CHAPMAN LAW REVIEW

Citation: Gregory S. McNeal, *The Compliance Stack: A Structural Comparison of the GDPR and the CCPA*, 29 CHAP. L. REV. 585 (2026).

--For copyright information, please contact chapman.law.review@gmail.com.

The Compliance Stack: A Structural Comparison of the GDPR and the CCPA

Gregory S. McNeal

CONTENTS

The Compliance Stack: A Structural Comparison of the GDPR and the CCPA

Gregory S. McNeal∗

Comprehensive privacy statutes now set the baseline terms for multinational data privacy compliance. Two regimes dominate the attention of scholars and practitioners—the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA)—yet the two are not the functional equivalents that corporate compliance discussions sometimes suggest. They differ in regulatory design, doctrinal architecture, and operative assumptions. This Article works through the primary sources to compare them across five dimensions: territorial scope, processing constraints, individual rights, cross-border transfer mechanisms, and enforcement. On transfers, the contrast is especially sharp. The GDPR carves out third-country data flows as a distinct legal question under chapter V, subjecting them to adequacy decisions, approved safeguards, or narrow derogations; the CCPA has no comparable regime and instead governs downstream disclosures through its sale-and-sharing rules and its taxonomy of service providers, contractors, and third parties. The Article's aim is descriptive, seeking to isolate where these regimes align in practice and where their legal triggers diverge.

∗ Gregory S. McNeal, JD/PhD, CIPM; Professor of Law and Public Policy, Pepperdine University Caruso School of Law. With sincere thanks to the organizers of this symposium issue. AI Disclosure: In writing this Article, the author used the following AI tools: Grammarly for proofreading and grammar; Wispr Flow for voice-to-text dictation in lieu of typing (due to a disability); Claude for outlining and organizational assistance; and Perplexity AI for identifying supplemental sources. All prose is original to the author and when AI was used it was for editing, not drafting.

I. INTRODUCTION

The regulatory story of the last decade in privacy law is, at bottom, a story about scope. For most of its history, the United States governed personal information through a patchwork of sector-specific statutes, each tailored to a particular category of risk. HIPAA covered health data. The Gramm-Leach-Bliley Act covered financial data. FERPA covered education records. COPPA covered children. If your data did not fall into one of those silos, you were largely on your own.[1] That model made sense when personal data was generated in discrete, identifiable contexts. It makes considerably less sense when a single smartphone generates and transmits health data, financial data, location data, and behavioral data to dozens of third parties before the user finishes breakfast.

The move toward omnibus privacy regulation reflects this reality. Rather than continuing to draw regulatory boundaries around specific industries, legislators in Europe and California chose to draw them around personal information itself, regardless of who holds it or what sector it came from.[2] The two regimes that emerged from this shift, the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), now function as the dominant reference points for privacy compliance worldwide. They are the frameworks that multinational companies build their data governance programs around. And they are the frameworks that other jurisdictions look to when drafting their own laws.[3]

Part of the reason for their influence is sheer jurisdictional reach. The GDPR applies to any entity that processes personal data in the context of offering goods or services to individuals in the Union, or that monitors their behavior within it, regardless of whether the entity has a physical presence in Europe.[4] The CCPA reaches any for-profit entity doing business in California that meets specified thresholds: (1) annual gross revenues ex-

1 *See* Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CALIF. L. REV. 877, 878–79 (2014) (describing the U.S. sectoral model as being a patchwork of federal and state laws).

2 *See* Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 776–78, 816–17 (2019) (analyzing the EU's comprehensive regulatory model and its influence on global privacy norms).

3 *See generally* ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD 132–59 (2020) (documenting the GDPR's influence on third-country regulatory adoption).

4 *See* Commission Regulation 2016/679, art. 3, 2016 O.J. (L 119) 1, 32–33 (EU).

ceeding $25,000,000, (2) processing of "personal information of 100,000 or more consumers or households," or (3) deriving 50% or more of annual revenue from selling or sharing personal information.[5] Given the size of these two markets, the practical effect is extraterritorial. Companies headquartered in Tokyo or São Paulo or Austin find themselves subject to one or both regimes simply because they have customers in those jurisdictions. The GDPR and the CCPA regulate their own markets, and they set the terms for global data practice.

But shared ambition does not mean shared architecture. The two regimes start from different legal traditions, operate through different regulatory mechanisms, and reach different conclusions about fundamental questions: what makes data processing lawful, how individual rights attach, whether the geographic movement of data matters, and what role contracts play in extending regulatory standards through the supply chain. This Article works through those differences systematically, drawing on the primary sources of both regimes to identify where they converge and, more often, where they diverge.

The GDPR is grounded in a specific constitutional commitment. Article 8 of the Charter of Fundamental Rights of the European Union recognizes the protection of personal data as an independent fundamental right, distinct from the right to privacy under article 7.[6] That distinction matters. It means the GDPR is implementing a constitutional mandate, and its regulatory architecture reflects that origin. The result is an omnibus framework that applies to virtually all processing of personal data by public and private actors alike, with the dual objective of protecting individual autonomy and facilitating the free movement of data within the internal market.[7] The CCPA comes from a different place entirely. It is a consumer protection statute, enacted through the California legislature and later amended by ballot initiative, situated within a legal tradition that treats privacy primarily as a matter of market regulation and individual choice.[8] The rights it creates attach to the commercial relation-

5 *See* CAL. CIV. CODE § 1798.140(d)(1) (West 2026).

6 *See* Charter of Fundamental Rights of the European Union arts. 7–8, Oct. 26, 2012, 2012 O.J. (C 326) 397.

7 *See* Commission Regulation 2016/679, art. 1, 2016 O.J. (L 119) 1, 32 (EU); *see also* Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 123 (2017) (situating the GDPR within the European tradition of treating data protection as a dignity-based right).

8 *See* CIV. §§ 1798.100–.199.100; *see also* Eric Goldman, An Introduction to the California Consumer Privacy Act (CCPA) 3–5 (July 1, 2020) (unpublished manuscript),

ship between a business and a consumer. They are contingent on the nature of the data transaction, and they are designed to give consumers visibility into and control over how businesses use their personal information. The CCPA does not ask whether a particular act of processing is justified. It asks whether the consumer knows about it and has the ability to say no.

That difference in legal origin shapes everything downstream. Because European lawmakers treat data protection as a fundamental right, the GDPR places the burden of justification on the data controller before processing begins. Article 6 provides that processing is lawful only if at least one of six enumerated bases applies: the data subject's consent, contractual necessity, a legal obligation, protection of vital interests, performance of a task in the public interest, or the legitimate interests of the controller.[9] Each basis carries its own conditions. Consent must be freely given, specific, informed, and unambiguous.[10] Legitimate interests, the most flexible basis and the one most commonly invoked for commercial processing, requires a three-part analysis: the controller must (1) identify a legitimate interest, (2) demonstrate that the processing is necessary to pursue it, and then (3) balance that interest against the fundamental rights and freedoms of the data subject.[11] The overall effect is a regime that requires affirmative justification for every category of data activity. California asks nothing comparable. Its framework assumes that commercial data processing is permitted and then layers on disclosure obligations, purpose limitations, and opt-out rights to constrain how that processing occurs. The starting points are different, and so are the compliance architectures that follow from them.

The CCPA takes the opposite approach. It treats commercial data processing as a permitted activity and then imposes conditions on it: disclose what you collect and why, give consumers the ability to opt out of sale and sharing, and honor purpose limitations on downstream use.[12] The model is rooted in consumer protection and unfair competition law, and it shows. The animating

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3211013 [https://perma.cc/CL63-DL7G] (framing the CCPA as consumer protection legislation).

9 *See* Commission Regulation 2016/679, art. 6(1), 2016 O.J. (L 119) 1, 36 (EU).

10 *See id.* art. 4(11), at 34.

11 *See id.* art. 6(1)(f), at 36; *see also* Article 29 Data Prot. Working Party, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC, at 25–37, 844/14/EN WP 217 (Apr. 9, 2014) (elaborating on the three-part test).

12 *See* CIV. §§ 1798.100(a)–(b), 1798.120–.121.

concern is information asymmetry. Businesses know far more about the data they collect than consumers do, and the CCPA's primary intervention is to close that gap by mandating notice at or before the point of collection and giving consumers meaningful choices about how their information is used.[13] The statute is realistic about how the data economy functions and tries to make it more fair.[14]

These are genuinely different theories of regulation, and they produce different compliance obligations. The European model positions the State as a guardian of individual dignity, intervening before processing begins to ensure that every use of personal data has an affirmative legal justification.[15] The California model positions the State as a referee in a commercial marketplace, ensuring that consumers have enough information to make their own decisions about the tradeoffs involved in sharing personal data. One regime controls the supply side. The other empowers the demand side. Both are incomplete, and both have produced substantial bodies of regulatory detail that reward close reading.

That close reading is what this Article provides. It proceeds in distinct parts, each focused on a specific axis of comparison. Starting with Part II, it maps the regulatory architecture of both frameworks: the GDPR's consistency mechanism and the CCPA's delegation of rulemaking authority to the California Privacy Protection Agency. Part III turns to territorial scope and definitional boundaries, including the GDPR's expansive jurisdictional reach under article 3, the CCPA's threshold-based applicability, and the structural complications created by California's inclusion of the household as a unit of protection. From there, Part IV examines what each regime requires before data can be processed. This is where the lawful basis requirement and the CCPA's reasonable expectations test do their heaviest lifting. Part V compares individual rights and enforcement mechanisms, including the access, opt-out, and appeal rights, as well as the eighteen-category cybersecurity audit framework established in the

13 *See id.* § 1798.100(a); CAL. CODE REGS. tit. 11, § 7012 (2026).

14 *See generally* ALICE MARINI ET AL., DATAGUIDANCE & FUTURE OF PRIV. F., COMPARING PRIVACY LAWS: GDPR V. CCPA (2018), https://ec.europa.eu/futurium/en/system/files/ged/gdpr_ccpa_comparison-guide.pdf [https://perma.cc/J7U8-CZBG] (explaining the key provisions in the CCPA that focus on accountability and collection limitations, and how they differ from the GDPR).

15 *See* Schwartz & Peifer, *supra* note 7, at 123–26 (describing the European model as rooted in a conception of data protection as a precondition of individual "self-determination").

CCPA's new Automated Decisionmaking Technology (ADMT). Part VI addresses the most significant structural asymmetry between the two regimes: the GDPR's restrictive cross-border transfer framework versus the CCPA's silence on the geographic movement of data. Part VII closes with the contractual mechanisms both regimes use to extend regulatory standards through the supply chain.

