With regulatory pressure, operational focus: Twelve action priorities for global privacy, AI governance, and cyber security compliance

Received (in revised form) 13th June, 2026

Lothar Determann
Partner, Baker McKenzie, Palo Alto, USA
Professor, Freie Universität Berlin/UC Berkeley Law, USA

Lothar Determann practises technology law at Baker McKenzie, Palo Alto, admitted in California and Germany. He teaches law at the Freie Universität Berlin (since 1994) and Berkeley School of Law (since 2004) and has authored more than 180 articles and six books, including 'Determann's Field Guide to Data Privacy Law' (6th edition, 2025, also available in Arabic, Chinese, French, German, Greek, Hungarian, Italian, Japanese, Korean, Portuguese, Russian, Spanish, Turkish, and Vietnamese), 'California Privacy Law — Practical Guide and Commentary on US Federal and California Law' (6th edition, 2026), and 'Determann's Field Guide to Artificial Intelligence Law' (2024, also available in Chinese, French, German, Korean, Spanish, and Turkish).

Baker McKenzie, 600 Hansen Way, Palo Alto, CA 94304, USA
Tel: +1 650 856 2400; E-mail: ldetermann@bakermckenzie.com

Graham Doyle
Deputy Commissioner and Head of Corporate Affairs, Media and Communications, Data Protection Commission, Ireland

Graham Doyle is a Deputy Commissioner and Head of Corporate Affairs, Media and Communications at the Irish Data Protection Commission (DPC). He develops and manages the DPC's communications strategy, including extensive national and international media engagement, and represents the DPC on the European Data Protection Board's Communications Network. He leads the DPC's Corporate Affairs team and serves on its Audit and Risk Committee. Graham previously served as Head of Communications and Research at the Garda Síochána Ombudsman Commission and as Head of Communications and Customer Service at Student Universal Support Ireland, and holds a graduate qualification in public management, specialising in law and the administration of justice.

Data Protection Commission Ireland, 6 Pembroke Row, Dublin 2, D02 X963, Ireland

Jennifer M. Urban
Clinical Professor, UC Berkeley Law, USA
Board Chairperson, California Privacy Protection Agency, USA

Jennifer M. Urban was appointed by California Governor Gavin Newsom in March 2021 as the inaugural Chair of the California Privacy Protection Agency (CPPA) Board. She is a Clinical Professor of Law at the University of California, Berkeley School of Law, where she directs policy initiatives at the Samuelson Law, Technology and Public Policy Clinic. Jennifer previously founded and directed the Intellectual Property and Technology Law Clinic at the University of Southern California, Gould School of Law, was the Samuelson Clinic's first fellow, and practised as an attorney with the Venture Law Group in Silicon Valley.

California Privacy Protection Agency, 400 R Street, Suite 350, Sacramento, CA 95811, USA

Michael Will
President, Bavarian State Office for Data Protection Supervision (BayLDA), Germany

Michael Will was appointed President of the Bavarian State Office for Data Protection Supervision (BayLDA) for a five-year term, first on 1st February, 2020 and again on 1st February, 2025. He began his career as an administrative lawyer in the service of the Free State of Bavaria in 1995 and subsequently held posts at the Supreme Building Authority in the Bavarian State Ministry of the Interior, the Bavarian State Chancellery, and the Landshut District Office. In 2009 Michael was appointed Head of the Data Protection Department at the Bavarian State Ministry of the Interior, Sport and Integration, serving also as official Data Protection Officer and as a member of the Data Protection Commission of the Bavarian State Parliament. On behalf of the Federal Council, Michael followed the deliberations of the Council Working Group on Data Protection and Information Exchange (DAPIX) on the EU General Data Protection Regulation from 2012 to 2015 and acted as country observer on the committee established under Article 93 of the GDPR.

