ChatGPT

# GDPR 與 CCPA 核心條款概述

GDPR（通用資料保護規範）是歐盟於2018年生效的全面性個人資料保護法規，適用於任何處理歐盟/歐洲經濟區居民個人資料的組織，不論企業是否位於歐盟，只要向歐盟人士提供商品服務或監測其行為即受其約束 [1] [2]。GDPR 將「個人資料」定義為與可直接或間接識別個人相關的任何資訊 [3]，並規定了七大處理原則（合法、公平、透明、目的限制、資料最小化、準確性、存儲限制、安全性及可追究性） [4]。資料主體擁有多項權利，包括知情、存取、更正、刪除（遺忘權）、限制處理、資料可攜、反對處理，以及自動化決策相關權利（共八大權利） [5]。違規最高可處以2,000萬歐元或全球營收4%（兩者擇高）罰款 [6]。

CCPA（加州消費者隱私法）是加州於2018年通過的隱私法案，專為保護加州居民個人資訊權益而設計 [7]。它適用於在加州經營且滿足任一門檻的營利企業：年營收超過2500萬美元、處理或分享5萬戶以上加州居民資料，或超過半數營收來自出售信息 [8]。CCPA將「個人資訊」定義為任何可識別或關聯至個人（或其家庭）的資訊，如姓名、地址、電子郵件、購物記錄、網路瀏覽習慣、定位數據等 [9]；並將精準定位、健康資訊、金融帳戶、遺傳資料等納入「敏感個人資訊」的額外保護範疇 [10]。CCPA　賦予消費者「知情權」、「刪除權」與「拒賣/分享權」（不賣個資）等基本權利 [11]，以及（CPRA增訂的）更正不正確資訊和限制敏感資訊使用的權利 [12] [13]；並明確禁止企業因消費者行使這些權利而歧視處理 [14]。違規者每次違規最高可處2,500美元（故意違規7,500美元）罰款 [15]；若發生資料洩漏，消費者可提告索賠，每筆資料賠償100至750美元 [16] [15]。

| 比較項目 | GDPR（歐盟法規） | CCPA（加州法案） |
|---|---|---|
| **適用範圍** | 凡處理歐盟/歐洲經濟區居民個人資料的組織都適用，包括向歐盟人士提供商品服務或在歐盟境內監測其行為者 [1] [2]。 | 適用於在加州經營且符合以下任一條件的營利企業：年營收超過2,500萬美元、持有50萬筆以上加州居民資料，或超過半數營收來自個資出售 [8]。 |
| **個資範疇** | 個人資料涵蓋所有可識別個人資訊，包括名稱、電子郵件、位置信息、種族、健康等特殊類別 [3]。 | 個人資訊廣義涵蓋可識別或聯繫至個人（或家庭）的資訊，如身份識別號、聯絡方式、購買紀錄、上網行為、定位等 [9]；將金融、健康、精準定位、遺傳等敏感資訊歸為「敏感個人資訊」額外保護 [10]。 |
| **法律依據** | 處理個資必須具備《GDPR》第6條所列合法依據（如明示同意、合約履行、法律義務等） [17]；且須遵循合法性、公平性、透明度、目的限制與資料最小化等原則 [4]。 | 雖不要求具體的「合法依據」，但企業必須在收集時向消費者提供明確通知，說明收集目的；未經同意不得出賣或分享個資 [13] [7]，並須尊重消費者行使權利的意願。 |
| **主要權利** | 資料主體享有八大權利：知情、存取、更正、刪除、限制處理、資料可攜、反對處理及自動化決策相關權利 [5]。 | 消費者享有「知情權」（了解企業收集、使用、分享的資料類別）、「刪除權」、要求「拒賣/分享其個資」、（CPRA新增的）「更正權」及「限制敏感資訊使用權」，並且企業不得因行使權利而對消費者歧視 [11] [13]。 |
| **罰則機制** | 違規最高罰款 2,000 萬歐元或全球年營收 4%（以較高者為準），此外資料當事人可請求損害賠償 [6]。 | 加州檢察長可處以每項違規最高 7,500 美元（普通違規 2,500 美元）；個資洩露時，受害消費者可提起訴訟，索賠每筆資料 100~750 美元 [15] [16]。 |