II. REGULATORY ARCHITECTURE

The constitutional ambitions described above would mean very little without institutional machinery to enforce them. Both the GDPR and the CCPA have built that machinery, but they have built it very differently.

The GDPR operates through a distributed enforcement model that spans the entire European Economic Area (EEA).[16] Every Member State is required to establish at least one independent supervisory authority with the power to investigate, correct, and sanction violations.[17] The independence requirement is taken seriously. Article 52 mandates that each authority "shall act with complete independence in performing its tasks and exercising its powers," free from external instruction by government or any other body.[18] This is a design choice with real consequences. It means that data protection enforcement in Europe is structurally insulated from the kind of political pressure that can shape enforcement priorities in other regulatory contexts.[19]

Sitting above these national authorities is the European Data Protection Board (EDPB), a body with its own legal personality, composed of the heads of one supervisory authority from each Member State and the European Data Protection Supervisor.[20] The EDPB's primary function is harmonization. It issues guidelines, recommendations, and best practices on contested doctrinal questions, and it administers the consistency mechanism that prevents the twenty-seven Member States from drifting into incompatible interpretations of the same regulation.[21] That con-

16 *See* Commission Regulation 2016/679, arts. 51–76, 2016 O.J. (L 119) 1, 65–80 (EU); *see also* Agreement on the European Economic Area, art. 36, 1994 O.J. (L 1) 1, 13 (incorporating GDPR into EEA law).

17 *See* Commission Regulation 2016/679, arts. 51(1), 52(1), 2016 O.J. (L 119) 1, 65–66 (EU).

18 *See id.* art. 52(1)–(2), at 66.

19 *See* Schwartz, *supra* note 2, at 790–95 (analyzing the GDPR's independence requirements as a mechanism for preserving the credibility of the fundamental rights framework).

20 *See* Commission Regulation 2016/679, art. 68(1)–(3), 2016 O.J. (L 119) 1, 76 (EU).

21 *See id.* arts. 63–64, 70(1), at 73–74, 76–78.

sistency mechanism is the architecture's pressure valve. When a national authority proposes a decision with cross-border implications, the EDPB can intervene to ensure the outcome is consistent with how the regulation is being applied elsewhere in the Union.[22]

Day-to-day enforcement, though, happens at the national level. Each supervisory authority serves as the frontline regulator for data subjects and businesses within its jurisdiction. For cross-border processing, the GDPR uses what it calls a "one-stop-shop" model: a single lead supervisory authority, determined by the location of the controller's main establishment, serves as the primary point of contact for the business.[23] The idea is efficiency. A company headquartered in Dublin should not have to negotiate simultaneously with twenty-seven different regulators. But the lead authority does not have the final word. Under article 60, it must share its draft decision with all concerned supervisory authorities, and if any of them raises a "relevant and reasoned objection," the lead authority must either accommodate the objection or refer the matter to the EDPB for binding dispute resolution.[24] In practice, this process has been slow and contentious. The Irish Data Protection Commission's (IDPC) handling of complaints against major U.S. tech companies drew years of criticism from other European regulators, and the EDPB has had to use its article 65 dispute resolution power on multiple occasions to override draft decisions it considered too lenient.[25] The result has been persistent tension between the one-stop-shop model's promise of regulatory efficiency and the reality that a single under-resourced authority can become a chokepoint for enforcement across the entire Union.

The article 65 procedure is, in effect, the EDPB's override power. When a concerned supervisory authority raises a relevant and reasoned objection to the lead authority's draft decision and the lead authority declines to follow it, the dispute lands on the EDPB's desk.[26] The Board then adopts a binding decision by a two-thirds majority of its members.[27] The lead authority has no discretion to ignore the result. It must adopt its final decision on

22 *See id.* art. 64, at 73–74.

23 *See id.* arts. 4(16), 56(1), at 34, 67; *id.* recitals 127–28, at 23–24.

24 *Id.* arts. 60(3)–(4), 65(1), at 71, 74–75.

25 *See* JOHNNY RYAN, IRISH COUNCIL FOR C.L., ECONOMIC & REPUTATIONAL RISK OF THE DPC'S FAILURE TO UPHOLD EU DATA RIGHTS 1, 4–6, 8–10 (Mar. 2021) (documenting delays in Irish enforcement of cross-border GDPR complaints).

26 *See* Commission Regulation 2016/679, art. 65(1)(a), 2016 O.J. (L 119) 1, 74 (EU).

27 *See id.* art. 65(2), at 75.

the basis of the Board's binding decision "without undue delay and at the latest by one month" of notification.[28] This is a remarkable delegation of authority. A supranational body composed of national regulators can, by majority vote, dictate the enforcement outcome in a case that a national authority investigated, drafted, and attempted to resolve on its own terms. The procedure has been used in several high-profile disputes, most notably in the EDPB's binding decisions directing the IDPC to impose substantially higher fines and broader corrective measures on Meta than the Commission had initially proposed.[29] The costs of this architecture are real. The multi-stage process of draft circulation, objection, Board deliberation, and final adoption routinely extends enforcement timelines by months, and in some cases by years. The IDPC's processing of the original *Schrems II* complaint is a well-known example, but it is hardly unique.[30] Speed is the tradeoff the GDPR makes for consistency. Whether that tradeoff is worth it depends on your perspective, but the structural choice is deliberate. The drafters of the GDPR were more concerned about regulatory fragmentation than regulatory delay, and the architecture reflects that priority. There is also a strategic dimension. The consistency mechanism functions as a check on forum shopping. A company that establishes itself in a Member State perceived as more permissive does not get to keep the benefit of that choice if other regulators object and the EDPB steps in.[31] The article 65 procedure is designed precisely to prevent that outcome: regulatory competition among Member States is limited by the Board's power to impose a uniform floor.

California took a different institutional path, and it took it in two steps.

When the CCPA went into effect in January 2020, enforcement belonged exclusively to the California Attorney General.[32] That was a traditional prosecutorial model: the Attorney General

28 *Id.* art. 65(6), at 75.

29 *See* Eur. Data Prot. Bd., Binding Decision 1/2023 on the Dispute Submitted by the Irish SA on Data Transfers by Meta Platforms Ireland Limited for Its Facebook Service (Art. 65 GDPR), ¶¶ 273–74 (Apr. 13, 2023), https://www.edpb.europa.eu/system/files/2023-05/edpb_bindingdecision_202301_ie_sa_facebooktransfers_en.pdf [https://perma.cc/F65G-ZWUE] (ordering the IDPC to impose higher fines due to aggravating factors).

30 *See* Eur. Parliament's Pol'y Dep't for Citizens' Rts. and Const. Affs., *Exchanges of Personal Data After the* Schrems II *Judgment*, § 2.3.1.2, at 31–33, PE 694.678 (2021) (discussing bottlenecks).

31 *See* ORLA LYNSKEY, THE FOUNDATIONS OF EU DATA PROTECTION LAW 67–68 (Paul Craig & Gráinne de Búrca eds., 2015) (analyzing the one-stop-shop mechanism's vulnerability to strategic corporate location decisions).

32 *See* CAL. CIV. CODE § 1798.155(a) (West 2025).

(AG) could bring civil actions for statutory damages, but there was no dedicated privacy regulator, no rulemaking apparatus beyond the AG's authority to adopt implementing regulations, and no administrative adjudication process.[33] The California Privacy Rights Act (CPRA) changed that. Approved by California voters in November 2020, Proposition 24 created the California Privacy Protection Agency (CPPA), which is described as "the first dedicated privacy enforcement agency in the United States."[34] The statute vests the CPPA with "full administrative power, authority, and jurisdiction to implement and enforce" the CCPA.[35] That is broad language, and the Agency has interpreted it broadly.

What makes the CPPA structurally distinctive is its enforcement mandate and its rulemaking power. The Agency operates under the California Administrative Procedure Act and has used notice-and-comment rulemaking cycles to build out the operational substance of the CCPA in ways the statutory text left open.[36] The ADMT regulations, the cybersecurity audit requirements, the risk assessment framework, and the insurance provisions all emerged from the Agency's regulatory process, not from the legislature.[37] This is a meaningful distinction from the European model. European Data Protection Authorities (DPAs) have investigative, corrective, and advisory powers under GDPR article 58, and they issue guidance that carries significant practical weight. But they do not engage in the kind of quasi-legislative gap-filling that the CPPA performs through formal rulemaking.[38] The CPPA does not just interpret the statute. It finishes writing it.

The Agency is governed by a five-member board, and the appointment structure deliberately fragments political control.[39] The Governor appoints the chair.[40] The AG, the Senate Rules

33 *See* CAL. CODE REGS. tit. 11, §§ 999.300–.341 (2026) (effective Aug. 14, 2020).

34 *See* CIV. § 1798.199.10; *see also* CAL. SEC'Y OF STATE, TEXT OF PROPOSED LAWS: CALIFORNIA GENERAL ELECTION §§ 2, 24, at 42–43, 71 (2020), https://vig.cdn.sos.ca.gov/2020/general/pdf/topl.pdf [https://perma.cc/J68E-Q3R6] (describing the CPPA as a first-of-its-kind agency); *CCPA vs CPRA: What Changed in California Privacy Law*, PRYVII, https://pryvii.com/en/compare/ccpa-vs-cpra [https://perma.cc/AU6W-3JV5] (last visited Apr. 17, 2026).

35 CIV. § 1798.199.10(a).

36 *See id.* § 1798.185 (enumerating specific rulemaking directives).

37 *See* tit. 11, §§ 7100–7222.

38 *See* Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1767–75 (2021) (analyzing the CPPA's rulemaking authority as a structurally distinct approach to privacy governance compared to European DPA advisory models).

39 *See* CIV. § 1798.199.10(a).

40 *Id.*

Committee, and the Speaker of the Assembly each appoint one additional member.[41] The fifth member is appointed by the Governor and all members must be Californians with expertise in data privacy.[42] The design is meant to insulate the Agency from any single branch or officeholder, an aspiration that echoes GDPR article 52's requirement that European supervisory authorities act with "complete independence."[43] But the analogy only goes so far. European DPA independence is anchored in EU primary law and the Charter of Fundamental Rights; the CPPA's independence is a creature of state statute, and while Proposition 24 included provisions making amendment difficult, the institutional safeguard is not constitutionally entrenched in the way its European counterparts are.[44] One other structural point worth noting: the AG did not lose enforcement authority when the CPPA was created. The two share concurrent jurisdiction, which means that California's privacy regime now has two independent enforcement actors.[45] The Agency can investigate, hold administrative hearings, impose fines up to $7,500 per intentional violation, and issue cease-and-desist orders.[46] And the AG can still bring civil enforcement actions on a parallel track. That is a considerable amount of enforcement firepower concentrated in a single state.

