欧盟数据保护白皮书

2016 年 11 月

(请访问 http://aws.amazon.com/compliance/aws-whitepapers/ 获取此白皮书的最新版本，访问 http://aws.amazon.com/de/data-protection/ 获取德语版本。)

介绍

本文档为希望使用 AWS 存储含个人数据的内容的客户提供帮助信息。具体而言，本文档介绍客户如何根据欧洲议会和理事会于 1995 年 10 月 24 日发布的有关个人数据处理的个人保护以及此类数据的自由移动的指令 95/46/EC（以下简称“指令”）使用 AWS 服务。目的是帮助客户理解：

- AWS 服务的运行方式，包括客户如何遵守欧盟法律，满足其安全需求和加密，或者保护其内容
- 客户对存储和访问其内容的地理位置的完全控制，以及其他相关合规性注意事项
- 在管理和保护 AWS 服务上所存储内容的过程中，客户和 AWS 分别担当的角色

本白皮书重点介绍 AWS 客户在考虑“指令”对其使用 AWS 服务存储包含个人数据的内容的影响时常见的典型问题。各客户还有其他相关注意事项需要考虑，如客户需要遵守行业特定要求以及客户业务所在司法辖区的其他法律。本白皮书仅提供信息参考；不是法律建议，不应理解为法律建议。由于客户的需求各不相同，AWS 鼓励客户寻求有关实施隐私和数据保护环境的适当建议，概括地说，就是与其业务相关的适用法律。

与客户内容相关的注意事项

内容存储为所有组织都带来了一些需要考虑的常见实际问题，包括：

- 内容是否有安全保障？
- 内容存储在哪里？
- 谁可以访问内容？
- 内容适用哪些法律和法规？如何才能遵守这些法律和法规？

这些注意事项并不是新出现的，也不是特定于云的。它们与内部托管和操作的系统以及传统的第三方托管服务相关。使用 AWS 服务时，客户对其内容保有控制权，并且负责 (且已获得完全授权) 管理和控制各自的内容安全要求，包括：

- 选择在 AWS 存储哪些内容
- 内容是否将加密 — 静态和传输中
- 内容用到了哪些 AWS 服务
- 内容是在哪里存储和处理的
- 内容的格式和结构以及是否进行遮蔽或匿名处理
- 他们允许谁访问内容以及如何授予、管理和撤销这些访问权限

客户内容的安全性取决于 AWS 和客户实施相应的措施。当 AWS 在其基础云环境中实施安全控制措施时，AWS 客户对其内容以及内容安全性保有控制权。关于 AWS 上存储的个人数据适用的数据保护要求，了解并区分客户和 AWS 各自的角色是非常重要的。

客户内容安全性：

将 IT 基础设施迁移到 AWS，意味着客户和 AWS 在其职责范围内都对运行和安全性的管理扮演着重要的角色。AWS 运行、管理和控制托管操作系统的组件和虚拟化层，甚至包括运行 AWS 服务的设施的物理安全性。客户负责管理来宾操作系统 (包括来宾操作系统更新和安全补丁) 和关联应用程序软件以及 AWS 提供的安全组防火墙和其他安全相关功能的配置。客户通常通过第三方 (例如 Internet 服务提供商) 提供的服务连接到 AWS 环境。AWS 不提供这些连接，客户应考虑此类连接的安全性以及与其系统相关的此类第三方的安全责任。这实际上与使用提供本地数据中心连接的网络服务提供商没有什么不同。

