CALIFORNIA CONSUMER
PRIVACY ACT

CCPA

《加州消费者隐私法案》解读

出海企业合规指南-北美篇

数美
NEXTDATA

前言

中国的互联网行业在海外不断夯实自己的领先优势。据信通院统计，从价值超过 100 亿美元的数字平台来看，中国和美国仍然保持绝对引领。2020 年，中、美百亿美元以上平台企业数量合计达 64 家，全球占比 84.2%，全球新增的 7 家平台均来自中美。2021 年，TikTok 更是首次取代谷歌，成为全球访问量最多的域名。越来越多的中国企业开始展现自己强大的国际竞争力，鼓舞着万千中国互联网企业进军海外。

另一方面，与互联网行业息息相关的隐私保护和数据合规立法也在不断完善。2018 年 5 月，欧盟最严个人数据保护法规《通用数据保护条例》（GDPR）正式生效，引起广泛关注。此后全球隐私立法按下加速键：2019 年 9 月，新加坡新修订的《个人资料保护条例》正式生效；2019 年 12 月，印度联邦内阁通过了《2019 个人数据保护法》；2020 年 7 月，美国加州正式实施《加州消费者隐私法案》（CCPA），又在 2020 年 11 月通过了 CCPA 的修正案《加州隐私权利法案》（CPRA）；2021 年 11 月，中国开始正式实施《个人信息保护法》。随着各国开始制定各自的隐私保护和数据合规法律，出海企业也有必要随时跟进当地立法进展，根据规定调整隐私政策以及业务方向。

数美数字风控研究院“风控 Law School”专栏聚焦数字风控行业，追踪国内外政策法规最新动态，帮助企业敏锐察觉政策趋势，驾驭合规风险，为企业数字化转型提供坚实后盾。“风控 Law School”将按照互联网企业出海地区推出“出海企业合规指南”，CCPA 为出海系列的第一册。

声明

本册由数美数字风控研究院（公众号 ID: ishumei2015）制作，版权归数美科技所有。

本册主要采用文献综述、桌面调研、行业访谈等调研方法写成，参考文献、数据引用及其来源均在脚注内标出，图片采集于网络公开信息并标注来源。

本册致力于为读者呈现海外监管法律的全貌，然而受研究方法与参考资料的限制，文内的观点仅为读者提供行业参考，并不视为针对企业提供的专业建议。

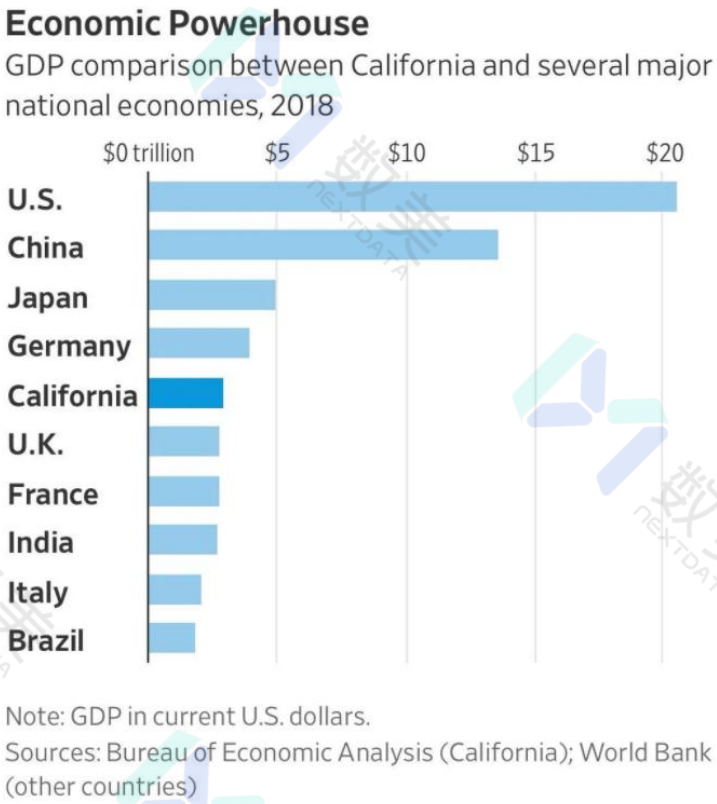
此版为首次发布版本，数美数字风控研究院之后可能会对内容进行再次修订。

目录

一、什么是 CCPA？

《加州消费者隐私法案》（CCPA）是继欧盟《一般数据保护条例》（GDPR）颁布后又一部数据隐私领域的重要法律。它于 2018 年 6 月 28 日正式颁布，在随后的两年内又陆续做了多次修订，2020 年 7 月 1 日开始正式执行。

CCPA 是美国首部关于数据隐私的全面立法。美国目前并没有 GDPR 一类的通用数据保护法律，只在一些特殊行业或领域立法里，有关于隐私保护的内容散落在其中。例如，《健康保险流通与责任法案》（HIPAA）中提到如何保护患者隐私信息，《儿童在线隐私保护法案》（COPPA）则是专门为保护儿童个人信息制定的联邦法律。CCPA 的出台弥补了美国在数据隐私专门立法方面的空白，它旨在加强加州消费者隐私权和数据安全保护，被认为是美国当前最严格的消费者数据隐私保护立法。