## 法規適用範圍

**GDPR** 的適用範圍極廣，不限企業所在地，只要處理歐盟居民個人資料即適用。具體來說，非歐盟企業若向歐盟或歐洲經濟區居民提供商品服務、或在歐盟境內監測其行為（如網站追蹤廣告等），都必須符合GDPR規定[2][1]。相對而言，GDPR不適用於純屬個人或家庭用途的資料處理，也不適用於法執行和國家安全等另有規範的情形。

**CCPA** 只保障加州居民的資料權利，且只針對達到規模門檻的營利組織生效。符合條件的企業包括在加州擁有業務、**且**年營收超過2,500萬美元、或持有50萬筆加州居民資料、或超過半數收入來自個資銷售者[8]。CCPA規定不適用於非營利機構、政府單位或企業組織等[18]。適用企業必須遵守法規，但對於不在加州經營或不符合規模的企業則無直接約束。

## 數據收集、使用、共享、存儲與刪除要求

- **收集與同意**：GDPR 要求企業在收集個人資料前獲得合法依據（常見的是明確同意或契約履行）[17]。收集時必須告知資料主體用途與第三方共享情況（資訊透明）[19]。CCPA 要求企業在收集消費者個資時提供易懂的隱私政策，告知資料蒐集種類、用途及分享對象[20]。此外，未經明確同意，企業不得出售或共享消費者資料（尤其是合約要求獲得用戶取消拒賣授權）[13]。對於未滿16歲的用戶，出售個資前需取得主動同意，13～16歲則需家長書面同意。

- **使用與共享**：GDPR 規定企業僅可將資料用於蒐集時明示的目的，不得另作不相關用途（目的限制）[21]；且應盡量最小化資料量，並確保資料準確和安全[22]。若須將資料提供給處理者或第三方，則需簽訂書面合約，明訂其處理責任與安全義務[23]。CCPA 強調「使用者控制」，企業應尊重消費者拒賣/不分享的意願，一旦收到拒賣請求就不得再將資料賣給第三方[13]。任何隱藏的資訊交換、分享也都需要在隱私政策清楚揭露，否則將被視為違規。

- **存儲與刪除**：GDPR 要求企業只保留與既定目的相關且必要的個人資料，超過使用期限或目的達成後應及時刪除（存儲限制與最小化原則）[21]。企業須對資料進行定期清查並建立刪除流程。GDPR 也賦予資料主體刪除權（遺忘權），任何個人有權要求企業刪除其資料，除非因法律義務或其他合法理由需保留[5]。CCPA 同樣賦予消費者刪除權，消費者可以要求企業刪除其資訊，且企業需通知其服務供應商一併刪除，僅在例外情形（如法規保存要求、法律訴訟保留等）下例外[24][25]。CCPA 未明文規定資料保留期限，但企業需能在消費者查詢時說明資料保留政策並落實刪除請求。

- **資料安全與事件通報**：GDPR 要求企業採取適當的技術及組織措施保護資料安全（例如加密與存取控管）[26]。若發生資料外洩且可能危害權利與自由，企業必須在72小時內通報監管機關，並在必要時通知受影響者[27]。CCPA 本身對資料安全未訂定具體技術標準，但企業仍應採行合理安全措施防止洩漏，並遵守加州一般資料洩漏通報法。在洩漏事件中，消費者可根據法規提起訴訟求償。

## 違規處罰與執行機制

違反 **GDPR** 可面臨嚴厲處罰：最高可罰款2,000萬歐元或全球營收4%，通常依據違規性質和嚴重程度進行處分[6]。各成員國設有監管機關（DPA）負責執法，並由歐洲資料保護委員會（EDPB）統籌指引。自GDPR實施以來，歐盟各國已經對多家大型企業開出天價罰單（例如對Meta、Amazon等數度罰款），顯示違規成本相當高[28][15]。

違反 **CCPA** 的罰則則依違規情況而定：一般違規由加州檢察長處以每違規項目最高2500美元罰款；若故意違規或不在修復期限內完成糾正，則可處7500美元罰款[15]。此外，個資洩露時受害消費者可提出私人訴訟，每筆受影響資料賠償100～750美元[16]。至2024年，加州已對多起違規案進行執法，例如**DoorDash**因未通知用戶參與資料銷售計畫被罰37.5萬美元[29]，**Google**因未徵得同意收集定位數據被罰9300萬美元[30]，**Sephora**未