此模型如下面的图 1 所示：

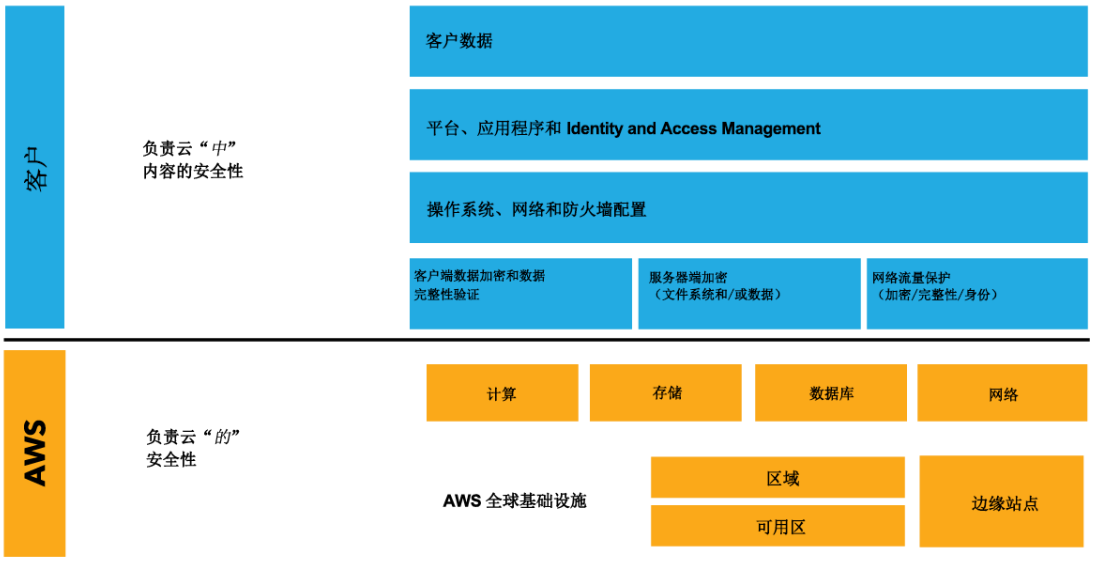

图 1 — 安全模型

此模型对客户内容安全性有何意义？

在评估云解决方案的安全性时，理解和区分以下几点对于客户而言非常重要：

- 云服务提供商 (AWS) 实施和运行的安全措施 — “云*的*安全性”；以及
- 客户实施和运行的安全措施，与使用 AWS 服务的客户内容和应用程序的安全相关 — “云*中*内容的安全性”

AWS 管理云*的*安全性，而确保云*中*内容的安全性则是客户的责任，因为选择何种安全措施来保护其内容、平台、应用程序、系统和网络是由客户控制的 — 这与保护本地数据中心中的应用程序没有区别。作为其不同服务产品的一部分，AWS 有很多安全措施供客户选择，我们的客户也可以选择使用各种第三方安全解决方案。AWS 客户可以完全自由地设计其安全架构以满足其合规性需求。这是与传统托管解决方案的重要不同，传统托管解决方案是提供商来决定架构。AWS 允许客户决定是否实施安全措施，因此，客户有权决定在云中实施哪些安全措施并确定这些措施是否适合其业务。举例来说，如果保护数据需要更高可用性的架构，客户可以添加冗余系统、备份、位置、网络上行链路等来创建更高弹性、更高可用性的架构。如果需要限制数据访问，AWS 控制允许客户在系统级别和通过加密在数据级别实施访问权限管理概念。因此，AWS 允许客户直接控制许多元素，这些元素构成了与数据安全相关的技术和组织措施。

理解云的安全性

AWS 负责管理基础云环境的安全性。AWS 云基础设施已成为当今可用的最灵活安全的云计算环境之一，其目的是提供最优可用性，同时提供完全的客户隔离。它提供一个可扩展性极强、高度可靠的平台，客户可以根据需要在全球范围大规模快速安全地部署应用程序和内容。AWS 服务是内容无关的，无论存储何种类型的内容或存储内容的地理位置，它们都为所有客户提供相同的高级别安全性。因为 AWS 不知道客户在 AWS 服务中存储什么数据，所以 AWS 无法将客户所存储内容中的个人数据与其他类型的数据区分开来。

AWS 世界一流、非常安全的数据中心利用先进的电子监视和多重访问控制系统。数据中心每周 7 天、每天 24 小时由训练有素的保安看守，访问严格遵循最小特权原则，限制于系统管理目的。有关核心 AWS 云基础设施、平台和服务中构建的所有安全措施的完整列表，请参阅我们的安全过程概述白皮书。

我们高度注意基础云环境的安全性，实施了精密的技术和组织措施来防止未经授权的访问。客户可以通过 AWS 认证和报告 (包括 AWS 服务组织控制 (SOC) 1 和 2 报告、ISO 27001 认证和 PCI-DSS 合规性报告) 验证 AWS 环境内的安全控制是否就位。这些报告和认证由独立第三方审计师发布，它们证实 AWS 安全控制的设计和运行的有效性。可以访问 https://aws.amazon.com/compliance/contact 索取适用的 AWS 合规性认证和报告。AWS 合规性网站提供有关 AWS 合规性认证、报告以及最佳实践和标准遵从性的更多信息。

AWS 提供了数据处理附录来帮助客户履行其数据保护职责。如果客户需要将个人数据从欧盟传输到欧洲经济区外的国家/地区，AWS 还可以将标准合同条款 2010/87/EU (通常称为“示范条款”) 加入客户的数据处理附录中。

