GLOBAL BIOMETRICS AND ARTIFICIAL INTELLIGENCE REGULATION CHART

Last updated: October 2024

Disclaimer: These materials do not constitute legal advice and should not be substituted for the advice of legal counsel

TABLE OF CONTENTS

Australia Privacy Act 1988 (Privacy Act) and Australian Privacy Principles (APPs) 1
California Consumer Privacy Act (CCPA) 1
California Labor Code § 1051 2
Canada Personal Information Protection and Electronic Documents Act (PIPEDA) 3
Quebec, Canada Act Respecting the Protection of Personal Information in the Private Sector (Quebec Privacy Act) 3
Colorado Artificial Intelligence Act (Colorado AI Act) 4
Colorado HB 1130 5
Colorado Privacy Act (CPA) 6
Connecticut Data Privacy Act (CTDPA) 7
Delaware Personal Data Privacy Act (DPDPA) 7
EU Artificial Intelligence Act (EU AI Act) 8
EU/UK General Data Protection Regulation (GDPR) 9
Florida Digital Bill of Rights (FDBR) 10
Illinois Artificial Intelligence Video Interview Act (AIVIA) 11
Illinois Biometric Information Privacy Act (BIPA) 11
Indiana Consumer Data Protection Act (INCDPA) 12
Iowa Consumer Data Protection Act (ICDPA) 12
Kentucky Consumer Data Protection Act (KCDPA) 13
Maryland HB 1202 (HB 1202) 13

Maryland Online Data Privacy Act (MODPA) 14
Minnesota Consumer Data Privacy Act (MNCDPA) 14
Montana Consumer Data Privacy Act (MCDPA) 15
Nebraska Data Privacy Act (NEDPA) 16
New Hampshire Privacy Act (NHPA) 16
New Jersey Data Privacy Act (NJDPA) 17
New York Labor Law § 201-a 18
New York State Education Department Facial Recognition Ban 18
New York City "Automated Employment Decision Tools" Ordinance (NYC AEDT Ordinance) 19
New York City "Commercial Establishments" Ordinance (NYC Commercial Establishments Ordinance) 19
New York City Tenant Data Privacy Act (TDPA) 20
Oregon Consumer Privacy Act (OCPA) 21
Portland, Oregon Facial Recognition Ordinance 21
Rhode Island Data Transparency and Privacy Protection Act (RIDPA) 22
Tennessee Ensuring Likeness, Voice, and Image Security Act of 2024 (ELVIS Act) 23
Tennessee Information Protection Act (TIPA) 23
Texas Capture or Use of Biometric Identifiers Act (CUBI) 24
Texas Data Privacy and Security Act (TDPSA) 24
Utah Artificial Intelligence Policy Act (Utah AI Policy Act) 25
Utah Consumer Privacy Act (UCPA) 26
Virginia Consumer Data Protection Act (VCDPA) 26
Washington My Health My Data Act (MHMDA) 27
Washington RCW Chapter 19.375 (HB 1493) 28

GLOBAL BIOMETRICS AND ARTIFICIAL INTELLIGENCE REGULATION

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
Australia **Australia Privacy Act 1988 (Privacy Act) and Australian Privacy Principles (APPs)** Act No. 119 of 1988, Privacy Act 1988, Compilation No. 97 (Oct. 18, 2023)	**Generally** Organizations (*i.e.*, person, body, corporate, partnership, unincorporated association, or trust) that: (1) have more than 3 million AUD annual turnover; or (2) are small businesses (*i.e.,* a business with an annual turnover of 3 million AUD or less) that meet certain requirements. **Biometric Systems** "Biometric system" has been defined by the Office of the Australian Information Commissioner (OAIC) as a system that "scans, measures, analyzes, and recognizes a particular and unique biometric (such as facial features), physical, biological, and behavioral traits and characteristics to identify a person."	**Biometric Information** "Biometric information" is generally regarded by Australian privacy authorities as information that relates to a person's physiological or biological characteristics and that are persistent and unique to the individual (including their facial features, irises, or hand geometry). **Sensitive Information** "Sensitive information" includes "biometric information that is to be used for the purpose of automated biometric verification or biometric identification" and "biometric templates."	**Organizations/Biometric Data** • Consent • Notice at Collection • Data Retention and Destruction • Disclosure Limitations • Data Security • Use/Purpose Limitation • Data Quality/Integrity	**Regulatory Enforcement** **Authority.** OAIC has authority to enforce Privacy Act (and APPs). **Remedies.** Civil penalties up to greater of: (1) 50 million AUD; (2) three times the value of any benefit obtained through misuse of personal information; or (3) 30 percent of the entity's adjusted turnover during period of noncompliance.
California **California Consumer Privacy Act (CCPA)** Cal. Civ. Code § 1798.100, *et seq.*	**Controllers** (1) Organized or operated for-profit or financial benefit; (2) collects consumers' personal information; (3) determines purposes and means of processing consumers' personal information; and (4) satisfies one or more of following	**Biometric Information** "'Biometric information' means individual's physiological, biological, or behavioral characteristics, including information pertaining to an individual's deoxyribonucleic acid (DNA), that is used or is intended to be used, singly or in	**Controllers/Sensitive Data** • Privacy Policy • Notice at Collection • Data Protection Assessment • Cybersecurity Audit • Use/Purpose Limitation • Consumer Rights Compliance • Employee Training	**Private Right of Action** **Private Right of Action.** Limited private right of action applicable to certain security breach events involving violation of CCPA duty to implement and maintain reasonable security procedures and practices.

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
Cal. Code Regs. tit. 11, § 7001, *et seq.*	thresholds: (a) gross global annual revenue in excess of $25 million; (b) annually buys, sells, or shares for cross-context behavioral advertising purposes personal information of at least 100,000 California consumers or households; or (c) derives at least 50 percent of annual revenue from selling or sharing personal information of California consumers. **Processors** Person or organization that processes personal information on behalf of the controller.	combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information." **Sensitive Personal Information** "Sensitive personal information" includes "the processing of biometric information for the purpose of uniquely identifying a consumer."	**Processors** • Data Retention and Destruction • Disclosure Limitation • Use/Purpose Limitation • Controller/Processor Contract • Controller Assistance • Controller Instruction Compliance • Direct Consumer Rights Request Compliance • Cross-Context Behavioral Advertising Contractual Prohibition	**Damages.** (1) Statutory damages between $100 and $750 per consumer per incident; and (2) injunctive or declaratory relief. **Regulatory Enforcement Authority.** Office of California Attorney General (AG) and California Privacy Protection Agency (CPPA) have authority to enforce CCPA. **Remedies.** Civil penalties up to $2,500 per violation or $7,500 per intentional violation.
California **California Labor Code § 1051** Cal. Lab. Code § 1051	**Generally** Employers and related third-party vendors.	**Fingerprint Data** Not defined by California Labor Code § 1051.	**Employers and Vendors** • Fingerprint Disclosure Prohibition[1]	**Criminal Penalties** **Penalties.** Violation constitutes a misdemeanor offense, subject to a fine up to $1,000 and/or imprisonment up to six months.

[1] California Labor Code § 1051 prohibits employers from obtaining current or prospective employee fingerprint data and then "furnishing" or sharing such data with third parties. The California AG has clarified that no violation of § 1051 occurs where the disclosure of fingerprint data satisfies two criteria: (1) disclosure is made solely to a third party acting as the employer's agent and for the employer's exclusive benefit; and (2) fingerprint data is not further furnished or disclosed by either employer or agent.

