了解 AWS 上的 GDPR 合规性

2019 年 *10* 月

声明

客户负责对本文档中的信息进行独立评估。本文档：(a) 仅供参考，(b) 代表 AWS 当前的产品服务和实践，如有变更，恕不另行通知，以及 (c) 不构成 AWS 及其附属公司、供应商或授权商的任何承诺或保证。AWS 产品或服务均“按原样”提供，没有任何明示或暗示的担保、声明或条件。AWS 对其客户的责任和义务由 AWS 协议决定，本文档与 AWS 和客户之间签订的任何协议无关，亦不影响任何此类协议。

目录

摘要 vi

通用数据保护条例概览 1

GDPR 给在欧盟运营的组织带来的变化 1

AWS 针对 GDPR 做出的准备 1

AWS 数据处理附录 (DPA) 1

根据 GDPR 规定 AWS 的作用 1

安全责任共担模型 2

强有力的合规框架和安全标准 3

AWS 合规计划 3

云计算合规性控制目录 4

CISPE 行为准则 4

数据访问控制 5

AWS Identity and Access Management 5

通过 AWS STS 创建临时访问令牌 6

多重身份验证 6

访问 AWS 对象资源 7

访问操作和配置数据 8

地理限制 10

控制对 Web 应用程序和移动应用程序的访问 10

监控和日志记录 10

使用 AWS Config 管理和配置资产 11

使用 AWS CloudTrail 进行合规性审计和安全分析 12

日志格式 13
集中式安全管理 14
在 AWS 上保护您的数据 15
加密静态数据 15
加密传输中的数据 16
加密工具 17
通过设计以及默认配置保护数据 21
AWS 如何提供帮助 23
贡献者 25
文档修订 25

摘要

本文档介绍了有关 Amazon Web Services (AWS) 为客户提供的服务和资源的信息，以帮助客户符合可能适用于其活动的通用数据保护条例 (GDPR) 的要求。此类要求包括遵守各项 IT 安全标准，获得 AWS 的云计算合规性控制目录 (C5) 认证，遵守欧洲云基础设施服务供应商 (CISPE) 行为准则，能够提供数据访问控制、监控和日志记录工具，加密和密钥管理功能。

通用数据保护条例概览

通用数据保护条例 (GDPR) 是一项欧洲隐私法[1]（欧洲议会和理事会于 2016 年 4 月 27 日[2]发布的第 2016/679 号条例），已于 2018 年 5 月 25 日强制执行。GDPR 取代了欧盟数据保护指令（指令 95/46/EC），在每个欧盟成员国应用具有约束力的单一数据保护法，从而协调整个欧盟 (EU) 的数据保护法。

GDPR 适用于以下组织对个人数据进行的所有处理：在欧盟设有机构的组织，或者向欧盟个人供应商品、服务或监控欧盟居民行为时处理欧盟居民个人数据的组织。个人数据是指与已识别或可识别的自然人相关的所有信息。

GDPR 给在欧盟运营的组织带来的变化

GDPR 尝试在欧盟成员国之间针对个人数据的安全处理、使用和交换建立一种一致性。组织必须实施和定期审查技术和组织措施以及适用于个人数据处理的合规性政策，从而持续证明其处理的数据的安全性与 GDPR 合规性。若违反 GDPR 规定，欧盟监管机构有权处以最高 2000 万欧元或全球年营业额 4% 的罚款，以较高者为准。

AWS 针对 GDPR 做出的准备

AWS 合规性和安全性专家将配合世界各地的客户，回答他们的问题，并帮助他们依照 GDPR 运行云中的工作负载。这些团队还会根据 GDPR 的要求审查 AWS 的责任。

我们可以确认所有 AWS 服务均按 GDPR 规定使用。

AWS 数据处理附录 (DPA)

AWS 提供了一项符合 GDPR 的数据处理附录 (GDPR DPA)，使客户能够符合 GDPR 合同义务。AWS GDPR DPA 包含在 AWS 服务条款中，自动适用于需要 AWS 遵守 GDPR 的全球所有客户。

根据 GDPR 规定 AWS 的作用

根据 GDPR 的规定，AWS 既是数据处理者，也是数据控制者。

AWS 作为数据处理者

当客户和 AWS 解决方案供应商使用 AWS 服务来处理其内容中的个人数据时，AWS 充当数据处理者。客户和 AWS 解决方案供应商可以使用 AWS 服务中提供的控制措施（包括安全配置控制措施）来处理个人数据。在这些情况下，客户或 AWS 解决方案供应商可能充当数据控制者或数据处理者，而 AWS 则充当数据处理者或子处理者。AWS 提供了一项符合 GDPR 的数据处理附录 (DPA)，其中包含 AWS 作为数据处理者的承诺。

AWS 作为数据控制者

当 AWS 收集个人数据并确定处理此类个人数据的目的和方式时，此时它充当数据控制者。例如，AWS 作为数据控制者，可存储账户信息，用于帐户注册、管理、服务访问、客户联系和支持。

GDPR 第 32 条规定，控制者和处理者必须“实施适当的技术和组织措施”，同时考虑到“现有技术和实施的成本与处理的性质、范围、背景和目的，以及处理给自然人的权利和自由带来的不同可能性和严重程度的风险”。GDPR 针对可能需要采取的安全措施提供了具体建议，包括：

- 对个人数据进行假名和加密处理。
- 能够确保处理系统和服务的持续机密性、完整性、可用性和恢复能力。
- 在发生物理或技术事故时，能够及时恢复个人数据的可用性和访问权限。
- 制定一个流程来定期测试、评估和评价技术和组织措施的有效性，以确保处理的安全性。

安全责任共担模型

安全性和合规性是 AWS 与客户的共同责任。当客户将计算机系统和数据迁移到云中时，客户及云服务供应商将共同承担安全责任。当客户转移到 AWS 云时，AWS 负责保护支持云的底层基础架构，而客户也要对放入云中或连接到云的任何内容负责。责任的这种区分通常称为云的安全性与云中的安全性。

该责任共担模型可以帮助客户减轻运营负担，并为他们提供必要的灵活性和控制权，以便在 AWS 云中部署其基础设施。AWS 运行、管理和控制基础设施组件，从托管操作系统和虚拟化层到运行该服务的设施的物理安全性。客户负责管理来宾操作系统（包括更新和安全补丁）、其他关联应用程序软件以及 AWS 提供的安全组防火墙的配置。有关更多信息，请参阅 AWS 责任共担模式。