2015 年 3 月 6 日，AWS 数据处理附录 (包括示范条款) 通过欧盟数据保护机构组 (称为 Article 29 Working Party) 批准。这一批准意味着需要示范条款的任何 AWS 客户现在都可以通过 AWS 数据处理附录提供足够的合同承诺，根据指令实现国际数据流动。有关 Article 29 Working Party 审批的更多详情，请访问 Luxembourg Data Protection Authority 网页：
http://www.cnpd.public.lu/en/actualites/international/2015/03/AWS/index.html

除了数据处理附录和示范条款，如果客户希望将个人数据从 AWS 的欧盟区域传输到美国区域，还将因 AWS 加入欧盟—美国隐私护盾框架而受益。Amazon.com, Inc.，以及它的一些美国附属公司 (包括 AWS) 已于 2016 年 10 月 21 日通过了欧盟—美国隐私护盾框架认证。欧盟—美国隐私护盾框架不会影响客户使用 AWS 或与 AWS 合作的方式，而是额外提供了一种由欧盟批准、将个人数据从欧盟传输到美国的机制。有关美国服务提供商在欧盟-美国隐私护盾下的义务的更多信息，请访问此处的欧盟委员会网站：http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm 以及此处的欧盟—美国隐私护盾框架网站：https://www.privacyshield.gov/welcome。

理解云“中”内容的安全性

在发布 AWS 服务时，客户对其内容保有控制权。是客户而不是 AWS 决定他们在 AWS 中存储哪些内容，控制配置环境和保护内容安全的方式，确定是否加密其静态和传输中的内容，决定谁可以访问内容以及需要哪些凭证 (包括多重身份验证的使用)，以及使用哪些其他安全功能和工具以及如何使用。

因为客户对其安全性保持控制，他们还对其组织放在 AWS 上或连接到其 AWS 基础设施的所有内容 (如来宾操作系统、其计算实例上的应用程序以及在 AWS 存储、平台和数据服务中存储和处理的内容) 的安全性负责。

客户可以配置其 AWS 服务以利用一系列可选的安全功能、工具和控制来保护其内容，包括先进的身份和访问管理工具、可用性配置、备份功能、安全功能、加密和网络安全性。为帮助客户设计、实施和运行其安全 AWS 环境，AWS 提供了广泛的安全功能供客户使用。客户也可以使用他们自己的或第三方的安全工具和控制措施。客户可以采取以下示例步骤来帮助保护其内容安全，这些步骤包括实施：

- 强密码策略，为用户分配合适的权限并采取可靠的步骤保护其访问密钥
- 适当的防火墙和网络隔离，包括 Virtual Private Cloud、加密内容、使用 SSL 并正确构建系统以降低数据丢失和未授权访问的风险
- 适当的冗余方案和备份策略以缓解数据丢失或不可用的风险

所有这些因素都由客户掌控，而不是 AWS。AWS 看不到客户放置在 AWS 上的内容，不会更改客户配置设置；这些由客户确定和控制。因为是由客户决定在 AWS 云中放置哪些内容，所以只有客户可以决定哪个安全级别适合所存储的数据。

为帮助客户将 AWS 安全控制集成到其现有控制框架中，并帮助客户针对其组织使用 AWS 服务的情况设计和执行安全评估，AWS 发布了很多与安全、监管、风险和合规性有关的白皮书，以及很多核对清单和最佳实践。客户也可以根据其偏好自由设计和执行安全评估，还可以申请对其云基础设施执行扫描 (假设这些扫描仅限于客户的计算实例并且不违反 AWS 可接受的使用策略)。

AWS 区域

AWS 数据中心是在全球多个国家/地区的集群中构建的。我们将给定国家/地区的每个数据中心群集称为一个“区域”。客户可以访问全球十四个 AWS 区域，包括欧盟的两个区域 — 爱尔兰 (都柏林) 和德国 (法兰克福)。客户可以选择使用一个区域、所有区域或任意区域组合。图 2 所示为 AWS 区域位置：

