至少提供与个人数据保护相同的保护级别，以及与数据主体相同的权利；以及

(j) 其将确保遵守条款 4(a) 至 (i)。

**条款 5：数据导入者的义务**

数据导入者同意并保证：

(a) 仅代表数据导出者处理个人数据，并且遵守其指示和条款；如果出于任何原因，无法遵守此类指示和条款，其同意立即通知数据导出者，此时数据导出者有权暂停数据传输并且/或者终止协议；

(b) 其没有任何理由相信，对其适用的法律可使其免于遵守从数据导出者获得的说明、免于根据协议履行义务，并且在该法律发生变更，且可能会对条款提供的保证和义务产生重大不利影响时，其一旦知道，会立即就这一变更通知数据导出者，此时数据导出者有权暂停数据传输并且/或者终止协议；

(c) 在处理传输的个人数据之前，其已实施附录 2 中指定的技术和组织安全措施；

(d) 其将立即通知数据导出者关于：

(i) 由执法机构提出、要求披露个人数据的任何具有法律约束力的请求，除非另有规定禁止，例如根据刑法保持执法调查的机密性而禁止披露的情况，

(ii) 任何意外或未授权的访问，以及

(iii) 直接从数据主体收到且未进行回应的请求，除非其已被授权这样做；

(e) 及时妥善处理数据导出者提出的关于其处理传输的个人数据的所有查询，以及遵守监督机构关于处理传输数据的建议；

(f) 在数据导出者的请求下，提交其数据处理设备以进行条款规定的处理活动审查，该审查应由数据导出者或由独立成员构成、具有受保密义务约束的所需专业资格的检查机构执行，并且在征得监督机构同意的情况下，应由数据导出者选定（如果适用）；

(g) 根据请求向数据主体提供条款或任何现有子处理协议的副本，除非条款或协议包含商业信息，在此情况下，其可以删除此类商业信息（应由安全措施概述替换的附录 2 除外，此时数据主体无法从数据导出者获得副本）；

(h) 如果进行子处理，其之前已通知数据导出者，并已事先获得数据导出者的书面同意；

(i) 子处理方提供的处理服务将依照条款 11 执行；以及

(j) 立即向数据导出者发送根据条款达成的任何子处理方协议的副本。

**条款 6：责任**

1.双方同意因任何一方或子处理方违反条款 3 或条款 11 中所提及的义务而遭受损失的任何数据主体均有权针对所遭受的损失从数据导出者那里得到相应补偿。

2.如果由于数据导出者事实上已消失、在法律上已不复存在或者已经破产，数据主体无法根据第 1 段的内容对数据导出者提出索赔（由数据导入者或其子处理方违反任何条款 3 或条款 11 中所提及的义务而产生），数据导入者同意数据主体可以对数据导入者提出索赔，如同其就是数据导出者，除非任何后续实体已根据协议或依照现行法律承担数据导出者的全部法定义务，在此情况下，数据主体可针对此类实体行使其权利。

数据导入者不得依赖于子处理方违反其义务的行为，来逃避其自身的责任。

3.如果由于数据导出者和数据导入者事实上已消失、在法律上已不复存在或者已经破产，数据主体无法对第 1 段和第 2 段中所提及的数据导出者或数据导入者提出索赔（由数据导入者或其子处理方违反任何条款 3 或条款 11 中所提及的义务而产生），子处理方同意数据主体可以根据条款对数据子处理方就其自有的处理操作提出索赔，如同其就是数据导出者或数据导入者，除非任何后续实体已根据协议或依照现行法律承担数据导出者的全部法定义务，在此情况下，数据主体可针对此类实体行使其权利。子处理方的责任应限于其根据条款的自有的处理操作。