Bavarian State Office for Data Protection Supervision (BayLDA), P.O. Box 1349, 91504 Ansbach, Germany

Abstract Global businesses face growing privacy and data protection obligations. Duties can vary by jurisdiction, and many businesses struggle to decide where to direct finite compliance resources. This paper, developed from a panel the authors prepared for the IAPP Global Summit 2026, argues that the European Union's (EU) General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), the most comprehensive and demanding regimes to which most global businesses are already subject, can serve as a common compliance core whose requirements can be leveraged to satisfy most other data protection regimes. It distils that core into 12 concrete priorities, grouped into five themes: securing the foundation; disciplining the data; respecting the individual; building accountability; and governing automation while anticipating legal change. The paper maps each priority to its anchoring GDPR and CCPA provisions and to the enforcement and litigation exposure that makes it consequential for global privacy, artificial intelligence (AI) governance, and cyber security compliance. The authors conclude that although obligations differ in some details and many organisations face additional sector and jurisdiction-specific rules, businesses that act on these 12 priorities will address the requirements common to data protection laws worldwide and materially reduce risk. The wider implication, underscored by recent deregulatory proposals in the EU and contests between federal and state authorities over AI in the US, is that organisations need a durable, principle-led compliance core and a standing process to monitor change. This article is also included in **The Business & Management Collection** which can be accessed at https://hstalks.com/business/.

KEYWORDS: GDPR, CCPA, global data protection compliance, data subject rights, automated decision making, accountability

DOI: 10.69554/REHE4351

INTRODUCTION

Global businesses are subject to privacy and data protection obligations under the laws of every jurisdiction in which they operate, and those obligations continue to multiply. Faced with overlapping and varying rules, compliance teams find it genuinely difficult to know where to begin and how to allocate finite resources.

The European Union's (EU) General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) offer a way through. They are among the most comprehensive, modern, and

demanding data protection regimes in the world, and most global businesses are already subject to both. Companies that manage to comply with these two regimes can leverage that effort to address the requirements of most other data protection laws.[1] The practical strategy that follows is to treat GDPR and CCPA compliance as a common core, calibrated locally where a particular jurisdiction demands something different.

The authors prepared the 12 action items set out in Table 1 for a panel at the IAPP Global Summit 2026 on privacy, artificial intelligence (AI) governance, and cyber security law.[2] The panel's organising philosophy was deliberately pragmatic: focus on principles rather than attempting to reconcile every jurisdictional variation at once. This paper retains those 12 priorities and groups them into five themes that track the life cycle of personal data through an organisation: securing the foundation; disciplining the data; respecting the individual; building accountability; and governing automation while anticipating legal change. Table 1 maps the 12 priorities to the GDPR and CCPA provisions that anchor each, illustrating how a single body of compliance work can be leveraged across both regimes and, by extension, much further.

SECURE THE FOUNDATION

Security is the precondition for privacy; without it, none of the other obligations that follow can be met. The first two priorities establish that foundation and prepare the organisation for the moment it is tested.

Action 1: Secure data

Without security, there can be no privacy. Under most data protection laws, companies must implement, document, and audit technical, administrative, and organisational data security measures, often referred to as technical and organisational measures (TOMs).[3] Effective 1st January, 2026, the CPPA issued regulations setting out detailed cyber security audit requirements[4] that companies anywhere in the world can use as a benchmark for keeping data secure and complying with the CCPA, to which many businesses within and outside California are subject.[5]

Table 1: The 12 priorities, by theme, and their GDPR and CCPA anchors

#	Action item	GDPR anchor	CCPA/CPPA anchor
A. Secure the foundation			
1	Secure data	Arts 24, 32	Cybersecurity-audit regs, tit. 11, §§ 7120–7124
2	Prepare for incidents	Arts 33, 34	Cal. Civ. Code § 1798.82; breach notification
B. Discipline the data			
3	Minimise data collection	Art. 5(1)(c)	Cal. Civ. Code § 1798.100(c); Reg. § 7002
4	Delete data	Art. 17	Cal. Civ. Code §§ 1798.100, 1798.105; Regs §§ 7002, 7022
C. Respect the individual			
5	Inform data subjects	Arts 12–14	Cal. Civ. Code §§ 1798.100(a), 1798.130; Regs §§ 7011–7012
6	Answer data subject requests	Arts 15 et seq.	Cal. Civ. Code § 1798.100 et seq.; Regs § 7001 et seq.
7	Do not sell or share	Consent rules; ePrivacy enforcement	Cal. Civ. Code § 1798.120 et seq.; Regs § 7026
D. Build accountability			
8	Contract for compliance	Arts 28(2), 44 et seq.	Cal. Civ. Code §§ 1798.100(d), 1798.140; Regs §§ 7051, 7053
9	Organise accountability	Arts 35(2), 38(1)	Cal. Code Regs §§ 7124(c), 7157(c)
10	Assess impacts	Arts 35, 36	Cal. Code Regs §§ 7150–7157
E. Govern AI and anticipate change			
11	Automate lawfully	Art. 22	Cal. Civ. Code § 1798.185(a)(15); Regs §§ 7200–7222
12	Monitor change	Digital Omnibus (proposed)	Federal–state AI measures (evolving)

