VALASYS MEDIA

Empowering marketers with powerful insights

Valasys Media

Official Data Privacy Compliance Statement

Valasys Media

Official Data Privacy Compliance Statement

Effective date: 12 September 2025

Scope: Valasys Media, Inc. and controlled affiliates (collectively, "Valasys," "we," "us," "our").

1) Purpose and applicability

This statement describes Valasys' privacy compliance program and confirms that we operate controls intended to meet the requirements of applicable data protection laws, including the EU and UK GDPR, California CCPA as amended by the CPRA, Brazil's LGPD, and comprehensive state privacy laws in the United States, to the extent those laws apply to our processing. Our program is grounded in the GDPR accountability principle and the core processing principles of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, and integrity and confidentiality.

Important note on "certifications." Most privacy statutes do not provide a government-issued certificate of compliance. Compliance is demonstrated through policies, controls, records, and audits. Where appropriate, Valasys may commission third-party assessments or legal reviews.

2) Laws covered by our program

Global frameworks

- General Data Protection Regulation in the EU and UK (GDPR and UK GDPR).
- California Consumer Privacy Act as amended by the CPRA (CCPA/CPRA)
- Lei Geral de Proteção de Dados (LGPD) in Brazil.

United States state privacy laws

We maintain a harmonized program that maps requirements across states. The following laws are within scope as applicable to our activities and thresholds.

Already effective

- Virginia VCDPA since January 1, 2023
- Colorado CPA since July 1, 2023
- Connecticut CTDPA since July 1, 2023
- Utah UCPA since December 31, 2023
- Florida Digital Bill of Rights since mid-2024
- Texas TDPSA since mid-2024
- Oregon OCDPA since mid-2024
- Montana MCDPA since October 2024

New in 2025

- Iowa CDPA effective January 1, 2025
- Delaware DPDPA effective January 1, 2025
- Nebraska NDPA effective January 1, 2025
- New Hampshire NHPA effective January 1, 2025
- New Jersey NJCPA effective January 15, 2025
- Tennessee TIPA effective July 1, 2025
- Minnesota MCDPA effective July 31, 2025
- Maryland MODPA effective October 1, 2025

Coming in 2026

- Indiana INCDPA effective January 1, 2026
- Kentucky KCDPA effective January 1, 2026
- Rhode Island RIDPA effective January 1, 2026

3) Governance and accountability

Policies and standards

Written privacy and security policies operationalize legal requirements and the GDPR principles referenced above.

Leadership and roles

A designated privacy lead coordinates data mapping, rights handling, impact assessments, vendor oversight, and incident response under executive oversight.

Records of processing

We maintain records appropriate to our processing activities and update them as operations change.

Training

Personnel with access to personal data receive role-specific privacy and security training on a recurring basis.

4) Lawful bases and transparency

GDPR and UK GDPR

We process data on recognized legal bases such as consent, contract, and legitimate interests balanced against the rights of individuals, and we apply the Article 5 principles listed above.

LGPD

We apply legal bases as defined by the LGPD and follow ANPD guidance, including the ability for the authority to require a privacy impact report when legitimate interest is used.

CCPA/CPRA and state laws

We provide notices that describe categories of personal information, purposes, retention, rights, and whether we sell or share personal information, along with how to exercise rights.

5) Consumer and data subject rights

We authenticate and fulfill requests to access, correct, delete, or obtain a portable copy of personal data, and to opt out of sale, sharing, targeted advertising, or certain profiling where applicable. Timeframes are aligned to law: under GDPR one month with possible extension of two months for complexity; under CCPA/CPRA and the Colorado CPA 45 calendar days with possible 45 day extension upon notice. We acknowledge and provide appeal mechanisms where required.

Signals and universal opt out. We honor user-enabled opt-out preference signals required by California and universal opt-out mechanisms required by Colorado, including recognition of Global Privacy Control as an approved mechanism in Colorado.