加州与全球大型经济体 GDP 对比

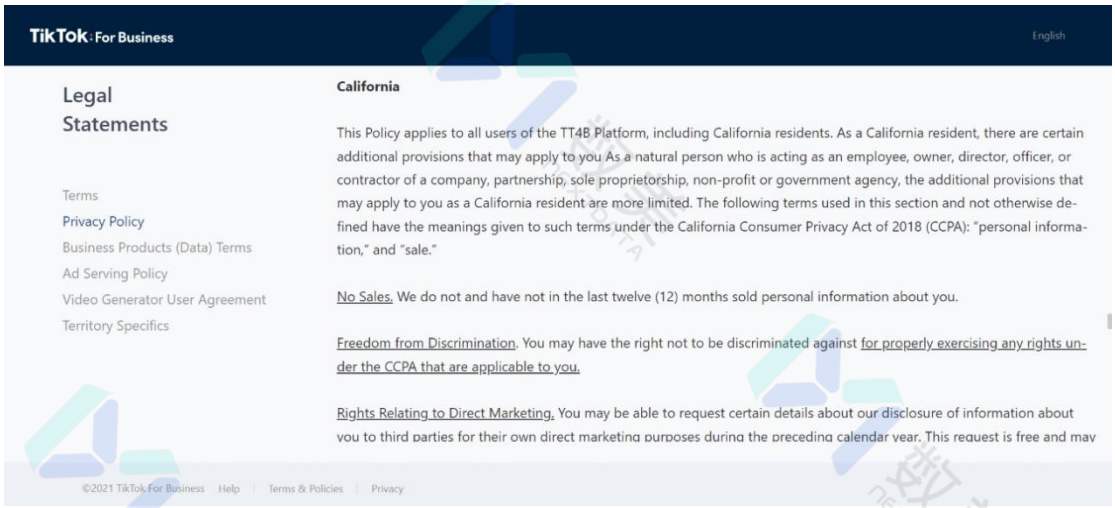
来源：Bureau of Economic Analysis (California)；世界银行

CCPA 虽然是州级立法，但它的立法意义远不止于美国地方。加州是美国经济最发达的州，2018 年其 GDP 达到 3 万亿美元，超越英国成为世界上第五大

经济体。被誉为全球创新之源的硅谷也坐落在加州，一大批对全球信息产业产生深远影响的科技公司孕育于此，对加州的经济增长起到了绝对的推动作用。对于任何想要出海美国的互联网企业而言，加州无疑是一个必争的重要市场。

CCPA 的保护对象为任何“加里福尼亚的居民的自然人”，这也就意味着，只要面向加州居民提供服务的企业达到 CCPA 适用门槛，在收集、处理、买卖用户个人信息时就必须遵守其隐私条款。

目前，绝大多数国际科技巨头如微软、亚马逊、苹果都已在它们的隐私政策中特别告知用户，当用户为加利福尼亚州居民时，会严格按照 CCPA 的相关规定收集、处理、出售个人信息。中国出海最为成功的抖音国际版 TikTok 也在其隐私政策中将加州列为特别管辖区域，承诺会遵守相关规定，保障消费者隐私权利。CCPA 作为一部地方立法，能被众多国际巨头写入其隐私政策，其影响之深远并不亚于欧盟的 GDPR。



TikTok 隐私条款中提及 CCPA 的条款
来源：TikTok 官网

二、适用门槛

CCPA 与 GDPR 在适用对象上也表现出不同的监管倾向。

CCPA 规定，该法案适用于在加利福尼亚州以获取利润或经济利益为目的开展经营活动的企业，其业务涉及收集及/或处理个人信息，且满足以下一项或多项条件：

（1）年收入超过 2500 万美元；

（2）为商业目的，每年单独或总计购买、收取、出售或共享 50000 人及以上消费者、家庭或设备的个人信息；

（3）年收入中有 50%及以上是通过销售消费者的个人信息获得[1]。

在设置适用门槛上，CCPA 更聚焦于为盈利目的开展数据处理活动的企业。CCPA 为被管辖企业设置了“2500 万美元年收入门槛”和“（5 万）消费者、家庭和设备数量门槛”，更侧重对影响范围大、风险程度高的规模企业进行管辖。要注意的是，2500 万美元指的是该企业的全球营收总额，并不单指在加州的营收。

与 CCPA 的“差异化对待”相比，GDPR 的监管范围几乎涵盖任何处理欧盟公民个人数据的组织或企业，而为中小企业设置的豁免门槛又过于严格，导致中小企业很难实际享受到豁免的好处，大大加重了中小企业的合规负担。GDPR 第 3 条规定，GDPR 适用于以下三种情形：

（1）数据控制者、数据处理者在欧盟有营业场所的，不论数据处理行为发生在欧盟还是境外；

（2）数据控制者、数据处理者未在欧盟设立营业场所，但向欧盟的数据主体提供商品或者服务，或者被追踪的网络行为发生在欧盟的；

（3）虽然数据控制者、数据处理者未在欧盟设立营业场所，但是根据国际

---

[1] CCPA 第 1798.140 条 c 项 1 款，原文如下：

(A) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.

(B) Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.

(C) Derives 50 percent or more of its annual revenues from selling consumers' personal information.

公法应当适用欧盟成员国法律的[2]。

CCPA 在规定适用对象之初就合理排除了非盈利机构和没有达到适用门槛的中小企业两类主体。加州作为全球 IT 产业龙头聚集地，在保护消费者隐私的基础之上，也充分考虑了如何避免立法造成中小企业合规负担过重、抑制企业创新活力。

1. 哪些企业不受 CCPA 管辖？

A) 金融、医疗等联邦立法已覆盖的行业不受 CCPA 管辖

美国法律规定，当联邦立法与州级立法的管辖内容有重合、甚至冲突时，应以联邦立法为优先。CCPA 是州级立法，应严格遵守州立法层级，联邦立法已经覆盖的行业隐私保护则不受 CCPA 管辖。出海美国的企业应判断其所属行业是否适用 CCPA。例如，消费分期互联网平台属于金融行业，应遵守《金融服务现代化法案》等联邦立法中关于用户隐私保护的规定，不再适用 CCPA。以下为一些适用联邦立法的行业：

（1）医疗行业——《健康保险流通与责任法案》

（2）金融行业——《金融服务现代化法案》

（3）驾驶员信息——《驾驶员隐私保护法》

（4）征信机构——《公平信用报告法》

（5）消费者报告机构——《美国法典》

B) 数据服务提供商（service provider）不受 CCPA 管辖

数据服务提供商指接受数据控制者的委托而提供数据处理服务的企业。CCPA 规定，只要满足以下两个条件，数据服务提供商便可得到豁免，不直接受

---

[2] GDPR 第 3 条 Territorial scope，原文如下：

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

CCPA 管辖：

（1）数据控制者在隐私条款中告知消费者，收集的个人信息会被分享给数据服务提供商；

（2）数据服务提供商不可额外收集、出售、使用消费者个人信息，为达成必要的商业目的除外[3]。

数据服务提供商虽然不直接受 CCPA 管辖，但其应遵守与数据控制者签订的合同条款，采取措施保障数据安全。此外，提供商仍应注意遵守其他联邦立法的隐私保护规定。例如，当受委托处理的数据中含有 13 岁以下儿童的个人信息时，数据服务提供商应按照《儿童在线隐私保护法》的规定，采取措施保障儿童数据安全。