So far, the comparison has focused on institutional structure: who regulates, how they're appointed, and what powers they hold. But there is another structural difference that shapes how these regimes actually function in practice, and it has to do with who gets to complain and what happens when they do.

Under the GDPR, any data subject has the right to lodge a complaint with a supervisory authority.[47] That complaint triggers a legal obligation: the authority must inform the complainant of the progress and outcome of the complaint, including the possibility of a judicial remedy.[48] If the authority fails to act, the data subject can sue the regulator itself.[49] And the data subject also has an independent right to bring a judicial action directly

41 *Id.*

42 *See id.*

43 Commission Regulation 2016/679, art. 52(1), 2016 O.J. (L 119) 1, 66 (EU).

44 *See* Schwartz, *supra* note 2, at 811–16 (discussing the treaty-level foundations of European DPA independence).

45 CIV. § 1798.199.10.

46 *Id.* §§ 1798.199.55, 1798.155.

47 Commission Regulation 2016/679, art. 77(1), 2016 O.J. (L 119) 1, 80 (EU).

48 *Id.* art. 77(2), at 80.

49 *Id.* art. 78(2), at 80 (providing a right to an effective judicial remedy where a supervisory authority "does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint").

against the controller or processor.[50] The practical consequence is that individuals function as a distributed enforcement mechanism. They can force regulatory action through complaints, challenge regulatory inaction through the courts, and pursue their own claims in parallel. The Court of Justice of the European Union (CJEU) has reinforced this architecture repeatedly, treating the right to lodge a complaint and the right to judicial review as essential components of the fundamental right to data protection.[51]

California made a different choice. The CCPA's private right of action is narrow by design. Section 1798.150 permits consumers to bring suit only for unauthorized access, theft, disclosure, or exfiltration of nonencrypted or nonredacted personal information resulting from a business's failure to implement and maintain reasonable security procedures and practices.[52] That covers data breaches, but it does not cover anything else. If a business ignores an access request, denies a deletion request without justification, or deploys dark patterns to prevent consumers from opting out, the consumer's only recourse is to file a complaint with the CPPA or the AG and hope that one of them acts on it.[53] For the full range of substantive CCPA rights, enforcement depends entirely on the discretion of state actors.

The California Legislature has had multiple opportunities to expand the private right of action and has declined each time.[54] Business groups have consistently opposed expansion, arguing that broad private litigation rights would generate abusive class action practice.[55] Whatever one thinks of that argument, the result is a regime where the individual consumer has meaningful leverage only in the breach context. For everything else, the consumer is a complainant, not a litigant. That is a fundamentally different relationship between the individual and the enforcement apparatus than what the GDPR provides, and it has downstream consequences for how effectively each regime's substantive rights translate into actual compliance pressure.

---

50 *Id.* art. 79, at 80.

51 *See* Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd (*Schrems II*), ECLI:EU:C:2020:559, ¶¶ 109, 174–76 (July 16, 2020) (emphasizing the obligation of supervisory authorities to act on complaints with "all due diligence"); *see also* LYNSKEY, *supra* note 31, at 177–85 (analyzing the enforcement role of individual complaint rights within the GDPR's institutional design).

52 CAL. CIV. CODE § 1798.150(a)(1) (West 2025).

53 *See id.* § 1798.199.40 (authorizing the CPPA to receive consumer complaints).

54 *See, e.g.*, Assemb. B. 1751, 2021–2022 Leg., Reg. Sess. (Cal. 2022) (proposing the expansion of private right of action to cover all CCPA violations, which failed in committee).

55 *See* Goldman, *supra* note 8, at 8 (discussing the political economy of the CCPA's limited private right of action).

III. TERRITORIAL SCOPE AND DEFINITIONS

Earlier, this Article addressed the normative foundations and institutional machinery of each regime. But none of that matters if the law doesn't reach you. Territorial scope determines who falls within the regulatory perimeter in the first place, and the GDPR and CCPA draw that perimeter in fundamentally different ways.

The GDPR's jurisdictional reach operates through two independent triggers, either of which is sufficient on its own.[56]

The first is the establishment criterion. Article 3(1) provides that the GDPR 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 within the Union."[57] The concept of establishment is deliberately flexible. Recital 22 defines it as "the effective and real exercise of activity through stable arrangements," a formulation broad enough to capture a branch office, a subsidiary, or even a single employee operating with a sufficient degree of permanence.[58] But the real bite of article 3(1) comes from the phrase "in the context of the activities of."[59] Processing does not need to be performed by the EU establishment itself. It is enough that the processing is "inextricably linked" to the establishment's activities.[60] The *Google Spain* decision is the leading example. Google's Spanish office sold advertising. Google's servers in the United States processed the data. The CJEU held that the processing fell under EU jurisdiction because the advertising revenue made the Spanish establishment's activities and the U.S. processing "inextricably linked."[61] For any company with a commercial presence in the EU, even a small one, that logic has significant reach.

The second trigger is the targeting criterion under article 3(2), and it extends the GDPR's jurisdiction to controllers and processors with no EU establishment at all. It applies when pro-

56 Commission Regulation 2016/679, art. 3, 2016 O.J. (L 119) 1, 32–33 (EU).

57 *Id.* art. 3(1), at 32.

58 *Id.* recital 22, at 4; *see also* Case C-230/14, Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, ECLI:EU:C:2015:639, ¶ 31 (Oct. 1, 2015) (holding that even "minimal" real activity through stable arrangements can constitute establishment).

59 Commission Regulation 2016/679, art. 3(1), 2016 O.J. (L 119) 1, 32 (EU).

60 *See* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, ECLI:EU:C:2014:317, ¶¶ 55–56 (May 13, 2014) (finding that Google Inc.'s processing of personal data was carried out "in the context of" its Spanish subsidiary's advertising sales, even though the subsidiary performed no data processing itself).

61 *Id.* ¶ 56.

cessing relates to offering goods or services to data subjects in the Union, whether or not payment is required, or to monitoring the behavior of data subjects within the Union.[62] The threshold question is intent. A website accessible from Paris does not, by that fact alone, fall under the GDPR.[63] The GDPR requires evidence that the controller intended to direct its activities toward individuals in one or more Member States. Recital 23 lists doctrinal indicators: use of a language or currency associated with a Member State, references to EU-based customers, or use of a country-specific top-level domain.[64] The monitoring prong captures behavioral tracking. Recital 24 specifies that tracking individuals on the internet to build profiles, analyze preferences, or predict behavior constitutes monitoring, provided the behavior takes place within the Union.[65] A U.S.-based analytics company with no office in Europe, no EU customers, and no intent to serve the European market can still fall under the GDPR if it tracks the browsing behavior of individuals located in France or Germany.[66] There is an administrative consequence that follows from article 3(2) jurisdiction: any controller or processor subject to the GDPR solely through the targeting criterion must designate a representative in the Union.[67] The representative serves as a point of contact for supervisory authorities and data subjects and can be held liable for compliance failures.[68] In practice, this requirement has proven difficult to enforce against entities with no EU assets or presence, but the obligation exists and regulators have begun to press on it.[69]

The monitoring prong deserves separate attention because its practical reach is enormous and its boundaries are poorly de-

62 Commission Regulation 2016/679, art. 3(2)(a)–(b), 2016 O.J. (L 119) 1, 33 (EU).

63 *See* Eur. Data Prot. Bd., Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3), at 17 (Nov. 12, 2019), https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf [https://perma.cc/2DE6-YKGR] (stating that "the mere accessibility of the controller's, processor's or an intermediary's website in the Union . . . is insufficient" (quoting Commission Regulation 2016/679, recital 23, 2016 O.J. (L 119) 1, 5 (EU))); *cf.* Joined Cases C-585/08 & C-144/09, Pammer v. Reederei Karl Schlüter GmbH & Hotel Alpenhof GesmbH v. Heller, ECLI:EU:C:2010:740 (Dec. 7, 2010) (establishing a similar targeting analysis under the Brussels I Regulation).

64 Commission Regulation 2016/679, recital 23, 2016 O.J. (L 119) 1, 5 (EU).

65 *Id.* recital 24, at 5.

66 *See* Christopher Kuner, *The Internet and the Global Reach of EU Law* 15–17 (Lond. Sch. of Econ. & Pol. Sci. L. Dep't, Working Paper No. 24/2017, 2017) (analyzing the extraterritorial implications of the monitoring criterion).

67 Commission Regulation 2016/679, art. 27, 2016 O.J. (L 119) 1, 48–49 (EU).

68 *Id.* art. 27(4)–(5), at 49.

69 *See* Eur. Data Prot. Bd., *supra* note 63, at 23–24, 28 (discussing the scope and limitations of the article 27 representative requirement).

fined. We have already seen the general framework: recital 24 captures tracking of individuals on the internet for the purpose of profiling, preference analysis, or behavioral prediction, provided the tracked behavior takes place within the Union.[70] What that means operationally is that a non-EU company deploying analytics pixels, behavioral advertising cookies, or fingerprinting scripts on a website visited by individuals in Germany or Italy may be processing personal data subject to the GDPR, even if the company has no office, no customers, and no commercial interest in Europe.[71] The trigger is the purpose of the tracking, not the location of the tracker. If the data collection is designed to analyze user behavior or build predictive profiles, and the users happen to be in the Union, article 3(2)(b) applies.[72] The jurisdictional logic is location-of-the-person, not location-of-the-business, and in a world where tracking scripts are deployed globally by default, the practical consequence is that the GDPR's reach extends well beyond any entity that consciously decided to serve the European market.[73] That breadth is by design. But it also creates enforcement gaps, because asserting jurisdiction over a company with no EU presence, no EU assets, and no EU representative is considerably easier on paper than in practice.

The CCPA draws its jurisdictional perimeter differently. The GDPR asks: are you processing data of people in the EU, and did you intend to reach them or monitor them? The CCPA asks: are you a for-profit business of sufficient commercial scale, doing business in California, and handling the personal information of California consumers?[74] Every element of that question matters. The statute applies only to for-profit legal entities that collect consumers' personal information, determine the purposes and means of processing, and do business in the State of California.[75] But meeting that definitional threshold alone is not enough. The entity must also satisfy at least one of three size-based criteria, as amended by the CPRA: (1) annual gross revenues exceeding $25,000,000; (2) buying, selling, or sharing the personal infor-

70 Commission Regulation 2016/679, recital 24, 2016 O.J. (L 119) 1, 5 (EU).

71 *See* Eur. Data Prot. Bd., *supra* note 63, at 20 (discussing the scope of the monitoring criterion in the context of internet tracking technologies).