6) Cookies, online tracking, and targeted advertising

We disclose the use of cookies and similar technologies and provide state-specific rights and choice. Where our activities meet a state law definition of sale, sharing, or targeted advertising, we provide required notices and easy-to-use opt-outs, and we recognize required preference signals as described above.

7) Sensitive data, children, and profiling

We apply heightened controls for sensitive data, including consent or opt-out as required, and we do not knowingly process children's data contrary to applicable laws. We account for stricter state standards, including Maryland's prohibitions relating to targeted advertising to minors and robust data minimization.

8) Privacy by design and risk assessments

We embed privacy by design and by default into products and processes. Where processing is likely to result in a high risk to individuals, we conduct Data Protection Impact Assessments or comparable state assessments before launch and implement mitigations.

9) Vendor management

We use written data processing agreements that require processors to implement appropriate safeguards, confidentiality, and rights assistance. We assess higher-risk vendors and maintain an updated register of sub processors where appropriate.

10) Cross-border data transfers

For GDPR and UK GDPR covered transfers, we use valid transfer tools such as the European Commission's Standard Contractual Clauses and, for the UK, the IDTA or UK Addendum, along with supplementary measures as needed.

11) Security measures

We implement technical and organizational safeguards appropriate to risk, including access controls, least privilege, encryption in transit and at rest where appropriate, secure development practices, vulnerability management, logging and monitoring, and incident response procedures.

12) Data retention and deletion

We retain personal data only as long as necessary for the purposes described in our notices and to meet legal, accounting, or reporting requirements. At the end of retention we delete or de-identify data in accordance with documented schedules and applicable law.

13) Incident response and regulatory cooperation

We maintain an incident response plan to assess, contain, and remediate security events and to provide legally required notifications. We cooperate with competent supervisory and enforcement authorities as required by law.

14) Public notices and accessibility

Our public-facing privacy notice is written in plain language and provides required disclosures, instructions for submitting requests, links for opt-out of sale or sharing where applicable, and jurisdiction-specific information.

15) Implementation evidence and operational commitments

Valasys maintains the following artifacts and processes to evidence compliance and ensure ongoing alignment.

Data mapping and Records of Processing

Comprehensive data inventory and records that include purposes, categories, recipients, retention, and transfer mechanisms. Minnesota law requires maintaining a data inventory as part of security practices, which our inventory supports.

Rights operations

DSAR intake via web form and dedicated email, identity verification appropriate to request type, confirmation of receipt within legally required time, tracking to closure within the applicable SLA, and an appeals workflow where required by state law.

Signals and choice

A mechanism to detect and respect Global Privacy Control and other approved universal opt-out mechanisms in Colorado, with periodic checks against the Colorado Department of Law list.

Cookie consent

A consent and preference tool configured to reflect state definitions of sale, sharing, and targeted advertising, and to surface required links.

Privacy impact assessments

DPIAs under GDPR and risk assessments under state laws for targeted advertising, sale or sharing, sensitive data processing, and profiling. Tennessee's TIPA and other state laws require such assessments for specified activities, which we conduct and document.

Vendor diligence

Risk-based onboarding and review, contractual SCCs or UK IDTA where applicable, and minimum-security requirements.

Training and awareness

Onboarding and recurring training tailored to roles with access to personal data.

Auditing and monitoring

Periodic internal reviews against this program and applicable guidance, with corrective actions tracked to completion.

Program updates

Ongoing horizon scanning to incorporate new or amended requirements across states, including MODPA and MCDPA obligations.

16) Attestation

Subject to the qualifications and ongoing obligations described above, Valasys affirms that it has implemented and maintains policies, controls, and procedures intended to ensure compliance with GDPR, CCPA/CPRA, LGPD, and the comprehensive state privacy laws listed in Section 2 to the extent those laws apply to our processing. This statement should be read together with our Privacy Notice and internal policies. It is not a guarantee of regulatory outcome.

17) Contact

Questions or requests can be submitted to **info@valasys.com**