Under a phased implementation keyed to annual gross revenue, members of the executive management team must submit annual certifications to the CPPA attesting to the completion of cyber security audits.[6] Allocating the resources needed to produce accurate audit reports matters both because it gives businesses insight into the cyber security risks they face and because the CPPA, other authorities, and private litigants are likely to require submission of those reports in the event of a data breach. With acceptable audit reports required by 2028, preparing now is essential.

Action 2: Prepare for incidents

Companies are required to notify individuals, authorities, investors, and corporate customers of personal data breaches, cyberattacks, serious AI incidents, and other events under myriad ever-evolving laws, which require formal notifications in official languages within strikingly different timeframes.[7] As Table 2 illustrates, the headline notification deadline ranges from 30 days in California to a single hour under China's cyber security incident reporting rules. Businesses must therefore develop, maintain, and regularly test processes to detect, mitigate, and report incidents, which in turn requires training and regular exercises.

DISCIPLINE THE DATA

Data that is never collected and data that is deleted once it is no longer needed cannot be breached, mishandled, or misused. The next two priorities impose that discipline on the data itself.

Action 3: Minimise data collection

The GDPR requires that personal data be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. The CCPA requires that a business's collection, use, retention, and sharing of personal information be reasonably necessary and proportionate to achieve the purposes for which it was collected or processed, or for another disclosed purpose that is compatible with the context in which it was collected.[8] Data subjects must be informed about those purposes and about collection, retention, and deletion practices.[9] Companies that collect or retain too much personal data can be sanctioned not only under privacy laws but also under consumer protection and unfair competition laws.[10]

Action 4: Delete data

Companies must delete personal data once they no longer need it, or when a data subject validly requests deletion.[11]

RESPECT THE INDIVIDUAL

Modern data protection law is built around the individual's ability to understand, access, and control the use of information about them. The following three priorities turn that principle into operational practice through clear notice, responsive rights handling, and restraint in the sale and sharing of personal information.

Action 5: Inform data subjects

Businesses must inform individuals about their data processing practices.[12] Privacy

Table 2: Illustrative headline breach- and incident-notification deadlines

Jurisdiction/regime	Headline notification timeframe
California (Cal. Civ. Code § 1798.82)	30 days
EU (GDPR, Arts 33–34)	72 hours
India (CERT-In Directions, 2022)	6 hours
China (Cybersecurity Incident Reporting regulations)	1 hour

policies should be easy to understand while still containing specific, mandated disclosures. Under the GDPR, for example, controllers must communicate 'in a concise, transparent, intelligible and easily accessible form, using clear and plain language', and must also disclose, where applicable, any intention to transfer personal data to a third country or international organisation and the relevant safeguards.[13] Under California law, businesses must likewise 'use plain, straightforward language and avoid technical or legal jargon' and must include several lists of personal information categories using statutorily prescribed terminology.[14] Global businesses can generally meet these requirements with a single, easy-to-read general privacy policy supplemented by jurisdiction-specific notices where mandatory disclosures would confuse individuals elsewhere.[15]

Action 6: Answer data subject requests

With respect to personal data about them, individuals have rights to know, to delete, to limit, to correct, and to opt out of direct marketing messages and of the sale or sharing of their information.[16] If companies do not respond within statutory deadlines, individuals complain to authorities, which then investigate and impose fines.[17] Companies may withhold information to protect the rights of others and do not have to provide copies of particular documents.[18] They must authenticate individuals before providing copies of personal information in response to a data access request, but must not add unnecessary friction to opt-out processes.[19]