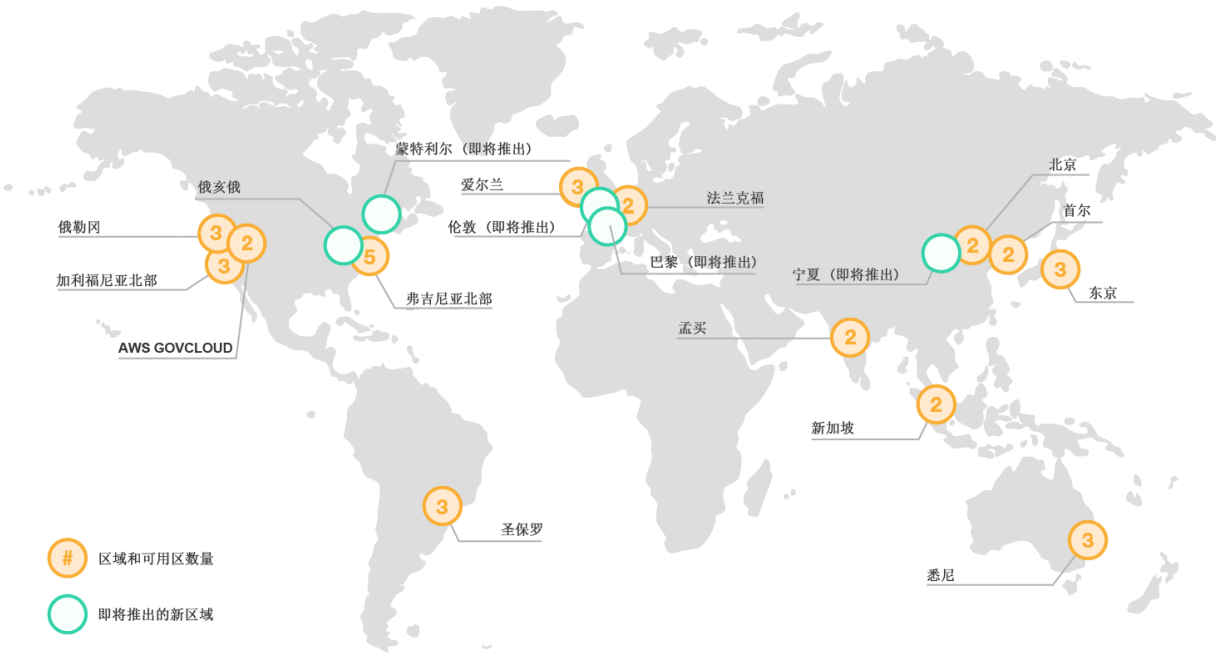

图 2 — AWS 全球区域

由 AWS 客户选择用来托管其内容的 AWS 区域。这样客户可以按照地理特定的要求在其选择的位置建立环境。例如，欧洲的 AWS 客户可选择仅在欧洲 (德国) 区域部署其 AWS 服务。如果客户这样选择，则其内容将存储在德国，除非客户选择其他 AWS 区域。

客户可在多个区域复制和备份内容，但 AWS 不会将客户内容移到客户所选区域之外。

客户如何选择区域？

在使用 AWS 管理控制台或通过 AWS 应用程序编程接口 (API) 发出请求时，客户指定希望使用 AWS 服务的特定区域。图 3：选择 AWS 全球区域会提供一个示例，说明何时将内容上传到 AWS 存储服务或使用 AWS 管理控制台配置计算资源。

图 3 — 在 AWS 管理控制台中选择 AWS 全球区域

客户也可以利用 Amazon Virtual Private Cloud (VPC) 功能为其计算资源指定要使用的 AWS 区域。Amazon VPC 允许客户配置部分 AWS 云，在这部分 AWS 云中，客户可以在客户定义的虚拟网络中启动 AWS 资源。借助 Amazon VPC，客户可以定义与自有数据中心内运行的传统网络非常相似的虚拟网络拓扑结构。

客户启动到 VPC 中的任何计算和其他资源都将放置到客户指定的区域中。

客户内容的客户控制和访问

客户控制内容

客户使用 AWS 对 AWS 环境中的内容保持控制。他们可以：

- 确定内容的放置位置，例如存储环境的类型和存储的地理位置
- 控制内容的格式，例如纯文本、遮蔽、匿名或加密，可以使用 AWS 提供的加密或客户选择的第三方加密机制
- 管理其他访问控制，如身份权限管理和安全凭证
- 控制是否使用 SSL、Virtual Private Cloud 和其他网络安全措施防止未授权访问

这样 AWS 客户可以控制其 AWS 上内容的整个生命周期，根据他们自己的特定需求管理其内容，包括内容分类、访问控制、保留和删除。

客户内容访问

除非需要向客户提供其所选的 AWS 服务，AWS 不会访问客户的任何内容。AWS 不会出于任何其他目的访问客户的内容。

AWS 不知道客户选择在 AWS 服务中存储什么内容，也无法区分个人数据与其他内容，因此 AWS 同等对待所有客户内容。这样，无论内容是否包含个人数据，所有客户内容都享有同样可靠的 AWS 安全措施保护。AWS 仅提供客户所选的计算、存储、数据库和联网服务，并对 AWS 提供的云基础设施应用一流的安全措施。客户可以根据自己的独特需求在此基础设施之上自由构建安全机制。

