New Online Privacy Laws

THE ISSUE: A new law in California, the California Consumer Privacy Act, goes into effect on Jan. 1, 2020 and will give citizens far more control over their personal data that companies in the state have collected. Federal legislation, the Online Privacy Act, has been introduced that will similarly place new requirements and limits on companies that collect and store users' personal data.

WHAT THIS MEANS FOR 3PLs: Unless exempt, 3PLs operating in California must comply with the California Consumer Privacy Act by June 2020 in order to avoid fines. This includes disclosing to customers, employees, and independent contractors what information they are collecting, setting up processes to let users opt out of having their information sold, and deleting customers' and employees' data if they request it. Companies that experience data breaches could also face damages if they are found not to have properly safeguarded the data that was stolen.

A study released by California's Department of Finance found that firms with fewer than 20 employees might have to spend around $50,000 to become compliant, while firms with more than 500 employees would pay an average of $2 million in initial costs.

BACKGROUND:

California Consumer Privacy Act: On Jan. 1, 2020, the California Consumer Privacy Act will go into effect with a six-month grace period before enforcement begins. The law applies to any business that meets at least one of the following criteria:

- Has annual gross revenue in excess of $25 million;
- Annually buys, sells, or shares personal information of 50,000 or more consumers; or
- Derives 50% or more of its annual revenues from selling consumers' personal information.

Under this new law, companies operating in California must disclose to users what personal data is being collected, whether it is sold and to whom. Companies must also allow users to opt out of sales, give users access to their data, and delete that data if the user requests it. The law also allows California residents to seek $100-$750 per incident in statutory damages when a data breach leads to the theft of personal information because the company didn't take steps to protect the data.

What is personal data?

Both bills define personal data as anything that could reasonably be linked, directly or indirectly, with a particular consumer or household. This would include an email address, passport or driver's license number, IP address, browsing history, biometrics, records of purchases, and employment or educational related information, among other things.

The law also applies to employers that collect information on their employees; employers in California must provide privacy notices to their employees that describe what personal information will be gathered and how it will be used, and allow employees to seek damages when data is stolen that the company didn't take proper steps to safeguard. Starting in 2021, companies must give employees, job candidates, and independent contractors the right to access and delete their personal information. Workers will also have the right to know if their personal information is being disclosed or sold to third parties, to opt out of the sale of their personal information, and to request a copy of all personal information the company has on file for them.

Online Privacy Act: Congresswoman Zoe Lofgren (D-CA) and Anna Eshoo (D-CA) have introduced the Online Privacy Act (H.R. 4978), federal legislation that is similar to the California law but goes further. The law applies to any entity that collects personal information and transmits it over an electronic network, unless the entity meets ALL of the following criteria:

- Does not earn revenue from the sale of personal information;
- Earns less than half of annual revenues from the processing of personal information for targeted or personalized advertising;
- Has not, during the past six months, maintained personal information of 250,000 or more individuals;
- Has fewer than 200 employees; AND
- Received less than $25 million in gross revenue in the preceding 12-month period.

Under the Online Privacy Act, companies must minimize the user data they collect and store; minimize employee and contractor access to user data; obtain consent from users before disclosing or selling their information; and employ reasonable cybersecurity policies to protect user data, among other things. The law would give users the right to access and delete data about themselves, request a human review of impactful automated decisions, be informed if an entity has collected their information, and choose how long their data can be kept. The bill also creates a new Digital Privacy Agency to enforce the law, including issuing fines for violations of up to $42,530 per incident.