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
Canada **Canada Personal Information Protection and Electronic Documents Act (PIPEDA)** S.C., 2000, c P-5	**Generally** Organizations (*i.e.*, person, corporation, association, partnership, other type of legal entity, or trade union) that collects, uses, or discloses personal information. **Biometrics** The Office of the Privacy Commissioner of Canada (OPC) has defined "biometrics" as the quantification of human characteristics into measurable terms, and refers to a range of techniques, devices, and systems that enable machines to recognize individuals, or confirm or authenticate their identities.	**Biometric Data** "Biometric data" is generally regarded by OPC broadly as data collected through use of biometrics. **Sensitive Personal Information** OPC guidance provides that "biometric data" falls within data considered to be "sensitive personal information" under PIPEDA, with "facial biometric information [being] particularly sensitive, as it may allow for the identification of an individual through comparison against a vast array of images available on the Internet or via surreptitious surveillance."	**Organizations/Sensitive Personal Information** • Consent • Notice • Privacy Policy • Disclosure Limitation • Data Security • Privacy Governance Program • Purpose Specification • Data Minimization • Use/Purpose Limitation • Data Quality/Integrity • Data Subject Rights Compliance • Data Protection Officer (DPO) Appointment • Employee Training	**Regulatory Enforcement** **Authority.** OPC has investigative authority; Canadian Federal Court has authority to impose monetary fines. **Remedies.** (1) Monetary fines up to 100,000 CAD per violation; and (2) potential referral to Attorney General of Canada for further legal action.
Quebec, Canada **Quebec, Canada Act Respecting the Protection of Personal Information in the Private Sector (Quebec Privacy Act)** CQLR, 2003, c P-6.5 SQ, 2021, c 25	**Generally** Enterprises (*i.e.*, person, corporation, association, partnership, or other type of legal entity) that collect, hold, use, or disclose personal information within the province, regardless of location of enterprise's place of business (*i.e.*, even if enterprise located outside of Quebec).	**Biometric Data** "Biometric data" is generally regarded by CAI broadly as data collected through use of biometrics. **Sensitive Personal Information** Personal information is sensitive if, "due to its nature, in particular medical, biometric, or otherwise intimate information or the context of its use or communication (*i.e.*,	**Controllers/Sensitive Personal Information** • Consent • Notice • Privacy Policy • Data Retention and Destruction • Disclosure Limitation • Data Security • Privacy Impact Assessment • Privacy Governance Program • Purpose Specification	**Private Right of Action** **Private Right of Action.** Any individual injured by intentional violation of Quebec Privacy Act or violation resulting from gross fault has the right of action against infringing party. **Damages.** Statutory damages of a minimum 1,000 CAD per violation.

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
	Biometrics The Office of the Privacy Commissioner of Quebec (CAI) has defined "biometrics" as "the mathematical analysis of a person's unique characteristics to determine or prove identity."	disclosure), it entails a high level of reasonable expectation of privacy."	• Data Minimization • Use/Purpose Limitation • Cross-Border Data Transfer Restrictions • Data Subject Rights Compliance • DPO Appointment • Security Incident Notification • Employee Training **Processors** • Privacy Policy • Data Retention and Destruction • Data Quality/Integrity • Controller/Processor Contract • Data Subject Rights Compliance • Internal Rules of Conduct • Regulatory Registration	**Regulatory Enforcement** **Authority.** CAI has authority to enforce the Quebec Privacy Act. **Remedies.** Administrative monetary and penal fines up to: (1) for enterprises, greater of: (a) 25 million CAD; or (b) four percent previous year worldwide turnover; and (2) for individuals, up to 50,000 CAD.
Colorado **Colorado Artificial Intelligence Act (Colorado AI Act)** **Effective Date: Feb. 1, 2026** C.R.S. § 6-1-1701, *et seq.*	**Generally** "Developers" and "deployers" of "high-risk AI systems." **Developers** Person doing business in Colorado that develops or intentionally modifies an AI system.	**Covered Data** N/A	**Developers** • Privacy Policy • Risk Management Program • Technical Documentation • AG Reporting • Duty to Avoid Algorithmic Discrimination **Deployers** • Notice • Privacy Policy	**Regulatory Enforcement** **Authority.** The Colorado AG and district attorneys have authority to enforce Colorado AI Act. **Remedies.** (1) Civil penalties up to $20,000 per violation under Colorado Consumer Protection Act (Colorado UDAP); (2) disgorgement; (3) restitution; (4) attorney's fees and costs; and (5) injunctive relief.

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
	Deployers Person doing business in Colorado that deploys (*i.e.*, uses) a high-risk AI system. **High-Risk AI Systems** Any AI system that, when deployed, makes, or is a substantial factor in making, a consequential decision.		• Privacy Impact Assessment • Independent Third-Party Audit • Consumer Rights Compliance • AG Algorithmic Discrimination Incident Reporting	
Colorado **Colorado HB 1130** **Effective Date: July 1, 2025** C.R.S. § 6-1-1314	**Controllers** (1) (a) Conducts business in Colorado; or (b) produces or delivers commercial products or services intentionally targeted to Colorado residents; and (2) processes or controls *any* amount/volume of biometric identifiers/biometric data. **Processors** Person or organization that processes biometric data or biometric identifiers on behalf of controller.	**Biometric Identifiers** "'Biometric identifier' means data generated by the technological processing, measurement, or analysis of a consumer's biological, physical, or behavioral characteristics, which data can be processed for the purpose of uniquely identifying an individual. 'Biometric identifier' includes: (a) A fingerprint; (b) A voiceprint; (c) A scan or record of an eye retina or iris; (d) A facial map, facial geometry, or facial template; or (e) Other unique biological, physical, or behavioral patterns or characteristics."	**Controllers** • Consent • Notice • Privacy Policy • Data Retention and Destruction • Disclosure Limitation • Transactional Prohibition • Data Security • Biometric Data Assessment[2] • Security Incident Response Program • Purpose Specification • Data Minimization • Use/Purpose Limitation • Data Subject Rights Compliance • Employment-Specific Requirements and Limitations	**Regulatory Enforcement** **Authority.** The Colorado AG and district attorneys have authority to enforce the Colorado Privacy Act (CPA). **Remedies.** (1) Civil penalties up to $20,000 per violation under Colorado UDAP; (2) disgorgement; (3) restitution; (4) attorney's fees and costs; and (5) injunctive relief.

[2] Colorado HB 1130 obligates controllers to conduct review at least once annually to evaluate whether storage of biometric data is no longer necessary, adequate, or relevant to express processing purpose(s) disclosed at initial time of collection; where biometric data is no longer necessary, adequate, or relevant, data must be deleted at "earliest reasonably feasible date," but no more than 45 days after date of determination.