72 *See* Lokke Moerel, *The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?*, 1 INT'L DATA PRIV. L. 28, 32–33 (2011) (analyzing the extraterritorial implications of behavioral targeting under EU data protection law).

73 *See* BRADFORD, *supra* note 3, at 132–33 (arguing that the GDPR's extraterritorial scope functions as a mechanism of unilateral regulatory globalization).

74 CAL. CIV. CODE § 1798.140(d)(1) (West 2026).

75 *Id.*

mation of 100,000 or more consumers or households annually; or (3) deriving 50% or more of annual revenue from selling or sharing consumers' personal information.[76] The phrase "doing business in California" is not independently defined by the CCPA; it imports the general concept from California tax and corporate law, which turns on whether the entity has sufficient economic nexus with the state.[77] The result is a jurisdictional model anchored in commercial identity and economic scale rather than in the act of processing itself. A small European startup that happens to collect data from a few California users is unlikely to meet any of the three thresholds. A major U.S. retailer with California customers almost certainly does. The CCPA's perimeter is narrower than the GDPR's, and deliberately so.

The three threshold triggers have already been described, so I won't restate them here except to note one detail worth emphasizing. The volume trigger counts consumers *or households*, which means that a smart home provider collecting data from a single connected device used by a four-person family may be counting one household rather than four individuals, but is still accumulating volume toward the 100,000 threshold.[78] The household concept does real jurisdictional work in the Internet of Things (IoT) context, and we will return to it below when discussing definitional scope.

The "doing business in California" requirement deserves a closer look because it is doing more structural work than it might appear. The CCPA does not define the phrase independently. Instead, it imports the concept from California's general corporate and tax law framework, where "'doing business' means actively engaging in any transaction for the purpose of financial or pecuniary gain or profit."[79] Some commentators have analogized this to the constitutional minimum contacts analysis under *International Shoe* and its progeny.[80] The analogy is tempting but im-

76 *Id.* § 1798.140(d)(1)(A)–(C); *see also* Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, *The European Union General Data Protection Regulation: What It Is and What It Means*, 28 INFO. & COMMC'NS TECH. L. 65, 72–74 (2019) (noting the CCPA's threshold-based applicability is a structural departure from the GDPR's universal coverage model).

77 *See* CAL. REV. & TAX. CODE § 23101 (West 2012) (defining "doing business" for franchise tax purposes).

78 *See* CIV. § 1798.140(d)(1)(B), (q).

79 REV. & TAX. § 23101(a); *see also* AMANDA SMITH, STATE OF CAL. FRANCHISE TAX BD., LEGAL RULING – 2022-01, at 3 (2022) (discussing economic nexus standards for out-of-state entities).

80 *See, e.g.*, Goldman, *supra* note 8, at 3–5 (2020) (noting the jurisdictional ambiguity of the "doing business" requirement).

precise. Minimum contacts is a constitutional floor imposed by the Due Process Clause on the exercise of personal jurisdiction; "doing business" under California law is a statutory coverage criterion that operates at a different level of analysis. The practical question for a non-California entity is whether its economic engagement with the California market is sufficient to bring it within the statute's scope, and administrative interpretations have leaned toward a broad reading that includes sustained digital commerce with California residents.[81] The result is a jurisdictional threshold that is more bounded than the GDPR's targeting criterion but still captures a wide range of entities operating in the digital economy.

Now, definitions. What counts as protected information under each regime? The GDPR's unit of protection is the natural person. Article 4(1) defines "personal data" as "any information relating to an identified or identifiable natural person."[82] The definition is intentionally broad. An identifiable person is anyone "who can be identified, directly or indirectly, . . . by reference to an identifier such as a name, an identification number, location data, [or] an online identifier."[83] That last category is where the definition shows its teeth. IP addresses, cookie strings, device fingerprints, advertising IDs: all of these qualify as personal data if they can be linked, even indirectly, to a specific individual.[84] The definition also maintains its grip on pseudonymized data. If the additional information needed to re-identify a data subject exists and is reasonably accessible, the data remains personal data subject to the full GDPR framework.[85] Only genuinely anonymous data, where the link to the individual has been irreversibly severed, falls outside the regulation.[86] The practical effect is that the GDPR casts an extraordinarily wide net. Almost any da-

81 *See California Consumer Privacy Act (CCPA)*, STATE OF CAL. DEP'T OF JUST.: OFF. OF THE ATT'Y GEN. (Mar. 13, 2024), https://oag.ca.gov/privacy/ccpa [https://perma.cc/J3VV-ADYT] (interpreting "doing business" broadly to encompass entities with recurring commercial interactions with California consumers).

82 Commission Regulation 2016/679, art. 4, 2016 O.J. (L 119) 1, 33 (EU).

83 *Id.*

84 *See* Case C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, ECLI:EU:C:2016:779, ¶¶ 38–49 (Oct. 19, 2016) (holding that dynamic IP addresses constitute personal data where the controller has legal means to obtain additional information enabling identification).

85 Commission Regulation 2016/679, recital 26, 2016 O.J. (L 119) 1, 5 (EU); *see also* Article 29 Data Prot. Working Party, Opinion 05/2014 on Anonymisation Techniques, at 9–10, 0829/14/EN WP216 (Apr. 10, 2014) (setting a high threshold for true anonymization and treating most pseudonymization techniques as insufficient to remove data from the GDPR's scope).

86 Commission Regulation 2016/679, recital 26, 2016 O.J. (L 119) 1, 5 (EU).

ta point that touches an individual, however indirectly, is presumptively within scope.[87]

The CCPA's definition of personal information is comparably broad in scope but structurally different in one important respect. Section 1798.140(v) defines personal information as information that "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[88] Those last two words are where the CCPA departs from the European model. The GDPR's definitional anchor is the natural person.[89] Full stop. The CCPA adds the household as a second, independent unit of protection.[90]

The CCPA defines what "household" means, and the definition is narrower than you might expect. Under section 1798.140, a household is a person or group of people who (1) reside at the same address and (2) share a common device or the same service provided by the business.[91] Both conditions must be met. A family of four sharing a Netflix account at the same address qualifies. Two roommates who each have their own separate accounts with a retailer probably do not, even though they share an address, because the business has not identified them as sharing a common account or identifier.

The household concept matters most in the IoT context, and a pair of examples helps illustrate why. Take a smart meter recording aggregate energy consumption for a residence. Under the GDPR, if the telemetry is aggregated at the household level and cannot be linked to a specific natural person's behavior, it may fall outside the definition of personal data entirely.[92] Under the CCPA, the same data is personal information by definition because it relates to a household.[93] The classification turns on the unit of protection, not the content of the data. Now consider a smart speaker capturing ambient audio in a shared living space.

87 *See* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1836–42 (2011) (analyzing the expansive reach of the EU's identification-based definition of personal data and its implications for regulatory scope).

88 CAL. CIV. CODE § 1798.140(v)(1) (West 2026).

89 Commission Regulation 2016/679, art. 1, 2016 O.J. (L 119) 1, 32 (EU).

90 *Id.*; *see* Schwartz, *supra* note 2, at 773, 816–17 (contrasting the EU's individual-centric data protection model with emerging U.S. approaches that recognize collective data interests).

91 CIV. § 1798.140(q).

92 *See* Article 29 Data Prot. Working Party, *supra* note 85, at 9 (noting that aggregation may, depending on context, prevent identification of individuals).

93 *See* CIV. § 1798.140(v)(1).

Under the GDPR, the controller faces an attribution problem: which natural person is the data subject for a given voice snippet? If attribution is impossible, the controller's obligations become murky.[94] The CCPA sidesteps that problem. The data relates to the household. Every voice snippet is personal information regardless of which family member was speaking.[95]

But the household concept creates its own set of problems, particularly around rights requests, which was recognized in a recent repeal of household specific provisions.[96] The CPPA's regulations initially required that when a consumer does not have a password-protected account with the business, the business may respond to a request to know or a request to delete household-level personal information only if all members of the household jointly submit the request and the business individually verifies each of them.[97] That requirement meant that one household member could not exercise rights over household data unless every other member of the household cooperated. If a spouse refused to participate in the verification process, the deletion request would fail. That is a procedural veto embedded in the rights architecture, and it has no analogue in the GDPR, where each data subject exercises rights independently as an individu-

94 *See* Eur. Data Prot. Bd., Guidelines 2/2019 on the Processing of Personal Data Under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects, ¶ 45 (Oct. 8, 2019), https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en [https://perma.cc/7KPP-9KPV] (discussing controller obligations where multiple data subjects are affected by the same processing operation).

95 *See* Lydia de la Torre, *What Is "Personal Information" Under the CCPA?*, CAL. LAWS. ASS'N (Sep. 2019), https://calawyers.org/privacy-law/what-is-personal-information-under-the-california-consumer-privacy-act/ [https://perma.cc/RAS8-NM32].

96 CAL. CODE REGS. tit. 11, § 7031(a) (repealed Mar. 29, 2023).

97 I*d.*; *see also* CYNTHIA COLE, MATTHEW BAKER & KATHERINE BURGESS, WOLTERS KLUWER, THE CCPA: FINAL REGULATIONS AND INSIGHT INTO KEY ADDITIONS EFFECTIVE IMMEDIATELY (Aug. 26, 2020), https://business.cch.com/srd/SP_The-CCPA-Final-Regulations_08-26-2020_final_locked.pdf [https://perma.cc/7N86-2E8V] (noting that "all members of a household must jointly submit requests and individually be verified"); Ken Dreifach et al., *Key Changes in the AG's Updated Proposed CCPA Regulations*, ZWILLGEN: BLOG (Mar. 20, 2020), https://www.zwillgen.com/ftc-state-ag/key-changes-california-ag-updated-proposed-ccpa-regulations/ [https://perma.cc/W2J4-F7RL] (observing that absent a password-protected household account, a business could only process a household request "if every member of the household submits a request, is independently verified by the business, and is able to show that they are currently members of that household").

The CPPA repealed the section as part of its first rulemaking package without replacing it. *See* No. 27-Z Cal. Regulatory Notice Reg. 770–75 (Jul. 8, 2022). The "household" concept survives in the statutory definition of personal information, California Civil Code § 1798.140(v)(1), but no procedural mechanism for household-level rights requests currently exists in the regulations.

al.[98] This tradeoff means the CCPA's household concept captures data that the GDPR's individual-centric model might miss, particularly in shared-device environments where attribution to a single person is difficult or impossible. But in its original form, the CCPA also introduced coordination costs that could prevent any single person from exercising rights over data they helped generate. Whether that tradeoff is worth it depends on how much weight you place on capturing shared-device data versus preserving the frictionless exercise of individual rights. That tension between definitional breadth and rights-exercise friction will resurface when we turn to the mechanics of individual rights in Part V.

