American Council of Life Insurers
American Property Casualty Insurance Association
Independent Insurance Agents of Wisconsin
National Association of Insurance and Financial Advisors - Wisconsin
National Association of Mutual Insurance Companies
Professional Insurance Agents of Wisconsin
Wisconsin Bankers Association
Wisconsin Council of Life Insurers
Wisconsin Credit Union League
Wisconsin Insurance Alliance

February 23, 2021

The Honorable Shannon Zimmerman
State Representative
Room 324 East
State Capitol
PO Box 8953
Madison, WI 53708

Dear Representative Zimmerman:

Thank you for taking the time to meet with us individually regarding the proposed Wisconsin Data Privacy Act ("WDPA"). We appreciate the opportunity to provide additional feedback outlining our concerns with the legislation as introduced last session and are committed to working with you to update Wisconsin's data privacy laws as appropriate. As representatives of the insurance, financial institutions, and financial services industries in the State of Wisconsin, we are writing collectively to share our concerns with the WDPA as introduced last session.

This past summer we submitted testimony to the Department of Agriculture, Trade, and Consumer Protection ("DATCP") Data Privacy and Security Advisory Committee ("DPSAC") which underscored three primary principles that need to be considered when developing recommendations for revising Wisconsin's data privacy and security laws and regulations:

1. Ensure harmonization between existing regulatory structure and requirements;

2. Retain and expand risk-based regulations, which balance consumer expectations with the ability of businesses to effectively operate and innovate; and

3. Proceed incrementally so that Wisconsin businesses and consumers have time to adapt and do not suddenly find themselves at a significant disadvantage.

We believe that by following these principles, the WDPA can be improved to protect consumers' interests in personal data through the efficient use of existing regulatory structures and processes, such as those already in place in the financial services sector.

As representatives of the insurance, financial institutions, and financial services industries, our member companies are committed to protecting data privacy and security. We operate in industries subject to numerous, specific data privacy and security requirements and regulations, and where additional industry specific regulations are already being contemplated by the regulatory bodies with knowledge of the various uses of data within our industries and expertise in how our industries operate.

The sweeping nature of the WDPA does not account for the existing regulations and regulatory authorities that oversee our industries. For regulated industries, this would create an additional web of regulations, subjecting different types of data to different regulatory requirements with different state agencies.

For this reason, we request that the WDPA be narrowed to further exempt highly regulated industries like insurance and financial services that are already subject to extensive data regulation. This exemption should apply at the "entity" level, rather than the type of data or information.[1] Recognizing the industry specific policy development and enforcement of our existing regulatory structures will allow for more targeted and effective regulations that protect consumers' privacy expectations. Importantly, it will also avoid stifling existing business practices and opportunities for innovation.

We believe this approach will ultimately result in numerous benefits, including:

- Promoting harmonization with existing data regulatory requirements and regulatory agencies.

- Encouraging development of complementary regulations and requirements administered by regulators with a knowledge of the regulated industry, how regulated entities use consumer information, and an understanding of the existing regulatory framework. For instance, this session the Legislature will again be considering the National Association of Insurance Commissioners' ("NAIC") model data cybersecurity law regulating all "licensees" of the Office of the Commissioner of Insurance.[2]

- Utilizing the subject matter expertise of existing regulators who already have regulatory authority over the entity, relationships with the entity, and insight into the entity's operations from other regulatory requirements.

[1] The WDPA already provides limited exemptions for certain classes of "information" regulated by various federal laws and certain specified entities (e.g. hospitals). *See* 2019 AB 870, p.9, line 8.

[2] Similarly, the NAIC's Privacy Protections Working Group was formed in late 2019 and is charged with reviewing "state insurance privacy protections regarding the collection, use and disclosure of information gathered in connection with insurance transactions" and making recommend changes to certain NAIC model laws. The working group is considering a "gap analysis" of the specific privacy requirements with which certain insurers and licensees must comply, including HIPAA, GLBA, CCPA, GDPR, and other NAIC models.

- Creating a more efficient regulation that minimizes the cost of compliance by avoiding duplicative or potentially inconsistent requirements.

- Creating stronger compliance with whatever requirements ultimately apply to a specific industry by granting enforcement authority with the primary licensing/permitting regulatory authority for the entity.

- Creating more efficient and effective regulation by locating enforcement within the various industry regulators (e.g., OCI or DFI), rather than a single entity (e.g., DOJ or DATCP) that would be burdened with every entity within the entire state.

Specific Concerns

You have requested that we provide a list of specific concerns or objections with the WDPA as currently drafted. We believe the list below underscores the challenge of enacting a single regulatory framework for all data "controllers" and "processors" in the state, and why industry specific regulations will lead to a better result for consumers and businesses in Wisconsin.