强有力的合规框架和安全标准

根据 GDPR，适当的技术和组织措施可能需要包括“确保处理系统和服务的持续机密性、完整性、可用性和恢复性的能力”，以及可靠的恢复、测试和整体风险管理流程。

AWS 合规计划

AWS 合规计划可以帮助客户了解 AWS 用于维护 AWS 云中安全性和实施数据保护的强大控制措施。如果系统是在 AWS 云中构建的，那么双方将共同承担合规性责任。通过将以治理为中心、便于审计的服务功能与适用的合规性或审计标准结合起来，AWS 合规性工具（如 AWS Config、AWS CloudTrail、AWS Identity and Access Management、Amazon GuardDuty 和 AWS Security Hub）基于传统流程构建，可以帮助客户建立 AWS 安全控制环境并在该环境中运营。AWS 为客户提供的 IT 基础设施的设计和管理方式符合安全性最佳实践和一系列 IT 安全标准，包括：

- SOC 1/SSAE 16/ISAE 3402（以前是 SAS 70）
- SOC 2
- SOC 3
- FISMA、DIACAP 和 FedRAMP
- DoD SRG
- PCI DSS 1 级
- ISO 9001/ISO 27001
- ITAR
- FIPS 140-2

- MTCS 3 级

此外，AWS 平台提供的灵活性和控制让客户可以部署符合多项行业特定标准的解决方案 3。

AWS 通过白皮书、报告、认证、评估认证和其他第三方证明向客户提供与 IT 控制环境相关的各种信息。有关更多信息，请参阅 Amazon Web Services：风险与合规性 白皮书。

云计算合规性控制目录

云计算合规性控制目录 (C5) 是一项由德国政府支持的认证计划，由德国联邦信息安全办公室 (BSI) 引入。该计划旨在帮助组织在德国政府针对云供应商的安全建议的范围内展示防范常见网络攻击的运营安全性。

数据保护技术和组织措施以及以数据安全为目标的信息安全措施确保数据的机密性、完整性和可用性。C5 定义了与数据保护相关的安全要求。AWS 客户及其合规顾问在将工作负载迁移到云中时，可以使用 C5 认证来了解 AWS 提供的 IT 安全保障服务的范围。C5 增加了与 IT-Grundschutz 相当的法规规定的 IT 安全级别，以及特定于云的控制力。

C5 增加了更多的控制，可提供有关数据位置、服务预置、管辖地、现有认证、信息披露义务的信息以及一个全方位服务说明。使用此信息，您可以评估与使用云计算服务相关的法律法规（如数据隐私）、自己的策略或威胁环境。

CISPE 行为准则

GDPR 规定了行为准则的批准，以帮助控制者和处理者证明其符合法规。等待欧盟数据保护机构官方批准的一个此类准则是 *CISPE* 云基础设施服务供应商行为准则（以下简称“准则”）4。该 “准则”让客户感到放心，因为他们的云供应商使用了符合 GDPR 要求的适当数据保护标准。

以下是该“准则”的一些主要优点：

- **澄清了在数据保护方面，谁对哪些东西承担责任** — 该“准则”解释了 GDPR 下供应商和客户的角色，特别是在云基础设施服务的背景下。

- **规定了供应商应该遵循的原则** — 该“准则”阐释了 GDPR 中的关键原则，说明了供应商应通过哪些明确的行动和承诺来证明他们遵守 GDPR 并可以帮助客户遵守相关要求。客户可以在自己的合规性和数据保护策略中使用这些具体行动和承诺。
- **为客户提供必要的隐私和安全信息，以帮助他们实现合规性目标** — 该“准则”要求供应商对其为履行隐私和安全承诺所采取的步骤保持透明。这些步骤包括实施隐私和安全保护机制、通知数据泄露、数据删除和第三方子处理的透明化。所有这些承诺均由第三方独立监控机构进行验证。客户可以使用此信息来充分了解所提供的高级别安全性。

发布时，AWS 已将 Amazon EC2、Amazon Simple Storage Service (Amazon S3)、Amazon Relational Database Service (Amazon RDS)、AWS Identity and Access Management (IAM)、AWS CloudTrail 和 Amazon Elastic Block Store (Amazon EBS) 注册为完全符合该“准则”。有关更多信息，请参阅 CISPE 公共注册。 这为 AWS 客户提供了额外的保证，即他们在使用 AWS 时可以在安全可靠且合规的环境中控制其数据。除了遵守该“准则”外，AWS 还获得了非常多的 国际证书和认证。 这包括 ISO 27001、ISO 27018、ISO 9001、SOC 1、SOC 2、SOC 3、PCI DSS Level 1 。

数据访问控制

GDPR 第 25 条规定，控制者“应实施适当的技术和组织措施以确保在默认情形下，仅处理为实现特定目的而必需的个人数据。”以下 AWS 访问控制机制仅允许得到授权的管理员、用户和应用程序访问 AWS 资源和客户数据，从而能够帮助客户符合此要求。

AWS Identity and Access Management

在您创建 AWS 账户时，会为您的 AWS 账户自动创建一个根用户。此用户账户对您 AWS 账户中的所有 AWS 服务和资源具有完全访问权限。您应当仅将此账户用于初次创建额外角色和用户账户，以及需要它的管理活动，而不应用于日常任务。AWS 建议您从开始就应用最小特权原则：为不同的任务定义不同用户账户和角色，并且指定完成每项任务所需的最小权限集。这种方法是一种机制，用于调整 GDPR 中引入的一个关键概念：通过设计保护数据。AWS Identity and Access Management (IAM) 是一项 Web 服务，可用于安全地控制对您的 AWS 资源的访问。

用户和角色使用特定权限定义 IAM 身份。借助 IAM 角色，您可以允许任何用户执行特定任务来承担角色，并利用角色会话的临时凭证。使用 IAM 角色，您可以安全地为 Amazon EC2 中运行的应用程序提供访问其他 AWS 资源（例如 Amazon S3 存储桶、Amazon RDS 或 DynamoDB 数据库）所需的凭证。

通过 AWS STS 创建临时访问令牌

使用 AWS Security Token Service (AWS STS)，您可以创建可信用户，并提供授予他们访问您的 AWS 资源的临时安全凭证。临时安全凭证的工作方式几乎与您为 IAM 用户提供的长期访问密钥凭证相同，但有以下区别：