政府访问权限

经常有人询问国内和国外政府机构对云服务中内容的访问权限。客户通常关心数据主权问题，包括政府是否有权访问其内容以及在何种环境下政府可以访问其内容。内容所在司法管辖区的当地适用法律是某些客户的重要考虑事项。不过，客户还需要考虑其他司法管辖区的法律是否适用于他们，这取决于他们 — 或其客户 — 从事业务的地区。客户应寻求建议以了解相关法律对其业务和运营的适用性。

当提出有关国内或国外政府对云中所存储内容的访问权限问题时，必须要了解一点，即相关政府机构有权根据该客户适用的法律索取相关内容。例如，在国家/地区 X 开展业务的公司可能需要处理信息方面的法律请求，即使内容存储在国家/地区 Y。通常，如果政府机构希望访问某一实体的数据，会直接针对实体而不是云提供商发出信息请求。

通常，欧盟成员国有法律支持公共执法机构和国家安全机构访问信息。国外执法机构也可以与当地执法机构和国家安全机构合作来获取对欧盟中信息的访问权限。事实上，大多数国家/地区都有程序 (包括司法互助协定) 来响应适当的法律信息请求 (例如与犯罪行为有关的信息)，允许将信息传输到其他国家/地区。不过请注意，必须在相关法律下满足特定条件，相关执法机构的访问请求才会被授权。例如，要求访问信息的政府机构可能需要出示其有正当理由要求一方提供内容访问权限，可能需要取得法庭命令或批准。

大多数国家/地区都有域外适用的数据访问法律。例如，云服务内容中经常提到的美国爱国者法案就是一条域外适用的美国法律。爱国者法案与很多其他发达国家允许政府获取与相关国际恐怖主义和其他外国情报问题调查有关信息的法律没什么不同。根据爱国者法案，任何文档请求都必须提供法庭命令，说明请求符合法律要求，例如请求与合法调查有关。

AWS 策略

无论对客户内容的请求是在哪里发出或客户是什么身份，AWS 始终对保护客户内容保持警惕。除非法律上有效并有约束力的命令要求 (如传票或法庭命令)，AWS 不会泄露客户内容。非美国政府或监管机构通常必须使用经认可的国际流程 (例如，与美国政府签订的司法互助协定) 以获取有效的、有约束力的指令。我们会仔细检查每个请求以验证其准确性并验证它符合适用法律。我们会向过分、超出请求者授权或不完全符合适用法律的请求挑战。如果我们被迫披露客户内容，我们会在披露之前先通知客户，以便他们有机会寻求披露保护，除非法律禁止这样做。

欧盟数据保护：指令

我们在“指令”中包含的职责范围内考虑[1]。广义地说，“指令”规定了一系列处理个人数据时适用的数据保护要求。在这种情况下，“处理”包括对个人数据执行的任何操作或操作集。“指令”对“个人数据”的定义是，可以或可能识别出生命个体 (称为“数据当事人”) 的信息。此外，“指令”还区分了 (a)“数据控制方”— 决定个人数据处理的目的和方式的一方，以及 (b)“数据处理方”— 代表控制方处理个人数据的一方。

数据控制方必须确保其在处理个人数据时遵守数据保护义务。例如，数据控制方需确保个人数据得到公正合法的处理，并且确保该数据经过加密以防未经授权或非法的处理。

AWS 意识到其服务在各种商业运营中得到使用，并且可能有多方参与到供应链中。然而作为通用指南，当使用 AWS 存储的客户内容中含有个人数据时：

- 如果客户决定了处理该数据的目的，并已选择数据处理的方式，则该客户将成为个人数据的相关控制方。
- 如果客户仅仅在 AWS 网络上以第三方名义或按第三方 (可能是数据控制方，供应链中的另一第三方，或者以纯粹的本地身份行事的个人) 的意愿处理个人数据，则该客户将成为个人数据的相关处理方。