公開出售信息被處120萬美元罰款 [31] 等。執法由加州檢察長（及新成立的加州隱私保護局CPPA）負責，隨著CPRA上路，執法權限與罰則有所增強。

## 企業合規措施

面對GDPR與CCPA的雙重要求，跨國企業需採取全面的合規策略，常見措施包括：

- **資料盤點與地圖**：全面盤點企業收集、處理的個人資料類別與流程，製作資料流轉圖。這一步驟是合規的基礎，可使企業清楚掌握資料來源、用途與儲存位置，並支撐後續權利請求與風險評估 [32] 。例如某跨國公司透過建立詳盡的個人資料庫與流轉地圖，據此制定存取請求、通知與安全控管流程，成功滿足GDPR與CCPA要求 [32] [33] 。

- **資料保護影響評估（DPIA）**：根據GDPR第35條，對高風險的資料處理活動（例如大規模分析或監控、公眾場所監控等）應進行DPIA，以評估並降低對資料主體權益的風險 [34] 。此程序有助企業及早發現隱私風險並記錄因應措施，是證明合規的重要文件。CCPA雖未明文要求DPIA，但類似風險評估同樣可幫助企業強化對敏感資料的保護。

- **資料最小化與保護**：嚴格遵守「只收集必要資料」原則，避免過度蒐集或保留過期資料 [21] 。實施分級資料分類、加密與存取控管等技術手段，保護個資不被未授權存取。對於跨境傳輸，GDPR要求採用歐盟認可的保護機制（適足性決定、標準契約條款或企業內規範） [35] ，而CCPA則無此要求，但也鼓勵企業在全球執行隱私保護。

- **同意與偏好管理**：GDPR規定多數處理須先取得明確的「積極同意」 [19] ；企業需提供清晰的同意選項與管理機制。CCPA則採取「選擇退出」（Opt-out）模式，企業要設置明顯的拒賣按鈕，並尊重用戶拒絕分享的決定 [13] 。一般而言，企業應同步管理不同法規下的同意偏好，例如在歐盟採用Opt-in，在加州提供Opt-out，並在隱私政策中分別說明。

- **供應鏈合規**：GDPR規定資料控制者必須與資料處理者簽訂符合標準的契約，明確要求處理者僅依指示作業並採取安全措施 [23] 。企業應檢視與其雲端服務商、外包夥伴等的契約，確保條款符合法規要求。CCPA則要求與「服務供應商/承包商」訂有書面協議，否則其行為可能被視為銷售或分享資料而違規。換言之，企業必須審慎遴選並監管合作夥伴的資料處理行為。

- **其他措施**：任命隱私責任人（GDPR下部分情形需設置DPO）、定期內部訓練、實施隱私設計（Privacy by Design）原則、定期審核與更新合規流程等，都是強化合規的常見做法。自動化合規工具、同意管理平台、資料庫存檔解決方案等科技手段，也能提高效率並降低風險。

## 案例研究：科技與金融行業

- **科技行業案例**：某B2B軟體公司為增強GDPR合規，重新設計產品介面以增強用戶對自身資料的掌控權，新增清晰的同意設定和自動資料刪除功能。結果不僅滿足GDPR要求，更提升了用戶的信任與忠誠度 [36] 。另有報導指出，若未獲同意擅自蒐集地點資訊或隱私資訊的科技公司，往往面臨高額罰款。例如Google因收集用戶定位數據未獲同意，遭加州處以9300萬美元罰款 [30] ，凸顯企業即使規模龐大也必須嚴格遵守隱私規範。

- **金融行業案例**：在金融服務領域，銀行與保險業者面臨的挑戰尤為複雜。一家跨國銀行指出，GDPR要求其必須加強客戶資料的保密性、確保有能力響應客戶的查詢請求（如存取或刪除申請），並依「必要性原則」只保留執行金融服務所需的資料 [37] 。另一項研究也顯示，隨著GDPR的推行，金融機構對資料進行了大規模清理與安全升級，結果導致所持有的客戶資料品質提升，反而增強了客戶對數據被妥善處理的信心 [38] 。也就是說，這些企業在初期投入資源梳理資料、強化安全後，獲得了更好的風險管控和品牌信任。