2. 合规建议

虽然 CCPA 是一部专门针对加州消费者的隐私保护法律，但考虑到加州世界领先的经济体量与科技创新实力，CCPA 的重要意义远不仅限于加州境内。作为全美首部数据隐私领域的全面立法，CCPA 的颁布对其他州的立法进程也有重要示范作用。

出海美国企业首先应明确，自己所处的行业是否受 CCPA 管辖，企业的营收规模与个人信息处理量是否达到适用门槛。例如，音视频、游戏、社交平台出海美国时应重点关注 CCPA，金融借贷、消费分期 APP 则应重点关注《金融服务现代化法案》等金融行业相关联邦法律，及时调整自己的隐私政策，避免违规。

---

[3] CCPA 第 1798.140 条 t 项第 2 款第 3 目，原文如下：

(i) The business has provided notice of that information being used or shared in its terms and conditions consistent with Section 1798.135.

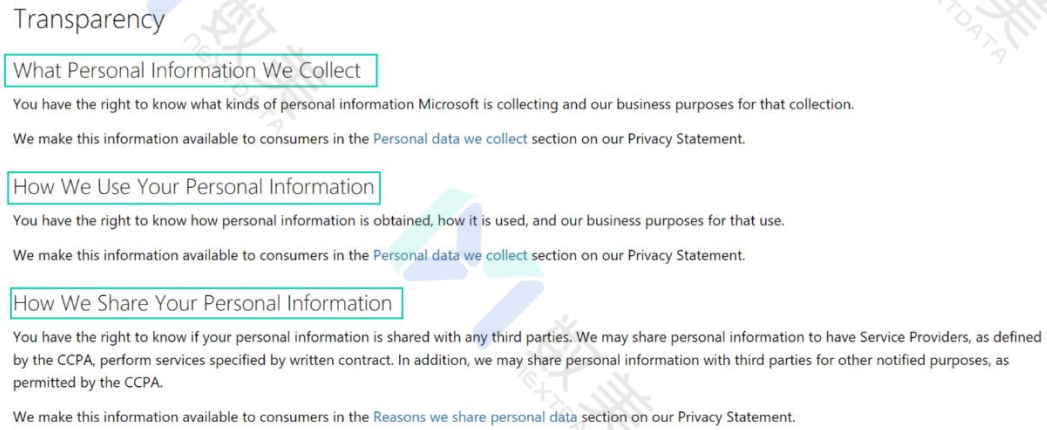
(ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.

三、消费者权利

《加州消费者隐私法案》(CCPA)是美国首部关于消费者隐私保护和数据安全的全面立法，其重要性不亚于欧盟的 GDPR。根据 CCPA 的规定，消费者主要拥有知情权、访问权、删除权、选择权、公平交易权、个人诉讼权六大权利。

1.知情权

消费者有权要求企业告知其收集的个人信息类型、信息来源、具体内容、用途以及第三方处理机构等。企业应在其隐私条款中明确告知消费者以上信息，否则其收集消费者个人信息的行为便视为不合规。



Transparency

What Personal Information We Collect

You have the right to know what kinds of personal information Microsoft is collecting and our business purposes for that collection.

We make this information available to consumers in the Personal data we collect section on our Privacy Statement.

How We Use Your Personal Information

You have the right to know how personal information is obtained, how it is used, and our business purposes for that use.

We make this information available to consumers in the Personal data we collect section on our Privacy Statement.

How We Share Your Personal Information

You have the right to know if your personal information is shared with any third parties. We may share personal information to have Service Providers, as defined by the CCPA, perform services specified by written contract. In addition, we may share personal information with third parties for other notified purposes, as permitted by the CCPA.

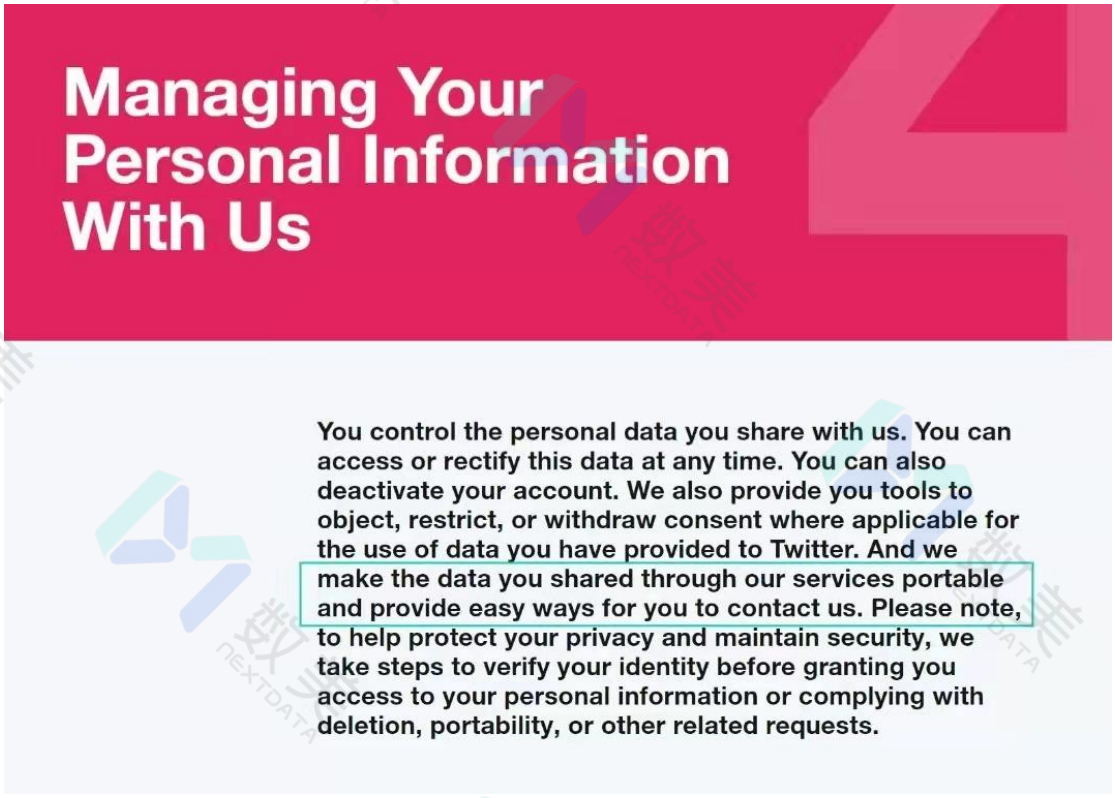
We make this information available to consumers in the Reasons we share personal data section on our Privacy Statement.