- 临时安全凭证供短期使用。您可以配置它们的有效时间，从几分钟到几小时不等。临时凭证到期之后，AWS 将无法识别，也不允许通过它们发出的 API 请求进行任何类型的访问。
- 临时安全凭证不随用户账户存储在一起。相反，它们是动态生成的，并在请求时提供给用户。临时安全凭证到期时（或之前），用户可以请求新的凭证，如果该用户有此权限。

由于存在这些差异，使用临时凭证具有以下优势：

- 您无需在应用程序中分发或嵌入长期 AWS 安全凭证。
- 临时凭证是角色和身份联合的基础。通过为用户定义一个临时的 AWS 身份，您可以为他们提供对 AWS 资源的访问。
- 临时安全凭证的可自定义生命周期是有限的。因此，在不需要这些凭证时，您不必轮换或显式撤消它们。临时安全凭证到期后，不能重复使用。您可以指定凭证的最长有效时间。

多重身份验证

为了增强安全性，您可以为您的账户和单个用户账户添加双重身份验证。借助多重身份验证 (MFA)，当您登录 AWS 网站时，系统会提示您输入用户名和密码（第一重），以及来自您的 AWS MFA 设备的身份验证响应（第二重）。您可以为您的 AWS 账户、在您账户中创建的各个 IAM 用户启用 MFA。您还可以使用 MFA 来控制对 AWS 服务 API 的访问。

例如，您可以定义一个策略，允许完全访问 Amazon EC2 中的所有 AWS API 操作，但明确拒绝访问特定 API 操作，如 *StopInstances* 和 *TerminateInstances* – 如果该用户未经过 MFA 身份验证。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAllActionsForEC2",
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*"
        },
        {
            "Sid": "DenyStopAndTerminateWhenMFAIsNotPresent",
            "Effect": "Deny",
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {"aws:MultiFactorAuthPresent": false}
            }
        }
    ]
}
```

图 *1* - 特定 *Amazon EC2 API* 操作需要 *MFA*

访问 AWS 对象资源

为了实现精细访问您的 AWS 对象，您可以向不同人员授予不同级别的权限来访问不同资源。例如，您可以仅允许某些用户完全访问 Amazon Elastic Compute Cloud (Amazon EC2)、Amazon Simple Storage Service (Amazon S3)、Amazon DynamoDB、Amazon Redshift 等 AWS 服务。

对于其他用户，您可以允许仅针对某些 Amazon S3 存储桶的只读访问权限，或是仅管理某些 Amazon EC2 实例的权限，或是仅访问您的账单信息。

以下策略是一种方法的示例，您可以通过它允许对特定 Amazon S3 存储桶执行所有操作，并明确拒绝访问 Amazon S3 之外的每个 AWS 服务。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ]
        },
        {
            "Effect": "Deny",
            "NotAction": "s3:*",
            "NotResource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ]
        }
    ]
}
```

图 *2* – 管理范围仅限于特定 *Amazon S3* 存储桶

您可以将策略附加到用户账户或角色。有关其 IAM 策略示例，请参阅示例 IAM 身份–基于某项内容的决策。

访问操作和配置数据

您可以使用 AWS Systems Manager 查看和管理您的 AWS 基础设施的运行。您可以审计并强制遵守已定义的状态。AWS Systems Manager Parameter Store 可以集中管理数据定义参数。这使您能够实现对参数数据的精细访问，无论是纯文本数据（如数据库字符串）还是密钥（如密码）。您可以通过用户和资源（如实例）的自定义权限来提供此类访问控制，以便实现参数访问和使用与 IAM 的集成。例如，在开发环境中，凭证通常为硬编码凭证。您可以使用 Parameter Store 保存密码，并允许您的开发人员使用 AWS API get-parameter 获取对凭证的访问权限，而无需对凭证进行硬编码。

以下 API 片段示例显示了密码检索 *get-parameter*：

```
password=$(aws ssm get-parameters --region us-east-1 --names MySecureSQLPassword
```

用于保护访问应用程序、服务和 IT 资源所需的密钥的另一个可用选项是 AWS Secrets Manager。该服务使您可以轻松地在其整个生命周期中轮换、管理和检索数据库凭证、API 密钥和其他密钥。用户和应用程序通过调用 Secrets Manager API 来检索密钥，从而无需以纯文本形式对敏感信息进行硬编码。

Secrets Manager 通过内置集成为 Amazon RDS、Amazon Redshift 和 Amazon DocumentDB 提供密钥轮换功能。

地理限制

您可以使用地理限制（也称为地域限制）来阻止特定地理位置的用户访问您通过 Amazon CloudFront Web 分发功能分发的内容。

有两个选项用于使用地理限制：

- **CloudFront 地理限制功能** – 选择此选项可限制访问与 CloudFront 分配相关的所有文件，并在国家/地区级别限制访问。
- **第三方地理位置服务** – 选择此选项可限制访问与分配相关的部分文件，或在比国家/地区级别更精细的级别限制访问。

除了这两个选项之外，新上线的地区还具有地理限制功能。虽然默认启用 2019 年 3 月 20 日之前引入的 AWS 地区，但默认禁用 2019 年 3 月 20 日之后引入的地区，例如亚太地区（香港）和中东（巴林）。您必须先启用这些地区，然后才能使用它们。如果 AWS 地区默认是禁用的，则您可以使用 AWS 管理控制台启用和禁用该地区。启用和禁用 AWS 地区可让您控制 AWS 账户中的用户是否可以访问该地区的资源。[5]

控制对 Web 应用程序和移动应用程序的访问

AWS 提供了用于在其应用程序中管理数据访问控制的服务。如果您需要在 Web 应用程序和移动应用程序中添加用户登录和访问控制功能，则可以使用 Amazon Cognito。Amazon Cognito 用户池提供了一个可扩展到数亿用户的安全用户目录。为了保护用户的身份，您可以向用户池添加多重身份验证 (MFA)。您还可以使用自适应身份验证，该机制使用基于风险的模型来预测您何时可能需要其他身份验证因素。

使用 Amazon Cognito，您可以查看您的资源访问者以及访问来源（移动应用程序或 Web 应用程序）。您可以使用此信息来创建安全策略，以基于访问源的类型（移动应用程序或 Web 应用程序）允许或拒绝访问资源。