作为自助式服务基础设施的提供者，AWS 仅为需要在 AWS 网络上上传并处理内容的客户提供基础设施服务。至于数据是否被“处理”以及如何处理，则完全受客户控制。由于这个原因，AWS 并不能看到或者了解客户正在其网络上上传的内容，包括该内容是否包含任何个人数据。AWS 客户还获得授权使用加密手段来呈现让 AWS 难以理解的内容。除非因提供服务 (或遵守法律或有效且有约束力的法院指令) 所必须，否则 AWS 不会处理客户的内容。

AWS 为防止 AWS 员工访问客户内容而制定了制度、规程和政策。此外，对于想要处理个人数据的客户而言，AWS 提供一份数据处理附录，以帮助客户履行其数据保护义务。如果客户需要将个人数据从欧盟传输到欧洲经济区外的国家/地区，AWS 还可以将“示范条款”加入客户的数据处理附录中。

2015 年 3 月 6 日，AWS 数据处理附录 (包括示范条款) 通过欧盟数据保护机构组 (称为 Article 29 Working Party) 批准。这一批准意味着需要示范条款的任何 AWS 客户现在都可以通过 AWS 数据处理附录提供足够的合同承诺，根据指令实现国际数据流动。有关 Article 29 Working Party 审批的更多详情，请访问 Luxembourg Data Protection Authority 网页：
http://www.cnpd.public.lu/en/actualites/international/2015/03/AWS/index.html

[1] 我们应记住，指令并不直接适用于在欧盟成员国内成立的组织。欧盟成员国须在各自国内法律范围内实施指令。因此，不同成员国内的确切法律义务性质可能有所差别，所以客户应就自己适用的国家法律寻求咨询。

数据控制方负责采取适当的技术组织措施，防止个人数据遭受意外或非法破坏或意外丢失、篡改、越权披露或访问。如果由数据处理方代表数据控制方执行数据处理，数据控制方还负责选择能提供足够技术和组织措施来监管数据处理的数据处理方。

在下表中，我们总结了客户在这种情况下一般会考虑的关键数据保护原则。我们还讨论了 AWS 与这些原则相关的方面。针对此表的用途，我们假设 AWS 客户将作为数据控制方。然而，如上所述，我们承认在很多情况下 AWS 客户将成为数据处理方。但是在这些情况下，AWS 客户仍然会发现下表在自己与数据控制方的关系中很有帮助。

数据保护原则	**数据保护义务汇总**	**注意事项**
公平性	应当将数据控制方的身份、数据处理的目的以及保证公平数据处理所必需的任何其他信息完整无误地告知数据当事人。	**客户：**由客户 (或客户的客户) 决定要收集什么信息，并决定将该信息用于何目的。在很多情况下，客户将与任何数据当事人产生直接关系，因此客户是与数据当事人直接沟通的最佳人选。此外，对于之前已经发给数据当事人的通知，客户应当了解通知的范围。 **AWS：**AWS 不能控制客户选择存储在 AWS 中的内容的类型以及用途。AWS 同样也不能随时监控此内容 (包括该内容是否含有个人数据)。对于客户选择存储在 AWS 基础设施中的个人数据，AWS 无法识别或联系相关数据当事人，因此无法向相关数据当事人提供任何信息。
合法依据	数据控制方必须具备数据处理的合法依据，该依据需至少满足“指令”所列标准中的一条。	**客户：**客户在决定是否要处理个人数据及处理个人数据的目的时，需考虑是否符合指令中的标准之一。例如，数据当事人已经同意的数据处理，或者数据当事人为履行其作为签约方签署的合同而必须进行的数据处理等情况。 **AWS：**如上所述，AWS 无法控制客户选择存储在 AWS 中的内容的类型 (包括该内容是否包含个人数据)。AWS 无法确定客户选择通过结合 AWS 服务产品而构建什么样的架构，也无法确定该架构是否符合顾客的具体需要。在关于是否处理该数据以及为何目的处理该数据的决策中，AWS 不发挥任何作用。相应地，AWS 无法确定该数据处理是否有合法依据。

