HongKe 虹科

数据表

符合 CCPA 标准

关于CCPA

《消费者隐私法案》有三个主要目的，以改善机构处理消费者个人信息的方式。第一个目标是让消费者了解企业正在收集的信息类型。第二是为消费者提供更多关于他们的信息如何与第三方共享或出售的权利。第三是为消费者提供额外的保护，防止企业不重视隐私和安全。

CCPA适用于谁

必须遵守CCPA的企业是指在加州为其股东的利润或经济利益而开展业务的任何实体，这些实体收集消费者的个人信息。符合这些标准的企业还必须至少满足以下一个门槛，才有资格符合CCPA:

1. 年总收入超过2500万美元
2. 每年收集(购买、接收或出售)5万以上消费者、家庭或设备的个人信息
3. 通过销售消费者个人信息获得50%或以上的年收入

CCPA有几个关键的豁免。

值得注意的是，如果您是已经受HIPAA保护的医疗保健提供商或受Gramm-Leach-Billey保护的金融服务提供商

几个关键定义

当涉及到定义所使用的特定术语时，一般的合规法规往往是模糊的，CCPA也不例外。我们已经定义了CCPA认为谁是受保护的实体——这个定义看起来很简单。

然而，消费者的定义有点模糊，值得注意。它被定义为任何居住在加利福尼亚州的人。居民被定义为在该州居住超过临时或过渡时期的人，或者居住在该州但暂时或过渡时期不在该州的个人。

同样，个人信息的定义非常模糊(就像大量合规法规的情况一样)。一般来说，个人信息是" 识别、关联、描述、引用、能够与特定消费者或设备直接或间接关联或可以合理关联" 的数据。在其他遵从性法规中，这类数据通常被称为个人身份信息(PII)。

CCPA确实提供了属于这一定义的数据示例列表，包括姓名、地址、财产记录、生物特征数据、浏览历史、护照号码等。如果您希望安全，您应该假定您收集的任何个人信息都应被视为个人信息，并保持适当的安全性和私密性。

消费者权益法

正如我们之前提到的，CCPA旨在让消费者更深入地了解和控制他们的个人信息是如何被收集、存储、处理和共享的。这是通过落实四项具体的消费者权利来实现的。

访问权:加州消费者将能够正式要求所覆盖的实体向他们披露收集了哪些信息，从哪里收集的，为什么收集的，将与谁共享的等等。

选择退出的权利:如果加州消费者不希望保险公司出售或分享他们的个人信息，他们有权选择退出——这有效地阻止了保险公司这样做。

删除权:加州消费者有权要求所覆盖的实体删除他们收集的个人信息，如果他们希望删除的话。

平等服务和价格的权利:这是一个警告，保护加州消费者在行使CCPA权利时不受歧视。从本质上讲，受保护实体不能拒绝向依法行使权利的消费者提供商品和服务。

控制描述-§1798.150 (a)

(1)　第1798.81.5条第(d)分段第(1)段(A)分段所定义的未加密或未编辑的个人信息，如因企业违反实施和维持与信息性质相适宜的合理安全程序和做法以保护个人信息的义务而遭受未经授权的访问、泄露、盗窃或披露，则消费者可就以下任何一项提起民事诉讼:

(A) 每位消费者每次事件或实际损害赔偿的金额不低于一百美元($100)，不超过750美元($750)，以金额较高者为准。

(B) 禁令性或宣告性救济

(C) 法院认为适当的其他救济。

控制流程

身份识别与认证
访问控制
配置管理
事件响应
风险评估
系统与信息完整性

由Lepide促进的控制过程

为了解决这个广泛的规定，组织需要实现一系列广泛的安全程序和来自几个不同控制族的组织改进;没有任何特定的控制过程可以单独确保符合这一要求。

身份识别和认证

此控制过程的目标是确保所有用户和设备在被授予访问权限之前是唯一可识别和可验证的真实的。

用户标识:使用我们的状态实时报告来确定哪些用户帐户可以访问系统。与HR交叉参考，以确定每个账户的业务需求。

识别不能与真人相关联的账户。

使用我们的用户行为分析引擎来审计共享账户的使用情况，确保它们被恰当地使用。

通过核对人力资源数据和登录活动报告，发现与员工缺勤相关的可疑用户活动。

设备识别:使用我们的状态及时报告交叉检查IT库存与计算机帐户。使用我们的变更报告来发现对计算机帐户的任何未经授权的变更。

标识符管理:使用我们的变更报告和交互式搜索来识别未经授权的用户和组的创建、修改或删除。使用我们的实时警报为未经授权的更改配置警报。

Authenticator管理:使用我们的更改报告来发现对帐户策略、密码策略和GPO链接更改的未经授权的更改。为与帐户密码相关的组策略更改设置警报。运行关于密码重置的报告。

访问控制

这样做的目的是确保用户只能访问他们完成工作所需的数据。

帐户管理审计:审计对用户帐户的更改，检测最近创建的用户帐户，以及使用预定义的报告。

设置警报，在检测到任何未经授权的更改时发送给指定人员。

帐户使用监控:通过主动监控审查用户对敏感行为的访问，并在用户行为被认为异常时接收实时警报。实时警报和自动威胁响应使安全团队能够及时响应威胁。

非活动帐户:使用预定义的报告轻松识别非活动帐户。

角色和组分配:使用预定义的报告确定任何安全组成员关系更改。

人员状态变化:审查详细的审计跟踪，以确认临时员工和离职员工已被禁用或不能再访问敏感数据。

访问强制:运行预定义的报告，以确定具有过多权限的用户。

管理来自解决方案内部的访问。

确定如何授予权限并在必要时撤销权限。

权限更改的实时警报和阈值报告。

最小特权:如上所述。可以报告对权限、配置和其他任何可能影响数据访问的更改。

审计及问责

本节的目的是确保您保持审计跟踪，可用于调查事件并使个人对其行为负责。leide保留了十多年的审计跟踪，以帮助您做到这一点。

为所有状态以及对基础设施和敏感数据所做的更改生成数百个审计报告。

事件响应

本节的目的是确保您有一种方法来快速有效地识别和应对事件。

事件检测:针对未授权更改的实时警报、异常发现和风险分析报告可帮助您检测潜在事件。

事件分析:我们的交互式搜索和易于阅读的事件审计线索使调查和分析变得容易。

事件缓解:在检测不需要的事件时运行自动化威胁响应模型，以实时定位和缓解威胁。轻松恢复不需要的更改和删除的对象。

风险评估:使用我们的风险评估仪表板来识别数据安全的任何潜在风险，包括过度的权限和过度暴露的数据。

系统和信息完整性

本节的重点是保护信息和系统免受外部和内部威胁的损害。

信息系统监控:实时发现异常用户行为，对任何潜在的恶意活动/更改发出警报。

信息管理和保留:识别PII和其他受保护/敏感数据，并通过查看谁可以访问/修改它来确保应用适当的访问控制。简化主题访问请求