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
		Biometric Data "'Biometric data' means one or more biometric identifiers that are used or intended to be used, singly or in combination with each other or with other personal data, for identification purposes."	**Processors** • Data Security • Security Incident Response Program • Employment-Specific Requirements and Limitations	
Colorado **Colorado Privacy Act (CPA)** C.R.S. § 6-1-1301, *et seq.* 4 CCR 904-3, Rule 1.01, *et seq.*	**Controllers** (1) (a) Conducts business in Colorado; or (b) produces or delivers commercial products or services intentionally targeted to Colorado residents; and (2) (a) during calendar year, processes or controls personal data of at least 100,000 consumers; or (b) (i) processes or controls personal data of at least 25,000 consumers; and (ii) derives revenue or receives discount from sale of personal data. **Processors** Person or organization that processes personal data on behalf of controller.	**Biometric Identifiers** "'Biometric Identifiers' means data generated by the technical processing, measurement, or analysis of an individual's biological, physical, or behavioral characteristics that can be processed for the purpose of uniquely identifying an individual, including but not limited to a fingerprint; voiceprint; scans or records of eye retinas or irises; facial mapping, facial geometry, or facial templates; or other unique biological, physical, or behavioral patterns or characteristics." **Biometric Data** "'Biometric Data,' as referred to in C.R.S. § 6-1-1303(24)(b) means Biometric Identifiers that are used or intended to be used, singly or in combination with each other or with other personal data, for identification purposes."	**Controllers/Sensitive Data** • Consent • Privacy Policy • Data Retention and Destruction • Data Protection Assessment • Data Minimization • Loyalty Program Compliance **Processors** • Data Security • Controller/Processor Contract • Controller Instruction Compliance • Controller Assistance • Duty of Confidentiality • Sub-Processor Engagement Requirements	**Regulatory Enforcement** **Authority.** The Colorado AG and district attorneys have authority to enforce CPA. **Remedies.** (1) Civil penalties to $20,000 per violation under the Colorado UDAP; (2) disgorgement; (3) restitution; (4) attorney's fees and costs; and (5) injunctive relief.

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
		Sensitive Data "Sensitive data" includes "biometric data that may be processed for the purpose of identifying an individual."		
Connecticut **Connecticut Data Privacy Act (CTDPA)** Conn. Gen. Stat. § 42-515, *et seq.*	**Controllers** (1) (a) Conducts business in Connecticut; or (b) produces products or services targeted to Connecticut residents; and (2) during preceding calendar year: (a) processed or controlled personal data of at least 100,000 consumers; or (b) (i) processed or controlled personal data of at least 25,000 consumers; and (ii) derived more than 25 percent of gross revenue from sale of personal data. **Processors** Person or organization that processes personal data on behalf of controller.	**Biometric Data** "'Biometric data' means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that are used to identify a specific individual." **Sensitive Data** "Sensitive data" includes "the processing of [] biometric data for the purpose of uniquely identifying an individual."	**Controllers/Sensitive Data** • Consent • Privacy Policy • Data Retention and Destruction • Data Protection Assessment • Data Minimization • Loyalty Program Compliance **Processors** • Controller/Processor Contract • Controller Instruction Compliance • Controller Assistance	**Regulatory Enforcement** **Authority.** Connecticut AG has authority to enforce CTDPA. **Remedies.** (1) Civil penalties up to $5,000 per violation under Connecticut Unfair Trade Practices Act; (2) disgorgement; (3) restitution; (4) attorney's fees and costs; and (5) injunctive relief.
Delaware **Delaware Personal Data Privacy Act (DPDPA)** **Effective Date: Jan. 1, 2025** Del. Code tit. 6, § 12D-101, *et seq.*	**Controllers** (1) (a) Conducts business in Delaware; or (b) produces products or services targeted to Delaware residents; and (2) during preceding calendar year: (a) processed or controlled personal data of at least 35,000 consumers; or (b) (i) processed or controlled personal data of at least 10,000 consumers; and (ii) derived more than 20	**Biometric Data** "'Biometric data' means data generated by automatic measurements of an individual's unique biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that are used to identify a specific individual."	**Controllers/Sensitive Data** • Consent • Data Protection Assessment **Processors** • Controller/Processor Contract • Controller Assistance • Controller Instruction Compliance	**Regulatory Enforcement** **Authority.** The Delaware AG has the authority to enforce DPDPA. **Remedies.** (1) Civil penalties up to $10,000 per violation under the Delaware Consumer Fraud Act; and (2) injunctive relief.

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
	percent of gross revenue from sale of personal data. **Processors** Person or organization that processes personal data on behalf of the controller.	**Sensitive Data** "Sensitive data" includes "biometric data."		
European Union **EU Artificial Intelligence Act (EU AI Act)** **Effective Date: May 21, 2026**[3] Regulation (EU) 2024/0138	**Generally** (1) "Providers" placing on market or putting into service AI systems or placing on market general-purpose AI models (GPAI models) in EU, irrespective of whether providers established/located within EU or in third country; (2) "deployers" of AI systems that have place of establishment or located within EU; (3) providers and deployers of AI systems that have place of establishment or located in third country, where output produced by AI system used in the EU; (4) "importers" and "distributors" of AI systems; and (5) "product manufacturers" placing on market or putting into service AI system together with manufacturer's product and under	**Biometric Data** "'[B]iometric data' means personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, such as facial images or dactyloscopic data." **Special Categories of Personal Data (Sensitive Data)** "'[S]pecial categories of personal data' means the categories of personal data referred to in Article 9(1)" of General Data Protection Regulation (GDPR)," and includes "processing of [] biometric data for the purpose of uniquely identifying a natural person."	**Risk-Based Regulatory Approach** EU AI Act utilizes risk-based regulatory framework, imposing different obligations based on three main risk levels: (1) unacceptable risk; (2) high-risk; and (3) transparency risk. Also included is fourth, non-risk-based classification pertaining to GPAI models.	**Regulatory Enforcement Authority.** EU Member State national competent authorities and newly created European Commission (EC) AI Office have authority to enforce EU AI Act. **Remedies.** Administrative monetary fines up to greater of: (1) 35 million EUR or seven percent worldwide annual turnover for prohibited AI violations; (2) 15 million EUR or three percent worldwide annual turnover for most other violations; and (3) 7.5 million EUR or one percent worldwide annual turnover for violations relating to incorrect, incomplete, or misleading information supplied to authorities.

[3] The bulk of the EU AI Act will go into effect on May 21, 2026, (*i.e.*, two years after publication in the Official Journal of the European Union). Certain elements, however, will take effect before or after the two-year mark; specifically: (1) the prohibition on unacceptable risk AI practices will become applicable in November 2024; (2) the majority of obligations pertaining to GPAI model governance will become applicable in May 2025; and (3) obligations relating to high-risk product components covered by EU harmonization legislation and GPAI models on the market as of the effective date of the AI Act will become applicable in May 2027.

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
	manufacturer's own name or trademark.			
European Union/United Kingdom **EU/UK General Data Protection Regulation (GDPR)** Regulation (EU) 2016/679 UK Data Protection Act 2018	**Generally** Controllers and processors: (1) established in EU/UK; or (2) not established in EU/UK, where personal data processing activities relate to: (a) offering goods or services to EU/UK data subjects; or (b) monitoring behavior of EU/UK data subjects within EU/UK.	**Biometric Data** "'[B]iometric data' means personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (fingerprint) data." **Special Categories of Personal Data (Sensitive Data)** "Special categories of personal data" refers to "[p]rocessing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a person, data concerning health or data concerning a natural person's sex life or sexual orientation."	**Controllers/Sensitive Data** • Consent • Privacy Policy • Data Security • Data Protection Assessment • Data Minimization • DPO Appointment • EU Representative Appointment • Recordkeeping **Processors** • Data Security • Controller/Processor Contract • Controller Instruction Compliance • Duty of Confidentiality • Sub-Processor Engagement Requirements • Cross-Border Data Transfer Restrictions • DPO Appointment • Security Incident Reporting • Recordkeeping	**Private Right of Action** **Private Right of Action.** Any person who suffers damages resulting from GDPR noncompliance has right to receive compensation for damages suffered. **Damages.** Actual material or non-material damage caused by noncompliance. **Regulatory Enforcement** **Authority.** EU and UK Data Protection Authorities have authority to enforce GDPR. **Remedies.** Administrative monetary fines up to greater of: (1) 20 million EUR; or (2) four percent total worldwide annual turnover for preceding financial year.
Florida	**Controllers** (1) Organized or operated for-profit or financial benefit;	**Biometric Data** "'Biometric data' means generated by automatic	**Controllers/Sensitive Data** • Consent • Notice	**Regulatory Enforcement** **Authority.** Florida Department of Legal Affairs