监控和日志记录

GDPR 的第 30 条规定“所有控制者及其代表（如适用）应保留其职责范围内的处理活动记录。”本文还包括有关根据 GDPR 要求在监控所有个人数据的处理时必须记录哪些信息的

详细信息。还要求控制者和处理者及时发送违规通知，因此快速检测事件非常重要。为了帮助客户履行这些义务，AWS 提供了以下监控和日志记录服务。

使用 AWS Config 管理和配置资产

AWS Config 提供 AWS 账户中 AWS 资源配置的详细视图。其中包括资源彼此之间的关系以及以前的配置方式，让您可以了解配置和关系随时间的变化。

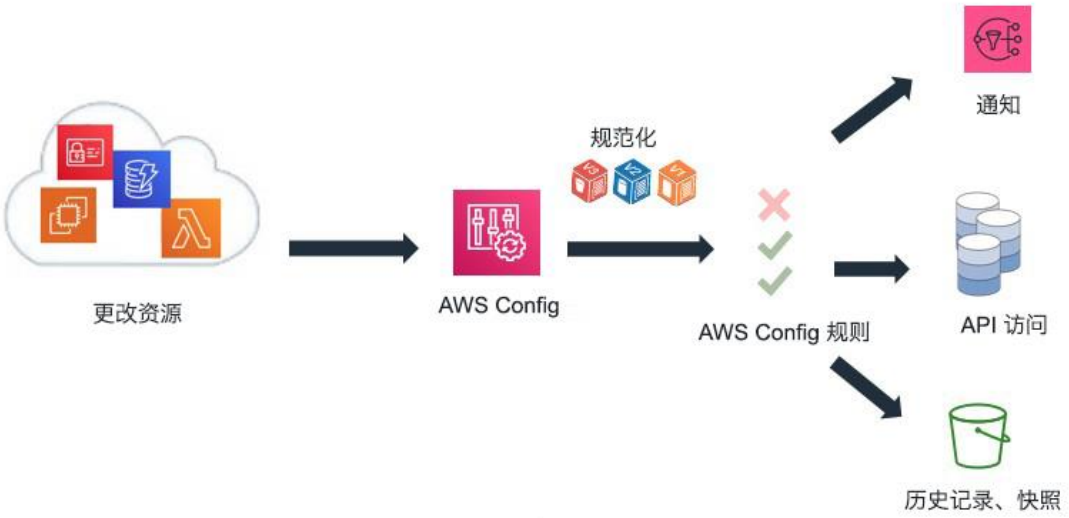

图 *3* – 使用 *AWS Config* 监控随时间推移的配置变化

AWS 资源是指您可以在 AWS 中使用的实体，例如 Amazon Elastic Compute Cloud (EC2) 实例、Amazon Elastic Block Store (EBS) 卷、安全组或 Amazon Virtual Private Cloud (VPC)。有关 AWS Config 支持的完整 AWS 资源列表，请参阅支持的 AWS 资源类型。

了解 *AWS* 上的 *GDPR* 合规性

使用 AWS Config，您可以执行以下操作：

- 评估您的 AWS 资源配置以验证设置是否正确。
- 获取与您的 AWS 账户关联的受支持资源的当前配置的快照。
- 获取账户中一个或多个资源的配置。
- 获取一个或多个资源的历史配置。
- 在创建、修改或删除资源时获取通知。

- 查看资源之间的关系。例如，您可能想查找使用特定安全组的所有资源。

使用 AWS CloudTrail 进行合规性审计和安全分析

借助 AWS CloudTrail，您可以持续监控 AWS 账户活动。捕获账户的 AWS API 调用历史记录，包括通过 AWS 管理控制台、AWS 软件开发工具包、命令行工具和更高级别的 AWS 服务执行的 API 调用。您可以识别哪些用户和账户调用了支持 CloudTrail 的服务的 AWS API、执行调用的源 IP 地址以及调用发生的时间。您可以使用 API 将 CloudTrail 集成到应用程序中，为组织自动创建跟踪，检查跟踪状态，以及控制管理员启用和禁用 CloudTrail 日志记录的方式。您可以将 CloudTrail 日志组织和存储在 Amazon S3 存储桶中，以进行审计或进行故障排除活动。

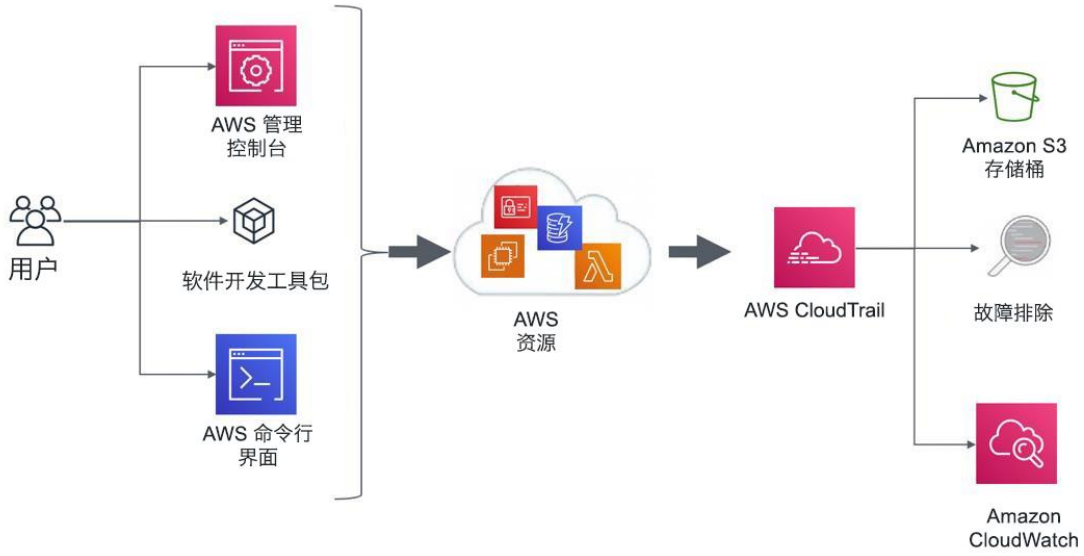

图 *4* – 使用 *AWS CloudTrail* 进行合规性审计和安全分析的示例架构

AWS CloudTrail 日志还可以触发预配置的 Amazon CloudWatch 事件。您可以使用这些事件来通知用户或系统发生了某个事件或需要执行修复操作。例如，如果您要监控 Amazon EC2 实例中的活动，您可以创建 CloudWatch 事件规则。 如果 Amazon EC2 实例中发生特定活动，并将事件捕获到日志中，该规则将触发 AWS Lambda 函数，该函数会向管理员发送一个关于该事件的通知电子邮件，其中包含该事件的发生时间、哪个用户执行的操作、Amazon EC2 详细信息等。下图显示了事件通知的架构。