IV. LAWFUL PROCESSING VS. PURPOSE LIMITATION

The most consequential difference between the GDPR and the CCPA is not who they regulate or how far they reach. It is the threshold question of what makes data processing permissible in the first place.

The GDPR and the CCPA give radically different answers.

The GDPR starts from prohibition. Article 6(1) provides that processing of personal data is lawful only if, and to the extent that, at least one of six enumerated legal bases applies.[99] No legal basis, no processing. The default state is that data processing is impermissible, and the controller bears the burden of establishing an affirmative justification before any processing begins.[100] This is a deliberate structural choice rooted in the GDPR's origins as a fundamental rights instrument. Articles 7 and 8 of the EU Charter of Fundamental Rights guarantee respect for private life and protection of personal data, and the CJEU has consistently treated the requirement of a lawful basis as the mechanism through which those guarantees are operationalized.[101] The six bases are consent, contractual necessity, legal obligation, vital interests, public interest, and legitimate interests.[102] In practice, most commercial processing relies on either consent or le-

98 *See* Commission Regulation 2016/679, arts. 15–22, 2016 O.J. (L 119) 1, 43–46 (EU) (establishing individual rights exercisable by each data subject independently).

99 *Id.* art. 6(1), at 36.

100 *See* Article 29 Data Prot. Working Party, *supra* note 11, at 9–10 (describing the requirement of a legal basis as one of the most fundamental aspects of EU data protection law).

101 *See* Case C-311/18, *Schrems II*, ECLI:EU:C:2020:559, ¶ 171 (July 16, 2020) (grounding the GDPR's processing requirements in the Charter's fundamental rights guarantees).

102 Commission Regulation 2016/679, art. 6(1)(a)–(f), 2016 O.J. (L 119) 1, 36 (EU).

gitimate interests, and the latter is where the real doctrinal complexity lives.

The legitimate interests basis under article 6(1)(f) is the GDPR's pressure valve for commercial data use, and it is heavily contested.[103] The controller must satisfy a three-part analysis. First, it must identify a specific legitimate interest being pursued, which can be commercial in nature; direct marketing, fraud prevention, network security, and similar purposes all qualify.[104] Second, the processing must be "necessary" for the purpose of that interest.[105] The Article 29 Working Party interpreted this as requiring that there be no reasonable, less intrusive alternative available to achieve the same objective, though the standard is closer to a proportionality analysis than a strict least-intrusive-means test.[106] Third, the controller must balance its interest against the fundamental rights and freedoms of the data subject, and the data subject's interests must not override those of the controller.[107] This balancing exercise is not optional and it is not informal. The accountability principle under article 5(2) requires that the controller be able to demonstrate compliance, which in practice means documenting the legitimate interest assessment in writing.[108] For companies processing personal data at scale across multiple product lines, each with its own purpose and risk profile, the procedural burden is substantial.[109]

The CCPA takes a structurally different approach. There is no requirement that a business identify a lawful basis before collecting or processing personal information. Processing is permitted as a default commercial activity.[110] The constraints come after the fact, through disclosure obligations, purpose limitation, and proportionality requirements, rather than through an up-

103 Eur. Data Prot. Bd., Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(f) GDPR, ¶¶ 12–18 (Oct. 8, 2024), https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_en [https://perma.cc/5DDF-2BNA].

104 *Id.* art. 6(1)(f), at 36; *see also id.* recital 47, at 9 (recognizing direct marketing as a potential legitimate interest).

105 *Id.* art. 6(1)(f), at 36.

106 *See* Article 29 Data Prot. Working Party, *supra* note 11, at 11, 29–30 (distinguishing the necessity requirement from absolute indispensability and framing it as a proportionality inquiry).

107 Commission Regulation 2016/679, art. 6(1)(f), 2016 O.J. (L 119) 1, 36 (EU).

108 *Id.* arts. 5, 24(1), at 35–36, 47; *see also* Eur. Data Prot. Bd., *supra* note 103, ¶¶ 12, 68 (public consultation version).

109 *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 1247–51 (7th ed. 2020) (discussing the compliance costs associated with the GDPR's lawful basis requirements).

110 *See* CAL. CIV. CODE § 1798.100(a)–(c) (West 2023).

front gatekeeping function. Section 1798.100(c) provides that a business's collection, use, retention, and sharing of personal information must be "reasonably necessary and proportionate" to the purposes for which the information was collected or processed.[111] The CCPA regulations operationalize this through section 7002's reasonable expectations framework: the five-factor test for determining whether processing is consistent with consumer expectations, the compatibility analysis for secondary uses, and the proportionality analysis that requires the business to use the minimum information necessary.[112] The difference from the GDPR is structural, not just tonal. The GDPR asks: do you have permission to process this data? The CCPA asks: are you being transparent about what you're doing with it, and is what you're doing reasonable? Both questions constrain processing, but they constrain it at different points in the lifecycle and through different mechanisms.[113]

It is worth pausing on what section 7002 accomplishes structurally, because the CCPA's critics sometimes describe it as a regime without meaningful processing constraints. That characterization is wrong.

The reasonable expectations test under section 7002(b) does not operate like a lawful basis. A business does not need to select from an enumerated list of justifications before processing begins.[114] But the five-factor inquiry imposes a functional discipline that is more rigorous than a pure notice-and-choice model would suggest. The question is not simply whether the business disclosed what it planned to do. The question is whether a reasonable consumer, given the nature of the relationship, the type and source of the data, and the clarity of the disclosures, would have expected the processing to occur.[115] That is a contextual, fact-intensive standard, and it has teeth. An email address collected to fulfill a purchase order cannot be quietly redirected into a cross-context behavioral advertising program. The consumer's

111 *Id.* § 1798.100(c).

112 CAL. CODE REGS. tit. 11, § 7002(b)–(d) (2026).

113 *See* Margot E. Kaminski & Gianclaudio Malgieri, *Algorithmic Impact Assessments Under the GDPR: Producing Multi-Layered Explanations*, 11 INT'L DATA PRIV. L. 125, 128–30 (2021) (contrasting ex ante authorization models with ex post accountability frameworks in data protection regulation).

114 *Cf.* Commission Regulation 2016/679, art. 6(1), 2016 O.J. (L 119) 1, 36 (EU) (requiring selection of one of six enumerated legal bases).

115 tit. 11, § 7002(b)(1)–(5).

expectations at the point of collection anchor what the business is permitted to do afterward.[116]

The compatibility analysis for secondary uses adds another layer. When a business wants to repurpose personal information for a new purpose, section 7002(c) requires it to evaluate the relationship between the original collection context and the proposed new use.[117] The regulation is explicit about where the line falls. A cloud storage provider that decides to feed user files into a facial recognition training pipeline is the kind of contextual leap that fails the compatibility standard.[118] And where neither the expectations test nor the compatibility analysis supports the new purpose, the business must obtain the consumer's consent before proceeding.[119] At that point, the CCPA starts to look structurally similar to the GDPR's treatment of secondary processing, which generally requires either a compatible purpose under article 6(4) or fresh consent.[120] The mechanisms are different. The GDPR routes the inquiry through a formal lawful basis framework; the CCPA routes it through expectations, compatibility, and consent as sequential filters. But the analytical destination is closer than the structural differences might suggest.

The proportionality standard in section 7002(d) reinforces this convergence. Even where the purpose is permissible, the business must demonstrate that its collection, use, and retention of personal information are reasonably necessary and proportionate to achieve that purpose, measured against the minimum information required, the potential negative impacts on consumers, and any additional safeguards.[121] The CCPA does not impose the GDPR's formal documentation requirements under the accountability principle.[122] But a business that cannot articulate why it needed the volume and type of data it collected, and why less intrusive alternatives would not have sufficed, will have difficulty defending itself in an enforcement proceeding before the

116 *See* CIV. § 1798.100(c) (requiring that collection, use, retention, and sharing be "reasonably necessary and proportionate" to disclosed purposes).

117 tit. 11, § 7002(c).

118 *Id.* (using the cloud-storage-to-facial-recognition scenario as an illustrative example of incompatible secondary use).

119 *Id.* § 7002(e).

120 *See* Commission Regulation 2016/679, art. 6(4), 2016 O.J. (L 119) 1, 37 (EU) (setting out factors for assessing compatibility of secondary purposes); Article 29 Data Prot. Working Party, Opinion 03/2013 on Purpose Limitation, at 21–26, 00569/13/EN WP 203 (Apr. 2, 2013) (analyzing the compatibility assessment under EU law).

121 tit. 11, § 7002(d).

122 *Cf.* Commission Regulation 2016/679, arts. 5(2), 24(1), 2016 O.J. (L 119) 1, 36, 47 (EU) (requiring controllers to demonstrate compliance through documented measures).

CCPA.[123] The absence of a formal documentation mandate does not mean the absence of compliance pressure. It just means the pressure comes from a different direction. The processing constraints described here define what businesses are permitted to do with personal data. The next question is what happens when individuals push back.

V. INDIVIDUAL RIGHTS AND ENFORCEMENT

The individual rights granted by both regimes look similar on the surface. Both provide access, deletion, and portability, and since the CPRA, the CCPA also recognizes a right to correction.[124] But the mechanics differ in ways that matter. The GDPR's right of access under article 15 entitles the data subject to a copy of their personal data along with detailed information about the purposes of processing, the categories of data concerned, the recipients, and the envisaged retention period, among other disclosures.[125] The CCPA's access right under section 1798.110 allows consumers to obtain both the categories and specific pieces of personal information a business has collected, though it does not require the same breadth of contextual detail about processing operations.[126] A CCPA response tells you what was collected. A GDPR response is supposed to tell you enough to evaluate whether the collection was lawful. On deletion, both frameworks impose conditions, but they structure them differently. The GDPR's right to erasure under article 17 is triggered only when one of several specified grounds is met, for instance, that the data is no longer necessary or that consent has been withdrawn, and is then subject to its own exceptions.[127] The CCPA's right to delete is triggered by a consumer request alone but is carved back by a broad set of statutory exceptions, including completing a transaction, detecting security incidents, and complying with legal obligations.[128] The GDPR places the initial burden on the data subject to establish a ground; the CCPA places it on the

123 *See* Chander, Kaminski & McGeveran, *supra* note 38, at 1780–85 (arguing that the CCPA's regulatory framework creates de facto accountability obligations through the mechanism of enforcement risk).

