INTERNATIONAL STANDARD

ISO/IEC 27018

Second edition
2019-01

Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII

Reference number
ISO/IEC 27018:2019(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 27018:2014), of which it constitutes a minor revision. The main change compared to the previous edition is the correction of an editorial mistake in Annex A.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

0.1 Background and context

Cloud service providers who process Personally Identifiable Information (PII) under contract to their customers need to operate their services in ways that allow both parties to meet the requirements of applicable legislation and regulations covering the protection of PII. The requirements and the way in which the requirements are divided between the cloud service provider and its customers vary according to legal jurisdiction, and according to the terms of the contract between the cloud service provider and the customer. Legislation which governs how PII is allowed to be processed (i.e. collected, used, transferred and disposed of) is sometimes referred to as data protection legislation; PII is sometimes referred to as personal data or personal information. The obligations falling on a PII processor vary from jurisdiction to jurisdiction, which makes it challenging for businesses providing cloud computing services to operate multinationally.

A public cloud service provider is a "PII processor" when it processes PII for and according to the instructions of a cloud service customer. The cloud service customer, who has the contractual relationship with the public cloud PII processor, can range from a natural person, a "PII principal", processing his or her own PII in the cloud, to an organization, a "PII controller", processing PII relating to many PII principals. The cloud service customer can authorize one or more cloud service users associated with it to use the services made available to it under its contract with the public cloud PII processor. Note that the cloud service customer has authority over the processing and use of the data. A cloud service customer who is also a PII controller can be subject to a wider set of obligations governing the protection of PII than the public cloud PII processor. Maintaining the distinction between PII controller and PII processor relies on the public cloud PII processor having no data processing objectives other than those set by the cloud service customer with respect to the PII it processes and the operations necessary to achieve the cloud service customer's objectives.

NOTE Where the public cloud PII processor is processing cloud service customer account data, it can be acting as a PII controller for this purpose. This document does not cover such activity.

The intention of this document, when used in conjunction with the information security objectives and controls in ISO/IEC 27002, is to create a common set of security categories and controls that can be implemented by a public cloud computing service provider acting as a PII processor. It has the following objectives:

— to help the public cloud service provider to comply with applicable obligations when acting as a PII processor, whether such obligations fall on the PII processor directly or through contract;

— to enable the public cloud PII processor to be transparent in relevant matters so that cloud service customers can select well-governed cloud-based PII processing services;

— to assist the cloud service customer and the public cloud PII processor in entering into a contractual agreement;

— to provide cloud service customers with a mechanism for exercising audit and compliance rights and responsibilities in cases where individual cloud service customer audits of data hosted in a multi-party, virtualized server (cloud) environment can be impractical technically and can increase risks to those physical and logical network security controls in place.

This document can assist by providing a common compliance framework for public cloud service providers, in particular those that operate in a multinational market.

0.2 PII protection controls for public cloud computing services

This document is designed for organizations to use as a reference for selecting PII protection controls within the process of implementing a cloud computing information security management system based on ISO/IEC 27001, or as a guidance document for implementing commonly accepted PII protection controls for organizations acting as public cloud PII processors. In particular, this document has been based on ISO/IEC 27002, taking into consideration the specific risk environment(s) arising from those

PII protection requirements which can apply to public cloud computing service providers acting as PII processors.

Typically, an organization implementing ISO/IEC 27001 is protecting its own information assets. However, in the context of PII protection requirements for a public cloud service provider acting as a PII processor, the organization is protecting the information assets entrusted to it by its customers. Implementation of the controls of ISO/IEC 27002 by the public cloud PII processor is both suitable for this purpose and necessary. This document augments the ISO/IEC 27002 controls to accommodate the distributed nature of the risk and the existence of a contractual relationship between the cloud service customer and the public cloud PII processor. This document augments ISO/IEC 27002 in two ways:

— implementation guidance applicable to public cloud PII protection is provided for certain of the existing ISO/IEC 27002 controls, and

— Annex A provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements not addressed by the existing ISO/IEC 27002 control set.

Most of the controls and guidance in this document also apply to a PII controller. However, the PII controller is, in most cases, subject to additional obligations not specified here.