微软隐私政策中关于知情权的条款
来源：微软官网

2.访问权

消费者有权要求企业免费提供其收集、处理过的个人信息。这意味着消费者可自行获取企业处理过的个人数据，并以一种简便的方式对个人数据进行自我管理和重复利用。访问权强化了信息主体对个人信息的利用和控制，有利于信息流通和共享，打破平台的数据垄断。

CCPA 规定，消费者需自行向企业发送请求以获取个人信息，企业只有在核实消费者请求后，方可通过邮寄或电子的方式传送给消费者。此外，企业应以轻便、易于使用的格式发送个人信息，而不应给消费者在二次利用时造成阻碍。



Twitter 隐私政策中关于访问权的描述
来源：Twitter 官网

访问权的落地可为实际生活带来许多便利。例如，在疫情期间，出于属地管控要求，居民在跨省流动时被要求申请当地的健康码，在此期间往往会重复填写个人信息，造成用户体验上的不便。如果居民能在首次申请健康码、填写个人信息后，将个人健康信息下载下来，此后重新申请健康码时，只需经过简单授权，便可将下载好的个人信息导入新系统内，无需反复填写。

值得注意的是，虽然消费者有权要求企业免费提供个人信息，但 CCPA 同时也规定，消费者每年只能提出两次申请。这一次数限制有效避免消费者滥用访问权，给企业带来过高的合规压力。

3.删除权

CCPA 第 1798.105 条规定，“消费者有权要求企业删除其收集的有关该消费者的任何个人信息”[4]。企业也应明确告知消费者其拥有删除权。企业收到消费者删除个人信息的请求时，应在核实后删除其个人信息，并要求其他数据服务提供

[4] 法条原文为：

A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.

商同时删除相关信息。

在特定情况下，企业有权拒绝消费者的删除请求，包括：

（1）企业与消费者之间的正常交易或合同履行须收集消费者个人信息；

（2）诊断安全事件；

（3）修补漏洞；

（4）保障言论自由；

（5）遵守《加州电子通讯隐私法》；

（6）为公共利益而进行的研究；

（7）仅用于符合消费者合理预期的企业内部使用；

（8）遵守其他法律义务；

（9）其他企业内部合法使用消费者个人信息的情形[5]。

删除权的引入能有效规范企业的信息收集行为，加强了消费者对个人信息的控制。在 CCPA 正式实施后，各大互联网公司也开始按照规定处理用户的删除请求。以元宇宙公司 Roblox 为例，CCPA 正式实施后，2020 年 Roblox 收到来自消费者的删除请求共 145 份，其中仅有 38 份为有效请求，3 份请求被驳回，

[5] CCPA 第 1798.105 条 d 项，原文如下：

A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to:

(1) Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.

(2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.

(3) Debug to identify and repair errors that impair existing intended functionality.

(4) Exercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law.

(5) Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.

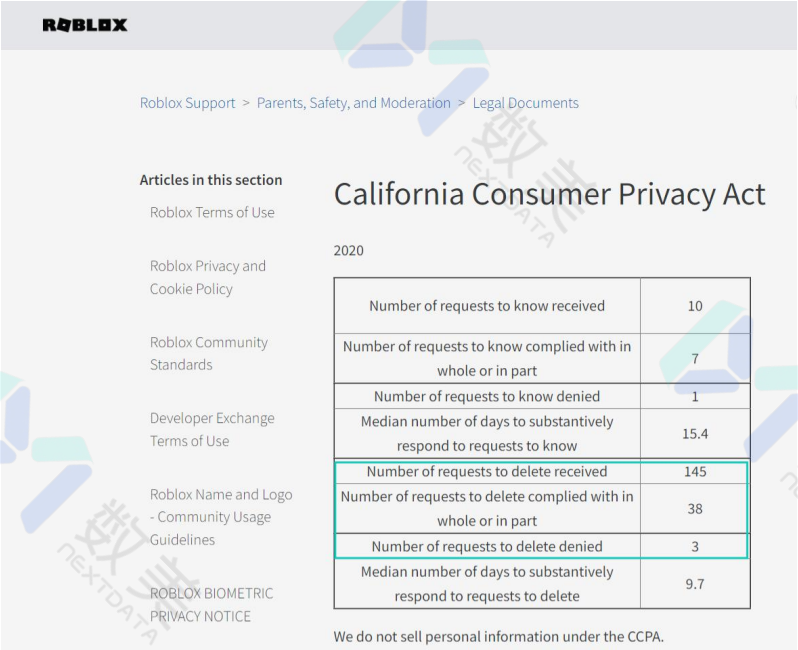
(6) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the business' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.

(7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

(8) Comply with a legal obligation.