124 Commission Regulation 2016/679, arts. 15–17, 20, 2016 O.J. (L 119) 1, 43–44, 45 (EU); CAL. CIV. CODE §§ 1798.100, .105, .106, .130 (West 2023).

125 Commission Regulation 2016/679, art. 15(1)(a)–(h), 2016 O.J. (L 119) 1, 43 (EU); *see* Case C-434/16, Nowak v. Data Prot. Comm'r, ECLI:EU:C:2017:994, ¶ 57 (Dec. 20, 2017) (emphasizing that the access right serves the data subject's ability to verify lawfulness of processing).

126 CIV. § 1798.110(a)(1)–(3).

127 Commission Regulation 2016/679, art. 17(1)(a)–(f), (3)(a)–(e), 2016 O.J. (L 119) 1, 43–44 (EU).

128 CIV. § 1798.105(a), (d)(1)–(8).

business to establish an exception.[129] That allocation shapes how deletion disputes play out in practice.

The regulation of automated decision-making technology represents an area where the regulatory impetus was there as a concept, but in practice, the ambition diverged structurally. Under the GDPR, article 22(1) provides that a data subject has the right not to be subject to a decision based solely on automated processing that produces legal effects or similarly significant effects.[130] Whether this operates as a self-executing prohibition or a right the data subject must invoke remains contested, but the practical effect is a default restriction on fully automated consequential decisions.[131] Where an exception applies (contract necessity, authorization by EU or Member State law, or explicit consent), the controller must implement suitable safeguards, including at minimum the right to obtain human intervention, to express a point of view, and to contest the decision.[132] California's approach, finalized in the CPPA's 2025 ADMT regulations, takes a different path.[133] Rather than imposing a default restriction, the regulations require businesses that use automated decision-making technology to make a "significant decision," defined as a decision concerning financial services, housing, education, employment, or health care, to provide pre-use notice, offer consumers the right to opt out, respond to access requests concerning the logic and output of the technology, and make available a process to appeal automated decisions to a qualified human reviewer.[134] Both regimes want consequential automated decisions subject to human oversight and individual challenge. The divergence is in the mechanism. The GDPR starts from restriction and carves out exceptions. California starts from permission and layers on transparency, opt-out, and appeal rights.

The California framework does not reach as broadly as earlier drafts proposed. The CPPA's initial rulemaking would have captured technology that merely *facilitated* human decisions, but the final regulations narrowed the definition of ADMT to tech-

129 *See* Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 978–82 (2017) (analyzing the structural significance of burden allocation in privacy rights frameworks).

130 Commission Regulation 2016/679, art. 22(1), 2016 O.J. (L 119) 1, 46 (EU).

131 *See* Article 29 Data Prot. Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, at 19–20, 17/EN WP251rev.01 (Feb. 6, 2018) (interpreting article 22(1) as a prohibition).

132 Commission Regulation 2016/679, art. 22(2)–(3), 2016 O.J. (L 119) 1, 46 (EU).

133 *See* CAL. CODE REGS. tit. 11, §§ 7220–7222 (2026).

134 *Id.* §§ 7001(ddd), 7200(a), 7220–7222.

nology that "replace[s] . . . or substantially replace[s] human decisionmaking."[135] This is a more constrained trigger than the facilitation standard, yet it still addresses the hybrid decision-making problem that makes article 22 difficult to apply in practice. The regulations define "human involvement" to require that the reviewer understands the technology's output, affirmatively evaluates it, and has genuine authority to override it.[136] A human who is present in the decision chain but merely ratifies an algorithmic recommendation without independent analysis does not satisfy this standard, meaning the underlying technology would still qualify as ADMT, and the business would remain subject to the regulations' notice, opt-out, access, and appeal requirements. In this way, California targets the same concern that animates article 22: the risk that nominal human oversight masks substantively automated decision-making, but does so through a definitional mechanism rather than a default prohibition. The practical result is that businesses cannot insulate themselves from the ADMT framework simply by inserting a human reviewer into the process; they must demonstrate that the reviewer exercised meaningful discretion.[137]

The 2025 regulations operationalize these protections through specific notice and rights requirements for ADMT used in significant decisions.[138] Before using ADMT to make a significant decision about a consumer, a business must provide a pre-use notice that explains, in plain language, the purpose for which it will use the technology and how the technology processes personal information to reach the decision.[139] The consumer then has the right to opt out of that processing—a right that applies to decisions concerning employment, education, financial services, housing, and health care—and that enables consumers to prevent their personal information from being fed into automated systems that determine access to core economic and social opportunities.[140] Separately, consumers may request access to information about the business's use of ADMT, including the logic of the technology, its output, and how that output was used in the

135 *Id.* § 7001(e); Christine Lyon et al., *California Privacy Agency Narrows Proposed AI-Related Regulations*, FRESHFIELDS (May 14, 2025), https://blog.freshfields.us/post/102kb60/california-privacy-agency-narrows-proposed-ai-related-regulations [https://perma.cc/BKQ8-QG2G].

136 tit. 11, § 7001(e).

137 *See id.* §§ 7221–7222.

138 *Id.* §§ 7220–7221.

139 *Id.* § 7220.

140 *Id.* § 7221.

decision-making process.[141] This access right is subject to limitations: businesses are not required to disclose trade secrets or information that could compromise physical safety.[142] The GDPR imposes a parallel but differently structured transparency obligation. Article 15(1)(h) requires that data subjects receive meaningful information about the logic involved in automated decision-making, along with its significance and envisaged consequences, a standard that is broader in framing but less granular about specific outputs and their application to individual decisions.[143] The practical burden on California businesses is nonetheless substantial: they must be prepared to document and explain the logic of their automated systems, the data inputs, and the decisional pathway on a per-consumer basis upon a valid request.

The cybersecurity audit regulations represent one of the places where California has moved ahead of the GDPR, and it is worth being specific about what the state now requires. Beginning in 2027, businesses must conduct annual cybersecurity audits if their data processing presents a "significant risk" to consumer security.[144] Two independent triggers define the threshold. The first captures data brokers: businesses deriving 50% or more of annual revenue from selling or sharing personal information.[145] The second is conjunctive, requiring both annual gross revenues exceeding approximately $26,625,000 and the processing of personal information of more than 250,000 consumers or households, or sensitive personal information of more than 50,000 consumers.[146] A business that meets either trigger must have a professional—who is qualified, objective, and independent—conduct an annual audit, using recognized auditing standards.[147] That professional can be internal or external, but independence is mandatory either way.[148] The GDPR has nothing comparable. Article 32 requires controllers to implement appropriate technical and organizational security measures, and article 35 mandates data protection impact assessments for high-risk

141 *Id.* § 7222.

142 *Id.*

143 Commission Regulation 2016/679, art. 15(1)(h), 2016 O.J. (L 119) 1, 43 (EU).

144 tit. 11, § 7120(a).

145 *Id.* § 7120(b)(1).

146 *Id.* § 7120(b)(2).

147 *Id.* § 7122(a).

148 *Id. See generally* DANIEL J. SOLOVE & WOODROW HARTZOG, BREACHED!: WHY DATA SECURITY LAW FAILS AND HOW TO IMPROVE IT (2022) (arguing that data security regulation should move from reactive, breach-focused enforcement toward proactive systemic oversight mechanisms, including auditing requirements).

processing.[149] But neither provision requires a standardized annual audit, performed by an independent professional, with results certified to a regulator. California built a recurring compliance cycle. Europe left security implementation to the controller's judgment, subject to enforcement after the fact.

The scope of these audits is broad but flexible. The regulations enumerate eighteen categories the auditor must assess "if applicable" to the business's information system: authentication, encryption, access controls, vulnerability scanning, penetration testing, network monitoring, audit-log management, incident response, data retention and disposal, personnel security training, and several others.[150] The phrase "if applicable" is doing important work. The auditor exercises professional judgment in determining which categories are relevant to a particular business. A small e-commerce company and a cloud infrastructure provider will not face identical assessments.[151] The audit report documents the scope of the review, the policies assessed, the criteria applied, and the auditor's findings, which the business retains for at least five years.[152] But here is the part that matters for the regulatory relationship: what the business files with the CPPA each year is a signed certification of completion, not the full report.[153] The certification is due by April 1, with phased deadlines running from 2028 to 2030 depending on revenue tier.[154] The full report stays with the business unless the CPPA or the AG comes looking for it in an enforcement proceeding.[155] That creates an interesting incentive structure. The business knows the regulator can demand the report at any time, which means the report needs to be thorough and defensible even though no one outside the company may ever read it.[156]

VI. CROSS-BORDER TRANSFERS: THE STRUCTURAL ASYMMETRY

The widest structural gap between the GDPR and the CCPA has nothing to do with processing requirements or individual rights. It concerns the regulation of cross-border data flows, and the gap is not a difference of degree. One regime treats the geo-

149 Commission Regulation 2016/679, arts. 32, 35, 2016 O.J. (L 119) 1, 51–52, 53–54 (EU).

150 tit. 11, § 7123(c).

151 *See id.* § 7120.

152 *Id.* §§ 7122(g), 7123(e).

153 *Id.* § 7124.

154 *Id.* § 7121(a).

155 *See id.* §§ 7123–7124.

156 *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 630–35 (2014) (discussing how the threat of regulatory action creates compliance incentives that operate independently of formal enforcement).

graphic movement of personal data as an independent regulatory event requiring its own legal justification. The other does not regulate it at all.

The GDPR's position follows from its constitutional foundations. If data protection is a fundamental right guaranteed by articles 7 and 8 of the Charter, then that right cannot be extinguished simply because personal data crosses a border.[157] The CJEU made this explicit in *Schrems II*, holding that the level of protection guaranteed by the GDPR and the Charter must travel with the data.[158] Chapter V of the GDPR operationalizes that principle through a restrictive framework governing transfers to countries outside the EEA.[159] California took a fundamentally different path. The CCPA regulates the commercial character of the downstream disclosure, governing data flows through its definitions of sale, sharing, and the service provider, contractor, and third-party taxonomy, without regard to where the recipient sits.[160] Geography is simply absent from the analysis.[161]

Chapter V follows the same prohibition-with-exceptions logic that runs through the rest of the GDPR. Article 44 restricts all transfers to third countries unless one of the regulation's prescribed mechanisms is satisfied.[162] The most comprehensive is an adequacy decision under article 45. The Commission examines the third country's legal framework and, if it concludes that the country provides a level of protection "essentially equivalent" to that of the Union, adopts a decision permitting transfers without additional safeguards.[163] That is a high bar. It requires more than formal legal protections; it requires effective enforcement, independent supervision, and adequate redress.[164] Where no adequacy decision exists, the exporter must provide "appropriate

157 Charter of Fundamental Rights of the European Union arts. 7–8, Oct. 26, 2012, 2012 O.J. (C 326) 391.

158 Case C-311/18, *Schrems II*, ECLI:EU:C:2020:559, ¶ 105 (July 16, 2020).

159 Commission Regulation 2016/679, arts. 44–49, 2016 O.J. (L 119) 1, 60–65 (EU); *see* BRADFORD, *supra* note 3, at 132–38 (analyzing chapter V as a mechanism for projecting EU regulatory standards onto third countries through the adequacy process).

