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 11月 15 日

这些承诺自 2022年 11 月 15 日起对世纪互联具有约束力。

**目录**

[简介 3](#_Toc118465750)

[适用的 DPA 条款与更新 3](#_Toc118465751)

[电子通知 3](#_Toc118465752)

[早期版本 3](#_Toc118465753)

[定义 4](#_Toc118465754)

[一般条款 5](#_Toc118465755)

[遵守法律 5](#_Toc118465756)

[数据保护条款 5](#_Toc118465757)

[范围 5](#_Toc118465758)

[数据处理的性质；所有权 5](#_Toc118465759)

[所处理数据的披露 6](#_Toc118465760)

[个人数据的处理 6](#_Toc118465761)

[数据安全性 7](#_Toc118465762)

[安全事件通知 8](#_Toc118465763)

[数据位置 8](#_Toc118465764)

[数据保留和删除 8](#_Toc118465765)

[处理方保密承诺 9](#_Toc118465766)

[关于使用子处理方的通知和控制 9](#_Toc118465767)

[敏感个人数据 9](#_Toc118465768)

[如何联系世纪互联 9](#_Toc118465769)

[附录 A – 安全措施 10](#_Toc118465770)

[附录 B – 数据主体和个人数据的类别 12](#_Toc118465771)

[附录 C – 额外保护措施附录 14](#_Toc118465772)

[附件 1–2021标准合同条款（控制方至处理方） 15](#_Toc118465773)

[附件 2 – 欧盟通用数据保护条例条款 23](#_Toc118465774)

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2021标准合同条款适用时，[附件 1](#Attachment1) 中的2021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2021标准合同条款的第 5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》。

“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（控制方到处理方模块，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）。2021标准合同条款位于[附件 1](#Attachment1) 中。

“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（无论 GDPR 是否适用）以及其他数据保护要求中的任何同等术语（如适用）。术语“数据导入者”和“数据导出者”具有2021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，包括任何安全违规行为通知要求和数据保护要求。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（定义见下文）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
* 持续更新在线服务并保持其功能正常，强化用户生产力、可靠性、效力、质量和安全性。

提供在线服务时须考虑数据保护要求中规定的安全义务。

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。

**为与提供在线服务有关的经营活动而进行处理**

就本 DPA 而言，“经营活动”指客户在本节中授权的处理活动。

客户授权世纪互联：

1. 从含有假名标识符的数据（例如含有唯一假名标识符的使用日志）中创建汇总统计的非个人数据；及
2. 计算与客户数据相关的统计数据，

上述每一情况下，作为与向客户提供在线服务相关的事项，均无须访问或分析客户数据的内容，且仅限于实现以下目的。

这些目的是：

* 帐单和帐户管理；
* 报酬（例如计算员工佣金和合作伙伴奖励）；
* 内部报告和业务建模（例如，预测、收入、产能规划、产品战略）；及
* 财务报告。

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。此外，正如本DPA项下的所有数据处理，为经营活动而进行的数据处理仍须符合世纪互联在“所处理数据的披露”一节中的保密义务和承诺。

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。

除非适用法律要求和允许，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，但法律另有要求和允许的除外。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上述处理中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，类似于GDPR中的控制方），而世纪互联是此类数据的“受托人”（在《个保法》下的用词，类似于GDPR中的处理方），但以下情况除外： (a) 当客户充当个人数据的受托人时，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人或子处理方时，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》适用且客户系受托人的情况下，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人或子处理方）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或者为管理和履行世纪互联客户协议须使用或以其他方式处理受《个保法》约束的个人数据，且如果世纪互联充当独立“个人信息处理者”，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。就该等处理，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。

如果世纪互联为管理和履行客户与世纪互联之间的世纪互联客户协议而使用或以其他方式处理个人数据，则客户有责任从《个保法》规定的相关数据主体处获得所有必要的同意（或者依照任何其他适用的法律依据），以便向世纪互联提供此类个人数据（为上述目的，世纪互联可能将这些个人数据传输至中国境外的第三方）。在所适用法律要求的范围内，世纪互联将遵循跨境数据传输的适当要求。