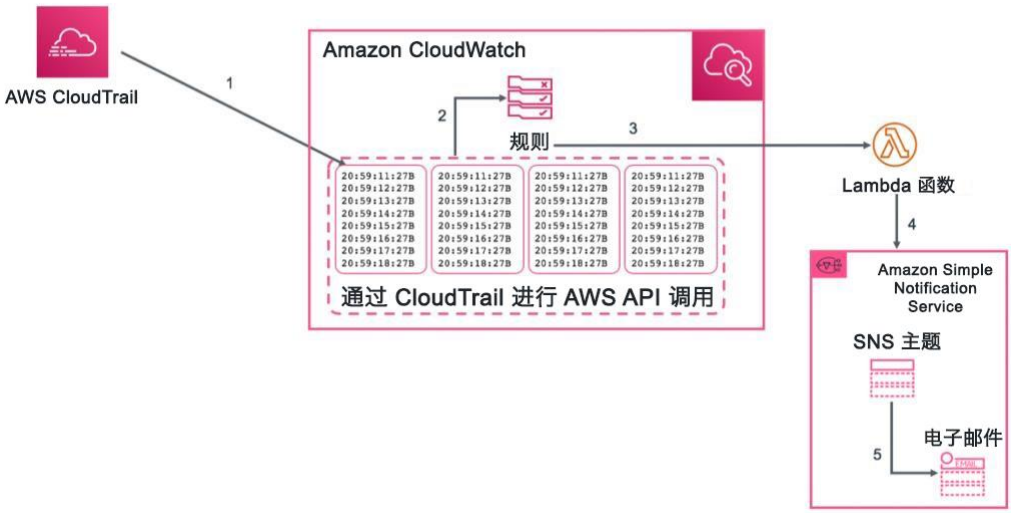

图 *5 – AWS CloudTrail* 事件通知示例

日志格式

启用日志记录后，您可以获取针对向 Amazon S3 存储桶发出的请求的详细访问日志记录。访问日志记录包含有关请求的详细信息，例如请求类型、请求中指定的资源，以及处理请求的时间和日期。有关日志消息内容的更多信息，请参阅《*Amazon Simple Storage Service* 开发人员指南》中的 Amazon S3 服务器访问日志格式。

服务器访问日志记录对许多应用程序都十分有用，因为它们让存储桶拥有者可以深入了解不受其控制的客户端所发出的请求的性质。默认情况下，Amazon S3 不会收集服务访问日志，但是当您启用日志记录后，Amazon S3 会按小时将访问日志传送到您的存储桶。

这些信息包括：

- 对 Amazon S3 对象的访问进行细粒度日志记录
- 有关通过 VPC-Flow Logs 的网络流量的详细信息
- 使用 AWS Config Rules 进行基于规则的配置验证和操作
- 在 CloudFront 中通过 WAF 功能对应用程序的 HTTP 访问进行筛选和监控

日志也是威胁检测的有用信息源。Amazon GuardDuty 会分析来自 AWS CloudTrail 的日志、VPC Flow Logs 和 AWS DNS，从而帮助您持续监控您的 AWS 账户和工作负载。每当记录到恶意活动或未经授权的行为时，该服务就会使用机器学习、威胁情报和异常检测来提供详细且可指导行动的警报。

集中式安全管理

许多组织都面临与环境的可见性和集中管理相关的挑战。随着运营范围的扩大，除非仔细考虑安全设计，否则这些挑战可能会更加复杂。缺乏知识、监管和安全流程管理分散且不均衡会导致您的环境易受攻击。

AWS 提供了一些工具帮助您解决 IT 管理和监管方面一些最具挑战性的要求，还提供了一些工具来支持按设计保护数据的方法。

AWS Control Tower 提供了一种简单的方法来设置和管理新的、安全的、多账户 AWS 环境。它会自动设置一个登录区 [6]，这是一个基于最佳实践蓝图的多账户环境，并使用您可从预先打包的列表中选择的防护工具提供监管。防护工具实施监管规则以实现安全性、合规性和运营。AWS Control Tower 使用 AWS Single Sign-On (SSO) 默认目录提供身份管理，并使用 AWS SSO 和 AWS IAM 启用跨账户审计。它还集中了来自 Amazon CloudTrail 的日志和存储在 Amazon S3 中的 AWS Config 日志。

AWS Security Hub 是另一个支持集中化的服务，可以提高组织的可见性。Security Hub 会集中来自各个 AWS 账户和服务的安全性与合规性调查结果并确定其优先级，还可以与第三方合作伙伴的安全软件集成，帮助您分析安全趋势并确定最高优先级的安全问题。

借助 **Amazon CloudWatch Events**，您可以设置 AWS 账户以将事件发送到其他 AWS 账户，还可以接收其他账户或组织的事件。通过在发生安全事件时根据需要及时采取纠正措施（例如，通过调用 Lambda 函数或对 EC2 实例运行命令），该机制对于实现跨账户事件响应场景非常有用。