**条款 7：仲裁和管辖权**

1.数据导入者同意，如果数据主体根据条款对其提出第三方受益者权利和/或损失索赔，数据导入者将接受数据主体的决定：

(a) 将争议提交独立人士或监督机构（如果适用）进行调解；

(b) 将争议提交到数据导出者所在成员国的法院。

2.双方同意数据主体作出的选择不会影响其依照其他国家/地区或国际法规定寻求补救措施的实体和程序权利。

**条款 8：与监督机构协作**

1.数据导出者同意备案与监督机构签署的协议的副本（如果其要求备案，或者适用的数据保护法要求备案）。

2.双方同意，监督机构有权对数据导入者和任何子处理方进行审查，审查范围和所依据的条件与根据适用的数据保护法审查数据导出者相同。

3.数据导入者应立即就存在对其或任何子处理方适用的法律（使其免于依照第 2 段对数据导入者或任何子处理方进行的审查）一事通知数据导出者。在此情况下，数据导出者应有权采取条款 5 (b) 中预见的措施。

**条款 9：管辖法律。**

这些条款应受在其中建立数据导出者的成员国的法律的约束。

**条款 10：合同的变动**

双方保证不改变或修改条款。但这并不排除双方还会在需要时就业务相关的问题添加条款（只要不与条款相矛盾）。

**条款 11：子处理**

1.在未事先获得数据导出者的书面同意时，数据导入者不应分包根据条款代表数据导出者执行的处理操作。当数据导入者征得数据导出者的同意并根据条款分包其义务时，其只应通过与子处理方签署书面协议的方式进行分包，该协议将向子处理方施加与根据条款向数据导入者施加的义务相同的义务。当子处理方无法根据此类书面协议履行其数据保护义务时，数据导入者应对数据导出者根据此类协议履行子处理方的义务完全负责。

2.数据导入者和子处理方事先签署的书面协议还应提供条款 3 中规定的第三方受益人条款，该条款适用于由于数据导出者或数据导入者事实上已消失或者在法律上已不复存在，或者已经破产且无后续实体根据协议或依照现行法律承担数据导出者或数据导入者的全部法定义务，数据主体无法对他们提出条款 6 第 1 段中所提及索赔的情况。子处理方的此类第三方责任应限于其根据条款的自有的处理操作。

3.第 1 段所提及的与合同中的子处理数据保护方面有关的规定应受在其中建立数据导出者的成员国的法律的约束。

4.数据导出者应保留根据条款签署、由数据导入者依照条款 5 (j) 通知的子处理协议的列表（应至少每年更新一次）。该列表应提供给数据导出者的数据保护监督机构。

**条款 12：个人数据处理服务终止之后的义务**

1.双方同意，在数据处理服务的规定终止之后，数据导入者和子处理方应根据数据导出者的选择，向数据导出者退回所有传输的个人数据和副本，或者应销毁所有个人数据并向数据导出者证明数据已销毁，除非法律禁止数据导入者退回或销毁传输的全部或部分个人数据。在此情况下，数据导入者应保证它能保证传输的个人数据的机密性，而且将不再主动处理传输的个人数据。