**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GDPR或《个保法》（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GDPR或《个保法》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，世纪互联可在符合适用法律的前提下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2021标准合同条款适用，则本节是2021标准合同条款中的条款 8.9的附加内容。DPA 本节中的任何内容均不会更改2021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2021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) 天将此新的子处理方告知客户，并且（如适用）更新网站并为客户提供获取该更新通知的机制。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) 个月将此新的子处理方告知客户，并且（如适用）更新网站并为客户提供获取该更新通知的机制。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《个保法》下类似的敏感个人数据类别；或者
* GDPR第4条或《个保法》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和/或世纪互联所适用的法律禁止，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2021标准合同条款第 3 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。**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）会阻止其履行从客户处收到的指令及其在本附录或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2021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。

# **附件 1–2021标准合同条款（控制方至处理方）**

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。

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GDPR第46条，客户（作为数据导出者）和世纪互联（作为签名出现在下方的数据导入者）均同意以下合同条款，以便针对数据导出者将本附录I.B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基本权利和自由方面的充分保护。

* 1. **宗旨和范围**
		+ 1. 本标准合同条款旨在确保为向第三方国家/地区传输数据而遵守欧洲议会和欧洲理事会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以及此类数据自由移动的法规(EU) 2016/679（《通用数据保护条例》）的要求。
			2. 缔约方：
			3. 传输个人数据的自然人或法人，公共机关、机构或其他实体（以下简称“实体”），详见附录I.A（以下简称“数据导出者”），及
			4. 直接或间接通过同样是本条款缔约方的另一实体从数据导出者接收个人数据的位于第三方国家/地区的实体，详见附录I.A（以下简称“数据导入者”）

已同意本标准合同条款（以下简称“本条款”）。

* + - 1. 本条款适用于附录I.B中规定的个人数据传输。
			2. 载有本条款所述附录的本条款附件构成本条款不可分割的组成部分。
	1. **条款效力和不可变更**
		+ 1. 依据法规(EU) 2016/679第46 (1)条和第46 (2)(c)条，本条款规定了适当的保护措施，包括可强制执行的数据主体权利和有效的法律补救措施，并在控制方向处理方和/或处理方向处理方传输数据方面，依据法规(EU) 2016/679第28 (7)条规定了标准合同条款，且除非选择该附件中的适当模块或添加或更新该附件中的信息，否则不得修改该等条款。这并不妨碍各方将本条款中规定的标准合同条款纳入更广泛的合同和/或添加其他条款或附加保护措施，前提是这些条款或措施不会直接或间接地与本条款相抵触或损害数据主体的基本权利或自由。
			2. 本条款不影响数据导出者根据法规(EU) 2016/679所承担的义务。
	2. **第三方受益人**
		+ 1. 数据主体可作为第三方受益人针对数据导出者和/或数据导入者援引和执行本条款，但以下条款除外：
				1. 第1条、第2条、第3条、第6条、第7条；
				2. 第8.1(b) 条、第8.9(a)、(c)、(d)和(e)条；
				3. 第9(a)、(c)、(d)和(e)条；
				4. 第12(a)、(d)及(f)条；
				5. 第13条；
				6. 第15.1(c)、(d)及(e)条；
				7. 第16(e)条；
				8. 第18(a)和(b)条。
			2. 第(a)款不影响法规(EU) 2016/679中数据主体的权利。
	3. **释义**
		+ 1. 如果本条款使用法规(EU) 2016/679中定义的术语，这些术语的含义与该法规中的术语相同。
			2. 本条款应结合法规(EU) 2016/679的规定进行解读。
			3. 对本条款的解释不应与法规(EU) 2016/679中规定的权利义务相冲突。
	4. **效力等级**

如果本条款与各方达成本条款时已存在或此后签订的相关协议的规定相冲突，应以本条款为准。

* 1. **传输的说明**

传输的详情，特别是传输的个人数据类别及其传输目的载于附录I.B。

* 1. **加入条款**
		+ 1. 经各方同意，非本条款缔约方的实体可通过填写附件一并签署附录I.A，随时以数据导出者或数据导入者的身份加入本条款。
			2. 一经填写附件一并签署附录I.A，加入实体即成为本条款缔约方，并根据其在附录I.A中的指定身份，具有数据导出者或数据导入者的权利和义务。
			3. 加入实体在成为缔约方之前的期间内，不具有本条款规定的权利或义务。
1. **– 各方的义务**
	1. **数据保护保护措施**

