

CYBERSECURITY AND DATA PRIVACY INFORMATION MEMO

JUNE 4, 2024

American Privacy Rights Act

On April 7, 2024, Representative Cathy McMorris Rodgers and Senator Maria Cantwell introduced the American Privacy Rights Act (APRA) setting forth national data privacy rights and proposing a single, comprehensive federal data privacy law. This bipartisan legislation, if enacted, will provide for enhanced consumer protections, transparency, and data minimization, while eliminating the patchwork, state-specific data privacy protections in place currently and creating a unified standard for data privacy across the United States.

Key Aspects of the APRA Include:

Covered Entities

As proposed, the APRA targets most individuals, entities, and nonprofits who collect, process, retain, or transfer covered data. Covered data is defined to include any information that identifies or is reasonably linked to an individual or device. Small businesses that do not collect such data are exempt under this proposed Act.

Enhanced Personal Data Protection

Under the APRA, individuals will have greater control over their personal data. For instance, a covered entity will be required to obtain the affirmative consent from individuals in order to transfer sensitive information, including genetic and biometric information, financial account and payment data, geolocation data, and online activities across third-party websites, to name a few. In addition, individuals will be given the option to access, export, correct, or even delete their data that is under the covered entity's control and restrict the use of their personal information for targeted advertising purposes.

Increased Transparency

Consistent with the goal of keeping individuals informed of their rights with respect to their data privacy, the APRA requires covered entities to make publicly available a privacy policy that, at minimum, defines the categories of data the covered entity or service provider collects, processes, and retains; the length of time each category will be retained; and the purpose for which each category is retained, processed, and collected; among others. Individuals must also be given notice of any material changes made to an entity's privacy policy and be given the option to opt out of the privacy policy if a material change is made.

Data Minimization

To prevent the unnecessary collection of user data, the ARPA proposes a restriction on the data collected outside of a specific and explicit purpose. Largely modeled after the European Union's General Data Protection Regulation (GDPR), covered entities will be restricted to collecting data

within what is necessary, proportionate, and limited to the purpose of their business, encouraging entities to only store information they need.

What this means for your organization

While the Act still faces the committee review process and must be voted on by both the House of Representatives and the Senate, the effective date of the Act is 180 days after enactment, providing a relatively short turnaround time once signed into law. Thus, it is recommended that businesses and individuals that likely fall under the definition of a “covered entity” be prepared and stay informed of any developments with respect to the APRA.

Bond attorneys regularly assist and advise clients on an array of data privacy and cybersecurity matters. For more information regarding the proposed American Privacy Regulations Act and to discuss compliance efforts businesses should be taking, contact any attorney in the [cybersecurity and data privacy practice group](#).