目的限制	个人数据的采集只能用于指定、明确而合法的目的，不得采用与这些目的不相符的方式进行进一步处理。	**客户：**由客户决定要收集哪些个人数据，并决定将该数据用于何目的。作出这一决定时，客户必须确保有指定、明确而合法的目的。客户决定是否将为任何其他用途而将该数据送交后续处理，并且就这些处理是否符合最初目的而进行评估。 **AWS：**AWS 不能控制客户使用其内容以及将其内容存储在 AWS 云服务中的目的。在客户内容含有个人数据的情况下，AWS 处理该数据时，仅以向每位客户提供其选定的 AWS 服务为目的 (需遵守法律或有效且有约束力的法令的有限情况除外)。
数据当事人的权利	数据当事人必须能够访问其个人数据，且有权对违反指令要求进行处理的个人数据进行整改、擦除或屏蔽。	**客户：**客户对存储于 AWS 的内容保留控制权，因此可以决定数据当事人对该内容所含其个人数据的访问方式。同理，回应数据当事人就客户数据处理活动的合法性提出的请求或投诉的最佳人选就是客户。 **AWS**：如上所述，AWS 不能控制客户选择存储在 AWS 中的内容的类型以及用途。AWS 不能随时监控此内容 (包括该内容是否含有个人数据)。对于客户选择存储在 AWS 基础设施中的个人数据，AWS 无法识别也无法联系相关数据当事人 (这些个人数据与客户本人有关的情况除外)，因此无法向相关数据当事人提供任何信息。AWS 不能将存储在 AWS 的数据与任何特定的个人相联系。该信息仅受该客户掌控。
准确度	数据控制方必须确保该个人数据的准确性，并在必要时确保及时更新该数据。	**客户：**客户可对其选择存储在 AWS 的个人数据保持控制。因此客户有责任验证并维护该数据的准确性 (并按需更新和更正该数据)。此外，客户还管理并负责云服务中的安全，因此客户有能力确保其实施适当的安全措施以防该数据毁坏。 **AWS**：AWS 不能控制客户选择存储在 AWS 中的内容的类型，也无法随时监控该内容。AWS 不会以客户的名义输入或修改任何数据。因此 AWS 无法验证该数据的准确性或更新该数据。但是，SOC 1 Type 2 报告包含了 AWS 为确保数据在基础云环境的完整性所进行的控制的详情。

数据安全	数据控制方必须采取适当的技术和组织措施，防止个人数据遭受意外或非法破坏、意外丢失、篡改、越权披露或访问。	**客户：**只有客户能确定其设计或实施的任何特定安全架构是否适合包括个人数据在内的任何特定类型的内容。客户负责云服务***中***的安全，包括其内容 (以及其内容中的任何个人数据) 的安全，同时负责运用 AWS 服务实施合适的架构。具体而言，客户要负责妥当地 (a) 配置 AWS 服务，(b) 使用与服务相关的可用控制，并且 (c) 必要时采取措施维持适当的安全控制，并对他们的个人数据进行备份 (例如运用加密技术防止个人数据遭受越权访问，并进行常规存档)。 **AWS：**AWS 负责管理基础云环境***的***安全性。有关核心 AWS 云基础设施、平台和服务中构建的所有安全措施的完整列表，请参阅我们的安全过程概述[3]白皮书。 AWS 使用外部审计验证其安全措施的有效性，包括 AWS 提供服务时所使用的物理数据中心的安全。若客户提出书面请求或签署 NDA，AWS 将向客户提供一份审计报告摘要，供客户合理验证 AWS 的安全措施。AWS 将按要求向数据保护部门提供此摘要。
数据保留	个人数据保留的时间不得超过为收集或进一步加工个人数据的目的所必需的时间。	**客户：**由客户决定 AWS 云中存储的任何个人数据的用途，并相应地决定这些个人数据有必要保留的时间。如果不再需要个人数据，客户可将其删除或匿名化。 **AWS：**AWS 无法随时监控所存储的数据是否包含个人数据，也无法监控客户对其存储在云服务中的特定数据进行处理的目的。因此，AWS 无法确定客户为此目的而有必要将数据保留多久。 当客户从 AWS 服务中删除内容时，该内容将呈现为无法读取或被禁用，同时，根据 AWS 标准政策与删除时间轴，AWS 网络上用来存储该内容的基础存储区将被擦除，然后被回收或覆盖。AWS 规程还规定，在清理用于提供 AWS 服务的存储介质之前需执行安全的退役过程。在这一过程中，将按行业标准做法对存储介质进行消磁或擦除，并进行物理销毁或禁用。