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
Florida Digital Bill of Rights (FDBR) Fla Stat. § 501.701, *et seq.* Fla. Admin. Code Ann. r. 2-3.001, *et seq.*	(2) conducts business in Florida; (3) collects personal data about consumers (or has personal data collected on its behalf); (4) determines purposes and means of processing personal data about consumers; (5) earns over $1 billion global gross annual revenue; and (6) (a) derives at least 50 percent of global gross annual revenue from targeted advertising or sale of online advertisements; (b) operates consumer smart speaker and voice command component service with integrated virtual assistant connected to cloud computing services that uses hands-free verbal activation; or (c) operates app store or digital distribution platform that offers at least 250,000 different software applications for consumers to download and install. **Controller Exemption** Any controller that meets the first four criteria listed above (*i.e.,* for-profit organization, conducts business in Florida, collects consumers' personal data, and determines the purposes and means of processing consumers' personal data) must comply	measurements of an individual's biological characteristics. The term includes fingerprints, voiceprints, eye retinas or irises, or other unique biological patterns or characteristics used to identify a specific individual." **Sensitive Data** "Sensitive data" includes "biometric data processed for the purpose of uniquely identifying an individual."	• Privacy Policy • Data Protection Assessment • Consumer Rights Compliance • Biometric Surveillance Device Prohibition **Controllers/Special Sensitive Data Sale Requirements** • Consent • Notice **Processors** • Controller/Processor Contract • Controller Assistance • Controller Instruction Compliance	has authority to enforce FDBR. **Remedies.** Civil penalties up to $50,000 per violation, which may be tripled for: (1) violation involving known child; (2) failure to delete or correct personal data after receiving authenticated consumer request or directions from controller to delete or correct personal data; and (3) continuing to sell or share personal data after consumer exercises opt-out right.

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
	with FDBR's special notice and consent requirements pertaining to sale of sensitive data. **Processors** Person or organization that processes personal data on behalf of controller.			
Illinois **Illinois Artificial Intelligence Video Interview Act (AIVIA)** 820 ILCS 42/1, *et seq.*	**Generally** Employers that use artificial intelligence analysis during applicant video interviews.	**Covered Data** N/A	**Employers** • Consent • Notice • Data Retention and Destruction • Disclosure Limitation • Data Subject Rights Compliance • AG Reporting	**Enforcement** AIVIA does not specify applicable enforcement mechanism or remedies for noncompliance.
Illinois **Illinois Biometric Information Privacy Act (BIPA)** 740 ILCS 14/1, *et seq.*	**Generally** "Private entities" that collect or process "biometric identifiers" or "biometric information." **Private Entities** "Any individual, partnership, corporation, limited liability company, association, or other group, however organized."	**Biometric Identifiers** "'Biometric identifier' means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." **Biometric Information** "'Biometric information' means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."	**Private Entities** • Consent • Notice • Privacy Policy • Data Retention and Destruction • Disclosure Limitation • Transactional Prohibition • Data Security	**Private Right of Action** **Private Right of Action.** Any person "aggrieved" by BIPA violation has right of action against offending party (actual injury/damage not required). **Damages.** (1) Statutory damages of: (a) $1,000 per negligent violation; or (b) $5,000 per reckless/intentional violation; (2) attorney's fees and costs; and (3) injunctive relief.

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
Indiana **Indiana Consumer Data Protection Act (INCDPA)** **Effective Date: Jan. 1, 2026** Ind. Code § 24-15-1-1, *et seq.*	**Controllers** (1) (a) Conducts business in Indiana; or (b) produces products or services targeted to Indiana residents; and (2) during calendar year: (a) processes or controls personal data of at least 100,000 consumers who are Indiana residents; or (b) (i) processes or controls personal data of at least 25,000 consumers who are Indiana residents; and (ii) derives more than 50 percent of gross revenue from sale of personal data. **Processors** Person or organization that processes personal data on behalf of controller.	**Biometric Data** "'Biometric data' means data that: (1) is generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, images of the retina or iris, or other unique biological patterns or characteristics; and (2) is used to identify a specific individual." **Sensitive Data** "Sensitive data" includes "biometric data that is processed for the purpose of uniquely identifying an individual."	**Controllers/Sensitive Data** • Consent • Data Protection Assessment **Processors** • Controller/Processor Contract • Controller Assistance • Controller Instruction Compliance	**Regulatory Enforcement** **Authority.** The Indiana AG has authority to enforce INCDPA. **Remedies.** (1) Civil penalties up to $7,500 per violation; and (2) attorney's fees and costs.
Iowa **Iowa Consumer Data Protection Act (ICDPA)** **Effective Date: Jan. 1, 2025** Iowa Code § 715D.1, *et seq.*	**Controllers** (1) (a) Conducts business in Iowa; or (b) produces products or services targeted to Iowa residents; and (2) during calendar year: (a) processes or controls personal data of at least 100,000 consumers; or (b) (i) processes or controls personal data of at least 25,000 consumers; and (ii) derives over 50 percent of gross revenue from sale of personal data.	**Biometric Data** "'Biometric data' means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual." **Sensitive Data** "Sensitive data" includes "biometric data that is processed for the purpose of	**Controllers/Sensitive Data** • Notice • Opportunity to Opt-Out **Processors** • Controller/Processor Contract • Controller Assistance • Controller Instruction Compliance	**Regulatory Enforcement** **Authority.** The Iowa AG has authority to enforce ICDPA. **Remedies.** (1) Civil penalties up to $7,500 per violation; (2) attorney's fees and costs; and (3) injunctive relief.

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
	Processors A person or organization that processes personal data on behalf of a controller.	uniquely identifying a natural person."		
Kentucky **Kentucky Consumer Data Protection Act (KCDPA)** **Effective Date: Jan. 1, 2026** Ky. Rev. Stat. Ann. § 367.3611, *et seq.*	**Controllers** (1) (a) Conducts business in Kentucky; or (b) produces products or services targeted to Kentucky residents; and (2) during the calendar year: (a) processes or controls personal data of at least 100,000 consumers; or (b) (i) processes or controls personal data of at least 25,000 consumers; and (ii) derives over 50 percent of gross revenue from sale of personal data. **Processors** Person or organization that processes personal data on behalf of controller.	**Biometric Data** "'Biometric data' means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that are used to identify a specific individual." **Sensitive Data** "Sensitive data" includes "the processing of [] biometric data that is processed for the purpose of uniquely identifying a specific natural person."	**Controllers/Sensitive Data** • Consent • Data Protection Assessment **Processors** • Controller/Processor Contract • Controller Assistance • Controller Instruction Compliance	**Regulatory Enforcement** **Authority.** The Kentucky AG has authority to enforce KCDPA. **Remedies.** (1) Civil penalties up to $7,500 per violation; and (2) attorney's fees and costs.
Maryland **Maryland HB 1202 (HB 1202)** Md. Code Ann., Lab. & Empl. § 3-717	**Generally** Employers that use facial recognition service for the purpose of creating facial template during applicant interview. **Facial Recognition Service** "'Facial recognition service' means technology that analyzes facial features and is used for recognition or persistent tracking of	**Facial Template** "'Facial template' means the machine-interpretable pattern of facial features that is extracted from one or more images of an individual by a facial recognition service."	**Employers** • Consent	**Enforcement** HB 1202 does not specify an applicable enforcement mechanism or remedies for noncompliance.