160 CAL. CIV. CODE § 1798.140 (West 2026).

161 *See* Paul M. Schwartz, *supra* note 2, at 830–35 (2019) (contrasting the EU's data sovereignty model with U.S. approaches that treat cross-border flows as a commercial rather than constitutional question).

162 Commission Regulation 2016/679, art. 44, 2016 O.J. (L 119) 1, 60 (EU).

163 *Id.* art. 45, at 61–62; Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r (*Schrems I*), ECLI:EU:C:2015:650, ¶ 73 (Oct. 6, 2015) (establishing the "essentially equivalent" standard).

164 *See* Christopher Kuner, *Reality and Illusion in EU Data Transfer Regulation Post* Schrems, 18 GERMAN L.J. 881, 893–97 (2017) (analyzing the substantive demands of the adequacy standard after *Schrems I*).

safeguards" while ensuring that enforceable data subject rights and effective legal remedies remain available.[165] Standard contractual clauses adopted by the Commission are the most widely used instrument, establishing binding obligations on the data importer and enforceable rights for data subjects as third-party beneficiaries.[166] Binding corporate rules, approved codes of conduct, and certification mechanisms are also available, though less commonly relied upon.[167] And where neither adequacy nor appropriate safeguards are in place, transfers may proceed only under the narrow derogations of article 49: explicit consent, contractual necessity, important reasons of public interest, and a handful of other limited bases.[168]

The stakes of this framework became concrete in *Schrems II*. The CJEU struck down the EU-U.S. Privacy Shield adequacy decision, holding that U.S. law failed to provide an essentially equivalent level of protection for personal data transferred from the Union.[169] The Court identified two deficiencies: the lack of proportionality constraints on U.S. surveillance programs operating under section 702 of the Foreign Intelligence Surveillance Act and Executive Order 12333, and the absence of effective judicial redress for EU data subjects whose data was accessed by U.S. intelligence authorities.[170] But the Court went further. It held that exporters relying on standard contractual clauses bear an independent obligation to assess whether the legal framework of the recipient country permits the importer to comply with the protections set out in the clauses.[171] Where the answer is no, the exporter must implement supplementary measures sufficient to close the gap, or suspend the transfer entirely.[172] The practical consequence is that every cross-border transfer decision now requires something close to a country-level legal risk assessment. Compliance teams must evaluate foreign surveillance authori-

165 Commission Regulation 2016/679, art. 46(1), 2016 O.J. (L 119) 1, 62 (EU).

166 *Id.* art. 46(2)(c), at 62.

167 *Id.* arts. 46(2)(e)–(f), 47, at 62–64.

168 *Id.* art. 49(1), at 64.

169 Case C-311/18, *Schrems II*, ECLI:EU:C:2020:559, ¶¶ 65, 201 (July 16, 2020).

170 *Id.* ¶¶ 178–185; *see also* Kuner, *supra* note 164, at 900–05 (anticipating the redress gap as a structural vulnerability in transatlantic transfer mechanisms).

171 Case C-311/18, *Schrems II*, ECLI:EU:C:2020:559, ¶ 134.

172 *Id.* ¶ 135; *see also* Eur. Data Prot. Bd., Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data (June 18, 2021), https://www.edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf [https://perma.cc/NR3G-W9R6] (explaining that when relevant legislation is lacking a party may decide to suspend, transfer, or implement supplementary measures).

ties, judicial independence, and the enforceability of contractual protections in legal systems they may know nothing about.[173]

The Commission's response was the EU-U.S. Data Privacy Framework (DPF), adopted in July 2023.[174] Its foundation is Executive Order 14086, which introduced necessity and proportionality constraints on U.S. signals intelligence activities and established a two-tier redress mechanism.[175] At the first tier, the Civil Liberties Protection Officer (CLPO) within the Office of the Director of National Intelligence investigates complaints alleging that U.S. surveillance activities violated the safeguards established by the Executive Order.[176] At the second tier, the complainant may appeal to the Data Protection Review Court (DPRC), a newly created body authorized to review the CLPO's determinations, obtain access to classified information, and issue binding remedial orders directed at U.S. intelligence agencies.[177] The entire apparatus is, candidly, an institutional workaround. The United States has no comprehensive data protection authority and no tradition of treating intelligence oversight as a judicial function in the European sense. So the Executive Order constructed a bespoke tribunal designed to satisfy a foreign court's requirements for effective judicial protection under article 47 of the Charter.[178] The European General Court upheld that conclusion in September 2025, dismissing a challenge to the adequacy decision and finding that the DPRC's fixed terms, removal protections, access to classified evidence, and obligation to issue reasoned decisions satisfied EU independence and impartiality

173 *See generally* Peter Swire & DeBrae Kennedy-Mayo, *The Risks to Cybersecurity from Data Localization — Organizational Effects*, 8 ARIZ. L.J. EMERGING TECHS. 1 (2025) (documenting the operational burdens that post-*Schrems II* compliance requirements impose on organizations managing cross-border data transfers); PETER SWIRE & DEBRAE KENNEDY-MAYO, FIVE CONCERNS ABOUT HARD DATA LOCALISATION WITHIN THE EUROPEAN UNION 2–3 (2020), https://peterswire.net/wp-content/uploads/Comments-to-EDPB-Recommendations-by-Swire-and-Mayo-2020.pdf [https://perma.cc/6E9H-KGY3] (criticizing the practical feasibility for many organizations of the EDPB's approach to supplementary measures and its implicit localization pressure).

174 *See* Commission Implementing Decision 2023/1795, 2023 O.J. (L 231) 118 (EU).

175 *See* Exec. Order No. 14086, 87 Fed. Reg. 62283 (Oct. 14, 2022).

176 *See id.* § 3(c).

177 *See id.* § 3(d); 28 C.F.R. pt. 201 (2022).

178 *See* Theodore Christakis, *Schrems III? First Thoughts on the EDPB Post-*Schrems II *Recommendations on International Data Transfers (Part 1)*, EUR. L. BLOG (Nov. 13, 2020), https://www.europeanlawblog.eu/pub/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-3/release/1 [https://perma.cc/V85A-A4FL] (characterizing the DPF as an attempt to construct functional equivalence with EU judicial protection standards through executive rather than legislative action).

standards.[179] That ruling provides stability for now. But the EDPB has already flagged concerns about government acquisition of personal data from commercial data brokers, a channel that falls entirely outside Executive Order 14086's scope and therefore outside the DPF's protective architecture.[180]

The CCPA has no equivalent to chapter V. California does not condition the movement of personal information on the legal adequacy of the destination country, and it draws no distinction between domestic and international transfers as a regulatory matter.[181] What California regulates is the commercial character of the downstream disclosure. The statute defines "sale" as disclosing personal information to a third party for monetary or other valuable consideration, and "sharing" as disclosing personal information for cross-context behavioral advertising; each carries its own notice and opt-out obligations.[182] Disclosures to service providers and contractors are permitted without opt-out rights so long as the recipient is bound by a written contract restricting its use of the data to the business purposes specified in the agreement.[183] None of these restrictions turn on geography. A business that discloses consumer data to a service provider in Texas faces exactly the same obligations as one that discloses to a service provider in Bangkok or Berlin. If the contractual and transactional requirements are satisfied, the location of the recipient is legally irrelevant.[184] The GDPR treats the cross-border movement of personal data as an independent regulatory event requiring its own legal justification. The CCPA treats it as a non-event, fully governed by the same sale, sharing, and service provider rules that apply to any other disclosure.

That indifference to geography runs deep. Nothing in the CCPA or the California regulations requires a business to assess the privacy laws of a foreign jurisdiction before transferring per-

179 Case T-553/23, Latombe v. Eur. Commission, ECLI:EU:T:2025:831, ¶ 38–63 (Sept. 3, 2025).

180 *See* Eur. Data Prot. Bd., EDPB Report on the First Review of the European Commission Implementing Decision on the Adequate Protection of Personal Data Under the EU–U.S. Data Privacy Framework, at 20 (Nov. 4, 2024), https://www.edpb.europa.eu/system/files/2024-11/edpb_report_20241104_reportonfirstreviewofeu-u.s.dpf_en.pdf [https://perma.cc/Y9SK-3SW6].

181 *See generally* CAL. CIV. CODE §§ 1798.100–.199.100 (West 2026) (containing no provision analogous to GDPR articles 44–49).

182 CIV. § 1798.140(ad)(1), (ah)(1), 1798.120–.121.

183 *See id.* § 1798.140(ag)(1), (j)(1).

184 *See* Anupam Chander, *Is Data Localization a Solution for* Schrems II*?*, 23 J. INT'L ECON. L. 771, 779–82 (2020) (contrasting regulatory approaches that condition data flows on destination-country adequacy with those that rely on transactional controls).

sonal information there.[185] The same goes for transfers to other U.S. states. There is no transfer impact assessment, no equivalence finding, no supervisory approval. The CCPA's theory of protection runs through the contract, not the border. Service providers and contractors are bound by written agreements that prohibit them from retaining, using, or disclosing personal information outside the direct business relationship, from selling or sharing it, and from combining it with personal information obtained from other sources.[186] If those contractual constraints hold, California treats the data as adequately protected. It does not matter whether the server is in Sacramento or Singapore.[187]

The GDPR operates on a fundamentally different premise. Chapter V is not just a compliance mechanism. It is a tool of regulatory projection, and frankly, it works. The adequacy process creates direct incentives for third countries to reshape their domestic privacy frameworks to secure an adequacy finding. Japan revised its Act on the Protection of Personal Information before obtaining its adequacy decision.[188] South Korea and the United Kingdom undertook similar reforms.[189] That is a remarkable amount of leverage for a single chapter of a regulation. California has no comparable provision and, to be clear, is not trying to have one. Its regulatory energy is directed inward, toward the contractual supply chain, not outward toward the legal systems of trading partners. The result is a gap that goes beyond regulatory design. It reflects two different theories of what data protection law is for. The GDPR pursues a form of data sovereignty rooted in fundamental rights, seeking to ensure that protection follows the data wherever it travels. The CCPA pursues transactional integrity. It wants to make sure businesses honor the terms of the commercial relationship through which the data was collected. Neither approach is obviously wrong. But the structural consequences for multinational compliance are significant, and

185 *See generally* CIV. §§ 1798.100–.199.100 (failing to contain a provision requiring consideration of foreign laws before transfer of data); CAL. CODE REGS. tit. 11, §§ 7000–7102 (2026) (failing to contain a provision requiring consideration of foreign laws before transfer of data).