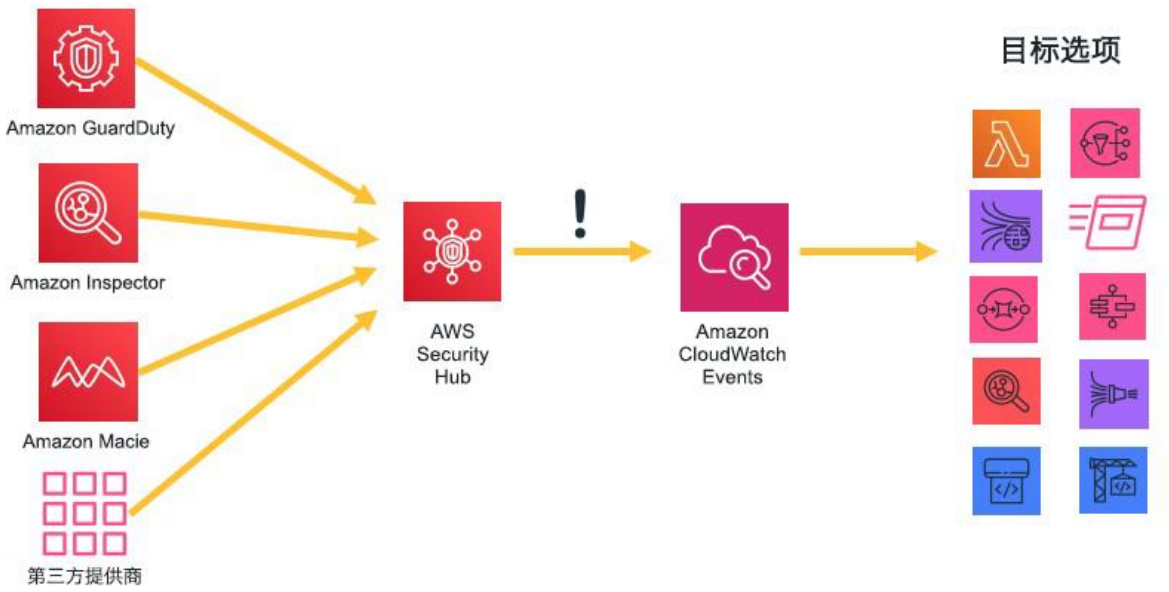

图 *6* – 使用 *AWS Security Hub* 和 *Amazon CloudWatch Events* 采取措施

AWS Organizations 可帮助您集中管理和控制非常复杂的环境。它使您能够在多账户环境中控制访问、合规性和安全性。AWS Organizations 支持服务控制策略 (SCP)，该策略定义了可用于组织中的不同账户的 AWS 服务操作。

在 AWS 上保护您的数据

GDPR 第 32 条要求组织必须“实施适当的技术和组织措施，以确保具有可避免风险的适当安全级别，包括…对个人数据进行假名和加密处理…。”此外，组织必须防止未经授权的个人数据披露或访问。

加密减少了与个人数据存储相关的风险，因为如果没有正确的密钥，数据将无法读取。细致的加密策略可以帮助减轻各种安全事件（包括某些安全漏洞）的影响。

加密静态数据

加密静态数据对于法规遵从性和数据保护至关重要。它有助于确保任何没有有效密钥的用户或应用程序都无法读取保存在磁盘上的敏感数据。AWS 为静态加密和加密密钥管理提供了多个选项。例如，您可以将 AWS Encryption SDK 与在 AWS Key Management Service (AWS KMS) 中创建和管理的客户主密钥 (CMK) 结合使用来加密任意数据。

加密的数据可以安全地以静态形式存储，并且只能由有权访问 CMK 的一方解密。因此，您可以获得机密的信封加密数据、用于授权和经过身份验证的加密的策略机制，以及通过 AWS CloudTrail 进行的审计日志记录。 一些 AWS 基础服务具有内置的静态加密功能，提供了在将数据写入非易失性存储之前对其进行加密的选项。例如，您可以使用 AES-256 加密对 Amazon Elastic Block Store (Amazon EBS) 卷进行加密，并配置 Amazon Simple Storage Service (Amazon S3) 存储桶以进行服务器端加密 (SSE)。Amazon Relational Database Service (Amazon RDS) 还支持透明数据加密 (TDE)。

在 Linux EC2 实例存储上加密数据的另一种方法是使用内置 Linux 库。这种方法可以透明地加密文件，保护机密数据。因此，处理数据的应用程序不会发现磁盘级别的加密。

您可以使用两种方法来加密实例存储上的文件。第一种方法是磁盘加密，即整个磁盘或磁盘中的一个整块使用一个或多个加密密钥进行加密。磁盘加密在文件系统级别以下运行，与操作系统无关，并隐藏目录和文件信息，如名称和大小。例如，加密文件系统是 Windows NT 操作系统新技术文件系统 (NTFS) 的 Microsoft 扩展，该系统提供磁盘加密。

第二种方法是文件系统级加密。通过这种方法，会加密文件和目录，但不是整个磁盘或分区。文件系统级加密在文件系统之上运行，并且可跨操作系统移植。

对于非易失性存储标准 (NVMe) SSD 实例存储卷，加密是默认选项。NVMe 实例存储中的数据是在实例上的硬件模块中实施的 XTS-AES-256 分组密码进行加密。加密密钥使用硬件模块生成，并且对于每个 NVMe 实例存储设备都是唯一的。所有加密密钥会在实例停止或终止时被销毁，并且无法恢复。您不能使用自己的加密密钥。

加密传输中的数据

AWS 强烈建议对从一个系统传输到另一个系统的数据进行加密，包括 AWS 内外的资源。

创建 AWS 账户时，会为其预配置 AWS 云的逻辑隔离部分，即 Amazon Virtual Private Cloud (Amazon VPC)。在那里，您可以在您定义的虚拟网络中启动 AWS 资源。您可以完全控制虚拟网络环境，包括选择自己的 IP 地址范围、创建子网，以及配置路由表和网络网关。您还可以在公司数据中心和您的 Amazon VPC 之间创建硬件虚拟专用网络 (VPN) 连接，以便您可以将 AWS 云用作公司数据中心的扩展。

为了保护您的 Amazon VPC 与公司数据中心之间的通信，您可以从多个 VPN 连接选项中进行选择，然后选择最符合您需求的一个选项。您可以使用 AWS Client VPN 通过基于客户端的 VPN 服务启用对 AWS 资源的安全访问。您也可以使用第三方软件 VPN 设备，您可以将其安装在 Amazon VPC 中的 Amazon EC2 实例上。或者，您可以建立 IPsec VPN 连接来保护 VPC 与您的远程网络之间的通信。要创建从远程网络到您的 Amazon VPC 的专用私有连接，您可以使用 AWS Direct Connect。您可以将此连接与 AWS 站点到站点 VPN 结合使用以建立 IPsec 加密的连接。