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
	individuals in still or video images."			
Maryland **Maryland Online Data Privacy Act (MODPA)** **Effective Date: Oct. 1, 2025** Md. Code Ann., Com. Law § 14-4701, *et seq.*	**Controllers** (1) (a) Conducts business in Maryland; or (b) provides products or services targeted to Maryland residents; and (2) during the preceding calendar year: (a) processed or controlled personal data of at least 35,000 consumers; or (b) (i) processed or controlled personal data of at least 10,000 consumers; and (ii) derived over 20 percent of gross revenue from sale of personal data. **Processors** Person or organization that processes personal data on behalf of controller.	**Biometric Data** "'Biometric data' means data generated by automatic measurements of the biological characteristics of a consumer that can be used to uniquely authenticate a consumer's identity. 'Biometric data' includes: (i) A fingerprint; (ii) A voiceprint; (iii) An eye retina or iris image; and (iv) Any other unique biological characteristics that can be used to uniquely authenticate a consumer's identity." **Sensitive Data** "Sensitive data" includes "biometric data."	**Controllers/Sensitive Data** • Privacy Policy • Transactional Prohibition • Data Protection Assessment • Use/Purpose Limitation[4] **Processors** • Controller/Processor Contract • Controller Assistance • Controller Instruction Compliance • Compliance Reporting	**Regulatory Enforcement** **Authority.** Maryland Division of Consumer Protection has authority to enforce MODPA. **Remedies.** (1) Civil penalties up to $10,000 per violation under Maryland Consumer Protection Act; (2) disgorgement; (3) restitution; (4) attorney's fees and costs; and (5) injunctive relief.
Minnesota **Minnesota Consumer Data Privacy Act (MNCDPA)** **Effective Date: July 31, 2025** Minn. Stat. § 325O.01, *et seq.*	**Controllers** (1) (a) Conducts business in Minnesota; or (b) produces products or services targeted to Minnesota residents; and (2) during a calendar year: (a) processes or controls personal data of at least 100,000 consumers; or (b) (i) processes or controls personal data of at least 25,000 consumers; and (ii) derives over 25 percent of	**Biometric Data** "'Biometric data' means data generated by automatic measurements of an individual's biological characteristics, including a fingerprint, a voice print, eye retinas, irises, or other unique biological patterns or characteristics that are used to identify a specific individual."	**Controllers/Sensitive Data** • Consent • Data Protection Assessment **Controllers/Special Sensitive Data Sale Requirement** • Consent **Processors** • Controller/Processor Contract	**Regulatory Enforcement** **Authority.** The Minnesota AG has authority to enforce MNCDPA. **Remedies.** (1) Civil penalties up to $7,500 per violation; (2) attorney's fees and costs; and (3) injunctive relief.

[4] Maryland MODPA contains unique provision that prohibits the collection, sharing, or processing of biometrics data (and other forms of sensitive data) "except where the collection or processing is strictly necessary to provide or maintain a specific product or service requested by the consumer to whom the personal data pertains."

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
	gross revenue from sale of personal data. **Controller Exemption** The MNCDPA provides exemption from compliance for small businesses as defined by federal Small Business Act but requires small businesses to comply with MNCDPA special consent requirement regarding sale of sensitive data. **Processors** Person or organization that processes personal data on behalf of controller.	**Sensitive Data** "Sensitive data" includes "the processing of biometric data [] for the purpose of uniquely identifying an individual."	• Controller Assistance • Controller Instruction Compliance	
Montana **Montana Consumer Data Privacy Act (MCDPA)** Mont. Code Ann. § 30-14-2801, *et seq.*	**Controllers** (1) (a) Conducts business in Montana; or (b) produces products or services targeted to Montana residents; and (2) during calendar year: (a) processes or controls personal data of at least 50,000 consumers; or (b) (i) processes or controls personal data of at least 25,000 consumers; and (ii) derives over 25 percent of gross revenue from the sale of personal data.	**Biometric Data** "'Biometric data' means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises, or other unique biological characteristics that are used to identify a specific individual." **Sensitive Data** "Sensitive data" includes "the processing of [] biometric data for the purpose of uniquely identifying an individual."	**Controllers/Sensitive Data** • Consent • Data Protection Assessment **Processors** • Controller/Processor Contract • Controller Assistance • Controller Instruction Compliance	**Regulatory Enforcement** **Authority.** The Montana AG has authority to enforce MCDPA. **Remedies.** MCDPA does not specify remedies for noncompliance.

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
	Processors Person or organization that processes personal data on behalf of controller.			
Nebraska **Nebraska Data Privacy Act (NEDPA)** **Effective Date: Jan. 1, 2025** Neb. Rev. Stat. § 87-1101, *et seq.*	**Controllers** (1) (a) Conducts business in Nebraska; or (b) produces products or services consumed by Nebraska residents; (2) processes or engages in the sale of personal data; and (3) is not a small business as determined under the federal Small Business Act. **Controller Exemption** Any controller that meets the first two criteria listed above, regardless of small business status, must comply with NEDPA special consent requirement pertaining to sale of sensitive data. **Processors** Person or organization that processes personal data on behalf of controller.	**Biometric Data** "Biometric data means that is used to identify a specific individual through an automatic measurement of a biologic characteristic of an individual and includes any: (i) fingerprint; (ii) voiceprint; (iii) retina image; (iv) iris image; (v) information derived from wastewater; or (vi) unique biological pattern or characteristic." **Sensitive Data** "Sensitive data" includes "biometric data that is processed for the purpose of uniquely identifying an individual."	**Controllers/Sensitive Data** • Consent • Privacy Policy • Data Protection Assessment **Controllers/Special Sensitive Data Sale Requirement** • Consent **Processors** • Controller/Processor Contract • Controller Assistance • Controller Instruction Compliance	**Regulatory Enforcement** **Authority.** The Nebraska AG has authority to enforce NEDPA. **Remedies.** (1) Civil penalties up to $7,500 per violation; (2) attorney's fees and costs; and (3) injunctive relief.
New Hampshire **New Hampshire Privacy Act (NHPA)** **Effective Date: Jan. 1, 2025**	**Controllers** (1) (a) Conducts business in New Hampshire; or (b) produces products or services targeted to New Hampshire residents; and (2) during a one-year period: (a) processed or controlled personal data of at least	**Biometric Data** "'Biometric data' means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises, or other unique biological	**Controllers/Sensitive Data** • Consent • Data Protection Assessment **Processors** • Controller/Processor Contract	**Regulatory Enforcement** **Authority.** The New Hampshire AG has authority to enforce NHPA. **Remedies.** (1) Civil penalties up to $10,000 per violation under New Hampshire Consumer Protection Act; (2)