数据导出者保证其已作出合理努力，确定数据导入者能够通过实施适当的技术和组织措施履行其在本条款下的义务。

* + 1. 指示
			1. 数据导入者应仅根据数据导出者的书面指示处理个人数据。数据导出者可在合同的整个有效期内发出此类指示。
			2. 如果数据导入者无法遵守这些指示，应立即通知数据导出者。
		2. 目的限制

除非数据导出者另行指示，否则数据导入者仅应出于附录I.B所述的特定传输目的处理个人数据。

* + 1. 透明度

数据导出者应根据要求免费向数据主体提供本条款的副本（包括经各方填写的附件一）。在为保护商业秘密或其他保密信息（包括附录II所述措施以及个人数据）所必需的范围内，数据导出者可在共享副本之前对本条款附件一的部分文本进行编辑，但在数据主体将无法理解附件内容或行使其权利的情况下，应提供有意义的概要。各方应尽可能在不披露经编辑的信息的情况下，应数据主体的要求向其提供编辑的理由。本条款不影响数据导出者在法规 (EU) 2016/679第13条和第14条项下的义务。

* + 1. 准确性

如果数据导入者知悉其收到的个人数据不准确或已经过时，应尽快通知数据导出者，不得无故拖延。在这种情况下，数据导入者应与数据导出者合作，以删除或纠正数据。

* + 1. 数据处理和删除或返还的持续时间

数据导入者应仅在附录I.B规定的期限内进行数据处理。在提供处理服务结束后，数据导入者应根据数据导出者的选择，删除代表数据导出者处理的所有个人数据，并向数据导出者证明其已这样做，或将代表数据导出者处理的所有个人数据返还给数据导出者，并删除现有副本。数据导入者应持续确保遵守本条款，直至数据予以删除或返还时止。如果对数据导入者适用的当地法律禁止返还或删除个人数据，数据导入者保证其将继续确保遵守本条款，并仅在当地法律要求的范围内和持续期内处理该等个人数据。此项规定并不影响第14条，尤其是第14(e)条项下数据导入者须在合同的整个有效期内，在其有理由相信其受或已受与第14(a)条项下要求不一致的法律或惯例约束的情况下通知数据导出者。

* + 1. 处理的安全性
			1. 数据导入者应（且在传输过程中数据导出者也应）采取适当的技术和组织措施，确保数据的安全，包括针对安全受到破坏，导致意外或非法销毁、丢失、更改、未经授权披露或访问该等数据（以下简称“个人数据泄露”）的保护。在评估是否具备适当的安全级别时，各方应适当考虑技术现状、实施成本、处理活动的性质、范围、情境和目的以及为数据主体处理数据所涉及的风险。各方应特别考虑在能够以加密或假名方式实现处理目的之情况下采用此等方式（包括在传输过程中）。在采用假名的情况下，用于将个人数据归属于特定数据主体的附加信息应在可能的情况下保持由数据导出者专属控制。数据导入者在履行其在本段项下的义务时，至少应实施附录II中规定的技术和组织措施。数据导入者应定期进行检查，以确保这些措施继续提供适当的安全级别。
			2. 数据导入者应仅在为实施、管理和监督合同所绝对必要的范围内允许其人员访问个人数据。数据导入者应确保获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。
			3. 如果数据导入者根据本条款处理的个人数据发生个人数据泄露，数据导入者应采取适当措施解决该泄露情况，包括采取措施减轻其不利影响。数据导入者还应在知悉泄露情况后尽快通知数据导出者，不得无故拖延。此类通知应包含可向之获得更多信息的联络点的详细信息、泄露行为性质的描述（如有可能，包括涉及的数据主体的类别和大致数量以及个人数据记录）、其可能产生的后果以及为处理泄露行为而已采取或拟采取的措施（包括在适当情况下，为减轻其可能产生的不利影响而已采取或拟采取的措施）。如果在不可能同时提供所有信息的情况下，初始通知应载列当时可获得的信息，并应在获得进一步信息后尽快提供，不得无故拖延。
			4. 数据导入者应与数据导出者合作并提供协助，使数据导出者能够遵守其在法规 (EU) 2016/679项下的义务，尤其是在考虑到处理的性质和数据导入者可获得的信息后通知主管监管机构和受影响的数据主体。
		2. 敏感数据