Action 7: Do not sell or share

Under the CCPA, companies must not sell or share personal information for cross-context behavioural advertising if consumers opt out, including by using an opt-out preference signal such as the Global Privacy Control; they must offer easy opt-out mechanisms, obtain opt-in consent from minors under 16 and parental/guardian consent for minors under 13, and comply with numerous related obligations.[20] The CPPA and California's Attorney General have focused their enforcement actions on violations of these requirements.[21]

Additionally, the CPPA has pursued several data brokers for selling personal information without registering as a data broker;[22] at the federal level, both a statute (the Protecting Americans' Data from Foreign Adversaries Act of 2024) and, under a separate Executive Order, a Department of Justice (DOJ) rule now restrict the sale and transfer of certain sensitive personal information to foreign adversaries and countries of concern.[23] The Federal Trade Commission (FTC) has pursued companies for selling health and children's information in the context of online advertising,[24] plaintiffs' companies have filed a barrage of class-action lawsuits concerning cookies, pixels, and other advertising technologies,[25] and in Europe, data protection authorities (DPAs) have imposed significant fines for failures to comply with consent requirements for cookies and other online advertising technologies.[26]

Companies find it difficult to adopt globally uniform compliance strategies because requirements vary significantly from jurisdiction to jurisdiction concerning opt-in, opt-out, and process details.[27] The CPPA has expressly stated in its regulations that EU-style cookie banners do not, by themselves, satisfy CCPA requirements concerning 'selling'.[28] Numerous vendors offer 'privacytech' compliance automation, but these may or may not fully comply with the relevant legal requirements; in some cases, their customers have also attracted fines.[29] In light of the extremely high enforcement and litigation exposure, businesses must either invest in jurisdiction-specific compliance mechanisms or refrain from selling and sharing personal information for online advertising purposes.

BUILD ACCOUNTABILITY

Compliance must be demonstrable. The next three priorities put in place the contracts, roles, and assessments through which an organisation can demonstrate to regulators, courts, and third parties that it has done what the law requires.

Action 8: Contract for compliance

Companies execute statutorily required contract terms with corporate affiliates, external service providers, and other business partners to provide adequate data protection levels for international data transfers,[30] to ensure that disclosures are made within an appropriate contractual relationship,[31] or because laws or regulations expressly require certain contract terms.[32] Both parties benefit from the execution of data processing agreements mandated by law. If the parties draft contracts to reflect what the law requires, and not more or less, they should be able to satisfy applicable requirements relatively quickly. By aligning contract wording closely with statutory requirements, companies can also demonstrate compliance more efficiently to authorities.

In practice, businesses find it much more complex, costly, and time-consuming to negotiate heavily customised contracts with added commercial clauses, such as limitations of liability, indemnification obligations, or contractual penalties. Businesses can achieve compliance more efficiently if they negotiate and document commercial terms separately from agreements mandated by applicable laws.[33] Authorities regularly review data processing agreements in the context of investigations.[34] With separate agreements optimised to achieve and document adherence to data protection law, companies can prove compliance more effectively to authorities, data protection officers (DPOs), and privacy professionals during the contract review process.

Action 9: Organise accountability

Companies must ensure that their DPO is involved, in a timely and proper manner, in all issues relating to the protection of personal data under the GDPR, including data protection impact assessments (DPIAs) concerning AI development and deployment.[35] Executive management team members must personally sign attestations for cyber security audits and risk assessments under the CCPA regulations.[36] In addition, companies should consider making a named individual accountable for each AI system, with responsibility for monitoring its performance and compliance.[37]

Action 10: Assess impacts

Businesses are required to document DPIAs and risk assessments,[38] which regulators, and in certain situations also individual plaintiffs and others, can access. Companies should conduct assessments in phases: first, assess the legality and risks associated with a project holistically, with all facts available, subject to confidentiality and legal privilege; secondly, decide whether and how to proceed; and thirdly, document an assessment that explains why the conduct assessed is lawful and how the company mitigated or eliminated the risks identified. Companies that conflate these three steps risk proceeding with projects that should have been stopped or adjusted after an initial review.