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
N.H. Rev. Stat. Ann. § 507-H:1, *et seq*.	35,000 unique consumers; or (b) (i) processed or controlled personal data of at least 10,000 unique consumers; and (ii) derived over 25 percent of gross revenue from the sale of personal data. **Processors** Person or organization that processes personal data on behalf of controller.	characteristics that are used to identify a specific individual." **Sensitive Data** "Sensitive data" includes "the processing of [] biometric data for the purpose of uniquely identifying an individual."	• Controller Assistance • Controller Instruction Compliance	restitution; (3) attorney's fees and costs; and (4) injunctive relief.
New Jersey **New Jersey Data Privacy Act (NJDPA)** **Effective Date: Jan. 15, 2025** N.J. Stat. Ann. § 56:8-166.4, *et seq.*	**Controllers** (1) (a) Conducts business in New Jersey; or (b) produces products or services targeted to New Jersey residents; and (2) (a) processes or controls personal data of at least 100,000 consumers; or (b) (i) processes or controls personal data of at least 25,000 consumers; and (ii) derives revenue, or receives discount on price of any goods or services, from sale of personal data. **Processors** Person or organization that processes personal data on behalf of controller.	**Biometric Data** "'Biometric data' means personal data generated by automatic or technological processing, measurements, or analysis of an individual's biological, physical, or behavioral characteristics, including, but not limited to, fingerprint, voiceprint, eye retinas, irises, facial mapping, facial geometry, templates, or other unique biological, physical, or behavioral patterns or characteristics that are used or intended to be used, singularly or in combination with each other or with other personal data, to identify a specific individual." **Sensitive Data** "Sensitive data" includes "biometric data that may be	**Controllers/Sensitive Data** • Consent • Data Protection Assessment **Processors** • Data Security • Controller/Processor Contract • Controller Assistance • Controller Instruction Compliance • Duty of Confidentiality • Sub-Processor Engagement Requirements	**Regulatory Enforcement** **Authority.** The New Jersey AG has authority to enforce NJDPA. **Remedies.** (1) Civil penalties up to: (a) $10,000 per violation for first offense; and (b) $20,000 per violation for subsequent offenses under the New Jersey Consumer Fraud Act; (2) restitution; and (3) reimbursement of costs.

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
		processed for the purpose of uniquely identifying an individual."		
New York **New York Labor Law § 201-a** N.Y. Lab. Law § 201-a	**Generally** Employers and related third-party vendors.	**Fingerprint Data** Not defined by Labor Law 201-a.	**Employers and Vendors** • Prohibition on Mandatory Fingerprinting of Employees or Job Applicants[5]	**Criminal Penalties** **Penalties.** Violation constitutes misdemeanor offense; first violation subject to a fine up to $100; second violation subject to a fine between $100 to $500, imprisonment up to 30 days, or both; subsequent violations subject to a minimum fine of $300, imprisonment up to 60 days, or both.
New York **New York State Education Department Facial Recognition Ban** N.Y. Tech. Law § 106-b	**Generally** Use of "facial recognition technology" or "facial recognition" by New York "Schools." **Facial Recognition/Facial Recognition Technology** Tool using an automated or semi-automated process that assists in uniquely identifying or verifying a person by comparing and analyzing patterns based on the person's face.	**Biometric Information** "'Biometric information' means physical, physiological, or behavioral characteristics that are attributable to a person, including but not limited to facial characteristics, fingerprint characteristics, eye characteristics, vocal characteristics, and any other characteristics that can be used to identify a person including, but not limited to: fingerprints; handprints; retina and iris patterns; DNA sequence; voice; gait; and facial geometry."	**Schools** • Facial Recognition Technology Prohibition	**Regulatory Enforcement** **Authority.** The New York State Commissioner of Education has authority to enforce N.Y. Tech. Law § 106-b. **Remedies.** Withholding of public funding from School.

[5] New York Labor Law § 201-a prohibits employers from requiring employees to be fingerprinted as condition of securing or continuing employment. The New York State Department of Labor (NYDOL) has clarified that it is the initial act of fingerprinting, rather than subsequent use or storage of fingerprints, which is prohibited. Thus, mandatory use of a biometric timekeeping device, for example, violates Labor Law § 201-a. With that said, *voluntary* fingerprinting of employees *is* permissible under Labor Law § 201-a.

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
	Schools New York public or nonpublic elementary schools, secondary schools, and charter schools.			
New York City **New York City "Automated Employment Decision Tools" Ordinance (NYC AEDT Ordinance)** N.Y.C. Admin. Code § 20-870, *et seq.*	**Generally** Employers and employment agencies that use automated employment decision (AEDT) tools[6] to screen candidates or employees for employment decisions.[7] **Employers** Not defined in NYC AEDT Ordinance. **Employment Agencies** Includes all persons who: (1) for a fee, render vocational guidance or counseling services[8]; or (2) maintain job opening/position lists.	**Covered Data** N/A	**Employers and Employment Agencies** • Notice • Privacy Policy • Data Retention and Destruction • Bias Audit	**Regulatory Enforcement** **Authority.** New York City Law Department has authority to enforce NYC AEDT Ordinance. **Remedies.** (1) Civil penalties: (a) up to $500 for first offense; and (b) between $500 and $1,500 for subsequent offenses.
New York City **New York City "Commercial Establishments" Ordinance (NYC**	**Commercial Establishments** "Commercial establishments" that process "biometric identifier information."	**Biometric Identifier Information** "The term 'biometric identifier information' means a physiological or biological characteristic that is used by	**Commercial Establishments** • Public Signage Notice[9] • Transactional Prohibition	**Private Right of Action** **Private Right of Action.** Any person "aggrieved" by violation may commence action against offending party.

[6] NYC AEDT Ordinance defines "automated employment decision tool" as "[a]ny computational process, derived from machine learning, statistical modeling, data analytics, or artificial intelligence, that issues simplified output, including a score, classification, or recommendation, which is used to substantially assist or replace discretionary decision making for making employment decisions that impact natural persons."
[7] NYC AEDT Ordinance defines "employment decision" as "to screen candidates for employment or employees for promotion within the city."
[8] NYC AEDT Ordinance defines "vocational guidance or counseling services" as "services which consist of one or more oral presentations and which: (1) provide information concerning the qualifications generally required for one or more positions or class of positions; or (2) assess, or attempt to assess, the suitability of a person seeking employment for one or more positions or class of positions; or (3) provide information concerning the availability of one or more positions or class of positions."
[9] NYC Commercial Establishments Ordinance requires posting of "clear and conspicuous signage" near all customer entrances providing notice of collection, retention, storage, or sharing (as applicable) of biometric data.

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
Commercial Establishments Ordinance) N.Y.C. Admin. Code § 22-1201, *et seq.*	**Commercial Establishments** "A place of entertainment, a retail store, or a food and drink establishment."	or on behalf of a commercial establishment, singly or in combination, to identify, or assist in identifying, an individual, including, but not limited to: (i) a retina or iris scan, (ii) a fingerprint or voiceprint, (iii) a scan of hand or face geometry, or any other identifying characteristic."		**Damages.** (1) Statutory damages of: (a) $500 per notice requirement violation; (b) $500 per negligent transactional prohibition violation; and (c) $5,000 per reckless or intentional transactional prohibition violation; (2) attorney's fees and costs; and (3) injunctive relief.
New York City **New York City Tenant Data Privacy Act (TDPA)** N.Y.C. Admin. Code § 26-3001, *et seq.*	**Generally** Owners and operators of "smart access buildings" that utilize "smart access systems" which process "biometric identifier information." **Smart Access Buildings** Building or structure used as home or residence that is rented, leased, or otherwise occupied by three or more families living independent of each other. **Smart Access Systems** System that uses biometric identifier information (or other digital technology) grant entry to smart access building, common areas, or individual dwelling units.	**Biometric Identifier Information** "The term 'biometric identifier information' means a physiological, biological or behavioral characteristic that is used to identify, or assist in identifying, an individual, including, but not limited to: (i) a retina or iris scan; (ii) a fingerprint; (iii) a voiceprint; (iv) a scan or record of a palm, hand or face geometry; (v) gait or movement patterns; or (vi) any other similar identifying characteristic."	**Smart Access Building Owners and Operators** • Consent • Privacy Policy • Data Retention and Destruction • Disclosure Limitation • Transactional Limitation • Data Security • Data Minimization • Use/Purpose Limitation	**Private Right of Action** **Private Right of Action.** Any dwelling occupant has the right to bring civil action for violation of TDPA disclosure or transactional limitations. **Damages.** (1) Statutory damages between $200 to $1,000 per violation of disclosure or transactional limitations; and (2) attorney's fees and costs.