186 CIV. § 1798.140(ag)(1)(B), (j)(1).

187 *See* Hoofnagle, van der Sloot & Borgesius, *supra* note 76, at 88–90 (noting the absence of any cross-border transfer restriction in the CCPA as a fundamental structural departure from the European model).

188 *See* Commission Implementing Decision 2019/419, 2019 O.J. (L 76) 1, 31–32 (EU); *see also* BRADFORD, *supra* note 3, at 132–38 (documenting the adequacy mechanism as a driver of regulatory convergence in third countries).

189 Commission Implementing Decision 2022/254, 2022 O.J. (L 44) 1, 29 (EU) (South Korea); Commission Implementing Regulation 2021/1772, 2021 O.J. (L 360) 1, 2–3 (EU) (United Kingdom).

companies attempting to operate under both regimes simultaneously will discover that the two frameworks cannot simply be stacked on top of each other.

VII. CONTRACTUAL FLOW-DOWNS AND PRIVATE GOVERNANCE

Both regimes have converged on the same basic insight: if you want privacy law to mean anything downstream, you have to write it into the contracts. The GDPR and the CCPA each require businesses to impose data protection obligations on the entities that process personal information on their behalf. But they do it differently, and the differences reflect the broader architectural choices each regime has made.[190]

The GDPR's approach runs through article 28, which requires that any processing carried out by a processor be governed by a binding contract or legal act.[191] The required terms are specific and nonnegotiable. The processor must act only on the controller's documented instructions. It must ensure that authorized personnel are bound by confidentiality. It must implement article 32 security measures. It must comply with the rules on subprocessor engagement, including obtaining the controller's prior authorization. It must assist the controller with data subject rights requests, breach notifications, impact assessments, and prior consultations with supervisory authorities. At the end of the relationship, it must delete or return all personal data. And it must submit to audits.[192] Eight mandatory clauses, oriented around a single principle: the processor is an extension of the controller, and the contract exists to keep it on a leash.

The CCPA takes a different angle. Its contract requirements exist not to govern the relationship between a controller and its agent, but to prevent a business disclosure from being reclassified as a sale or sharing of personal information.[193] If a business

190 *See* W. Gregory Voss, *European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting*, 72 BUS. LAW. 221, 226–27, 233 (2017) (analyzing the GDPR's contractual flow-down requirements as a mechanism for extending regulatory standards through private ordering).

191 Commission Regulation 2016/679, art. 28(3), 2016 O.J. (L 119) 1, 49–50 (EU); *see also* Eur. Data Prot. Bd., Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR, ¶¶ 108–43 (Sep. 2, 2020), https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf [https://perma.cc/BPU2-KW5G] (interpreting the mandatory content requirements of article 28 contracts).

192 Commission Regulation 2016/679, art. 28(3), 2016 O.J. (L 119) 1, 49–50 (EU).

193 CAL. CIV. CODE § 1798.140(j)(1), (ag)(1) (West 2026); *see* Christy Harris & Charlotte Kress, *Examining Industry Approaches to CCPA "Do Not Sell" Compliance*, FUTURE OF PRIV. F. (Dec. 19, 2019), https://fpf.org/blog/examining-industry-approaches-to-ccpa-do-not-sell-compliance/ [https://perma.cc/NW8J-PGED].

discloses personal information to a service provider or contractor without a qualifying written contract, that disclosure may trigger the CCPA's opt-out rights. That is the last thing most businesses want.[194] So the contract does real work. It must prohibit the recipient from selling or sharing the personal information, retaining or using it for any purpose other than the business purposes specified in the agreement, using it outside the direct business relationship, and combining it with personal information obtained from other sources.[195] The CPPA's regulations add further layers, requiring the contract to obligate the service provider or contractor to comply with the CCPA, provide the same level of privacy protection as the statute requires of businesses, and grant the business monitoring and audit rights.[196] Contractors must also certify that they understand and will comply with these restrictions.[197] The orientation is different from article 28. The GDPR's contract regime is about ensuring the processor follows the controller's instructions and cooperates with regulatory obligations. The CCPA's regime is about preventing unauthorized commercialization of consumer data. The GDPR asks: is the processor doing what it was told? The CCPA asks: is the recipient doing something with this data that the consumer did not sign up for?

Both regimes require these obligations to flow downstream. It is not enough to bind your immediate vendor. The obligations have to follow the data through the entire processing chain.

Under the GDPR, article 28(4) is explicit: where a processor engages a sub-processor, the same data protection obligations from the controller-processor contract must be imposed on the sub-processor by way of a separate contract.[198] If the sub-processor fails to meet those obligations, the initial processor remains fully liable to the controller.[199] That is a strict liability chain. The controller does not get to plead ignorance about what is happening three levels down. California's regulations take a parallel approach. Section 7051(b) requires that a service provider or contractor who subcontracts with another person must enter into a contract with the subcontractor that complies with the

194 See CAL. CODE REGS. tit. 11, § 7050(e) (2026).

195 CIV. § 1798.140(ag)(1)(A)–(D), (j)(1)(A)(i)–(iv).

196 *See* tit. 11, § 7051(a)(6)–(7).

197 CIV. § 1798.140(j)(1)(B).

198 Commission Regulation 2016/679, art. 28(4), 2016 O.J. (L 119) 1, 50 (EU).

199 *Id.*; see *also* Eur. Data Prot. Bd., *supra* note 191, ¶¶ 147–55 (discussing the cascading liability structure for sub-processing under article 28(4)).

full set of CCPA contractual requirements.[200] The statute separately requires that if a contractor engages any other person to assist in processing, the engagement must be pursuant to a written contract binding the subcontractor to the same restrictions.[201] On both sides of the Atlantic, the result is the same: compliance obligations cascade down through the supply chain, and every link in the chain must be papered.[202]

What this creates, in practice, is a system of private governance. Both regimes have conscripted businesses into performing a regulatory function.[203] The GDPR's audit rights under article 28(3)(h) require the processor to make available all information necessary to demonstrate compliance and to allow for and contribute to audits and inspections.[204] The CCPA's regulations go further in one specific respect: they tie the business's own legal exposure to whether it exercises its oversight rights. Section 7051(c) provides that a business's due diligence of its service providers and contractors is a factor in determining whether the business had reason to believe the service provider was violating the CCPA.[205] A business that never enforces its contract terms, never audits, and never tests its vendor's compliance posture may lose the ability to argue that it did not know the vendor was misusing consumer data. That is a regulatory incentive to police your own supply chain, and a penalty for looking the other way. No agency has the resources to audit every data processing relationship in a modern digital economy. The GDPR and the CCPA both recognize this, and their shared solution is to turn the businesses themselves into the front line of enforcement, using contracts as the delivery mechanism for regulatory standards. The question that neither regime has fully answered is what happens when the business at the top of the chain lacks the technical capacity or commercial leverage to meaningfully audit the entities further down it.[206]

200 tit. 11, § 7051(b).

201 CIV. § 1798.140(j)(2).

202 *Cf.* Woodrow Hartzog, *The New Price to Play: Are Passive Online Media Users Bound by Terms of Use?*, 15 COMMC'N L. & POL'Y 405, 425–28 (2010) (examining the enforceability of terms of use agreements imposed on passive online users).

203 *Cf.* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 286–87 (2011) (documenting the emergence of corporate privacy management as a form of decentralized regulatory implementation).

204 Commission Regulation 2016/679, art. 28(3)(h), 2016 O.J. (L 119) 1, 49 (EU).

205 tit. 11, § 7051(c).

206 *See* Solove & Hartzog, *supra* note 156, at 640–45 (discussing the gap between regulatory expectations of corporate oversight and the practical capacity of businesses to monitor third-party data practices).

VIII. CONCLUSION

This Article set out to do something straightforward: read the primary sources of both regimes side by side and map where they align and where they diverge. The answer, in short, is that they diverge more than most compliance discussions acknowledge.

The GDPR is built on a fundamental rights architecture. It requires an affirmative legal basis before any processing begins. It treats cross-border data flows as an independent regulatory event, conditioning them on the adequacy of foreign legal systems or the adoption of binding contractual safeguards. It projects its standards outward, using the adequacy mechanism to reshape the domestic privacy laws of trading partners. And it backs all of this with a contractual flow-down regime that turns every processor agreement into a vehicle for regulatory enforcement. The intellectual commitment is to continuity of protection: the rights of the data subject should not diminish because a server sits in a different country.

The CCPA starts from a different place. It does not require a lawful basis for processing. It does not care where the data goes, as long as the commercial terms governing the disclosure are met. Its theory of protection runs through transparency, purpose limitation, and the contractual supply chain. The 2025 regulations on automated decision-making technology, cybersecurity audits, and risk assessments represent a significant maturation of the California model, but they do not change its fundamental orientation. California is regulating commercial conduct. The EU is regulating the conditions under which personal data may exist outside its borders.

That is a difference of kind, and it has practical consequences that anyone doing business across both regimes will recognize. A multinational company cannot simply map its GDPR compliance program onto its CCPA obligations and call it done. The triggers are different. The contractual architectures serve different purposes. The enforcement mechanisms point in different directions. The two regimes share vocabulary, and they sometimes reach similar outcomes, but they are answering fundamentally different questions about what data protection law is for.

I also want to be honest about the limitations of both models. The GDPR's ambition comes at a cost: a compliance burden that can be paralyzing for smaller organizations, a transfer regime that has been invalidated twice by its own court, and an accountability framework that sometimes prioritizes documentation over

substance. The CCPA's pragmatism has its own blind spots. A framework that ignores the geographic movement of data may prove inadequate as governments increasingly treat data flows as instruments of geopolitical leverage. Both regimes are works in progress. Both will continue to evolve. The value of comparing them with this level of granularity is that it gives scholars and practitioners an honest map of what each regime actually requires, where they overlap, and where the gaps between them create compliance risk.