27018, (27017) & 29151

Cloud en/of PII protection

Beer Franken, AMC

Chief information security & privacy protection officer

Programma

- ISO/IEC 27018:2014
  CoP for protection of PII in public clouds acting as PII processors

- (ISO/IEC 27017:2015
  CoP for information security controls for cloud services)

- ISO/IEC DIS 29151:2016
  CoP for PII protection

CoP? PII?

CoP Code of Practice = Praktijkrichtlijn

ISO 27002 is een CoP

PII Personally Identifiable Data = Persoonsgegeven

elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (Wbp)

Nummers, nummers...

ISO **27001** is een managementsysteem waartegen certficering mogelijk is

ISO **27002** is een praktijkrichtlijn (CoP) waarmee je bij implementatie van ISO 27001 rekening moet houden

ISO **27017** is een *uitbreiding* op ISO 27002 voor cloud dienstenaanbieders

ISO **27018** is een *uitbreiding* op ISO 27002 voor bewerkers die persoonsgegevens bewerken

ISO **29151** is een *uitbreiding* op ISO 27002 voor partijen die zelf persoonsgegevens verwerken of laten bewerken

Certificering

Een certificaat tonen/bekijken is niet genoeg

- toont een geldigheidsperiode
- bevat verwijzing naar toepasselijkheidsverklaring

De toepasselijkheidsverklaring geeft aan

- welke maatregelen van ISO 27002 zijn ingevoerd
- welke aanvullende maatregelen (29151, of 27018 al dan niet in samenhang met 27017)

27018 Objectives

Processor: to comply with applicable obligations, directly or through contract; and be transparent so that customers can select well-governed services.

Customer & **processor**: enter into a contract.

Provide **customers** with mechanism for exercising audit and compliance rights and responsibilities in (multi-party) cloud environment.

Aanvulling op ISO 27002 h5-18

Behalve:

8 Asset management

14 System acquisition, development and maintenance

15 Supplier relationships

17 Information security aspects of business continuity management

Aanvulling op ISO 27002 h5-18

Uitsluitend aanvulling implementation guidance:

5 Information security policies

6 Organization of information security

7 Human resource security

10 Cryptography

12 Operations security

16 Information security incident management

Aanvulling op ISO 27002 h5-18

Aanvullingen controls (via verwijzingen naar bijlage A):

9 Access control
11 Physical and environmental security
13 Communications security
18 Compliance

en in bijlage A op basis van privacy principles

Privacy principles (uit ISO 29100)

1 Consent and choice (1 controls/maatregelen)
2 Purpose legitimacy and specification (2)
3 Collection limitation (0)
4 Data minimization (1)
5 Use, retention and disclosure limitation (2)
6 Accuracy and quality (0)
7 Openness, transparency and notice (1)
8 Individual participation and access (0)
9 Accountability (3)
10 Information security (13)
11 Privacy compliance (2)

A.1 Consent and choice

A.1.1 Obligation to co-operate regarding PII principals' rights

The public cloud PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them.

A.2 Purpose legitimacy and specification

A.2.1 Public cloud PII processor's purpose

PII to be processed under a contract should not be processed for any purpose independent of the instructions of the cloud service customer.

A.2.2 Public cloud PII processor's commercial use

PII processed under a contract should not be used by the public cloud PII processor for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving the service.

A.4 Data minimization

A.4.1 Secure erasure of temporary files

Temporary files and documents should be erased or destroyed within a specified, documented period.

A.5 Use, retention and disclosure limitation

A.5.1 PII disclosure notification

The contract between the public cloud PII processor and the cloud service customer should require the public cloud PII processor to notify the cloud service customer, in accordance with any procedure and time periods agreed in the contract, of any legally binding request for disclosure of PII by a law enforcement authority, unless such a disclosure is otherwise prohibited.

A.5.2 Recording of PII disclosures

Disclosures of PII to third parties should be recorded, including what PII has been disclosed, to whom and at what time.

A.7 Openness, transparency and notice

A.7.1 Disclosure of sub-contracted PII processing

The use of sub-contractors by the public cloud PII processor to process PII should be disclosed to the relevant cloud service customers before their use.

A.9 Accountability

A.9.1 Notification of a data breach involving PII

The public cloud PII processor should promptly notify the relevant cloud service customer in the event of any unauthorized access to PII or unauthorized access to processing equipment or facilities resulting in loss, disclosure or alteration of PII.

A.9.2 Retention period for administrative security policies and guidelines

Copies of security policies and operating procedures should be retained for a specified, documented period upon replacement (including updating).

A.9.3 PII return, transfer and disposal

The public cloud PII processor should have a policy in respect of the return, transfer and/or disposal of PII and should make this policy available to the cloud service customer.

A.10 Information security

A.10.1 Confidentiality or non-disclosure agreements

A.10.2 Restriction of the creation of hardcopy material

A.10.3 Control and logging of data restoration

A.10.4 Protecting data on storage media leaving the premises

A.10.5 Use of unencrypted portable storage media and devices

A.10.6 Encryption of PII transmitted over public data-transmission networks

A.10.7 Secure disposal of hardcopy materials

A.10.8 Unique use of user IDs

A.10.9 Records of authorized users

A.10.10 User ID management

A.10.11 Contract measures

A.10.12 Sub-contracted PII processing

A.10.13 Access to data on pre-used data storage space

A.11 Privacy compliance

A.11.1 Geographical location of PII

The public cloud PII processor should specify and document the countries in which PII might possibly be stored.

