Kentucky Consumer Data Protection Act Summary

On April 4, 2024 Governor Andy Beshear (D) signed HB 15, the "**Kentucky Consumer Data Protection Act**" into law. The Act's provisions take effect on **January 1, 2026**. A non-comprehensive summary of significant elements of the Act follows:

Covered Entities	The **Kentucky Consumer Data Protection Act** applies to a person that conducts business in Kentucky or produces products or services that are targeted to residents of Kentucky and that during a calendar year control or process personal data of at least 100,000 consumers, or 25,000 consumers and derive over 50% of gross revenue from the sale of personal data.
Covered Data	***"Personal data"***: any information that is linked or reasonably linkable to an identified or identifiable natural person. Personal data does not include de-identified data or publicly available information. ***"Biometric data"***: 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. "Biometric data" does *not* include a physical or digital photograph, a video or audio recording or data generated therefrom unless that data is generated to identify a specific individual or information collected, used, or stored for health care treatment, payment, or operations under HIPAA. "***Publicly available information"***: information that is lawfully made available through federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience. ***"Sensitive data"***: personal data that includes: (a) data indicating racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; (b) the processing of genetic or biometric data that is processed for the purpose of uniquely identifying a specific natural person; (c) the personal data collected from a known child, or; (d) precise geolocation data.
Key Definitions	***"Consent"***: a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. "Consent" may include a written statement, written by electronic means, or any other unambiguous affirmative action. ***"De-Identified Data"***: data that cannot reasonably be linked to an identified or identifiable natural person. ***"Process"***: any operation or set of operations performed whether by manual or automated means, on personal data or on sets of personal data, including but not limited to the collection, use, storage, disclosure, analysis, deletion or modification of personal data. ***"Pseudonymous Data"***: personal data that cannot be attributed to a specific natural person without the use of additional information, provided that the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person. ***"Targeted Advertising"***: displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across

	nonaffiliated websites or online applications to predict such consumer's preferences or interests. ***"Sale of Personal Data"***: the exchange of personal data for monetary consideration by the controller to a third party. "Sale of personal data" does not include: (a) the disclosure of personal data to a processor that processes the personal data on behalf of the controller; (b) the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer; (c) the disclosure or transfer of personal data to an affiliate of the controller; (d) the disclosure of information that the consumer intentionally made available to the general public via a channel of mass media and did not restrict to a specific audience; (e) the disclosure or transfer of personal data to a third party as an asset that is part of a proposed or actual merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.
Consumer Rights	**Access:** A consumer has the right to confirm whether a controller is processing the consumer's personal data and to access such personal data, unless the confirmation and access would require the controller to reveal a trade secret. **Affirmative Consent:** A controller shall not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of processing of sensitive data collected from a known child, process the data in accordance with COPPA. **Correction:** A consumer has the right to correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of processing the data. **Deletion**: A consumer has the right to delete personal data provided by or obtained about the consumer. **Portability:** A consumer has the right to obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically practicable, readily usable format that allows the consumer to transmit the data to another controller without hindrance, weather the processing is carried out by automated means. The controller shall not be required to reveal any trade secrets. **Opt Out Rights**: A consumer has the right to opt out of the sale of personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.
Business Obligations	**Responding to Consumer Requests**: A controller shall respond to a consumer without undue delay, but in all cases within 45 days of receipt of a request. The response period may be extended once by 45 days when reasonably necessary, taking into consideration the complexity and number of the consumer's requests, so long as the controller informs the consumer of any extension within the initial 45-day response period, together with the reason for the extension. If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer no later than 45 days after receipt of the request, of the justification for declining to take action and instructions on how to appeal the decision. A controller must provide a response to a consumer request free of charge, up to twice annually per consumer. The controller bears the burden of demonstrating the excessive, repetitive, technically infeasible, or manifestly unfounded nature of any denied requests. A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process shall be conspicuously available and similar to the process for submitting requests. Within 60 days of receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is

	denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Attorney General to submit a complaint. **Purpose Specification:** A controller shall not process personal data for any purpose other than those expressly listed. A controller may process personal data to the extent that such processing is: (a) reasonably necessary and proportionate to the purposes listed, and; (b) adequate, relevant and limited to what is necessary in relation to the specific purposes listed. **Avoid Secondary Use**: A controller shall not process personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which the personal data is processed as disclosed to the consumer, unless the controller obtains the consumer's consent. **Data Security**: A controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data security practices shall be appropriate to the volume and nature of the personal data at issue. **Disclosure**: A controller shall clearly and conspicuously disclose the sale of personal data to third parties or processing of personal data for targeted advertising in addition to the manner in which a consumer may exercise the right to opt out of such activity. **No Unlawful Discrimination:** A controller shall not process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers. A controller shall not discriminate against a consumer for exercising any consumer rights, including denying goods and services, charging different prices or rates for goods or services, or providing a different level of quality of goods and services to the consumer. **Transparency**: Controllers shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes (1) the categories of personal data processed by the controller; (2) the purpose for processing personal data; (3) how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request; (4) the categories of personal data that the controller shares with third parties; (5) the categories of third parties, if any, with whom the controller shares personal data.
Data Protection Assessments	A controller shall conduct and document a data protection impact assessment of each of the following processing activities involving personal data: (a) the processing of personal data for purposes of targeted advertising; (b) the processing of personal data for the purposes of selling of personal data; (c) the processing of personal data for the purposes of profiling, where the profiling presents a reasonably foreseeable risk of (i) unfair or deceptive treatment of consumers or disparate impact on consumers; (ii) financial, physical, or reputational injury to consumers; (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where an intrusion would be offensive to a reasonable person, or; (iv) other substantial in injury to consumers; (d) the processing of sensitive data, and; (e) any processing of personal data that presents a heightened risk of harm to consumers. Data protection impact assessments must identify and weigh the benefits that may flow, directly or indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce the risk. The use of de-identified data and the reasonable expectations of the consumers as well as the context of the processing of personal data and the relationship between the controller and the consumer whose personal data will be

	processed shall be factored into the controller's assessment. The attorney general may require that a controller disclose any data protection assessment that is relevant to an investigation being conducted by the attorney general and reporter and the controller shall make assessment available. The attorney general may evaluate the assessment for compliance. Data protection assessments are confidential and exempt from disclosure, public inspection, and copying.
Controller / Processor Distinction	**A processor shall adhere to the instructions of a controller and assist the controller** in meeting its obligations under the Kentucky Consumer Data Protection Act. A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and shall clearly set forth instructions for processing personal data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The contract shall also include requirements that the processor shall: (1) ensure that each person processing personal data is subject to a duty of confidentiality; (2) at the controller's discretion, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law; (3) upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with obligations; (4) allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor. Alternatively, the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of obligations of this Act using an appropriate and accepted control standard or framework and assessment procedure for assessments. The processor shall provide a report of the assessment to the controller upon request, and; (5) engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor.
Exceptions and Exemptions	A controller may disclose pseudonymous data or de-identified data with an exercise of reasonable oversight to monitor compliance with any contractual commitments. The Kentucky Consumer Data Protection Act shall not be construed to restrict a controller's or processor's ability to: (a) comply with laws; (b) comply with inquiries by government authorities; (c) cooperate with law-enforcement agencies; (d) prepare for and defend legal claims; (e) provide a product or service requested by a consumer or parent or guardian of a known child; (f) perform a contract to which the consumer or parent or guardian of a known child is party, including fulfilling the terms of a written warranty; (g) take steps at the request of the consumer or parent or guardian of a known child prior to entering into a contract; (h) protect interests essential for life or physical safety of the consumer; (i) prevent, detect and protect against security incidents; (j) preserve the security of systems; (k) investigate, report or prosecute those responsible for any such action; (j) engage in scientific or statistical research in the public interest; (i) assist third parties with the obligations of the Kentucky Consumer Data Protection Act. Data exempt from the Kentucky Consumer Data Protection Act includes: protected information under HIPAA, the Health Care Quality Improvement Act of 1986, the Patient Safety and Quality Improvement Act, the Fair Credit Reporting Act, the Driver's Privacy Protection Act of 1994, FERPA, the Farm Credit Act, Combat Methamphetamine Epidemic Act of 2005, and COPPA.

Enforcement	The Kentucky Consumer Data Protection Act does not provide the basis for, or give rise to, a private right of action for violations of this Act. **Right to Cure**: The Attorney General shall have exclusive authority to enforce violations of the Act and shall provide a controller or processor 30 days' written notice identifying specific provisions being violated. Any controller or processor that violates the Act is subject to an injunction and liable for a civil penalty of not more than $7,500 for each violation. All civil penalties collected under the Act shall be paid into the consumer privacy fund established under Section 10 of the Act. There is no sunset specified for the right to cure.