0.3 PII protection requirements

It is essential that an organization identifies its requirements for the protection of PII. There are three main sources of requirement, as given below.

a) Legal, Statutory, Regulatory and Contractual Requirements: One source is the legal, statutory, regulatory and contractual requirements and obligations that an organization, its trading partners, contractors and service providers have to satisfy, and their socio-cultural responsibilities and operating environment. It should be noted that legislation, regulations and contractual commitments made by the PII processor can mandate the selection of particular controls and can also necessitate specific criteria for implementing those controls. These requirements can vary from one jurisdiction to another.

b) Risks: Another source is derived from assessing risks to the organization associated with PII, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated. ISO/IEC 27005 provides information security risk management guidance, including advice on risk assessment, risk acceptance, risk communication, risk monitoring and risk review. ISO/IEC 29134 provides guidance on privacy impact assessment.

c) Corporate policies: While many aspects covered by a corporate policy are derived from legal and socio-cultural obligations, an organization can also choose voluntarily to go beyond the criteria that are derived from the requirements of a).

0.4 Selecting and implementing controls in a cloud computing environment

Controls can be selected from this document (which includes by reference the controls from ISO/IEC 27002, creating a combined reference control set for the sector or application defined by the scope). If required, controls can also be selected from other control sets, or new controls can be designed to meet specific needs as appropriate.

NOTE A PII processing service provided by a public cloud PII processor can be considered as an application of cloud computing rather than as a sector in itself. Nevertheless, the term "sector-specific" is used in this document, as this is the conventional term used within other standards in the ISO/IEC 27000 series.

The selection of controls is dependent on organizational decisions based on the criteria for risk acceptance, risk treatment options, and the general risk management approach applied to the organization and, through contractual agreements, its customers and suppliers. It is also subject to relevant national and international legislation and regulations. Where controls from this document are not selected, this needs to be documented with justification for the omission.

Further, the selection and implementation of controls is dependent on the public cloud provider's actual role in the context of the whole cloud computing reference architecture (see ISO/IEC 17789). Many different organizations can be involved in providing infrastructure and application services in a cloud computing environment. In some circumstances, selected controls can be unique to a particular service category of the cloud computing reference architecture. In other instances, there can be shared roles in implementing security controls. Contractual agreements need to clearly specify the PII protection responsibilities of all organizations involved in providing or using the cloud services, including the public cloud PII processor, its sub-contractors and the cloud service customer.

The controls in this document can be considered as guiding principles and applicable for most organizations. They are explained in more detail below along with implementation guidance. Implementation can be made simpler if requirements for the protection of PII have been considered in the design of the public cloud PII processor's information system, services and operations. Such consideration is an element of the concept that is often called "Privacy by Design" (see Bibliographic entry [9]).

0.5 Developing additional guidelines

This document can be regarded as a starting point for developing PII protection guidelines. It is possible that not all of the controls and guidance in this code of practice are applicable. Furthermore, additional controls and guidelines not included in this document can be required. When documents are developed containing additional guidelines or controls, it can be useful to include cross-references to clauses in this document where applicable to facilitate compliance checking by auditors and business partners.

0.6 Lifecycle considerations

PII has a natural lifecycle, from creation and origination through storage, processing, use and transmission to its eventual destruction or decay. The risks to PII can vary during its lifetime but protection of PII remains important to some extent at all stages.

PII protection requirements need to be taken into account as existing and new information systems are managed through their lifecycle.

Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

1 Scope

This document establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in line with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.

In particular, this document specifies guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of PII which can be applicable within the context of the information security risk environment(s) of a provider of public cloud services.

This document is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which provide information processing services as PII processors via cloud computing under contract to other organizations.