如果传输涉及的个人数据披露种族或民族、政见、宗教或哲学信仰、或工会成员资格、遗传数据、或用于唯一识别自然人的生物数据、有关健康的数据或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（以下简称“敏感数据”），数据导入者应适用附录I.B中所述的特定限制和/或额外保护措施。

* + 1. 再传输

数据导入者仅应根据数据导出者的书面指示向第三方披露个人数据。此外，只有在欧盟以外的第三方（与数据导入者位于同一国家/地区或位于另一第三方国家/地区，以下简称“再传输”）根据适当的模块接受或同意受本条款约束的情况下，或在以下情况下，才可向该第三方披露数据：

* + - 1. 再传输至受益于根据法规 (EU) 2016/679第45条（涵盖再传输）作出充份性决定的国家/地区；
			2. 第三方根据法规 (EU) 2016/679第46条或第47条以其他方式确保对有关处理采取适当的保护措施；
			3. 在特定的行政、监管或司法程序中，为确立、行使法律权利要求或就法律权利要求进行抗辩而必须进行再传输；或
			4. 为了保护数据主体或另一个自然人的重大利益而必须进行再传输。

任何再传输均以数据导入者遵守本条款下的所有其他保护措施为前提，尤其是目的限制。

* + 1. 文件记录和合规性
			1. 数据导入者应及时充分地处理数据导出者就本条款下的处理事宜提出的询问。
			2. 各方应能够证明本条款得到遵守。尤其是，数据导入者应保存有关代表数据导出者进行的处理活动的适当文件记录。
			3. 数据导入者应向数据导出者提供为证明本条款规定的义务得到遵守而必需的所有信息，并应数据导出者的要求，允许并协助按合理的时间间隔或在有迹象表明存在不合规的情况下对本条款所涵盖的处理活动进行审计。在决定审查或审计时，数据导出者可考虑数据导入者持有的相关证书。
			4. 数据导出者可选择自行或委托一名独立审计师进行审计。审计可包括在数据导入者的场所或实际设施进行检查，并应在适当情况下经合理通知后进行。
			5. 各方应根据要求向主管监管机构提供(b)段和(c)段提及的信息，包括任何审计结果。
	1. **使用子处理方**
		+ 1. 数据导入者拥有数据导出者的一般授权，可聘用商定清单中的子处理方。数据导入者应至少提前六个月以书面形式明确通知数据导出者其拟对该清单作出的任何变更，包括增加或更换子处理方，以便数据导出者有足够的时间在聘用子处理方之前对该等变更提出反对意见。此外，数据导入者应在向任何新的子处理方提供个人数据（客户数据中所包含的除外；个人数据及客户数据的定义见《数据保护补充协议》（<https://www.21vbluecloud.com/ostpt/>））访问权限之前提前至少30天明确通知该子处理方的控制方。数据导入者应向数据导出者提供必要的信息，以使数据导出者能够行使其提出反对的权利。本条项下的信息提供应按照《数据保护补充协议》的条款进行。
			2. 如果数据导入者聘请子处理方（代表数据导出者）开展特定处理活动，其应通过签署书面合同的方式进行，合同中应规定与数据导入者在本条款项下的义务实质上相同的数据保护义务，包括关于数据主体的第三方受益人权利。各方同意，数据导入者遵守本条规定即履行了其在第8.8条项下的义务。数据导入者应确保子处理方遵守数据导入者在本条款下应遵守的义务。
			3. 应数据导出者要求，数据导入者应向数据导出者提供上述子处理方协议的副本及其任何后续修订。在为保护商业机密或其他保密信息（包括个人数据）所必需的范围内，数据导入者可在提供副本之前对协议文本进行编辑以隐去该等信息。
			4. 数据导入者应始终就子处理方在其与数据导入者签订的合同项下的义务履行对数据导出者承担全部责任。如子处理方未履行其在上述合同项下的任何义务，数据导入者应通知数据导出者。
			5. 数据导入者应与子处理方商定第三方受益人条款，以便在数据导入者事实上消失、法律上不再存在或破产的情况下，数据导出者有权终止与子处理方的合同并指示子处理方删除或返还个人数据。
	2. **数据主体权利**
		+ 1. 数据导入者应将其从数据主体收到的任何请求及时通知数据导出者。除非经数据导出者授权，否则其不应自行回应该等请求。
			2. 数据导入者应协助数据导出者履行其义务，回应数据主体根据法规 (EU) 2016/679行使其权利的请求。就此，各方应根据处理的性质在附录II中规定提供协助的适当技术和组织措施，以及所需协助的范围和程度。