GOVERN AI AND ANTICIPATE CHANGE

Finally, two forward-looking priorities address the automated and AI-driven systems that now make consequential decisions about people, and the rapid evolution of privacy law itself.

Action 11: Automate lawfully

Under the GDPR and a French predecessor law from 1978, Europeans have the right

not to be subject to a decision based solely on automated data processing, including profiling, which produces legal effects or similarly significantly affects them.[39] The CCPA also provides opt-out rights for automated decision making, and CPPA regulations specify the requirements with which businesses must comply by 1st January, 2027.[40]

As companies deploy automated decision making (ADM) systems in recruiting, employment, enrolment, financial services, healthcare, and other sensitive areas, they must obtain meaningful information and commitments from vendors, provide meaningful information to individuals, document risk assessments, arrange for opt-out and human-in-the-loop (HITL) processes, and ensure safety and security. To safeguard against unlawful decisions, companies should examine whether data used to train machines could perpetuate human biases and should retain independent auditors.[41]

Action 12: Monitor change

Businesses, technologies, and laws are constantly in a rapid state of change. After almost a decade of issuing new regulations, from the GDPR in 2016 to the Artificial Intelligence Act (AI Act) in 2024,[42] the European Commission (EC) published a simplification and deregulation proposal in November 2025 that would delay the application of restrictions on high-risk AI systems under the AI Act, narrow the definition of 'personal data', and relax the restrictions on automated decision making under Article 22 of the GDPR.[43] In the US, the federal executive seeks to prevent or pre-empt state regulation of AI, even as state and federal legislators continue to enact laws regulating AI systems and protecting consumer privacy.[44] Companies therefore need a standing process to adjust their compliance programmes as both the law and their own business change over time.

CONCLUSION

The 12 priorities set out in this paper do not capture everything that privacy and data protection law requires. Many organisations face additional sector, jurisdiction, and situation-specific obligations, and some will need to address requirements that do not appear on this list at all. These 12 recur, however, in one form or another across the comprehensive data protection regimes that now govern most of the world's commerce; as shown In Table 1, each is anchored in both the GDPR and the CCPA. A business that does these 12 things well will have addressed the requirements common to data protection laws worldwide and will have materially reduced its enforcement and litigation exposure. This is the answer to the question with which this paper began: an organisation confronted with a proliferation of obligations and finite resources need not reconcile every jurisdiction at once; it can begin with the common core shared by the two most demanding regimes it is already likely to face, the GDPR and the CCPA, and then leverage that work across the rest.

Two features of the present moment make that common core more valuable, not less. First, the priorities are operational rather than aspirational. The thread connecting security, minimisation, transparency, rights handling, accountability, and lawful automation is not a restatement of abstract rights; it is a set of controls that work in practice and that an organisation can evidence under scrutiny. Secondly, the law is moving in more than one direction at once. In Europe, the Commission's simplification proposal would delay parts of the AI Act, narrow the definition of personal data, and relax the rules on automated decision making; in the US, the federal executive seeks to pre-empt state regulation of AI even as state and federal legislators continue to enact privacy and AI laws. Deregulation in one forum does not extinguish obligations in another, and today's relaxation may be tomorrow's tightening. The twelfth priority,

monitoring change, is therefore not an afterthought but the mechanism that keeps the other 11 current.

For all the complexity, the authors' message is deliberately simple. Companies should act on these priorities even if specific obligations vary from jurisdiction to jurisdiction and even though no list can be complete. As Graham Doyle summed up the panel's practical guidance at the IAPP Global Summit on 30th March, 2026: 'Doing something is better than doing nothing. Focus on principles. And don't let perfect become the enemy of good.' The priorities in this paper are where that work should begin.

AUTHORS' NOTE

This paper reflects remarks the authors prepared for the IAPP Global Summit 2026. It is based on their personal opinions and must not be attributed to their agencies, boards, law schools, law company, clients or others.

