Published on *The National Law Review* https://natlawreview.com

Thinking Beyond the Law: If Our Organization Adopts the ISO 27701 Privacy Framework, How Many Controls Do We Need to Address?

Article By:

David A. Zetoony

While theoretically an organization could adopt ISO 27701 as a separate standalone framework to apply to an organization's privacy program, the framework was conceptualized as an extension of the ISO data security standards. As a result, it is organized based upon the assumption that an organization already has a security program that is built off of ISO/IEC 27001:2013 (Information security management systems) and ISO/IEC 27002:2013 (Code of practice for information security controls).

The requirements and controls of the ISO 27701 framework are divided into four sections. The first two sections identify which of the ISO 27701 and ISO 27002 security controls are adopted (either directly or with slight modification or additional guidance) for purposes of the privacy framework:

ISO 27701 Section	Description	Number of subparts / controls a from the ISO security framewor ISO privacy framework
Section 5	Amendments and modifications to ISO/IEC 27001:2013 to account for data privacy related concepts. This section is intended to apply to all organizations.	21
Section 6	Amendments and modifications to ISO/IEC 27002:2013 to account for data privacy related concepts. This section is intended to apply to all organizations.	114

Most security sections were adopted with little modification other than to interpret the term "information security" as referring to "information security and privacy." The following provides an example of a side-by-side comparison of the requirements under the security framework and the privacy framework:

ISO 27001 (security)	ISO 27701 (privacy)
§ 5.3. Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated. Top management shall assign the responsibility and authority for: (a) ensuring that the information security management system conforms to the requirements of this International Standard; and (b) reporting on the performance of the information security management system to top management.	§ 5.3.3 Top management shall ensure that th responsibilities and authorities for roles relev information security and privacy are assigned communicated. Top management shall assig responsibility and authority for: (a) ensuring t information security and privacy managemer conforms to the requirements of this Internati Standard; and (b) reporting on the performan information security and privacy managemer top management.

Other security sections were adopted in conjunction with textual refinements or additional implementation guidance.

The next two sections identify new guidance (separate and apart from guidance contained in the security frameworks) that apply to controllers and to processors as those terms are understood under the European GDPR:

ISO 27701 Section	Description	Number of new subparts / cont
Section 7	New guidance for controllers	31
Section 8	New guidance for processors	18

National Law Review, Volume XI, Number 174