			3. 数据导入者在履行(a)段和(b)段规定的义务时，应遵从数据导出者的指示。
	3. **补救**
		+ 1. 数据导入者应通过单独通知或在其网站上通告的方式，以透明和易于访问的格式向数据主体告知有权处理投诉的联络点，并及时处理其从数据主体收到的任何投诉。
			2. 如果数据主体与某一方就本条款的履行存在争议，该方应尽其最大努力及时友好地解决争议。各方应相互告知此类争议，并在适宜的情况下合作解决该等争议。
			3. 如果数据主体根据第3条援引第三方受益人权利，数据导入者应接受数据主体的如下决定：
				1. 向其经常居住地或工作地所在成员国的监督机构或第13条规定的主管监督机构提出投诉；
				2. 将争议提交第18条所定义的有管辖权的法院。
			4. 各方同意数据主体可根据法规(EU) 2016/679第80 (1)条规定的条件由非盈利机构、组织或协会代表。
			5. 数据导入者应遵守根据适用的欧盟或成员国法律具有约束力的决定。
			6. (数据导入者同意，数据主体所作的选择不会影响其依照适用法律寻求救济的实体和程序权利。
	4. **责任**
		+ 1. 每一方应就其因违反本条款而给其他一方/多方造成的任何损害向其他一方/多方承担责任。
			2. 对于数据导入者或其子处理方因违反本条款规定的第三方受益人权利而给数据主体造成的任何实质性或非实质性损害，数据导入者应向数据主体承担责任，数据主体应有权获得赔偿。
			3. 尽管有(b)段的规定，对于数据导出者或数据导入者（或其子处理方）因违反本条款规定的第三方受益人权利而给数据主体造成的任何实质性或非实质性损害，数据导出者应向数据主体承担责任，数据主体应有权获得赔偿。上述规定不影响数据导出者和控制方（如数据导出者作为处理者代表控制方行事）在法规(EU) 2016/679或法规(EU) 2018/1725（视情况而定）项下的责任。
			4. 各方同意，如果数据导出者根据(c)段对数据导入者（或其子处理方）造成的损害承担责任，数据导出者应有权向数据导入者追偿与数据导入者对损害的责任相应的部分赔偿。
			5. 如果多于一方对因违反本条款而给数据主体造成的任何损害负有责任，则所有责任方应承担连带责任，数据主体有权向法院起诉当中的任何一方。
			6. 各方同意，如果一方根据(e)段承担责任，该方应有权向其他一方/多方追偿与其对损害的责任相应的部分赔偿。
			7. 数据导入者不得援引子处理方的行为来逃避其自身的责任。
	5. **监督**
		+ 1. 负责确保数据导出者就数据传输遵守法规 (EU) 2016/679的监督机构（如附录I.C所载）应为主管监督机构。
			2. 数据导入者同意就任何旨在确保遵守本条款的程序接受主管监督机构的管辖并与主管监督机构合作。特别是，数据导入者同意回应监督机构的查询、接受监督机构的审查及执行监督机构采取的措施，包括补救和补偿措施，并应向监督机构提供已采取必要行动的书面确认。
1. **–在公共机构访问情况下的当地法律和义务**
	1. **影响遵守本条款的当地法律和惯例**
		* 1. 各方保证，他们没有理由相信第三国目的地适用于数据导入者处理个人数据的法律和惯例（包括披露个人数据的任何要求或授权公共机构访问的措施）会阻碍数据导入者履行其在本条款下的义务。这是基于以下理解，即尊重基本权利和自由的本质且不超过在民主社会中保障法规 (EU) 2016/679第23(1)条所列目标之一所必需和相称的法律和惯例与本条款并不冲突。
			2. 各方声明，在提供(a)段所述保证时，它们特别地适当考虑到下列因素：
				1. 数据传输的具体情况，包括处理链条的长度、所涉及的参与者的数量和所使用的传输渠道；拟进行的再传输；接收方的类型；处理的目的；所传输的个人数据的种类和格式；发生数据传输所在的经济部门；所传输数据的存储地点；
				2. 第三国目的地的法律和惯例（包括要求向公共机构披露数据或授权该等机构访问数据的法律和惯例）— 与传输的具体情况相关，以及适用的限制和保护措施；
				3. 作为对本条款项下保护措施的补充而采取的任何相关合同的、技术的或组织的保护措施，包括在传输过程中以及在目的地国家处理个人数据时采用的措施。
			3. 数据导入者保证，在根据(b)段进行评估时，其已尽最大努力向数据导出者提供相关信息，并同意其将继续与数据导出者合作以确保遵守本条款。