References

1. IAPP (March 2026), 'Top 12 Compliance Action Items for Global Businesses', IAPP Global Summit 2026, available at https://iapp.org/conference/iapp-global-summit/agenda/top-12-compliance-action-items-for-global-businesses; A shorter version was published on 11th May, 2026, available at https://iapp.org/news/a/top-12-data-protection-action-items-for-global-businesses (both accessed 29th May, 2026).
2. *Ibid*.
3. European Union (EU), 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)', Arts. 24 and 32, available at https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng; see also Allen, J. and Jones, C. (eds) (2026), 'ABA Cybersecurity Handbook: Cybersecurity, Its Legal Implications, and the Emerging Risks of AI,', 4th edn, Chs. 7–9, American Bar Association (ABA), available at https://www.americanbar.org/products/inv/book/456112440/ (both accessed 29th May, 2026).
4. California Privacy Protection Agency (CPPA), 'California Code of Regulations', § 7123(c), available at https://cppa.ca.gov/regulations/pdf/ccpa_statute_eff_20260101.pdf (accessed 29th May, 2026).
5. California Legislation, 'California Civil Code', § 1798.140(d), available at https://law.justia.com/codes/california/code-civ/division-3/part-4/title-1-8/ (accessed 29th May, 2026).
6. California Privacy Protection Agency (CCPA), ref. 4 above, § 7124; § 7120 et seq. (applicability thresholds and deadlines).
7. California enacted the first data-breach notification law in 2002: California Legislation, ref. 5 above, § 1798.82. Most US states and many countries followed; see, eg European Union (EU), ref. 3 above, Arts. 33 and 34 (effective 2018). Reporting obligations also arise under AI regulation (eg EU AI Act), European Union (EU), 'Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)', Art. 73, available at https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng; Infrastructure-security law (eg NIS2 Directive), European Union (EU), Consolidated text: Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)', Art. 23, available at https://eur-lex.europa.eu/eli/dir/2022/2555 (both accessed 29th May, 2026); Sector-specific laws, see Allen and Jones, ref. 2 above, Chs. 8 and 9.
8. European Union (EU), ref. 3 above, Art. 5(1)(c); California Legislation, ref. 5 above, § 1798.100(c); California Privacy Protection Agency (CPPA), ref. 4 above, § 7002.
9. European Union (EU), ref. 3 above, Art. 13(1)(c); California Legislation, ref. 5 above, §§ 1798.100(a), 1798.130; California Privacy Protection Agency (CPPA), ref. 4 above, §§ 7011–7012.
10. See California Privacy Protection Agency (CPPA), 'Applying data Minimization to consumer requests', Enforcement Advisory No. 2024-01, available at https://cppa.ca.gov/pdf/enfadvisory202401.pdf; Office of the Information and Data Protection Commissioner (Malta), 'Data Protection Principles', available at https://idpc.org.mt/for-organisations/data-protection-principles/; and, eg US Federal Trade Commission (FTC), 'Legal Library: Cases and Proceedings', available at https://www.ftc.gov/legal-library/browse/cases-proceedings/ (accessed 29th May, 2026). Actions in Blackbaud, Everalbum, and Drizly.
11. European Union (EU), ref. 3 above, Art. 17; California Legislation, ref. 5 above, §§ 1798.100,

1798.105; California Privacy Protection Agency (CPPA), ref. 4 above, §§ 7002, 7022; Case C-131/12 *Google Spain SL and Google Inc. v AEPD and Mario Costeja González*, ECLI:EU:C:2014:317 (13th May, 2014) (right to be forgotten).