(9) Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

其余百余份请求未被采纳可能是因为无法核实消费者信息[6]。



Roblox2020 年 CCPA 用户数据请求统计
来源：Roblox 官网

4.选择权

消费者有权在任何时候要求企业不得销售其个人信息。企业应尽到告知义务，在其平台显眼位置提供“Do Not Sell My Personal Information”选项，这一选项也被称为“选择退出权（Opt-out）”。在尽到合理告知的前提下，只要消费者未拒绝，企业便默认消费者同意出售其个人信息。

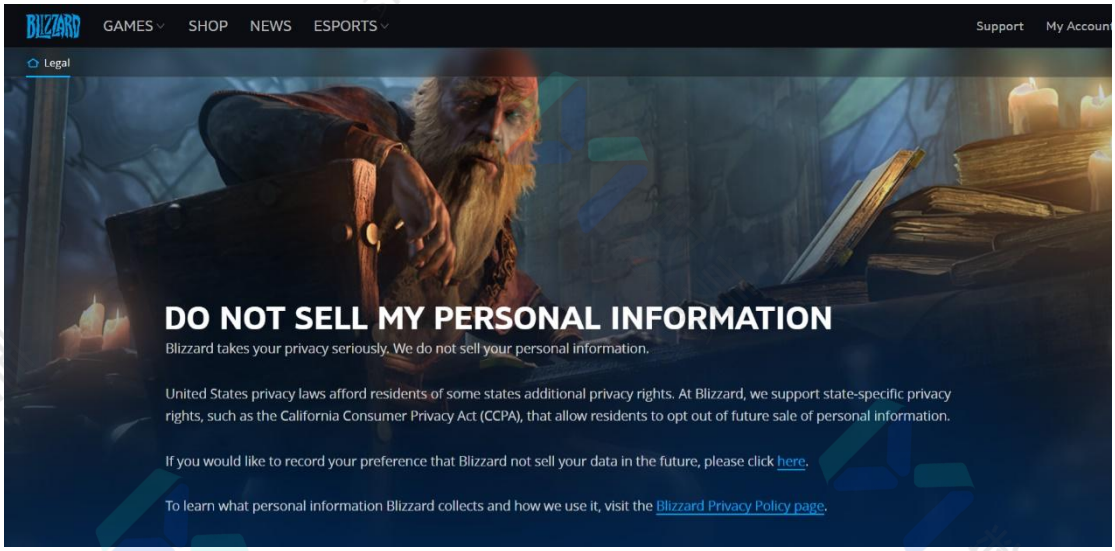
与“选择退出权”相对应的，还有专门针对 16 岁以下未成年人的“选择加入权（Opt-in）”。未成年人信息在美国受到严格保护。CCPA 明确规定，“企业任何故意忽视消费者年龄的行为应被视为其已明确知晓该消费者年龄”[7]。对于未成年人（不满 16 岁）的个人信息，企业应当在取得消费者本人（13-16 岁之间的消费者）或其父母、监护人（对于小于 13 岁的消费者）明确同意的情况下方可出售其个人信息。

---

[6] 数据来自 Roblox 统计的 2020 年 CCPA 用户数据请求，原文链接 https://en.help.roblox.com/hc/en-us/articles/4402871541140-California-Consumer-Privacy-Act

[7] CCPA 第 1798.120 条第 3 项，原文如下：

A business that willfully disregards the consumer’s age shall be deemed to have had actual knowledge of the consumer’s age.



暴雪娱乐“Do Not Sell My Personal Information”链接页面
来源：暴雪娱乐官网

5.公平交易权

企业不得因消费者行使 CCPA 相关权利而歧视消费者，包括：

（1）拒绝向消费者提供商品或服务；

（2）对商品或服务收取不同的价格或费率，包括通过给予不同的折扣、其他福利或处罚；

（3）向消费者提供不同等级或质量的商品或服务；

（4）暗示消费者将获得不同价格或费率的商品或服务，或者将向消费者提供不同水平或质量的商品或服务[8]。

但 CCPA 同时也规定了一些豁免情形。例如，当企业提供的服务或商品质量与其收集的个人信息直接挂钩时，企业可以提供不同价格或质量的商品或服务。企业还可为个人信息的收集、出售或删除提供经济激励，包括向消费者支付赔偿金等。CCPA 在保障消费者权利的基础上，也充分肯定了数据流动的经济价值，提倡在合法的情形下合理使用个人信息。

---

[8] CCPA 第 1798.125 条 a 项第 1 款，原文如下：

(A) Denying goods or services to the consumer.

(B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(C) Providing a different level or quality of goods or services to the consumer.

(D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

6.个人诉讼权

CCPA 的一个重要突破是它赋予消费者提起个人诉讼的权利。CCPA 第 1798.150 条规定，“由于企业违反义务，未实施和维护合理的安全措施以及与信息性质相符的做法来保护个人信息，从而导致未经授权的访问和泄露、盗窃或披露，消费者可提起民事诉讼。[9]”消费者可就每次安全事件追讨 100 至 750 美元的损害赔偿，同时还可申请禁止令等其他法律救济行为。

然而，CCPA 也给个人诉讼权附加了较高的门槛，在个人信息保护执法落地中的作用有限。CCPA 的私人诉讼权仅针对数据泄露事故，只有在企业因自身原因导致消费者个人数据泄露时，消费者才可提起个人诉讼。

对于企业尚未造成损害的不合规行为，个人诉讼权并不支持。例如，针对企业未在其网站显眼位置设置“Do Not Sell My Personal Information”选项这一行为，虽然它并不合规，但并未造成隐私数据泄露等严重后果，因此也就不满足个人诉讼案的条件。截止目前，加州法院已收到 150 多起控告企业隐私保护不合规的个人诉讼案，但尚未有一起案件被成功受理。

7.合规建议

CCPA 强化了消费者在隐私数据保护领域拥有的六大权利，并就如何保障消费者的个人信息提出了具体的操作规定。

出海企业应在其隐私条款中尽到提醒义务，以易懂的方式向消费者解释其拥有的权利。同时，企业应配备专人，在规定时间内处理消费者提出的各种请求，并做好相应的记录留存工作。

---

[9] CCPA 第 1798.150 条 a 项第 1 款，原文如下：

Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, or whose email address in combination with a password or security question and answer that would permit access to the account is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