			4. 各方同意根据将(b)段项下的评估记录在案，并且一经要求向主管监督机构提供。
			5. 如果在数据导入者同意本条款之后以及在合同期内，数据导入者有理由相信它受到或已经受到不符合(a)段要求的法律或惯例的约束（包括在第三国的法律发生变化或有措施（如披露请求）表明该等法律在实践中的应用不符合(a)段的要求之后），数据导入者同意迅速通知数据导出者。
			6. 在根据(e)段发出通知后，或者如果数据导出者有理由相信数据导入者无法再履行其在本条款下的义务，数据导出者应立即确定数据导出者和/或数据导入者为应对这种情况拟采取的适当的措施（例如为确保安全和保密拟采取的技术的或组织的措施）。如果数据导出者认为无法确保对数据传输采取适当保护措施，或者如果主管监督机构指示须中止数据传输，则数据导出者应中止数据传输。在这种情况下，数据导出者应有权终止根据本条款处理个人数据的合同。如果合同涉及两方以上，则数据导出者可仅对相关方行使终止权，除非各方另有约定。在根据本条规定终止合同的情况下，应适用第16(d)和(e)条规定。
	2. **在公共机构访问情况下数据导入者的义务**
		1. 通知
			1. 数据导入者同意在以下情况下及时通知数据导出者，并在可能的情况下及时通知数据主体（如有必要，在数据导出者的帮助下）：
				1. 收到公共机构（包括司法当局）根据目的地国家的法律提出的关于披露根据本条款传输的个人数据的具有法律约束力的要求；该通知应包括关于被要求的个人数据的信息、提出要求的机构、提出要求的法律依据和所提供的答复；或
				2. 获悉任何公共机构根据目的地国家的法律直接访问根据本条款传输的个人数据；该通知应包括导入者可获得的所有信息。
			2. 如果目的地国家的法律禁止数据导入者通知数据导出者和/或数据主体，则数据导入者同意尽最大努力获得该禁令的豁免，以便尽快通报尽可能多的信息。数据导入者同意记录其所做的最大努力，以便能够在数据导出者提出要求时予以证明。
			3. 在目的地国家的法律允许的情况下，数据导入者同意在合同有效期内定期向数据导出者提供尽可能多的关于收到的要求的相关信息（特别是要求的数量、所要求的数据类型、提出要求的机构、要求是否受到质疑以及此类质疑的结果等)。
			4. 数据导入者同意在合同有效期内根据(a)至(c)段规定保存信息，并一经要求向主管监督机构提供该等信息。
			5. (a)至(c)段规定不影响数据导入者根据第14 (e)条和第16条规定在其无法遵守本条款时及时通知数据导出者的义务。
		2. 合法性审查和数据最小化
			1. 数据导入者同意审查披露要求的合法性，特别是审查该要求是否仍在向提出要求的公共机构授予的权力范围之内，并且如果在数据导入者经过仔细评估后，认定有合理理由认为根据目的地国家的法律、国际法项下的适用义务和国际礼让原则该要求为非法的，则数据导入者同意对该要求提出质疑。数据导入者应在相同条件下寻求上诉的可能性。在对要求提出质疑时，数据导入者应寻求临时措施，以期在主管司法当局对其案情作出决定之前暂停该要求的效力。在根据适用的程序规则要求披露个人数据之前，数据导入者不得披露所要求的个人数据。这些要求不影响第14(e)条规定的数据导入者的义务。
			2. 数据导入者同意将其法律评估和对披露要求提出的任何质疑记录在案，并在目的地国家的法律允许的范围内，将文件提供给数据导出者。应主管监督机构要求，数据导入者也应向其提供该等文件。
			3. 数据导入者同意在回应披露要求时，根据对要求的合理解释，提供允许的最少数量的信息。
2. **–附则**
	1. **不遵守本条款和终止**
		* 1. 数据导入者若因任何原因无法遵守本条款，应尽快通知数据导出者。
			2. 如果数据导入者违反本条款或无法遵守本条款，数据导出者应暂停向数据导入者传输个人数据，直至再次确保符合本条款或合同终止。这不影响第14(f)条的规定。
			3. 在以下情况下，只要涉及本条款下的个人数据处理，数据导出者有权终止合同：
				1. 数据导出者已根据(b)款暂停向数据导入者传输个人数据，且未在合理时间内（无论如何须在暂停后一个月内）恢复遵守本条款；
				2. 数据导入者严重或持续违反本条款；或
				3. 数据导入者未能遵守有管辖权的法院或监管机构就其在本条款下的义务作出的具有约束力的决定。

