CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 41574-2022

Information technology - Security techniques - Code of practice for protection of personal information in public clouds

Issued on: July 11, 2022 **Implemented on: February 1, 2023**

Issued by: State Administration for Market Regulation, China National Standardization Administration

Table of Contents

foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for Standardization Work Part 1.Structure and Drafting Rules of Standardization Documents"

drafted.

This document is modified to adopt ISO /IEC 27018.2019 "Information technology security technology Personally identifiable information (PII) processors in the public

There is a practical guide to protecting PII in the cloud.

Compared with ISO /IEC 27018.2019, this document has more structural adjustments. Comparison of structure number changes between two files

See Appendix A for a list.

The technical differences between this document and ISO /IEC 27018.2019 and their reasons are as follows.

--- Changed the term "Personally Identifiable Information (PII)" to "Personal Information" and changed the definition, consistent with GB/T 35273-2020

Terms and definitions remain consistent (see 3.1, 3.2 of ISO /IEC 27018.2019);

--- Changed the term "PII controller" to "personal information controller" and changed the definition to match the term of GB/T 35273-2020

Be consistent with the definition (see 3.2, 3.3 of ISO /IEC 27018.2019);

--- Changed the term "PII subject" to "Personal information subject", and changed the definition to match the terms and definitions of GB/T 35273-2020

The definition is consistent (see 3.3, 3.4 of ISO /IEC 27018.2019);

--- Changed the term "PII processor" to "Personal information processor" and changed the definition to match the term of GB/T 35273-2020

Be consistent with the definition (see 3.4, 3.5 of ISO /IEC 27018.2019);

--- Changed the term "PII processing" to "personal information processing", and changed the definition, and the terms and definitions of GB/T 35273-2020

The definition is consistent (see 3.5, 3.6 of ISO /IEC 27018.2019);

--- Change ISO /IEC 27002 in the title of the table to GB/T 22081 (see Table 1, Table 1 of ISO /IEC 27018.2019);

---Add the suggestion that processors entrust subcontractors to process personal information, and GB/T 35273-2020 9.1c) 2) about entrusting

be consistent with the requirements of the operator (see 5.1.1);

---Delete the statement in "Public Cloud PII Protection of Other Information" that laws and regulations have different requirements for processors and controllers, in order to comply with my country's

Rules for the drafting of standardized documents (see 5.1.1 of ISO /IEC 27018.2019);

---Delete the requirements of laws and regulations on punishment for processors in "Public Cloud PII Protection of Other Information", in order to comply with my country's standardization documents

Drafting rules (see 7.2.2 of ISO /IEC 27018.2019);

--- Increase the requirements for the use of cryptographic techniques to address confidentiality, integrity, authenticity, and non-repudiation requirements (see 10.1.1);

--- Increase the proposal for processors to transfer personal information, consistent with the relevant provisions of GB/T 35273-2020 (see B.2.3);

---Add suggestions for processors to provide personal information overseas to adapt to my country's technical conditions and facilitate the application of this document (see

B.4.1, B.7.14);

---Increase the suggestion that the processor entrusts an agent to process personal information, and GB/T 35273-2020 9.1c) 2) about entrusted

conform to the requirements of the other party (see B.7.1);

--- Increase the suggestion that the data recovery log contains information (see B.7.3);

---Delete the relevant legal expressions on the processor's notification obligation in the "Public Cloud PII Protection Implementation Guide" to comply with my country's standardization

Rules for drafting documents (see ISO /IEC 27018.2019, A.10.1).

The following editorial changes have been made to this document.

--- In order to be consistent with the existing standard series, the name of the standard was changed to "Practice of Personal Information Protection in Public Cloud of Information Technology Security Technology".

Practice Guide;

--- Change the classification principles of the new control measures in Appendix B to be consistent with my country's personal information protection principles (see B.1,

A.1 of ISO /IEC 27018.2019);

--- Add the explanation of "off-chain" to improve the readability of the terms and facilitate the application of this document (see Note 1 of B.2.3);

--- Add the explanation of "degaussing" to improve the legibility of the terms and facilitate the application of this document (see Note 2 of B.2.3);

--- Add Appendix A (informative) "Comparison of this document with ISO /IEC 27018.2019 structure number";

--- Add Appendix C (informative) "Relationship between cloud service providers, cloud service customers and cloud service users";

--- Delete Note 9.2.1 of ISO /IEC 27018.2019;

--- Delete Note 10.1.1 of ISO /IEC 27018.2019;

--- Delete Note 1 and Note 2 of 12.3.1 of ISO /IEC 27018.2019;

--- Delete the example of A.6.1 of ISO /IEC 27018.2019;

--- Delete the first sentence of Note A.11.3 of ISO /IEC 27018.2019;

--- Change the other principles that this control measure and guide can be classified into to the principle of "openness and transparency", which is in line with my country's personal information protection principles

Be consistent (see Note 3 of B.2.3, Note A.10.3 of ISO /IEC 27018.2019);

---Changed the expression of the principles followed in the "Public Cloud PII Protection Implementation Guide" involving the collection and use of PII, which is consistent with the

personal information of our country.

information protection principles (see B.3.1, A.3.1 of ISO /IEC 27018.2019);

--- Changed "PII Controller" in "Public Cloud PII Protection Implementation Guide" to "Cloud Service Client" to improve readability and facilitate this article

application of the software (see B.8.1, A.2.1 of ISO /IEC 27018.2019).

Please note that some content of this document may be patented. The issuing agency of this document assumes no responsibility for identifying patents.

This document is under the jurisdiction of the National Information Security Standardization Technical Committee (SAC/TC260).

0.1 Background and environment

In recent years, more and more cloud service customers use the services of cloud service providers and entrust them with personal information processing.

GB/T 35273-2020 stipulates that the party who accepts the entrusted processing (9.1 in GB/T 35273-2020 is called "the entrusted person", this article

"Processor" in the document, that is, "entrusted person") requirements. This document provides a

A general compliance framework for the protection of personal information in the public cloud, which guides processors to carry out personal information processing operations in the public cloud.

Public cloud service providers are usually required to sign contracts with cloud service customers and comply with personal information protection laws on both sides

Provide services under the premise of relevant regulations. For these requirements of personal information protection, cloud service providers and cloud service customers are based on the law

laws and regulations and the contracts between them.

When the public cloud service provider processes personal information in accordance with the requirements of cloud service customers, the public cloud service provider acts as a "personal information"

The role of "processor". Cloud service customers who have a contractual relationship with public cloud personal information processors are "personal information controllers". In cloud computing

Under the environment, the personal information controller has the right to control personal information, and it also has the authority to process and use personal information. Personal