Privacy and protection of PII

ISO 27002 Control 5.34

Control

The organization should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements

Purpose

To ensure compliance with legal, statutory, regulatory and contractual requirements related to the information security aspects of the protection of PII

What is it exactly ?

- Given that the ISO is an international standard, it does not know what the European GDPR is. Hence the generic wording of Personally Identifiable Information which can be translated into personal data

What needs to be done ?

- Ensure that a Data Protection Officer is defined
- Identify PII and create a record of processing activities
- Perform Data Privacy Impact Assessment
- Implement protection measures based on the DPIA
- Ensure that the rights of people are respected
- Define the responsibilities of the PII Controllers and the PII Processors

What about the third parties ?

You have to :

- Define contractually Data Processing Agreements (DPAs)
- Conduct Third-Party Due Diligence and Risk Assessments
- Define the measures / controls that are the responsibility of the PII processors
- Investigate the measures defined in the ISO 27701

Link with other frameworks

- NIST 800-53 rev5 : PM-18, PT-1, PT-3, PT-7, CA-9*, CA-3*, PL-2*, PL-8*
- NIST CSF 2.0 : GV.RR-04

Renaud Dardenne
Asphalia Consulting