在上述情况下，数据导出者应将此类违规行为通知主管监督机构。如果合同涉及两个以上缔约方，数据导出者只能对相关一方行使终止权，除非各方另有约定。

* + - 1. 已在根据(c)款终止合同之前传输的个人数据应按照数据导出者的选择立即返还数据导出者或全部删除。该规定同样适用于数据的任何副本。数据导入者应向数据导出者证明数据已删除。在删除或返还数据之前，数据导入者应继续确保遵守本条款。如果适用于数据导入者的当地法律禁止返还或删除已传输的个人数据，数据导入者保证其将继续确保遵守本条款，并仅在当地法律要求的范围内和期间内处理数据。
			2. 如果(i)欧盟委员会根据法规(EU) 2016/679第45 (3)条通过了涉及本条款所适用个人数据传输的决定；或(ii)法规(EU) 2016/679成为个人数据传输目的地国家/地区法律框架的一部分，则任何一方均可撤销其受本条款约束的协议。这不影响适用于法规(EU) 2016/679项下相关处理的其他义务。
	1. **管辖法律**

本条款应受欧盟某一成员国的法律管辖，前提是该法律允许第三方受益人的权利。各方同意，该法律应是数据导出者成立地所在成员国的法律。

* 1. **法院地和司法管辖权的选择**
		+ 1. 因本条款引起的任何争议应由欧盟成员国的法院解决。
			2. 各方同意这些法院应是数据导出者成立地所在成员国的法院。
			3. 数据主体还可在其经常居住地所在成员国的法院对数据导出者和/或数据导入者提起法律诉讼。
			4. 各方同意接受上述法院的司法管辖。
	2. **缔约方名单**

**数据导出者：**

客户是数据导出者。数据导出方是数据导出方与数据导入方之间的《数据保护补充协议》（“DPA”）和《世纪互联在线服务条款》（“OST”）中定义的在线服务的用户。在本附录I和附录II中，所有未作定义的首字母大写术语均具有DPA中赋予的含义。

与本条款项下所传输数据相关的活动：

需要进行数据传输 ，以便成功、高效地向我们的客户提供世纪互联在线服务，并管理个人数据的处理和安全。

世纪互联将仅按照DPA和OST中的规定并在符合其中限制条件的情况下使用和以其他方式处理客户数据和个人数据，(a)以便根据客户的书面指示向DPA下所提供在线服务的用户（“客户”）提供在线服务，并(b)用于与向客户提供在线服务相关的业务运营。

|  |  |  |
| --- | --- | --- |
|  |  |  |

**数据导入者：**

名称：上海蓝云网络科技有限公司（“世纪互联”）

地址：

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

联系人姓名、职位和联系方式：

上海蓝云网络科技有限公司

收件人：刘玉岩  风险管理高级经理

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

与本条款项下所传输数据相关的活动：

需要进行数据传输，以便成功、高效地向我们的客户提供世纪互联在线服务，并管理个人数据的处理和安全。

世纪互联将仅按照DPA和OST中的规定并在符合其中限制条件的情况下使用和以其他方式处理客户数据和个人数据，(a)以便根据客户的书面指示向DPA下所提供在线服务的用户（“客户”）提供在线服务，并(b)用于与向客户提供在线服务相关的经营活动。

