The terms “deidentified” and “deidentification” are commonly used in modern privacy statutes and are functionally exempt from most privacy and security-related requirements. As indicated in the chart below, differences exist between how the term was defined in the California Consumer Privacy Act (CCPA) and how it was defined in later state privacy statutes that are set to go into force in 2023:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>California CCPA</th>
<th>California CPRA</th>
<th>Virginia VCDPA</th>
<th>Colorado CPA</th>
<th>Utah UCPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>Technical safeguards.</strong> An organization must implement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Tuesday, May 17, 2022
2. Policy against reidentification. An organization must implement business processes that specifically prohibit reidentification.

3. Inadvertent release. An organization must implement processes to prevent inadvertent release of the deidentified information.

4. No reidentification. An organization must make no attempt to reidentify the information.

5. Data not reasonably associated to an individual. An organization must make a reasonable attempt to ensure that the data cannot be associated with specific individuals.

6. Public commitment. An organization must publicly commit (e.g., in its privacy policy) to maintain and use the information in deidentified form and not attempt to reidentify it.

7. Downstream recipient contracts. An organization must contractually obligate recipients of the information to abide by the same restrictions.

FOOTNOTES


©2022 Greenberg Traurig, LLP. All rights reserved.

Source URL: https://www.natlawreview.com/article/finding-delta-understanding-differences-state-deidentification-standards