(A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

四、企业义务

2020 年 1 月 1 日，《加州消费者隐私法案》（CCPA）正式生效。经过六个月的合规宽限期，CCPA 从当年 7 月 1 日开始步入执法阶段，加州司法部长有权就不合规的企业提起诉讼、征收罚款。政府监管倒逼企业加大隐私保护投入。 另一方面，随着 CCPA 逐渐为大众所熟悉，消费者的数据保护意识也在不断强化，企业陆续收到来自消费者的数据请求。据 DataGrail 发布的 CCPA Trends 2021 Report[10]显示，自 CCPA 实施以来，2020 年 B2C 企业平均每月收到 11 份来自用户的数据处理请求/百万用户，其中又以 2020 年 1 月收到的请求数最高，达到 33 份。1 月是 CCPA 正式实施的时间，很多公司也在此时更新隐私政策，导致用户的数据请求猛增。这一数据表明，用户逐渐了解 CCPA 以及自己所拥有的权利，开始主动采取行动保护自己的个人信息。

2020 年 B2C 企业每月处理用户数据请求数量
来源：DataGrail

在政府监管和消费者数据保护意识提升的双重压力下，出海企业应积极理解 CCPA 给企业施加的新义务，在隐私政策、数据管理架构和内部处理流程三方面提前做好部署，将合规成本尽量降到最低。

1. 调整隐私政策

CCPA 赋予消费者六大权利。企业应在其线上隐私政策或网站上，使用普通用户易于理解的措辞及语种，向用户告知 CCPA 赋予其的数据保护权利，且应保持每年一次的更新频率。

[10] 数据来自 DataGrail 于 2021 年发布的报告 The State of CCPA: Benchmarking CCPA Trends Across Consumer (B2C) bRANDS，报告链接 https://www.datagrail.io/resources/reports/ccpa-trends-report-2021/

知情权

企业应在隐私政策中披露其收集、出售或分享的消费者信息类别、信息来源、使用目的、具体内容以及第三方处理机构等。

访问权

企业应免费向消费者提供其收集、处理过的个人信息，且应使用简便、通用的格式，确保消费者可毫无障碍地二次使用。

删除权

企业应在隐私政策中向消费者披露“可要求删除个人信息的权利”。企业在收到消费者删除请求时，应核实请求者身份，确认是本人后才能删除相关信息。

同时，企业应通知其他服务提供商、承包商、其他第三方删除相关信息。

选择（退出）权

企业应在其网站主页提供一个显著的“Do Not Sell My Personal Information”链接，允许消费者或其代理人选择拒绝出售其个人信息。

除添加上述链接外，企业还应在其线上通用隐私政策或加州消费者专用主页中告知消费者拥有选择退出权。

公平交易权

企业不得因消费者行使 CCPA 赋予的权利而歧视消费者。但企业可为个人信息的收集、出售或删除提供经济激励，包括向消费者支付赔偿金等。

需要注意的是，企业提供经济激励应取得消费者同意，且用户应拥有随时撤回的权利。如果消费者拒绝，在接下来的 12 个月内，企业不得再次邀请消费者加入激励计划。

个人诉讼权

企业应在隐私政策中告知消费者拥有个人诉讼的权利。

2.调整数据管理架构

除了在隐私条款中尽到告知义务，企业还应调整其数据管理架构，确保其能够快速响应消费者请求。在新的隐私保护义务框架下，企业的数据库不再是单纯的信息存储载体，它将成为一个智能仓库，能够对海量数据实现精细化管理。从收集、分类、提取到删除、分析，这些功能无一不要求数据管理架构的升级，从而实现灵活、便捷的数据管理。

以删除请求为例，在收到消费者的删除申请后，企业要在其数百万量级的用户数据库中，快速定位该消费者的个人信息，明确哪些信息是可以删除的，哪些信息是为提供服务所必需的，再结合实际业务需要和消费者请求，删除消费者的全部或部分个人信息。

企业还应做好数据标记、数据分类工作，区分出售数据、共享数据和营销数据等，确保在收到相关数据处理请求后，能快速通知数据服务提供商或第三方处理机构，实现相应的消费者数据请求。 除了企业自身，其第三方处理机构、承包商以及数据服务提供商等也应具备类似的数据管理功能。 随着民众的数据隐私保护意识不断提升，消费者开始要求更好地控制个人信息，可以预见，企业在未来收到的消费者数据请求会越来越多。出海企业应尽早优化自己的数据管理架构，对消费者个人信息实行精细化管理，高效处理消费者的数据请求，降低处理成本。

3.制定数据请求处理规范

CCPA 也规定了企业处理消费者数据请求的操作规范。

请求形式

企业应提供至少两种指定方式，允许消费者提交数据请求，其中一种方式应为免费电话热线。

此外，若企业仅提供线上服务，仅提供邮件地址即可；若企业拥有网站，网站应可供消费者提交信息披露、删除或更正信息的请求。

处理时间

企业应在收到消费者请求起的 45 日内，免费向消费者披露或提供其要求的信息，更正不准确的个人信息，或删除个人信息。在合理必要的情形下，处理期限可再延长 45 日，但应在第一个 45 日期限内告知消费者延期事项。

验证

企业在收到消费者数据请求后，应对消费者进行验证，但不得要求消费者为验证目的创建新账号。

数据请求范围

企业应能够提供收到消费者请求前 12 个月的消费者信息，但消费者也可要求企业披露超过 12 个月的信息，除非企业可证明此做法不可行或涉及过多的工作。

员工培训

企业应确保处理数据请求的员工了解 CCPA 赋予的消费者权利，并能够指导消费者行使这些权利。

第三方义务

企业应重新审查与第三方机构签订的关于消费者信息披露、出售、共享等方面的合同，确保第三方机构在处理消费者个人信息时符合 CCPA 的规定。

此外，第三方不得出售或共享已被企业出售或共享的消费者个人信息，除非该消费者收到明确通知，并拥有拒绝的权利。

4.合规建议

由于监管压力和消费者数据保护意识提升，企业必然要在隐私保护上加大投入。Gartner 数据[11]显示，企业人工处理单个请求平均花费 1,406 美元，按照每百万用户月均提出 11 份数据请求来计算，一个拥有 1 千万注册用户的平台每年要花费约 185 万美元，企业的人力成本和运营成本大幅上涨。