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
Oregon **Oregon Consumer Privacy Act (OCPA)** Or. Rev. Stat. § 646A.570, *et seq*.	**Controllers** (1) (a) Conducts business in Oregon; or (b) provides products or services to Oregon residents; and (2) during calendar year: (a) processes or controls personal data of at least 100,000 consumers; or (b) (i) processes or controls personal data of at least 25,000 consumers; and (ii) derives at least 25 percent annual gross revenue from the sale of personal data. **Processors** Person or organization that processes personal data on behalf of controller.	**Biometric Data** "'Biometric data' means personal data generated by automatic measurements of a consumer's biological characteristics, such as the consumer's fingerprint, voiceprint, retinal pattern, iris pattern, gait or other unique biological characteristics that allow or confirm the unique identification of the consumer." **Sensitive Data** "Sensitive data" includes "personal data [] that is biometric data."	**Controllers/Sensitive Data** • Consent • Privacy Policy • Data Protection Assessment **Processors** • Controller/Processor Contract • Controller Assistance • Controller Instruction Compliance	**Regulatory Enforcement** **Authority.** The Oregon AG has authority to enforce OCPA. **Remedies.** (1) Civil penalties up to $7,500 per violation; (2) attorney's fees and costs; and (3) injunctive relief.
Portland, Oregon **Portland, Oregon Facial Recognition Ordinance** Portland, Or. City Code Ch. 34.10	**Generally** "Private entities" that use "face recognition technologies" in places of public accommodation within boundaries of the City of Portland. **Private Entities** "Any individual, sole proprietorship, partnership, corporation, limited liability company, association, or any other legal entity, however organized."	**Covered Data** N/A	**Private Entities** • Face Recognition Technologies Prohibition[10]	**Private Right of Action** **Private Right of Action.** Any person "injured by a material violation" of ordinance has cause of action against non-compliant entity. **Damages.** (1) Statutory damages of $1,000 per day of violation; and (2) attorney's fees.

[10] Portland Facial Recognition Ordinance prohibits use of face recognition technologies in places of public accommodation within boundaries of city of Portland.

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
	Face Recognition Technologies "Automated or semi-automated processes using face recognition that assist in identifying, verifying, detecting, or characterizing facial features of an individual or capturing information about an individual based on an individual's face." **Face Recognition** "Automated searching for a reference image in an image repository by comparing the facial features of a probe image with the features of images contained in an image repository (one-to-many search)."			
Rhode Island **Rhode Island Data Transparency and Privacy Protection Act (RIDPA)** **Effective Date: January 1, 2026** R.I. Gen. Laws § 6-48.1-1, *et seq.*	**Controllers** (1) For-profit entity (2) that (a) conducts business in Rhode Island; or (b) produce products or services targeted to Rhode Island residents; and (3) during the preceding calendar year: (a) processed or controlled personal data of at least 35,000 consumers; or (b) (i) processed or controlled personal data of at least 10,000 consumer; and (ii) derived more than 20 percent of gross revenue from sale of personal data.	**Biometric Data** "'Biometric data' means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual." **Sensitive Data** "Sensitive data" includes "the processing of [] biometric	**Controllers/Sensitive Data** • Consent • Data Protection Assessment **Processors** • Controller/Processor Contract • Controller Assistance • Controller Instruction Compliance	**Regulatory Enforcement** **Authority.** Rhode Island AG has authority to enforce RIDPA. **Remedies.** (1) Civil penalties of up to $10,000 per violation; and (2) injunctive relief.

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
	Processors Person or organization that processes personal data on behalf of controller.	data for the purpose of uniquely identifying an individual."		
Tennessee **Tennessee Ensuring Likeness, Voice, and Image Security Act of 2024 (ELVIS Act)** Tenn. Code Ann. § 47-25-1101, *et seq.*	**Generally** "Persons" who use the name, photograph, voice, or likeness of another individual without consent. **Persons** Individual, firm, association, partnership, corporation, joint stock company, syndicate, receiver, common law trust, conservator, statutory trust or any other concern however organized, formed, or created; includes non-profit corporations, associations, educational and religious institutions, political parties, community and civic organizations, and other organizations. **Individuals** "Human being, living or dead."	**Likeness** "Use of an image of an individual for commercial purposes." **Photographs** "Any photograph or photographic reproduction, still or moving, or any videotape or live television transmission, of any individual, so that the individual is readily identifiable." **Voice** "A sound in a medium that is readily identifiable and attributable to a particular individual, regardless of whether the sound contains the actual voice or a simulation of the voice of the individual."	**Persons** • Prohibition on Unauthorized Use of Name, Photograph, Voice, or Likeness	**Private Right of Action** **Private Right of Action.** Any person subject to knowing violation of ELVIS Act has cause of action against infringing person. **Damages.** (1) Actual damages; (2) attributable profits; (3) seizure or destruction of infringing materials; and (4) other injunctive relief.[11] **Criminal Penalties** **Penalties.** Violation constitutes a Class A misdemeanor offense, subject to fine up to $2,500 and/or imprisonment up to 12 months.
Tennessee **Tennessee Information Protection Act (TIPA)**	**Controllers** (1) (a) Conducts business in Tennessee; or (b) produces products or services that target Tennessee residents; (2) exceeds $25 million revenue; and (3) during	**Biometric Data** "'Biometric data' means data generated by automatic measurement of an individual's biological characteristics, such as a fingerprint, voiceprint, eye	**Controllers/Sensitive Data** • Consent • Data Protection Assessment	**Regulatory Enforcement** **Authority.** The Tennessee AG has authority to enforce TIPA. **Remedies.** (1) Civil penalties up to $7,500 per violation; (2)

[11] Tennessee ELVIS Act provides for trebling of actual damages and attributable profits, as well as attorney's fees and costs, for knowing violation involving member of armed forces.

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
Effective Date: July 1, 2025 Tenn. Code Ann. § 47-18-3301, *et seq.*	calendar year: (a) processes or controls personal information of at least 175,000 consumers; or (b) (i) processes or controls personal information of at least 25,000 consumers; and (ii) derives more than 50 percent of gross revenue from the sale of personal data. **Processors** Person or organization that processes personal data on behalf of controller.	retina or iris, or other unique biological patterns or characteristics that are used to identify a specific individual." **Sensitive Data** "Sensitive data" includes "the processing of [] biometric data for the purpose of uniquely identifying a natural person."	**Processors** • Controller/Processor Contract • Controller Assistance • Controller Instruction Compliance	treble damages for willful or knowing violations; (3) attorney's fees and costs; and (4) injunctive relief.
Texas **Texas Capture or Use of Biometric Identifiers Act (CUBI)** Tex. Bus. & Com. Code § 503.001	**Generally** "Persons" that capture or collect "biometric identifiers" for a commercial purpose. **Persons** Not defined by CUBI.	**Biometric Identifiers** "'[B]iometric identifier' means a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry."	**Persons** • Consent • Notice • Data Retention and Destruction • Disclosure Limitation • Transactional Limitation • Data Security	**Regulatory Enforcement Authority.** The Texas AG has authority to enforce CUBI. **Remedies.** Civil penalties of up to $25,000 per violation.
Texas **Texas Data Privacy and Security Act (TDPSA)** Tex. Bus. & Com. Code § 541.001, *et seq.*	**Generally** (1) (a) Conducts business in Texas; or (b) produces a product or service in Texas; (2) processes or engages in sale of personal data; and (3) is not a small business as defined by the U.S. Small Business Administration. **Controller Exemption** Any controller that meets the first two criteria listed above,	**Biometric Data** "'Biometric data' means data generated by automatic measurements of an individual's biological characteristics. The term includes a fingerprint, voiceprint, eye retain or iris, or other unique biological pattern or characteristic that is used to identify an individual."	**Controllers/Sensitive Data** • Consent • Notice • Privacy Policy • Data Protection Assessment **Controllers/Special Sensitive Data Sale Requirement** • Consent	**Regulatory Enforcement Authority.** The Texas AG has authority to enforce TDPSA. **Remedies.** (1) Civil penalties up to $7,500 per violation; (2) attorney's fees and costs; and (3) injunctive relief.