12. California has required operators of online services to post website privacy policies since 2004: California Legislation, 'California Business and Professions Code', § 22575 et seq. (California Online Privacy Protection Act), available at https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=BPC&sectionNum=22575. (accessed 29th May, 2026); See also European Union (EU), ref. 3 above, Art. 12 et seq.; California Legislation, ref. 5 above, §§ 1798.100(a), 1798.130; California Privacy Protection Agency (CPPA), ref. 4 above, §§ 7011–7012 (CCPA).
13. European Union (EU), ref. 3 above, Arts. 12(1) and 13(1)(f).
14. California Legislation, ref. 5 above, §§ 1798.100(a), 1798.130(c); California Privacy Protection Agency (CPPA), ref. 4 above, §§ 7003(a), 7011–7012.
15. Determann, L. (2025), 'Determann's Field Guide to Data Privacy Law', 6th edn, Edward Elgar Publishing, Cheltenham, § 3.31.
16. European Union (EU), ref. 3 above, Art. 15 et seq.; California Legislation, ref. 5 above, § 1798.100 et seq.; California Privacy Protection Agency (CPPA), ref. 4 above, § 7001 et seq.
17. See, eg UK Information Commissioner's Office (ICO) (2025), 'Jason Blake', available at https://ico.org.uk/action-weve-taken/enforcement/2025/09/jason-blake/; European Central Bank (ECB), 'Right of access: Data Protection Authority fines bank 100 000 EUR. Customers can access their data contained in telephone order recordings', available at https://www.edpb.europa.eu/news/national-news/2025/right-access-data-protection-authority-fines-bank-100-000-eur-customers-can_en (both accessed 29th May, 2026).
18. See case studies published by the Irish Data Protection Commission (DPC), 'Case Studies', available at https://www.dataprotection.ie/en/dpc-guidance/case-studies/ (accessed 29th May, 2026).
19. See, for example, California Legislation, ref. 5 above, § 1798.110(b); California Privacy Protection Agency (CPPA), ref. 4 above, §§ 7024, 7026(d), 7060(b); California Privacy Protection Agency (CCPA) (March 2026), 'Ford to change practices, pay fine for adding unnecessary friction to opt-out process', available at https://privacy.ca.gov/2026/03/ford-to-change-practices-pay-fine-for-adding-unnecessary-friction-to-opt-out-process/ (accessed 29th May, 2026).
20. California Legislation, ref. 5 above, § 1798.120 et seq.; California Privacy Protection Agency (CPPA), ref. 4 above, § 7001 et seq.
21. See, for example, California Office of the Attorney General, 'Privacy enforcement actions', available at https://oag.ca.gov/privacy/privacy-enforcement-actions (accessed 29th May, 2026); Ford action, ref. 18 above.
22. See, for example, California Privacy Protection Agency (CPPA) (January 2026), 'CalPrivacy Brings New Round of Enforcement Actions Against Data Brokers', available at https://cppa.ca.gov/announcements/2026/20260108.html (accessed 29th May, 2026).
23. Congress, 'Protecting Americans' Data from Foreign Adversaries Act of 2024', (PADFAA), Pub. L. No. 118-50, 15 U.S.C. § 9901 (enforced by the Federal Trade Commission), available at https://www.congress.gov/bill/118th-congress/house-bill/7520/text; Federal Register (2024), 'Executive Order 14117 of 28th February, 2024, "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern", 89 Fed. Reg. 15421 (1st March, 2024)', available at https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related; US Department of Justice (DOJ), 'Data Security Program FAQ No. 12', final rule, 28 C.F.R. Part 202, 90 Fed. Reg. 1636 (8th January, 2025), effective 8th April, 2025: On the overlap between the statute and the rule, available at https://www.justice.gov/opa/media/1396351/dl (all accessed 29th May, 2026).
24. US Federal Trade Commission (FTC), 'Collecting, using, or sharing consumer health information?', available at https://www.ftc.gov/business-guidance/resources/collecting-using-or-sharing-consumer-health-information-look-hipaa-ftc-act-health-breach; US Federal Trade Commission FTC, 'Privacy and security enforcement', available at https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement (both accessed 29th May, 2026).
25. See Corporate Counsel (June 2023), 'Suits flooding courts seize on decades-old wiretapping laws to allege data-privacy breaches', available at https://www.law.com/corpcounsel/2023/06/22/suits-flooding-courts-seize-on-decades-old-wiretapping-laws-to-allege-data-privacy-breaches/ (accessed 29th May, 2026).
26. See Commission Nationale de l'Informatique et des Libertés (National Commission on Informatics and Liberty) (CNIL), 'Cookies and advertisements inserted between emails: Google fined', available at https://www.edpb.europa.eu/news/national-news/2025/french-sa-cookies-and-advertisements-inserted-between-emails-google-fined_en (accessed 29th May, 2026).
27. See IAPP, 'Opting in and out: Five key analyses for adtech privacy law compliance', available at https://iapp.org/news/a/opting-in-n-out-five-key-analyses-for-adtech-privacy-law-compliance (accessed 29th May, 2026).
28. California Privacy Protection Agency (CPPA), ref. 4 above, § 7026(a)(4).

