Accenture Security

ARTICLE 32: SECURITY OF PROCESSING

A WAY HOW TO IMPLEMENT APPROPRIATE TECHNICAL AND ORGANIZATIONAL MEASURES

Intars Garbovskis

Accenture Latvia, Security practice lead

May 25, 2018

AGENDA

What's behind the Article 32?

A way how to demonstrate compliance with the Article 32

Key takeaways

WHAT'S BEHIND THE ARTICLE 32?

ARTICLE 32: SECURITY OF PROCESSING

"tostarp attiecīgā gadījumā cita starpā:"

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement **appropriate technical and organisational measures to ensure a level of security appropriate to the risk**, including inter alia as appropriate:

a) the pseudonymisation and encryption of personal data;

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

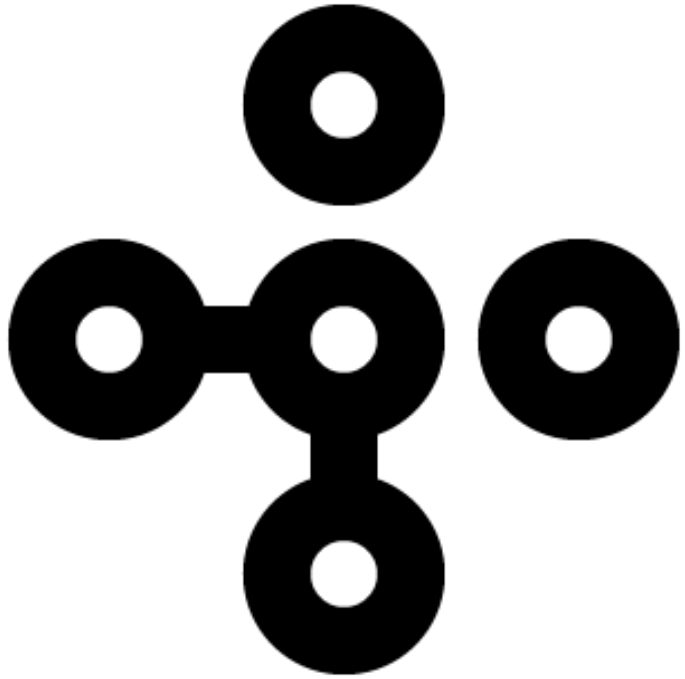
c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

WE CANNOT CERTIFY COMPLIANCE WITH THE GDPR AS SUCH...

…BUT CERTIFICATION CAN DEMONSTRATE COMPLIANCE WITH SPECIFIC REQUIREMENTS

Article 32 states that adherence to an approved certification mechanism may be used as an element by which to demonstrate compliance with the requirements set out in Article 32.



A WAY HOW TO DEMONSTRATE COMPLIANCE WITH THE ARTICLE 32

EXISTING DATA PROTECTION-RELATED CERTIFICATION SCHEMES*

ePrivacy
European seal for your privacy

PrivacyMark System

LABEL CNIL

EuroPriSe
European Privacy Seal

Information Security Management System
ISO 27001
Certified

ico.
Information Commissioner's Office

ICO Privacy Seal (under development)

ISO 27018
International Organization for Standardization

CERTIFIED PbD
RYERSON UNIVERSITY
Privacy Certified by Design

Privacy by Design by Ryerson University and Deloitte Canada

*Source: ENISA Recommendations on European Data Protection Certification VERSION 1.0 NOVEMBER 2017

A LINK BETWEEN GDPR AND ISO 27001

GDPR requirements (Article 32)

- The controller and the processor shall implement **appropriate technical and organisational measures**
- **...ensure a level of security appropriate to the risk**
- ...implement the pseudonymisation and **encryption** of personal data
- ...ensure the ongoing **confidentiality, integrity, availability** and resilience of processing systems and services
- ...**restore the availability and access** to personal data in a timely manner
- a process for regularly **testing**, **assessing** and **evaluating the effectiveness** of technical and organisational measures

=

ISO 27001 requirements

- ...requirements for **establishing**, **implementing**, **maintaining** and **continually improving** an ISMS
- ...by **applying a risk management process**, identify risks associated with the loss of **confidentiality, integrity and availability**
- ...ensure **proper and effective use of cryptography** to protect the confidentiality, authenticity and/or integrity of information
- ...preserve the **confidentiality, integrity and availability of information**
- ...**ensure availability** of information processing facilities
- ...**evaluate** the IS performance and the **effectiveness** of the ISMS

… AND THAT'S NOT ALL

By implementing ISO 27001 standard you can demonstrate compliance not only with the Article 32…

We have identified that properly implemented ISO 27001 controls and requirements to some extent overlap with most of the GDPR articles which sets specific information security or privacy related requirements (Article 5 to Article 39)

KEY TAKEAWAYS

DO NOT START FROM THE SCRATCH, BUT TAKE IT SERIOUSLY

- **Build on the foundation of existing, already implemented information security controls and best practices. For example, ISO 27001 standard could be one of the options as it covers most of the GDPR information security, privacy requirements**

- **Do not take GDPR only formally or as an another compliance requirement – use it to develop your ISMS, improve security culture within the company or organization, to decrease the number of security incidents**

- **Use GDPR as an opportunity to get a competitive advantage (proof customers you take protection of their data seriously – information security and data privacy by design). Again, ISO 27001 or any other IS/Data Privacy certification might be a way to proof it**

THANK YOU!

ACCENTURE LATVIA SECURITY PRACTICE

DATA PRIVACY & GDPR · SECURITY RISK ASSESSMENTS SECURITY · ADVISORY SERVICES

CYBER SECURITY TESTING · VULNERABILITY MANAGEMENT

ISO 27001 · SPLUNK · CyberArk

CREST Registered Penetration Tester

AppScan IBM Security

ISO-27001 Lead Auditor

CISA Certified Information Systems Auditor

splunk> Splunk Certified Power User

splunk> Splunk Certified Admin

CEH Certified Ethical Hacker

CPTE CERTIFIED PENETRATION TESTING ENGINEER

CIPP/E Certified Information Privacy Professional/Europe

CIPM Certified Information Privacy Manager

CDFE CERTIFIED DIGITAL FORENSICS EXAMINER

CISSP Certified Information Systems Security Professional

CONTACTS: intars.garbovskis@accenture.com