ISO 27001, 27002, 27701, CCPA, and GDPR Explained

What is ISO 27001?
Organizations can achieve certification for ISO 27001.

ISO 27001 is the leading international standard for a framework of policies and procedures that is integrated through an Information Security Management System (ISMS).

What is ISO 27002?
While organizations cannot achieve certification for ISO 27002, they can comply with the standard.

ISO 27002 is an information security standard that suggests additional security controls for the cloud that weren't fully defined in the earlier standard.

What is ISO 27701?
Organizations must be ISO 27001 certified before becoming ISO 27701 certified.

ISO 27701 was developed to provide a framework for those who are looking to implement a system to support compliance with the EU's GDPR, among other data privacy requirements.

What is the GDPR?
The General Data Protection Regulation (GDPR) is the toughest privacy and security law, drafted and passed by the European Union, imposed on all organizations who collect private data from EU residents.

The price of noncompliance with GDPR is €20 million or 4% of annual revenue.

California Consumer Data Privacy Act (CCPA)
The California Privacy Rights Act, also known as "GDPR Light", is a statewide data privacy law that strengthened the rights of California residents, tightening business regulations for the usage of personal information. This law only applies to any for-profit business that collects the personal information of California residents or does business in California.

The price of noncompliance with CCPA is a maximum fine of $7,500 per user.

Lei Geral de Proteçao Dados (LGPD)
The Lei Geral de Proteçao Dados is very similar to the GDPR, as this privacy act has a similar scope and applicability but lesser fines.

The maximum fines are 50 million reais or 2% of global revenue.

Australia Privacy Act (APA)
The Australia Privacy Act specifies that an organization has 30 days to disclose any data breaches that would cause serious harm or face significant fines.

The maximum fine for noncompliance with the APA is 1.8 million AUD.

Japan's Act of Protection of Personal Information (APPI)
Japan's Act of Protection of Personal Information has recently been amended to include both foreign and domestic organizations.

The maximum penalty for breach of APPI is either up to one year of imprisonment or a fine up to JP¥500,000.

South Korean Personal Information Protection Act (PIPA)
This act has a wide selection of penalties depending on the severity of the violation. This can include criminal fines, surcharges, and penalties.

The maximum fine for serious penalties can be more than ₩ 500 million or up to 3% of a company's global revenue.

Thailand Personal Data Protection Act (PDPA)
The maximum penalty for breach of PDPA is a maximum of ฿5 million or up to one year in prison in severe cases.

Ley 19,628 (Chile's Data Privacy Law)
The latest edition of Chile's Data Privacy Law will have similar protections as the GDPR, with serious implications for repeat offenders.

The maximum fine is upwards of 530,000€ for breach of this data privacy law.

India Personal Data Protection Bill (PDPB)
Modeled after Europe's GDPR, the PDPB gives more discretion to India's central government on how and when it will be enforced.

These fines are similar to the GDPR, with potential to go as high as 4% of global revenues.

New Zealand Privacy Act
While this privacy act has some similarities to the GDPR, New Zealand's fines are significantly lower. There is no "Right to Be Forgotten", and the portability of data offshore does not include cloud providers.

What's So Special About ISO 27701?

ISO 27701 allows organizations to put a globally recognized Privacy Information Management System in place along with their ISO 27001 certification. ISO 27701 will show how your organization takes different Data Privacy laws, such as GDPR and CCPA, seriously.

How Does It Work?

You first get your Information Security Management System certified against ISO 27001, and then you have your Privacy Information Management System certified against ISO 27701.

Fast Facts:

The price of noncompliance with GDPR is €20 million or 4% of annual revenue.

83% of enterprise workloads were forecasted to move to the cloud by the end of 2020.

Damage related to cybercrime was projected to hit $6 trillion annually by 2021.

61% of all organizations have experienced an Internet of Things security incident.

The United States is the number one target for cyberattacks – half of all global data breaches will occur within the US by 2023.

TÜV SÜD America

Learn more about TÜV SÜD's cybersecurity services.

www.tuvsud.com/en-us/cybersecurity