然而，尽管隐私合规成本高昂，实践证明，它也可以带来额外的回报。根据思科的一项调查显示，“大多数组织在隐私保护上的投资能收获良好的收益，超过 40%的企业可收获至少两倍回报。[12]”隐私合规虽然在短期内会带来运营压力，但长远来看，主动提升企业的隐私合规水平有助于获取消费者的信任，为企业品牌注入更多价值。

出海企业面临陌生的地域环境、文化、语言，在获取用户信任方面比本土企业更难，更应在隐私合规上做好万全准备。CCPA 对企业的信息保护义务上做出了具体的规定，企业应在隐私政策、数据管理架构和内部处理流程上做好提前部署，从容应对政府监管与消费者的数据请求，将隐私保护投入转化为新的增长点。

---

[11] 数据来自 DataGrail 报告，链接同上

[12] 数据来自思科于 2020 发布的研究 Cisco 2020 Data Privacy Benchmark Study Confirms Positive Financial Benefits of Strong Corporate Data Privacy Practices, 原文链接 https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=2047256

五、法律责任

CCPA 自 2020 年 1 月开始正式实施以来，尚未传出过天价罚单的新闻。与之形成鲜明对比的是高调而严苛的 GDPR。据 Atlas VPN 统计[13]，2021 年，共有 412 家企业因违反 GDPR 被罚，其中不乏亚马逊、WhatsApp 等互联网巨头，罚款总额更是高达 10 亿欧元。CCPA 的处罚标准似乎比 GDPR 更为温和，事实果真如此吗？

1.罚款标准

CCPA 第 1798.155 条规定，“对每一次违法行为处以最高 2,500 美元的行政处罚，对每一次故意的违法行为和每一次涉及未成年消费者个人信息的违法行为处以最高 7,500 美元的行政罚款。[14]”

再来看 GDPR 的处罚标准。对于一般性的违法，GDPR 的罚款上限是 1000 万欧元，或最高为上一个财政年度全球全年营业收入的 2%（两者中取数额大者）；对于严重的违法，罚款上限是 2000 万欧元，或者最高为上一个财政年度全球全年营业收入的 4%（两者中取数额大者）。

我国 2021 年 11 月新颁布的《个人信息保护法》也效仿 GDPR，对违法企业按照营业额营收比例收取罚款。其规定，“……拒不改正的，并处一百万元以下罚款……情节严重的，并处五千万元以下或者上一年度营业额百分之五以下罚款……”

与 GDPR 和《个人信息保护法》动辄千万级别的罚款相比，CCPA 最高不过 7,500 美元的数字确实显得微不足道。但要注意的是，CCPA 是“按次收费”的。对拥有大量用户数据的平台而言，一旦数据泄露造成用户实际损失，按照每项违

---

[13] 数字来自 Atlas VPN 于 2022 年发布的新闻 GDPR Fines Hit over €1 Billion in 2021，原文链接 https://atlasvpn.com/blog/gdpr-fines-hit-over-1-billion-in-2021

[14] CCPA 第 1798.155 条 b 项，原文如下：

Any business, service provider, or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General.

法行为最高处罚 7,500 美元计算的话，罚款总额很容易便会达到上亿美元。而且 CCPA 并没有罚款上限，无限累加的罚款计算方式也有着不小的威慑作用。

上述罚款必须通过加州检察长提起诉讼才可收取，也叫做“行政罚款”。

除“行政罚款”外，消费者可利用个人诉讼权提起诉讼，申请“民事救济”。CCPA 规定，如果消费者的个人信息因企业保护义务不到位而遭到泄露，消费者可提起民事诉讼，并要求以下赔偿：

（1）为每名消费者每件事故赔偿不少于 100 美元、不多于 750 美元的损害赔偿金或实际损害赔偿金，以数额较高者为准。

（2）禁令性或宣告性法律救济。

（3）法院认为适当的其他救济[15]。

750 美元的罚款上限虽然不高，但若是提起集体诉讼的人数足够多，违法企业也有可能面临千万罚款。 个人诉讼权往往被视作消费者捍卫自身权益的有力武器。不过，CCPA 在赋予消费者这一权利的同时，也对它的发动设置了严苛的条件：1）仅限于特定的信息泄露；2）企业未尽到保护义务；3）已造成实际损害。

严苛标准的制定主要是防止有人滥用个人诉讼权，浪费有限的执法资源。同样赋予消费者个人诉讼权的 GDPR 也设置了类似的条件。截至目前，加州法院尚未成功受理一例起诉企业违反 CCPA 的个人诉讼案。由此可见，CCPA 并不将个人诉讼视为保障消费者权益的主要手段。

2.整改期

CCPA 赋予消费者提起个人诉讼的权利，违法公司也有可能被提起行政诉讼。不过，加州司法部长曾坦言，每年司法部的资源只够处理几起诉讼案件，这也意

---

[15] CCPA 第 1795.150 条 a 项第 1 款，原文如下：

(A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

味着大多数公司都不会被起诉[16]。提起诉讼并非 CCPA 执法的最终目的，最重要的是督促企业采取恰当的措施，从而保护消费者的隐私权利。

为了将有限的资源用到刀刃上，CCPA 特地设置了 30 天的整改期，这也是 CCPA 的程序设置优于 GDPR 的一个地方。CCPA 第 1798.150 条规定，如果在发起针对企业的任何基于个人或集体的法定损害的诉讼前，消费者提前 30 天向企业提供了书面通知，表明消费者指控的企业已经或正在违反本法之具体规定，则消费者可依照本条提起诉讼。

如果企业在 30 天内实际纠正了被通知的违规行为，并向消费者提供明确的书面声明以表明相关违规行为已被纠正，且不会再发生违规行为，则不得发起针对企业的基于个人或集体法定损害的诉讼。

如果企业再次违反 CCPA 的相关规定，消费者可对企业发起诉讼，要求其执行书面声明，也可针对书面声明的任一项违反行为请求法定损害赔偿金。

消费者提起个人诉讼应遵守 30 天整改期的规定，行政诉讼也不例外。执法机构在发现企业有不合规行为后，应立即向企业发出通知，指导其在 30 天内进行整改。企业未能在 30 天内完成整改的，检察长可依法提起行政诉讼。