传输	个人数据不得传输到欧洲经济区以外的国家或地区，除非该国家或地区能确保与个人数据处理相关的数据当事人的权利和自由得到充分的保障。	**客户：**客户可选择其内容和服务器将位于的 AWS 区域。客户可选择仅在德国或爱尔兰的 AWS 欧洲区域部署其 AWS 服务。 **AWS：**除非因遵守法律或有效且有约束力的法令而必需，否则 AWS 不会将客户内容传输到客户选定的地区以外；AWS 将提供数据处理附录，帮助客户履行其数据保护义务。如果客户需要将个人数据从欧盟传输到欧洲经济区外的国家/地区，AWS 还可以将“示范条款”加入客户的数据处理附录中。2015 年 3 月 6 日，AWS 数据处理附录 (包括示范条款) 通过欧盟数据保护机构组 (称为 Article 29 Working Party) 批准。这一批准意味着需要示范条款的任何 AWS 客户现在都可以通过 AWS 数据处理附录提供足够的合同承诺，根据指令实现国际数据流动。有关 Article 29 Working Party 审批的更多详情，请访问 Luxembourg Data Protection Authority 网页：http://www.cnpd.public.lu/en/actualites/international/2015/03/AWS/index.html 除了数据处理附录和示范条款，如果客户希望将个人数据从 AWS 的欧盟区域传输到美国区域，还将因 AWS 加入欧盟—美国隐私护盾框架而受益。欧盟—美国隐私护盾框架不会影响客户使用 AWS 或与 AWS 合作的方式，而是额外提供了一种由欧盟批准、将个人数据从欧盟传输到美国的机制。有关美国服务提供商在欧盟—美国 Privacy Shield Framework, please see the European Commission website here:http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm 以及此处的欧盟—美国 Privacy Shield Framework website here:https://www.privacyshield.gov/welcome。

数据外泄

由于客户在使用 AWS 时保持对个人数据的管理和控制，客户有责任监控自身的环境防止隐私泄露，并依适用法律要求通知监管机构和受害人。只有客户能够管理这一责任。

客户管控自己的访问密钥并决定谁有权访问其 AWS 账户。AWS 无法随时监控访问密钥以及登录账户的人是否经过授权，因此客户有责任监控访问密钥的使用、误用、分发或丢失。

如果适用的法律有要求，AWS 在实际得知违反与 AWS 网络相关的 AWS 安全标准的情况已得到证实时，将会立即通知客户。

分包商

AWS 使用众多第三方分包商来协助其提供服务。但是，我们的分包商没有访问客户内容的权限。此外，AWS 只使用我们信任的分包商，而且我们使用受我们监督的适当的合约安全保障，以确保有关标准得到遵守。

客户的第三方服务供应商

如本文之前提到的，AWS 环境同时还连接到第三方 (例如 Internet 服务提供商) 直接提供的其他服务。这些第三方对自己的系统负责，其中包括安全，且 AWS 对这些第三方的活动不承担责任。

其他考虑因素

除了可能同样与客户相关的指令，本白皮书不涉及与隐私相关的其他法律，包括任何特定于行业的要求。适用于个别客户的隐私和数据保护相关法律法规将取决于多种因素，包括客户开展业务的地点、经营的行业、客户希望存储的内容的类型、该内容来自何处或何人，以及该内容将存储在何处。

担心隐私监管义务的客户应当首先确保其认清并理解适用于自己的要求，并寻求适当的咨询。

总结说明

安全性永远是 AWS 的第一要务。我们为数以十万计的单位提供服务，其中包括 190 多个国家/地区的企业、教育机构和政府机构。我们的客户包括金融服务供应商以及医疗保健供应商，这些客户将他们最敏感的信息存放在我们这里，其中包括个人健康数据和财务记录。

AWS 服务设计用来让客户灵活地配置和部署其解决方案并对其内容加以控制，其中包括内容的存储地点、存储方式以及谁能访问其内容。AWS 客户可以在 AWS 上构建自己安全的应用程序并安全地存储内容。

其他资源

为帮助客户进一步了解如何满足隐私及数据保护方面的要求，我们鼓励客户阅读 AWS 网站上发表的风险、合规性与安全白皮书、最佳实践、检查表与指南。这些资料可从 http:/aws.amazon.com/compliance 以及 http://aws.amazon.com/security 处获得。

AWS 还提供培训，能够帮助客户学习如何在 AWS 云服务上设计、开发以及操作可用、高效而安全的应用程序，并熟练掌握 AWS 服务及解决方案。我们提供免费教学视频、自主进度动手实验室和讲师指导课程。更多关于 AWS 培训的信息，可从 http://aws.amazon.com/training/ 处获得。

AWS 认证能证明在使用 AWS 技术构建安全可靠的基于云的应用程序时，实施最佳实践所需的相关技术技能和知识。更多关于 AWS 认证的信息，可从 http://aws.amazon.com/certification/ 处获得。

如需了解更多信息，请通过下面的链接联系 AWS：https://aws.amazon.com/contact-us/；或者，也可以联系您当地的 AWS 账户代表。