- **跨國企業實踐**：例如跨國消費品公司Modere，因其歐洲業務涵蓋面廣且處理大量個人資料，聘請顧問團隊進行全公司GDPR合規檢視。透過與各部門協作，該公司建立了完善的個人資料盤點制度和流程，並基於此開發了存取請求、通知揭露與安全控制的政策 [32]。同時，Modere借助已建立的GDPR合規控制措施，很快完成了CCPA合規部署，確保在法規生效前達標 [33]。依靠透明且一致的個資處理原則，Modere 不僅成功合規，也「維持了消費者對其個資以合法、安全方式處理的信任」 [39]。

## 合規對企業營運的長期影響

GDPR與CCPA等隱私法規對企業營運帶來顯著影響：合規成本通常很高，有研究報告指出**88%**的大型公司認為僅GDPR合規一年就耗資超過100萬美元，**40%**更超過1000萬美元 [40]。這包括人力培訓、流程改造、技術升級等直接成本，以及可能因業務調整而延遲上市的間接成本 [40]。然而，長期來看，嚴格的隱私保護也能成為企業競爭優勢：一方面，合規推動企業檢視並優化資料流程（如精簡冗餘資料、加強安全防護），提升了營運效率和資料品質 [38] [41]；另一方面，落實隱私法規往往增進客戶信任，提高企業形象。如前述案例所示，採用**Privacy by Design**理念的企業不僅滿足法規，更讓用戶感到安全與受尊重，進而提高忠誠度 [36] [42]。實際上，GDPR推行後消費者對數據隱私的意識大幅提高，企業若能將隱私視為「信任基石」，則有助於開拓市場和品牌價值。正如研究者所言：「隱私並非創新之絆腳石，兩者可以並存。」 [42] 換言之，企業若能以隱私合規為契機，完善數據治理、強化客戶關係，從長遠來看可轉化為持續獲利和信任的動力。

**參考資料：** 本報告綜合歐盟與加州官方資料、專業合規指南及業界案例所得之最新資訊 [1] [8] [17] [32] [19] 等文獻。

---


[1] [3] [4] [6] What is GDPR, the EU’s new data protection law? - GDPR.eu
https://gdpr.eu/what-is-gdpr/

[2] Understanding How GDPR Applies to Non-EU Businesses: A Practical Guide
https://pandectes.io/blog/how-gdpr-applies-to-non-eu-businesses/

[5] [17] [21] [22] [23] [26] [27] [34] [35] Summary of 10 Key GDPR Requirements - IT Governance Blog
https://www.itgovernance.eu/blog/en/summary-of-the-gdprs-10-key-requirements

[7] [8] [9] [10] [11] [12] [13] [14] [16] [18] [20] [24] [25] California Consumer Privacy Act (CCPA) | State of California - Department of Justice - Office of the Attorney General
https://oag.ca.gov/privacy/ccpa

[15] CCPA Penalties And Fines: What Happens if You Fail to Comply
https://usercentrics.com/knowledge-hub/ccpa-penalties/

[19] [28] How Has the GDPR Affected Business?
https://www.businessnewsdaily.com/15510-gdpr-in-review-data-privacy.html

[29] [30] [31] Privacy Enforcement Actions | State of California - Department of Justice - Office of the Attorney General
https://oag.ca.gov/privacy/privacy-enforcement-actions

[32] [33] [39] Case Study: Achieving GDPR Compliance
https://www.compliancepoint.com/articles/case-study-gdpr-ccpa-compliance/

[36] [41] GDPR Implementation Examples: Success Stories for B2B SaaS Companies
https://complydog.com/blog/gdpr-implementation-examples

[37] Top challenges firms face with GDPR compliance | Insights | UK Finance
https://www.ukfinance.org.uk/news-and-insight/blog/top-challenges-firms-face-gdpr-compliance

38 42 One Year On: The Impact of the GDPR on Digital Banking
https://internationalbanker.com/finance/one-year-on-the-impact-of-the-gdpr-on-digital-banking/

40 Privacy reset: from compliance to trust-building: PwC
https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/privacy-reset.html