3.合规建议

2021 年 7 月，加里福尼亚检察署发布一份 CCPA 执法总结，细致地描述了 27 例典型案例以及企业后续的整改措施[17]。绝大多数企业都能在检察署的指导下，在 30 天内改正自己的不合规行为，很少有企业走到诉讼罚款这一步。即使真的被起诉，截至目前也没有开出 GDPR 那样的天价罚单：CCPA 发出的第一张罚单不过 40 万美元。在政府监管层面上，CCPA 的执法机构更注重通过日常监督与整改期来加强企业隐私保护的意识与实践，诉讼与罚款更多是起到威慑和兜底作用。

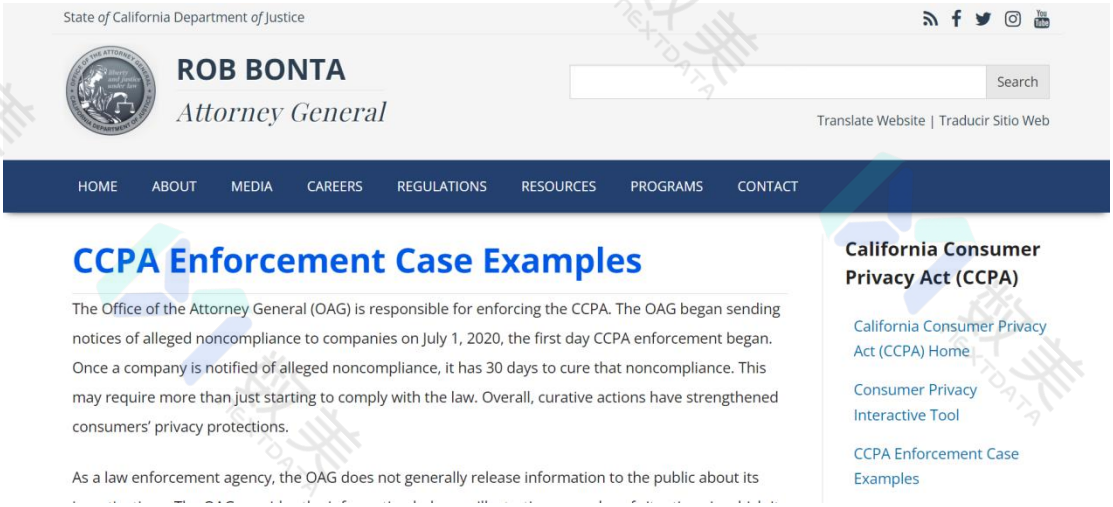
对出海企业而言，温和的处罚标准意味着较低的试错成本，但这并不意味着企业就可以放松对 CCPA 的执行。事实上，在 CCPA 实施后，加州在 2020 年

---

[16] 引用 iapp 于 2020 年发布的新闻 CCPA Update: Calif. Attorney General Comments, New Amendments Signed into Law, 原文链接 https://iapp.org/news/a/ccpa-update-calif-attorney-general-comments-and-new-amendments-signed-into-law/

[17] 引用自加拿大检察署发布的执法案例，原文链接 https://oag.ca.gov/privacy/ccpa/enforcement

11 月又通过了 CCPA 的修正案《加州隐私权利法案》（CPRA）。CPRA 设立了专门的监管机构——隐私保护署（California Privacy Protection Agency），负责 CCPA 与 CPRA 的日常监管与执法，加强公众教育。



加州检察署的执法案例
来源：加州检察署

专门的机构意味着更专业的人力，可调用的资源也更加充裕。随着隐私保护署的人员配置逐渐齐全，它的执法范围和内容也会不断扩大，企业的不合规行为被发现的几率也会上升。在此背景下，出海企业应及时追踪最新的隐私政策法规，发现问题后积极配合执法机构，在规定时间内完成整改，避免被开罚单。

关于数美科技

数美科技成立于 2015 年 6 月，是一家专业的在线业务风控解决方案提供商，致力于解决在线业务中广泛存在的业务风险与内容风险，为企业数字化转型保驾护航，以两大核心产品：天网——全栈式智能业务风控产品、天净——全栈式智能内容风控产品，推动数字风控行业变革。

数美科技独创全栈式数字风控引擎系统，现已实现全球化 AI SaaS 多集群部署，覆盖中国大陆、欧洲、北美、东南亚、印度等十余个国家和地区，日均风控服务达 30 亿次以上。

目前，数美科技积累了工商银行、银联、小红书、爱奇艺、麦当劳等全球 3000 余家国内外知名企业的服务和客户成功经验，覆盖音视频社交、游戏、银行、新零售、电商、金融等超 15 个行业，被评为企业数字风控行业领军者。

数美科技总部位于北京，并在杭州、上海、深圳、广州设有研发中心和子公司。团队核心成员均来自百度、阿里、腾讯、360、小米等知名互联网企业，拥 10 余年搜索、安全、语音等互联网在线产品研发经验，以及相关领域百余项国家级技术专利。

公司拥有人工智能研究院、黑产研究院、舆情中心、政策研究中心等多个专家服务团队，为客户提供业务风控、内容生态治理相关的技术咨询、解决方案和专业服务，并携手中国信通院、中国科学技术大学等权威机构和院校，成立专项技术实验室，实现产学研用一体化。

公司当前已完成 D 轮融资，由 CPE、经纬中国、厚朴投资、腾讯、襄禾资本等知名机构联合投资。

关于数美数字风控研究院

数美数字风控研究院（公众号 ID: ishumei2015）致力于打造数字风控行业根据地，为从业者带来最前沿的产品、技术、政策解读及深度报告研究。汇聚专业力量，洞悉行业趋势！

数美数字风控研究院

公众号 ID: ishumei2015

数美科技

公众号 ID: ShumeiTech

联系我们

电话：400-610-3866

邮箱：pr@ishumei.com

官网：www.ishumei.com