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
	regardless of small business status, must comply with TDPSA special consent requirement pertaining to sale of sensitive data. **Processors** Person or organization that processes personal data on behalf of controller.	**Sensitive Data** "Sensitive data" includes "biometric data that is processed for the purpose of uniquely identifying an individual."	**Processors** • Controller/Processor Contract • Controller Assistance • Controller Instruction Compliance	
Utah **Utah Artificial Intelligence Policy Act (Utah AI Policy Act)** Utah Code Ann. § 13-70-101, *et seq.*	**Generally** "Actors" and "persons" that use "generative artificial intelligence" (Gen AI). **Actors/Persons** Not defined by the Utah AI Policy Act. **Gen AI** An artificial system that: (1) is trained on data; (2) interacts with a person using text, audio, or visual communication; and (3) generates non-scripted outputs similar to outputs created by a human, with limited or no human oversight.	**Biometric Data** "(a) 'Biometric data' means data generated by automatic measurements of an individual's biological characteristics. (b) 'Biometric data' includes data described in Subsection (6)(a) that are generated by automatic measurements of an individual's fingerprint, voiceprint, eye retinas, irises, or any other unique biological pattern or characteristic that is used to identify a specific individual." **Sensitive Data** "Sensitive data" includes "the processing of [] biometric data, if the processing is used for the purpose of identifying a specific individual." **Synthetic Data** "'Synthetic data' means data that has been generated by	**Actors and Persons** • Notice • Prohibition on Gen AI Outputs That Violate Utah Consumer Protection Law	**Regulatory Enforcement** **Authority.** Utah Division of Consumer Protection has authority to enforce Utah AI Policy Act. **Remedies.** (1) Civil penalties up to $2,500 per violation; (2) monetary disgorgement; (3) restitution; and (4) injunctive relief.

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
		computer algorithms or statistical models and does not contain personal data."		
Utah **Utah Consumer Privacy Act (UCPA)** Utah Code Ann. § 13-61-101, *et seq.*	**Controllers** (1) (a) Conducts business in Utah; or (b) produces a product or service targeted to consumers who are Utah residents; (2) annual revenue of at least $25 million; and (3) (a) during calendar year, processes or controls personal data of at least 100,000 consumers; or (b) (i) processes or controls personal data of at least 25,000 consumers; and (ii) derives over 50 percent of gross revenue from sale of personal data. **Processors** Person or organization that processes personal data on behalf of controller.	**Biometric Data** "'Biometric data' means data generated by automatic measurements of an individual's biological characteristics. 'Biometric data' includes data generated by automatic measurements of an individual's fingerprint, voiceprint, eye retinas, irises, or any other unique biological pattern or characteristic that is used to identify a specific individual." **Sensitive Data** "Sensitive data" includes "the processing of [] biometric data, if the processing is used for the purpose of identifying a specific individual."	**Controllers/Sensitive Data** • Notice • Opportunity to Opt-Out **Processors** • Controller/Processor Contract • Controller Assistance • Controller Instruction Compliance	**Regulatory Enforcement** **Authority.** The Utah AG has authority to enforce UCPA. **Remedies.** (1) Civil penalties up to $7,500 per violation; and (2) actual damages.
Virginia **Virginia Consumer Data Protection Act (VCDPA)** Va. Code Ann. § 59.1-575, *et seq.*	**Controllers** (1) (a) Conducts business in Virginia; or (b) produces products or services targeted to Virginia residents; and (2) during calendar year: (a) processes or controls personal data of at least 100,000 consumers; or (b) (i) processes or controls personal data of at least 25,000 consumers; and (ii)	**Biometric Data** "'Biometric data' means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual."	**Controllers/Sensitive Data** • Consent • Data Protection Assessment **Processors** • Controller/Processor Contract • Controller Assistance • Controller Instruction Compliance	**Regulatory Enforcement** **Authority.** The Virginia AG has authority to enforce VCDPA. **Remedies.** (1) Civil penalties up to $7,500 per violation; (2) attorney's fees and costs; and (3) injunctive relief.

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
	derives over 50 percent of gross revenue from sale of personal data. **Processors** Person or organization that processes personal data on behalf of controller.	**Sensitive Data** "Sensitive data" includes "the processing of [] biometric data for the purpose of uniquely identifying a natural person."		
Washington **Washington My Health My Data Act (MHMDA)** Wash. Rev. Code § 19.373.050, *et seq.*	**Controllers** (1) (a) Conducts business in Washington; or (b) produces or provides products or services targeted to consumers in Washington; and (2) determines purpose and means of processing consumer health data. **Processors** Person or organization that processes consumer health data on behalf of a controller.	**Biometric Data** "'Biometric data' means data that is generated from the measurement or technological processing of an individual's physiological, biological, or behavioral characteristics and that identifies a consumer, whether individually or in combination with other data. 'Biometric data' includes but is not limited to: (a) Imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template can be extracted; or (b) keystroke patterns or rhythms and gait patterns or rhythms that contain identifying information." **Consumer Health Data** Includes "biometric data."[12]	**Controllers** • Consent • Data Security • Consumer Rights Compliance • Geofencing Restrictions • Authorization for Sale of Consumer Health Data **Processors** • Controller/Processor Contract • Controller Assistance	**Regulatory Enforcement** **Authority.** The Washington AG has authority to enforce MHMDA. **Remedies.** (1) Civil penalties up to $7,500 per violation under Washington CPA; (2) disgorgement; (3) restitution; (4) attorney's fees and costs; and (5) injunctive relief.

[12] Washington MHMDA defines "consumer health data" as "personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status."

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
Washington **Washington RCW Chapter 19.375 (HB 1493)** Wash. Rev. Code § 19.375.010, *et seq.*	**Generally** "Persons" who capture or enroll a "biometric identifier" for a commercial purpose. **Persons** "An individual, partnership, corporation, limited liability, company, organization, association, or any other legal or commercial entity."	**Biometric Identifiers** "'Biometric identifier' means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual."	**Persons** • Consent • Notice • Data Retention and Destruction • Disclosure Limitation • Transactional Limitation • Data Security • Use/Purpose Limitation • Mechanism to Prevent Subsequent Use of Biometric Data[13]	**Regulatory Enforcement** **Authority.** The Washington AG has authority to enforce HB 1493. **Remedies.** (1) Civil penalties up to $7,500 per violation under Washington Consumer Protection Act (Washington UDAP); (2) disgorgement; (3) restitution; (4) attorney's fees and costs; and (5) injunctive relief.

[13] Washington HB 1493 requires implementation of mechanism to prevent subsequent use of biometric data; must be in place prior to collection of biometric data.