A.11.2 Intended destination of PII

PII transmitted using a data-transmission network should be subject to appropriate controls designed to ensure that data reaches its intended destination.

No additional controls

A.3 Collection limitation

A.6 Accuracy and quality

A.8 Individual participation and access

A.10 Controls

1 Individuals under the public cloud PII processor's control with access to PII should be subject to a confidentiality obligation.

2 The creation of hardcopy material displaying PII should be restricted.

3 There should be a procedure for, and a log of, data restoration efforts.

4 PII on media leaving the organization's premises should be subject to an authorization procedure and should not be accessible to anyone other than authorized personnel (e.g. by encrypting the data concerned).

5 Portable physical media and portable devices that do not permit encryption should not be used except where it is unavoidable, and any use of such portable media and devices should be documented.

6 PII that is transmitted over public data-transmission networks should be encrypted prior to transmission.

7 Where hardcopy materials are destroyed, they should be destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc.

8 If more than one individual has access to stored PII, then they should each have a distinct user ID for identification, authentication and authorization purposes.

9 An up-to-date record of the users or profiles of users who have authorized access to the information system should be maintained.

10 De-activated or expired user IDs should not be granted to other individuals.

11 Contracts between the cloud service customer and the public cloud PII processor should specify minimum technical and organizational measures to ensure that the contracted security arrangements are in place and that data are not processed for any purpose independent of the instructions of the controller. Such measures should not be subject to unilateral reduction by the public cloud PII processor.

12 Contracts between the public cloud PII processor and any sub-contractors that process PII should specify minimum technical and organizational measures that meet the information security and PII protection obligations of the public cloud PII processor. Such measures should not be subject to unilateral reduction by the sub-contractor.

13 The public cloud PII processor should ensure that whenever data storage space is assigned to a cloud service customer, any data previously residing on that storage space is not visible to that cloud service customer.

Additionele ISO 27017 controls *CoP (...) for cloud services (1)*

6.3.1 Shared roles and responsibilities within a cloud computing environment

Responsibilities for shared information security roles in the use of the cloud service should be allocated to identified parties, documented, communicated and implemented by both the cloud service customer and the cloud service provider.

8.1.5 Removal of cloud service customer assets

Assets of the cloud service customer that are on the cloud service provider's premises should be removed, and returned if necessary, in a timely manner upon termination of the cloud service agreement.

9.5.1 Segregation in virtual computing environments

A cloud service customer's virtual environment running on a cloud service should be protected from other cloud service customers and unauthorized persons.

Additionele ISO 27017 controls *CoP (...) for cloud services (2)*

9.5.2 Virtual machine hardening

Virtual machines in a cloud computing environment should be hardened to meet business needs.

12.1.5 Administrator's operational security

Procedures for administrative operations of a cloud computing environment should be defined, documented and monitored.

12.4.5 Monitoring of Cloud Services

The cloud service customer should have the capability to monitor specified aspects of the operation of the cloud services that the cloud service customer uses.

13.1.4 Alignment of security management for virtual and physical networks

Upon configuration of virtual networks, consistency of configurations between virtual and physical networks should be verified based on the cloud service provider's network security policy.

Concept ISO 29151 CoP for PII (1)

A.1 General policies for the use and protection of PII

A.1.1 General policies for the use and protection of PII

A.2 Consent and choice

A.2.1 Consent

A.2.2 Choice

A.3 Purpose legitimacy and specification

A.3.1 Purpose legitimacy

A.3.2 Purpose specification

A.4 Collection limitation

A.4.1 Collection limitation

A.5 Data minimization

A.5.1 Minimization

Concept ISO 29151 CoP for PII (2)

A.6 Use, retention and disclosure limitation

A.6.1 Use, retention and disclosure limitation

A.6.2 Secure erasure of temporary files

A.6.3 PII disclosure notification

A.6.4 Recording of PII disclosures

A.6.5 Disclosure of sub-contracted PII processing

A.7 Accuracy and quality

A.7.1 Data quality

A.8 Openness, transparency and notice

A.8.1 Privacy notice

A.8.2 Openness and transparency

A.9 PII principal participation and access

A.9.1 PII principal access

A.9.2 Redress and participation

A.9.3 Complaint management

Concept ISO 29151 CoP for PII (3)

A.10 Accountability

A.10.1 Governance

A.10.2 Privacy risk assessment

A.10.3 Privacy requirement for contractors and PII processors

A.10.4 Privacy monitoring and auditing

A.10.5 PII protection awareness and training

A.10.6 PII protection reporting

A.11 Information security

A.11.1 Information security

A.12 Privacy compliance

A.12.1 Compliance

A.12.2 Cross border data transfer restrictions in certain jurisdictions

Vragen?

Beer Franken

b.franken@amc.nl of via NEN (Jan Rietveld)