What is the NIST privacy framework?

In 2020, the National Institute of Standards and Technology, a part of the United States Department of Commerce, developed a privacy framework that was intended to help organizations identify and manage privacy risks. Like the ISO 29100 privacy framework that predated it, the NIST privacy framework is designed to provide common terminology to communicate privacy-related activities. Also like the ISO 29100 privacy framework, the NIST framework was designed to be compatible with domestic and international legal and regulatory regimes (e.g., GDPR, CCPA), but it does not include all of the requirements of those regimes.

What is the NIST privacy ‘core’?

The NIST privacy framework refers to the term “core” to describe a set of privacy activities and outcomes. The core is composed of three nested levels: Function, Category, and Subcategory. So, for example, the concept that a data subject should have the right to access their personal information is found within NIST under the Core Function of Control, which describes those activities that are intended to help develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks, the Core Category of Data Processing Management, and the Subcategory of “Data elements can be accessed for review.”
How many core functions does the NIST privacy framework identify?

The NIST privacy framework refers to the term “core” to describe a set of privacy activities and outcomes. The core is composed of three nested levels: Function, Category, and Subcategory. The core “Function” is the broadest category level and consists of five recommended Functions: Identify, Govern, Control, Communicate, and Protect.

©2021 Greenberg Traurig, LLP. All rights reserved.

Source URL: https://www.natlawreview.com/article/department-commerce-nist-privacy-framework