2.数据导入者和子处理方保证，其将按照数据导出者和/或监督机构的请求，提交其数据处理设备以进行第 1 段中所提及的措施的审查。

**标准合同条款的附录 1**

**数据导出者：**客户是数据导出者。数据导出者是 DPA 和 OST 中定义的在线服务的用户。

**数据导入者：**数据导入者是世纪互联，其是Microsoft Azure、Microsoft Dynamics 365、Office 365以及Microsoft Power BI服务在中国的运营商。

**数据主体：**数据主体包括数据导出者的代表和最终用户，包括数据导出者的员工、承包商、合作者和顾客。

**数据类别**：传输的包含在电子邮件或文档中的个人数据，以及在线服务环境中的其他电子数据。世纪互联确认，根据客户对在线服务的使用情况，客户可以选择包含本DPA的附录B中详述的任何类别的个人数据。

**处理操作**：传输的个人数据将受以下基本处理活动的约束：

**a. 数据处理的持续时间和目标。**数据处理的持续时间应为数据导出者与被附加这些标准合同条款的世纪互联实体（以下简称“世纪互联”）之间签订的适用世纪互联客户协议所指定的期限。数据处理的目的是提供在线服务。

**b. 数据处理的范围和目的。**DPA 的“个人数据的处理；GDPR”一节中介绍了处理个人数据的范围和目的。依照 DPA 的“安全实践和策略”一节，数据处理可在数据导入者或其子处理方运营此类设施的任何法律管辖范围内进行。

**c. 客户数据和个人数据访问。**在适用的世纪互联客户协议下指定的期限内，数据导入者将依据适用的法律，根据需要自行选择实施欧盟数据保护指令第 12(b) 条，以便：(1) 让数据导出者能够更正、删除或阻止客户数据和个人数据，或 (2) 世纪互联能够代表数据导出者执行此类更正、删除或阻止操作。

**d. 数据导出者的指示。**对于在线服务，数据导入者将仅遵照数据导出者的指示（如世纪互联所转达）行事。

**e. 客户数据和个人数据删除或返还。**依照适用于本协议的 DPA 条款的规定，数据导出者使用在线服务的权利期满或终止后，可提取客户数据和个人数据，并且数据导入者将删除客户数据和个人数据。

**分包商**：依照 DPA，数据导入者可以聘请其他公司代表其提供有限服务，例如提供客户支持。仅允许所有此类分包商为了交付数据导入者委托提供的服务而获取客户数据和个人数据，不得将客户数据和个人数据用于任何其他目的。

**标准合同条款的附录2**

数据导入者依照条款 4(d) 和 5(c) 实施的技术和组织安全措施说明：

1.**人员。**在未获得授权的情况下，数据导入者的人员将不会处理客户数据或个人数据。这些人员有义务维护任何此类客户数据和个人数据的保密性，即便在离职之后仍有义务继续保密。

2.**数据隐私联系人。**可以通过以下地址联系数据导入者的数据隐私官：

上海蓝云网络科技有限公司（“世纪互联”）

中国北京市朝阳区酒仙桥6号电子城国际电子总部6号楼 12-13层 邮编：100015

3.**技术和组织措施。**数据导入者已经实施并将维持适当的技术和组织措施、内部控制和信息安全例程，以保护客户数据和个人数据（如 DPA 的“安全实践和策略”部分中所定义），防止意外丢失、销毁或更改；未经授权的披露或访问；或者非法销毁，如下所述：DPA 的“安全实践和策略”部分中规定的技术和组织措施、内部控制和信息安全例程在此通过提及方式纳入本附录 2，并且对数据导入者有约束力，如同它们全部在本附录 2 中规定一样。

**代表数据导入方签署标准合同条款、附录 1和附录 2：**

签署人：Johnny Liu



职位：总裁

上海蓝云网络科技有限公司（“世纪互联”）

中国北京市朝阳区酒仙桥6号电子城国际电子总部6号楼 12-13层 邮编：100015

附件 2 – 欧盟通用数据保护条例条款

世纪互联在 GDPR 条款中向所有客户作出的承诺将于 2018 年 5 月 25 日生效。对于客户而言，这些承诺对世纪互联具有约束力，无需考虑 (1) 适用于任何给定在线服务订购的 OST 和 DPA 版本，或 (2) 任何引用此附件的其他协议。

在这些 GDPR 条款中，客户和世纪互联同意，客户是个人数据的控制方，而世纪互联是此类数据的处理方，但由客户充当个人数据处理方的情况除外，此时世纪互联是子处理方。这些 GDPR 条款适用于世纪互联代表客户在 GDPR 的范围内处理个人数据的情况。这些 GDPR 条款并不会限制或减少世纪互联在使用权利或与客户签署的其他协议中向客户所作出的数据保护承诺。这些 GDPR 条款不适用于由世纪互联充当个人数据控制方的情况。