AWS 提供使用 TLS（传输层安全性）协议进行通信的 HTTPS 终端节点，当您使用 AWS API 时，该协议可在传输过程中提供加密。您可以使用 AWS Certificate Manager (ACM) 服务来生成、管理和部署用于在工作负载的系统之间建立加密传输的私有和公有证书。Amazon Elastic Load Balancing 已经与 ACM 集成，用于支持 HTTPS 协议。如果您的内容是通过 Amazon CloudFront 分发的，则它支持加密的终端节点。

加密工具

AWS 提供各种高度可扩展的数据加密服务、工具和机制，以帮助保护您在 AWS 上存储和处理的数据。有关 AWS 服务功能和隐私的信息，请参阅 AWS 服务功能的隐私注意事项 [7]。

AWS 提供的加密服务使用了广泛的加密和存储技术，旨在维护静态或传输中数据的完整性。AWS 提供了四种用于加密操作的主要工具。

- **AWS Key Management Service (AWS KMS)** 是一种 AWS 托管服务，可用于生成和管理主密钥和数据密钥。 AWS KMS 已经与许多 AWS 服务集成，以使用客户账户中的 KMS 密钥提供服务器端数据加密。KMS 硬件安全模块 (HSM) 通过了 FIPS 140-2 Level 2 认证。
- **AWS CloudHSM** 提供通过了 FIPS 140-2 Level 3 认证的 HSM。它们可以安全地存储您的各种自管理加密密钥，包括主密钥和数据密钥。
- **AWS 加密服务和工具**
- ○ **AWS 加密软件开发工具包**提供了一个客户端加密库，用于对所有类型的数据实施加密和解密操作。
  - ○ **Amazon DynamoDB 加密客户端**提供了一个客户端加密库，用于在将数据表发送到数据库服务（例如 Amazon DynamoDB）之前对其进行加密。

AWS Key Management Service

AWS Key Management Service (AWS KMS) 是一项托管服务，可让您轻松创建和控制用于加密数据的加密密钥，并使用硬件安全模块 (HSM) 来保护密钥的安全性。AWS KMS 已经与其他几项 AWS 服务集成，可帮助您保护通过这些服务存储的数据。AWS KMS 还与 AWS CloudTrail 集成，可为您提供记录所有密钥使用情况的日志，以满足您的法规和合规性需求。

您可以通过 AWS 管理控制台或者使用 AWS 开发工具包或 AWS 命令行界面 (AWS CLI) 轻松创建、导入和轮换密钥，还可以定义使用策略并审计使用情况。

AWS KMS 中的主密钥，无论是由您导入还是由 AWS KMS 代表您创建的（即客户主密钥 [CMK]），都以加密格式存储在高度持久的存储中，以帮助确保在需要时可以使用它们。您可以选择让 AWS KMS 每年自动轮换一次在 AWS KMS 中创建的 CMK，而无需重新加密已使用主密钥加密的数据。您不需要跟踪旧版本的 CMK，因为在需要自动解密以前加密的数据时，AWS KMS 可以提供这些密钥。

对于 KMS 中的任何 CMK，您可以通过许多访问控制（包括授予、密钥策略或 IAM 策略中的密钥策略条件）来控制谁有权访问这些密钥以及它们可用于哪些服务。您还可以从自己的密钥管理基础设施导入密钥，并在 KMS 中使用这些密钥。

例如，以下策略使用 *kms:ViaService* 条件，仅当请求来自代表特定用户 (*ExampleUser*) 的特定区域 (*us-west-2*) 中的 Amazon EC2 或 Amazon RDS 时，才允许将客户托管的 CMK 用于指定的操作。