We believe it is important to consider the challenges that the uniform application of the WDPA to all data controllers and processors creates. As currently drafted, the WDPA would apply uniformly to: (1) an insurance company using data to underwrite its insureds, (2) a small pizza parlor using consumer data to market a promotion to its consumers, and (3) to a company that is actively engaged in the commoditization of consumer data for sale to others.

Each of these entities would have vastly different purposes for the processing consumer data and importantly, consumers would have vastly different interests and expectations regarding how a business processes their data. Accordingly, the appropriate regulatory approach to address each of these concerns may vary greatly.

- *Personal Data.* The defined term "personal data" should be further clarified and harmonized for consistency with regulations of other states. As currently proposed the definition is broad and encompasses nearly any information relating to a consumer through which the consumer could be directly or indirectly identified, including routine information (e.g., name, address, email address, phone number), highly personal information (e.g., genetic, mental, physiological, economic), and vague information (e.g., cultural or social identity).[3] This definition should be further refined to be more risk focused in addressing information in which the consumer has a greater expectation in privacy, through which harm could come from the use of the data, or in which the controller has no legitimate use of the information. There should also be some consideration for the legitimate uses of data by various industries. Finally, personal data should exclude business contact information that is freely posted online, as well as any other information that can be shown to be publicly available (through no violation of the law) or otherwise exists in federal, state, or local governmental records. Delineating between personal data that is already public or in governmental records, and more sensitive personal data, will more closely match consumer expectations and allow the sharing of business contact information without onerous legal requirements. The California

[3] *See* 2019 AB 870, p.3, line 1.

Consumer Privacy Act ("CCPA") excludes publicly available information from its definition of personal information and currently has a moratorium on the majority of its requirements applying to business-to-business personal information, for that exact reason. The California Privacy Rights Act, which will go into effect on January 1, 2023, continues this structure by broadening its holistic exclusion of publicly available information from its regulatory scope. Harmonizing this definition and the scope of the WDPA with the requirements of other states would also decrease the cost of compliance for businesses and avoid making Wisconsin an outlier.

- *Notifications*. The WDPA requires that if a controller intends to process a consumer's personal data and the controller did not receive it directly from the consumer, the controller must notify the consumer within thirty days.[4] This will lead to the proliferation of notices between businesses and consumers as some of the more routine "personal data" under the WDPA is shared amongst business contacts and referrals, like the business contact information (or business-to-business personal information) discussed above. For instance, if an insurance agent was provided the name, email address, and telephone number of a prospect by a friend, the agent would need to contact the prospect and provide the full disclosure identified in WDPA. While this notification requirement has exemptions,[5] those exemptions do not account for a variety of situations, including where: (a) the consumer has provided consent to transfer the personal data to the controller; (b) the transfer of personal data is required by applicable law; or (c) the transfer is necessary for fraud prevention, information security, or other compliance purposes.

- *Broad definition of "controller*." The WDPA does not contain any exemptions for small businesses, and would require significant resources for small businesses to obtain compliance.[6] Some accommodations for smaller entities that lack the resources for large scale data processing operations in the first place would be appropriate. It also may be appropriate to focus on the purposes for which the controller uses consumer data. Furthermore, the regulations do not explain how joint-controllers may comply with the law—do they each need to provide notice, or can just one controller meet the requirements of the WDPA?

- *Broad definition of "process."* The WDPA contains a broad definition of "process" that includes collecting, storing, using, and even deleting personal information.[7] This fails to consider the legitimate uses of personal data, or target perceived problematic uses of personal data. The WDPA could be improved by addressing any specific problematic business practices or models. For instance, a more tailored approach would be to create an exemption for processing that is consistent with an entity's existing business practices (e.g., insurance

[4] *See* 2019 AB 870, p.4, line 13.

[5] *See* 2019 AB 870, p.5, line 12.

[6] *See* 2019 AB 870, p.2, line 4.

[7] *See* 2019 AB 870, p.3, line 10.

underwriting) or marketing (e.g., business card drawings at a sandwich shop), or focusing specifically on entities that process and sell personal data as a business practice.

- *Opt-In Structure.* The WDPA creates a new "opt-in" structure that is inconsistent with the existing "opt-out" approach of other states as well as the longstanding obligations of insurers under Gramm-Leach-Bliley Act, the CCPA, and the Fair Credit Reporting Act.[8] The WDPA could be improved by adopting an "opt-out" structure that is consistent with existing consumer expectations, as well as the approach of other states and existing laws. The existing structures allow for joint marketing efforts (GLBA) or the sale of information (CCPA), while allowing making it easy for consumers to opt-out.

- *Administrative Burden.* The WDPA would also require all businesses to maintain records of processing activities.[9] Documenting how an entity processes personal information, including in emails, on phone calls, and in in-person interactions, would cost significant time and financial resources. This is one of the most challenging aspects of GDPR, and companies across the globe continue to struggle with this requirement. Additionally, there is limited benefit to consumers from requiring businesses maintain these records to offset the substantial compliance costs for businesses.