29. See California Privacy Protection Agency (CPPA) (May, 2025), 'Todd Snyder', available at https://privacy.ca.gov/wp-content/uploads/sites/357/2026/01/20250501_snyder_order.pdf; Bloomberg Law, 'Companies sought help from privacy vendors. They still got fined', available at https://news.bloomberglaw.com/privacy-and-data-security/companies-sought-help-from-privacy-vendors-they-still-got-fined (both accessed 29th May, 2026).
30. European Union (EU), ref. 3 above, Art. 44 et seq.; see also European Commission, (EC) 'Standard contractual clauses (SCC)', available at https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en (accessed 29th May, 2026).
31. European Union (EU), ref. 3 above, Art. 28(2); California Legislation, ref. 5 above, §§ 1798.100(d), 1798.120, 1798.140(ad)(1), (ah)(1), (ai)(2).
32. Code of Federal Regulations, 'Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule', 45 CFR § 164.504(e), available at https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.504; see US Department of Health and Human Services, 'Sample business associate agreement provisions', available at https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html (both accessed 29th May, 2026); See also California Legislation, ref. 5 above, § 1798.100(d); California Privacy Protection Agency (CPPA), ref. 4 above, §§ 7051, 7053.
33. Determann, ref. 15 above, § 3.73.
34. See BayLDA, 'Data processing without adequate agreement can be expensive', available at https://www.lda.bayern.de/media/pm/pm2015_11.pdf; European Data Protection Supervisor (EDPS) March 2024), 'EDPS investigation into use of MS 365 by EU Commission, Case 2021-0518', available at https://www.edps.europa.eu/system/files/2024-03/24-03-08-edps-investigation-ec-microsoft365_en.pdf; California Privacy Protection Agency (CPPA) (March 2025), 'Honda Settles With CPPA Over Privacy Violations', available at https://cppa.ca.gov/announcements/2025/20250312.html (all accessed 29th May, 2026).
35. European Union (EU), ref. 3 above, Arts 38(1) and 35(2).
36. California Privacy Protection Agency (CPPA), ref. 4 above, §§ 7124(c), 7157(c).
37. Determann, L. (2026), 'Determann's Field Guide to Artificial Intelligence Law', 2nd edn, Edward Elger Publishing, Cheltenham, Ch. 2.1.
38. See, eg European Union (EU), ref. 3 above, Arts. 35 and 36; California Privacy Protection Agency (CPPA), ref. 4 above, §§ 7150–7157.
39. European Union (EU), ref. 3 above, Art. 22.
40. California Legislation, ref. 5 above, § 1798.185(a)(15); California Privacy Protection Agency (CPPA), ref. 4 above, §§ 7200–7222.
41. Specifically required by New York City Law 144 with respect to automated employment decision tools; see New York State Comptroller, Enforcement of Local Law 144 – Automated Employment Decision Tools', available at https://www.osc.ny.gov/state-agencies/audits/2025/12/02/enforcement-local-law-144-automated-employment-decision-tools (accessed 29th May, 2026). Recommended or expected under many other jurisdictions' anti-discrimination laws.
42. European Commission (EC), 'Shaping Europe's digital future', available at https://digital-strategy.ec.europa.eu/en (accessed 29th May, 2026).
43. European Commission (EC), 'Digital Omnibus Regulation Proposal', available at https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal (accessed 29th May, 2026).
44. See Executive Order on eliminating state-law obstruction of national artificial intelligence policy, The White House (December 2025), 'Ensuring a National Policy Framework for Artificial Intelligence', available at https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/; National Conference of State Legislatures, 'Artificial Intelligence 2025 Legislation', available at https://www.ncsl.org/technology-and-communication/artificial-intelligence-2025-legislation; National Conference of State Legislatures (NCSL) (June 2022), 'State laws related to digital privacy', available at https://www.ncsl.org/technology-and-communication/state-laws-related-to-digital-privacy (both accessed 29th May, 2026).