ISO 27701, an international standard addressing personal data protection

02 April 2020

ISO 27701 is an international standard which defines the management system and security requirements for the processing of personal data (in 27701 context, Personally identifiable information (PII)).

ISO 27701 was published in August 2019. It is based on two information security standards and extends them to cover personal data protection:

- ISO 27001, that provides certification of an information security management system;
- ISO 27002, that provides guidance to implement the necessary security measures.

ISO 27701 requirements

In order to normalize and enhance personal data protection,

- ISO 27701 extends the ISO information security management systems to cover the specificities of the processing of personal data:
  - determination of the role of the organization as a data controller and/or a data processor (in 27701, “PII controller” and “PII processor”);
  - unified risk management regarding the risks for the organization and for the data subjects (in 27701, “PII principals”), designation of a data protection officer (in ISO 27701, “privacy officer”) ;
  - staff members awareness, information classification, protection of removable media, access management, data encryption, backups, event logging;
  - conditions for data transfer, *privacy by design and by default*, incident management;
  - compliance with legal and regulatory requirements, etc.
- ISO 27701 provides specific measures for the processing of personal data, relating to the role of the organization (as controller, processor or sub-processor) :
  - fundamental principles: purpose of the processing, legal basis, consent collection and withdrawal, records of the processing operations, privacy impact assessment;
  - data subject rights: notice, access, correction, erasure, automated decision;
  - *privacy by design and by default*: minimization, data de-identification and deletion, data retention;
  - subcontracts, data transfers and data sharing.

Contributions from experts and data protection authorities

This standard was drafted at international level with contributions from experts from all continents and the participation of several data protection authorities. Experts from the CNIL actively contributed to this standard, with support from AFNOR and the European Data Protection Board.

GDPR was taken into account, as well as other data protection legislation (including Australia, Brazil, California, Canada). The proximity of the standard with GDPR is materialized in a specific annex that maps each clause of the standard with the corresponding GDPR article. Implementing a management system for data protection is a key to the general provisions of *accountability* in the GDPR.

In short, ISO 27701 is a global standard: it is not GDPR specific, nor does it constitute, as such, a GDPR certification instrument as described in Article 42 of the regulation. However, it represents the state of the art in terms of privacy protection and will allow organizations adopting it to increase their maturity and demonstrate an active approach to personal data protection.

Keywords associated to this article

#Standardization #GDPR

This can also interest you ...

Privacy shield

CNIL CALLS FOR CHANGES IN THE USE OF US COLLABORATIVE TOOLS BY FRENCH UNIVERSITIES

Following the Schrems II ruling, the CNIL was asked by the Conférence des présidents d'université and the Conférence des grandes écoles to comment on the use of "collaborative...

31 May 2021

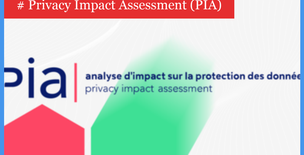
GDPR

RECORD OF PROCESSING ACTIVITIES

The record of processing activities allows you to make an inventory of the data processing and to have an overview of what you are doing with the concerned personal data.

19 August 2019

Privacy Impact Assessment (PIA)



THE OPEN SOURCE PIA SOFTWARE HELPS TO CARRY OUT DATA PROTECTION IMPACT ASSESMENT

25 June 2019