**相关 GDPR 义务：第 28、32 和 33 条**

**1.**在未事先获得客户的特定或一般书面授权的情况下，世纪互联不得雇用其他处理方。如果获得的是一般书面授权，则世纪互联应将有关增加或更换其他处理方的任何拟议变更通知客户，以便客户有机会就此类变更提出反对意见。（第 28(2) 条）

**2.**依照欧洲联盟（以下简称“欧盟”）法律或欧盟成员国法律的规定，世纪互联处理个人数据的活动应受这些 GDPR 条款的约束，对于客户而言，这些条款对世纪互联具有约束力。世纪互联客户协议（包括这些 GDPR 条款）规定了处理的内容和持续期间、处理的性质和目的、个人数据的类型、数据主体的类别以及客户的义务和权利。特别是，世纪互联应满足以下要求：

**(a)** 只能依照客户已成文的指令处理个人数据，包括有关将个人数据传输到第三方国家/地区或国际组织，但对世纪互联有约束力的欧盟法律或欧盟成员国法律要求这样做的情况除外；在此类情况下，世纪互联应在处理个人数据之前通知客户收到该法律要求，除非该法律以保护公共利益为由禁止发出此类通知；

**(b)** 确保授权处理个人数据的人员承诺对个人数据进行保密或承诺履行相应的法定保密义务；

**(c)** 采取 GDPR 第 32 条所要求的所有措施；

**(d)** 遵守第 1 段和第 3 段中所述的有关雇用其他处理机构的条件；

**(e)** 根据处理性质，通过采取适当的技术和组织措施，竭尽所能协助客户履行其义务，以满足 GDPR 第 III 章中规定的行使数据主体权利的要求；

**(f)** 根据处理性质并结合世纪互联所掌握的信息，协助并确保客户履行 GDPR 第 32 至 36 条所规定的义务；

**(g)** 在停止提供与处理相关的服务时，根据用户所做出的选择，删除所有个人数据或将所有个人数据返还给客户，并删除现有副本，但欧盟法律或欧盟成员国法律要求存储个人数据的情况除外；

**(h)** 为客户提供所有必要信息，以证明已履行 GDPR 第 28 条所规定的义务，并允许客户或受客户委托的其他审计师进行审计（包括检查）并积极配合审计工作。

如果世纪互联认为某条指令违反了 GDPR 或其他欧盟数据保护条例或欧盟成员国数据保护条例，应立即通知客户。（第 28(3) 条）

**3.**如果世纪互联雇用其他处理方来代表客户执行特定的处理活动，则本 GDPR 条款中规定的相同数据保护义务将以合同或欧盟法律或欧盟成员国法律所规定的其他法定形式强制施加给该其他处理方，特别是，应提供充分的保障，以实施适当的技术和组织措施，确保个人数据处理符合 GDPR 的相关要求。如果该其他处理方未能履行其数据保护义务，则世纪互联应继续对客户负责，并全面履行该其他处理方的义务。（第 28(4) 条）

**4.**考虑到技术现状、实施成本、数据处理的性质、范围、上下文环境和目的，以及自然人的权利和自由发生变化的可能性和严重性风险，客户和世纪互联应采取适当的技术和组织措施，以确保实施与相关风险相应的安全级别，尤其是酌情包括：

**(a)** 个人数据的假名化和加密；

**(b)** 确保处理系统和服务具有持续的保密性、完整性、可用性和故障恢复能力；

**(c)** 当发生物理或技术事件时，及时恢复个人数据的可用性和可访问性的能力；以及

**(d)** 对技术和组织措施的有效性进行定期测试、考核和评估的流程，以确保数据处理的安全性。（第 32(1) 条）

**5.**在评估是否具备适当的安全级别时，应考虑数据处理所带来的风险，特别是因传输、存储或以其他方式处理的个人数据遭到意外或非法破坏、丢失、更改、未经授权的披露或访问所带来的风险。（第 32(2) 条）

**6.**客户和世纪互联应采取措施，以确保在未获得客户指令的情况下，经客户或世纪互联授权访问个人数据的任何自然人不得处理个人数据，除非欧盟法律或欧盟成员国法律要求其这样做。（第 32(4) 条）

**7.**在发现个人数据违规情况时，世纪互联应立即通知客户，不得无故延误。（第 33(2) 条。）此类通知应包含第 33(3) 条规定的处理方必须向控制方提供的信息，但前提是世纪互联可以合理地获得这些信息。