* 1. **传输详细信息**

*个人数据被传输的数据主体的类别*

**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、合作者和客户，详见DPA的附件B。

*所传输个人数据的类别*

**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，根据数据导出者对在线服务的使用情况，数据导出者可以选择包含DPA附件B中详述的任何类别的个人数据。

*传输的敏感数据（如适用）以及充分考虑到数据性质和所涉风险的应用限制或保护措施，例如严格的目的限制、访问限制（包括仅允许经过专门培训的员工访问）、保存数据访问记录、对再传输的限制或额外安全措施。*

数据导入者已实施并将保持附录II中规定的安全措施。

*传输频率（例如，数据是一次性传输还是连续传输）。*

数据可以连续传输。

*处理的性质/数据传输和进一步处理的目的*

将仅按照DPA的规定并在符合其中限制条件的情况下使用和以其他方式处理客户数据和个人数据，(a)以便根据数据导出者的书面指示向数据导出者提供在线服务，并(b)用于与向数据导出者提供在线服务相关的经营活动。

*个人数据将被保留的期限，或者如果没有可能，用于确定该期限的标准*

除免费试用外，在数据导出者的订购期满或终止后，数据导入者会将仍然存储在在线服务中的客户数据在功能受限制的账户中保留九十(90)天,以便数据导出者提取这些数据。为期九十(90)天的保留期限结束后，数据导入者将禁用数据导出者的账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，除非适用法律允许或要求或者DPA授权数据导入者予以保留。

在线服务可能不支持数据导出者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，数据导入者不承担任何责任。

*对于向（子）处理方传输，还应表明处理的标的、性质和持续时间*

数据导入者可能会聘用子处理方来代表数据导入者提供某些有限或辅助服务。数据导入者应负责保证其子处理方履行DPA中规定的世纪互联的义务。数据导入者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,数据导入者将通过书面合同确保子处理方仅会出于交付数据导入者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。数据导入者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。数据导入者同意监督子处理方，以确保履行这些合同义务。

* 1. **主管监督机**

*根据第13条确定主管监督机构*

数据导出者成立地所在成员国的主管监督机构。

**技术和组织措施，包括确保数据安全的技术和组织措施**

数据导入者按第8.6(a)条和第10(b)条实施的技术和组织安全措施的描述：

**技术和组织措施**

就在线服务涉及的客户数据或个人数据的处理和安全而言，数据导入者已实施并将维持DPA之附录A –安全措施中所述的安全措施。

数据导入者就其作为数据导入方向其传输的数据，提供DPA之附录 C – 额外保护措施附录中所述的额外保护措施。

数据导入者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客户数据和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。世纪互联安全政策会规定这些措施。数据导入者将向数据导出者提供该政策，以及数据导出者合理要求获取的有关世纪互联安全实践和政策的其他信息。

此外，这些措施应符合ISO 27001、ISO 27002和ISO 27018中规定的要求。数据导出者可以获得针对上述要求的安全控制措施的说明。

**适用于瑞士的补充内容**

就将客户数据和个人数据从瑞士出境以提供在线服务而言（受2021标准合同条款管辖，并且（除受GDPR约束外）还受《瑞士联邦数据保护法》（FADP）约束），2021标准合同条款应作如下修订：

* 第4条a款：本条款中使用的“个人数据”和“数据主体”等术语应解释为包括FADP中的相应定义。
* 第13条：在数据传输受FADP管辖的情况下，主管监督机构（将在附录I.C中命名）是瑞士联邦数据保护和信息专员（FDPIC）。
* 第18条c款：应以以下方式对本条款进行解释：经常居住在瑞士的数据主体也可向瑞士法院提起针对数据导出者和/或数据导入者的法律诉讼。

**代表数据导入者签署标准合同条款、附件：**

签名：Johnny Liu



职称：总裁

上海蓝云科技有限公司（“世纪互联”）

北京市朝阳区酒仙桥路6号院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：
			1. 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；
			2. 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；
			3. 采取 GDPR 第 32 条所要求的所有措施；
			4. 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；
			5. 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；
			6. 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；
			7. 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；
			8. 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）

* + 1. 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）
		2. 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：
1. 个人数据的假名化和加密；
2. 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；
3. 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
4. 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）
	* 1. 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）
		2. 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）
		3. 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。