- *Excessive Fines.* The WDPA propose fines over $20 million, and could be read to propose a minimum fine of $10 million.[10] These fines are far in excess of those imposed under the CCPA, which provides fines of $2,500 for negligent violations and $7,500 for intentional violations. The CCPA also provides a thirty (30) day period to cure any violation, which demonstrates the understanding that most violations of privacy statutory regimes are unintentional or arise from a lack of resources. Any fine amounts that are measured in the millions of dollars (or even hundreds or tens of thousands of dollars) are sure to make Wisconsin an unappetizing place to conduct business.

- *Decreased opportunities for Wisconsin consumers*. All that is required to come under regulation of the WDPA is collecting personal data of a Wisconsin consumer. The regulatory compliance costs associated with the notice, restriction, and deletion components of the WDPA and the excessive fines associated with noncompliance are likely to deter non-Wisconsin businesses from doing business with a Wisconsin consumer, let alone consider relocating to or expanding an existing presence in the state. Other privacy laws have revenue thresholds (like $25 Million under CCPA) or relate to the number of personal information records subject to the regulation that are in the possession of a particular entity, rather than applying the law to every business, sole proprietorship, independent contractor, or other "person" that collects personal data.

[8] *See* 2019 AB 872, p.4, line 5.

[9] *See* 2019 AB 872, p.8, line 8.

[10] *See* 2019 AB 870, p.10, line 16.

- *Breach notification requirements*.[11] Highly regulated industries, such as insurance and financial institutions, should be subject to breach notification requirements administered by their functional regulators instead of creating a new requirement to notify DOJ of any personal data breach. For other entities, the WDPA should harmonize the breach notifications with those already administered by the DATCP, rather than creating a new, notification to DOJ covering all personal data. Notifications should be targeted to breaches of sensitive information such as credit numbers, social security numbers, and biometric information. This is the standard under data breach laws across the United States. Even the CCPA, which defines personal information broadly, has limited the data breach notification requirements to sensitive information, rather than any unauthorized disclosure of personal data. Requiring breach notification for any personal data will flood regulators and consumers with breach notification letters and make it more likely that consumer will ignore such notifications when they should be taking them seriously.

- *Data Subject Rights*. The WDPA contains various data subject rights, including the right of access[12] and the right of deletion,[13] but fails to consider other reasonable clarifications or exemptions to those data subject rights that are consistent with consumer expectations and necessary for the operation of a business. Specifically, the right to access personal data should include, for example: (a) an exemption from disclosing personal data that is subject to an ethical or statutory obligation of confidentiality; (b) a clarification that a controller need not disclose records containing duplicate personal data; (c) a clarification that entities are permitted to redact other personal data or confidential information in any record before disclosing it to a consumer; and (d) a clarification, like in CCPA, that Social Security numbers, bank account information, passwords and other sensitive information, need not be disclosed if it could cause fraud or data security concerns. Similarly, the right to deletion should include, for example: (x) an exemption that controllers are not required to delete personal data if it is used solely for internal purposes consistent with the expectations of consumers; (y) a clarification that deletion of personal data in backups or other archival systems of a controller is not required; and (z) a clarification that controllers may aggregate, anonymize, or otherwise de-identify personal data rather than delete it.

- *Undefined Terms.* There are several undefined terms within the WDPA that require greater specificity and would likely require tailoring to the practices of specific industries. Controllers are required to inform the consumer of whether they will use the consumer's personal data to conduct "automated decision-making."[14] This term is undefined and to the extent that it involves underwriting or eligibility decisions, it may relate to other regulations adopted by financial and insurance functional regulators. Similarly, the WDPA provides exceptions allowing the processing of information "for reasons of substantial public interest"

[11] *See* 2019 AB 870, p. 7, line 18.

[12] *See* 2019 AB 870, p.5, line 18.

[13] *See* 2019 AB 871, p.2, line 7.

[14] *See* 2019 AB 870, p.4, line 6; p.5, line 5.

or if processor or a 3rd party "has a legitimate ground to process the personal data."[15] Rather than further prescribing these terms in the WDPA or delegating rulemaking authority to a central regulator, the WDPA should allow functional regulators to take the lead in developing industry specific data privacy regulations.

- *Private Right of Action.* We recommend expressly stating in the WDPA that a violation should not be construed as providing a private cause of action, similar to language in the proposed the insurance data cybersecurity legislation that will be considered again this session.

Thank you again for the opportunity to comment on the WDPA. We appreciate your commitment to updating Wisconsin's data privacy laws and hope to continue working with you to find solutions that appropriately balance the numerous important policy considerations this issue presents.

24879077.1

[15] *See* 2019 AB 872, p. 5, line 14; p. 6, line 16.