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/ExampleUser"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:CreateGrant",
    "kms:ListGrants",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "kms:ViaService": [
        "ec2.us-west-2.amazonaws.com",
        "rds.us-west-2.amazonaws.com"
      ]
    }
  }
}
```

图 *7 – Amazon KMS* 策略示例

AWS 服务集成

AWS KMS 已与许多 AWS 服务集成（在撰写本文时已超过 50 个）。这些集成意味着您可以轻松使用 AWS KMS CMK 来加密使用这些服务存储的数据。除了使用客户托管的 CMK，许多集成服务还允许您使用自动为您创建和管理的 AWS 托管的 CMK，但仅在创建它的特定服务中可用。

审计功能

如果您为自己的 AWS 账户启用了 AWS CloudTrail，则存储在 KMS 中的密钥的每一次使用都会记录在一个日志文件中，该文件将传送到您启用 AWS CloudTrail 时指定的 Amazon S3 存储桶中。记录的信息包括用户、时间、日期和使用的密钥等详细信息。

安全性

AWS KMS 旨在确保任何人都无法访问您的主密钥。该服务的基础系统广泛采用了各种强化技术来保护主密钥，例如不将纯文本主密钥存储在磁盘上、不将其保留在内存中，并且限制哪些系统可以访问使用密钥的主机。服务中更新软件的所有访问都由多方访问控制来管理，该访问控制由亚马逊内的独立组审核和审查。

有关 AWS KMS 的更多信息，请参阅 AWS Key Management Service 白皮书。

AWS CloudHSM

AWS CloudHSM 服务通过在 AWS 云中使用专用的“硬件安全模块”(HSM) 设备，帮助您满足数据安全方面的企业、合同和监管合规性的要求。使用 CloudHSM，您可以控制 HSM 执行的加密密钥和加密操作。

AWS 和 AWS Marketplace 合作伙伴提供了各种用于保护 AWS 平台内敏感数据的解决方案，但对于需要遵守严格的合同或法规要求来管理加密密钥的应用程序和数据，有时需要进行额外的保护。以前，您唯一的选择是将敏感数据（或保护敏感数据的加密密钥）存储在本地数据中心。这可能会阻止您将这些应用程序迁移到云或显著降低其性能。借助 AWS CloudHSM，您可以在根据政府标准设计和验证的 HSM 中保护您的加密密钥，以实现安全的密钥管理。您可以安全地生成、存储和管理用于数据加密的加密密钥，以确保只有您可以访问它们。AWS CloudHSM 可帮助您遵守严格的密钥管理要求，而不会牺牲应用程序性能。

AWS CloudHSM 服务可与 Amazon Virtual Private Cloud (Amazon VPC) 配合使用。CloudHSM 实例在您的 Amazon VPC 内配置了您指定的 IP 地址，为您提供与 Amazon Elastic Compute Cloud (Amazon EC2) 实例的简单的专用网络连接。如果将 CloudHSM 实例放在 Amazon EC2 实例附近可减少网络延迟，从而提高应用程序性能。AWS 提供对 CloudHSM 实例的专用和独占（单租户）访问，与其他 AWS 客户隔离。AWS CloudHSM 可在多个区域和可用区中使用，让您可以为应用程序添加安全持久的密钥存储。

与 AWS 服务和第三方应用程序集成

您可以将 CloudHSM 和 Amazon Redshift、Amazon Relational Database Service (Amazon RDS) for Oracle 或第三方应用程序（如 SafeNet Virtual KeySecure）一起用作信任根、Apache（SSL 终端）或 Microsoft SQL Server（透明数据加密）。您还可以在编写自己的应用程序时使用 CloudHSM，并继续使用您熟悉的标准加密库，包括 PKCS#11、Java JCA/JCE 以及 Microsoft CAPI 和 CNG。

审计活动

如果您需要跟踪资源变更或审计活动的安全性和合规性目的，您可以通过 AWS CloudTrail 查看由您账号发出的所有 CloudHSM API 调用。此外，您可以使用 syslog 审计 HSM 设备上的操作或向您的日志采集器发送 syslog 日志消息。

AWS 加密服务和工具

AWS 提供了符合各种加密安全标准的机制，您可以使用这些机制来实现加密最佳实践。AWS Encryption SDK[8] 是一个客户端加密库，在 Java、Python、C、JavaScript 中，以及支持 Linux、macOS 和 Windows 的命令行界面中可用。AWS Encryption SDK 提供了高级数据保护功能，包括安全的、经过身份验证的对称密钥算法套件，例如，具有密钥派生和签名功能的 256 位 AES-GCM。由于该 SDK 是专为使用 Amazon DynamoDB 的应用程序设计的，所以 DynamoDB 加密客户端 [9] 使用户能够在数据发到数据库之前保护他们的表数据。它还会在检索数据时验证和解密数据。该开发工具支持 Java 和 Python。

Linux DM-Crypt 基础设施

Dm-crypt 是一种 Linux 内核级加密机制，允许用户挂载加密的文件系统。挂载文件系统是将文件系统附加到目录（挂载点）的过程，这使其可供操作系统使用。挂载后，文件系统中的所有文件都可供应用程序使用，而无需任何其他交互。但是，将这些文件存储在磁盘上时会对其进行加密。

设备映射器是 Linux 2.6 和 3.x 内核中的基础设施，它提供了创建块设备虚拟层的通用方法。该设备映射器 crypt 目标使用内核加密 API 提供块设备的透明加密。本文中的解决方案将 dm-crypt 与由逻辑卷管理器 (LVM) 映射到逻辑卷的磁盘备份文件系统结合使用。LVM 为 Linux 内核提供逻辑卷管理功能。

通过设计以及默认配置保护数据

每当用户或应用程序尝试使用 AWS 管理控制台、AWS API 或 AWS CLI 时，都会向 AWS 发送请求。AWS 服务收到请求后执行一组步骤，根据特定策略评估逻辑确定是允许还是拒绝该请求。默认情况下，AWS 上的所有请求都被拒绝（应用默认拒绝策略）。这意味着会拒绝一切未明确允许的策略。在策略定义中，并且作为最佳实践，AWS 建议您应用最小特权原则，这意味着每个组件（例如用户、模块或服务）必须只能访问完成其任务所需的资源。

此方法遵守 GDPR 第 25 条规定，控制者“应实施适当的技术和组织措施，确保在默认情形下，仅处理为实现每个特定目的而必需的个人数据。”

AWS 还提供了实施“基础设施即代码”的工具，这是从架构设计开始就重视安全性的强大机制。AWS CloudFormation 提供了一种通用语言来描述和预置所有基础设施资源（包括安

全策略和流程）。借助这些工具和实践，安全性已成为代码的一部分，您可以根据组织要求进行版本控制、监控和修改（使用版本控制系统）。

这可实现“通过设计保护数据”的方法，因为安全流程和策略可以包含在您的架构定义中，并且还可以通过您组织中的安全措施连续监控。

AWS 如何提供帮助

领域	描述	AWS 服务和工具
数据访问控制	控制者“应实施适当的技术和组织措施，确保默认情况下仅处理每种具体处理目的所需的个人数据。”	AWS Identity and Access Management (IAM) Amazon Cognito AWS WAF AWS CloudFormation AWS Systems Manager
监控和日志记录	“每个 控制者及（如适用）其代表均应保留各自责任范围内的处理活动记录。”	AWS CloudTrail AWS Config Amazon CloudWatch AWS Control Tower Amazon GuardDuty AWS Security Hub
保护您在 AWS 上的数据	组织必须“实施适当的技术和组织措施，确保提供与风险相符的安全级别，包括假名、加密个人数据。”	AWS 工具和开发工具包 AWS CloudHSM AWS Key Management Service

强有力的合规框架	适当的技术和组织措施可能需要包含“确保处理系统和服务的持续机密性、完整性、可用性和恢复性的能力。”	SOC 1/SSAE 16/ISAE 3402（以前是 SAS 70）/SOC 2/SOC 3 PCI DSS 1 级 ISO 9001/ISO 27001/ISO 27017/ISO 27018 NIST FIPS 140-2 常见云计算控制目录 (C5)

贡献者

本文的贡献者包括：

- Amazon Web Services 技术行业专家 Tim Anderson
- Amazon Web Services 公共部门解决方案架构师 Carmela Gambardella
- Amazon Web Services 安全保证经理 Giuseppe Russo
- Amazon Web Services 高级项目经理 Marta Taggart

文档修订

日期	描述
2019 年 10 月	更新包含 AWS 新服务。
2018 年 9 月	次要更新。
2017 年 11 月	首次发布

备注

1 https://ec.europa.eu/info/law/law-topic/data-protection_en

2 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

3 https://aws.amazon.com/compliance/programs/

4 https://cispe.cloud/

5 https://docs.aws.amazon.com/general/latest/gr/rande-manage.html

6 https://aws.amazon.com/solutions/aws-landing-zone/

7 https://aws.amazon.com/compliance/data-privacy/service-capabilities/

8 https://docs.aws.amazon.com/crypto/latest/userguide/awscryp-service-encrypt.html

9 https://docs.aws.amazon.com/crypto/latest/userguide/awscryp-service-ddb-client.html