The guidelines in this document can also be relevant to organizations acting as PII controllers. However, PII controllers can be subject to additional PII protection legislation, regulations and obligations, not applying to PII processors. This document is not intended to cover such additional obligations.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 17788, *Information technology — Cloud computing — Overview and vocabulary*

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17788, ISO/IEC 27000 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
data breach
compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, protected data transmitted, stored or otherwise processed

[SOURCE: ISO/IEC 27040:2015, 3.7]

国际标准 ISO/IEC 27018

第二版
2019-01

信息技术 - 安全技术 个人身份信息（PII）处理者在公有云中保护PII的实施规范。

参考号
ISO/IEC 27018:2019E

国际标准化组织

前言

ISO（国际标准化组织）和 IEC（国际电工委员会）构成了全球标准化的专门系统。作为 iso 或 icc 成员的国家机构通过各自组织所建立的技术委员会参与国际标准的制定。 技术活动的特定领域 ISO 和 IEC 技术委员会在共同感兴趣的领域进行合作。其他政府和非政府国际组织同 ISo 和 IEC 联络，也参加信息技术领域的工作，ISo 和 IEC 建立了联合技术委员会，ISO / IEC JTC l。

用于开发本文档的程序和用于进一步维护的程序如下.在 ISO / IEC 指令的第 l 部分中进行了详细描述。特别要注意的是，不同类型的文档需要不同的批准标准。本文件是根据 ISo/EC 指令第 2 部分的编辑规则起草的(参见 wvwiso, org/directives)，

请注意，本文档的某些内容可能是专利权的主题。 ISo 和 IEC 对识别任何或所有此类专利权概不负责。 在文档开发过程中确定的任何专利权的详细信息将在“引言和/或收到的专利声明的独立性”上（请参见 www.iso，orglpatents）。

本文档中使用的任何商品名称都是为了方便用户而提供的信息，并不构成对本产品的认可。

对于标准的自愿性的解释，ISO 特定术语的含义和与合格评定有关的表述，以及有关 ISO 遵守、技术性贸易壁垒（TBT）中的世界贸易组织（WTO）原则，请参见 www.iso.org/iso/foreword.html。

本文档由 ISO / IEC TC l 技术委员会准备的，信息技术、SC 27 小组委员会、IT 安全技术。

本第二版取消并替代了第一版（ISO / EC 27018：2014），对第一版仅作小修改。 与上一版本相比，主要的变化是对附件 A 中编辑错误的更正。

关于本文档的任何反馈或问题应直接发送给用户的国家标准机构。 这些机构的完整列表可以在 www.iso.org/members.html 上找到。

介绍

0.1 背景和语境

根据与客户签订的合同处理个人可识别信息（PII）的云服务提供商需要以允许双方都满足适用法律和法规（涉及保护 PII 的要求）的方式来运营其服务。云服务提供商及其客户的要求和要求的方式因法律管辖权以及云服务提供商与客户之间的合同条款而有所不同。 有时被称为数据保护法规；有时会将 PII 称为个人数据或个人信息。PII 处理者所承担的义务因司法管辖区而异，这使得提供云计算服务的企业在跨国运营中面临挑战。

当公有云服务提供商根据云服务客户的指示处理 PII 时，它就是一个“ PII 处理者”。与公有云 PII 处理者有合同关系的云服务客户，可以从自然人(处理他或她自己在云中的 PII 的 PII 主体)到组织(处理与许多 PII 主体相关的 PII 的 PII 控制者)。云服务客户可以授权一个或多个与其关联的云服务用户使用根据其与公有云 PII 处理者的合同提供的服务。请注意，云服务客户有权处理和使用数据。与公有云 PII 处理者相比，同时也是 PII 控制者的云服务客户在管理 PII 保护方面需要承担更广泛的义务。维持 PII 控制者和 PII 处理者之间的区别依赖于公有云 PII 处理者，PII 处理者没有其他数据处理目标，不同于为实现云服务客户要求的遵守 PII 处理要求和实现云服务客户目标所必需的操作目标。

注：公有云 PII 处理者在处理云服务客户账户数据时，可以充当此目的的 PII 控制者。本文档不包括此类活动。

当与 ISo/IEC 27002 中的信息安全目标和控制结合使用时，本文档的目的是创建一套通用的安全类别和控制，可以由公有云计算服务提供商作为 PII 处理者来实现。它的目标如下:

—帮助公有云服务提供商在作为 PII 处理者时遵守适用的义务，无论这些义务是由 PII 处理者直接承担还是通过合同承担;

—使公有云 PII 处理者在相关事务上透明，以便云服务客户可以选择管理良好的基于云的 PII 处理服务;

—协助云服务客户和公有共云 PII 处理者签订合同协议

—为云服务客户提供一种机制，以在多方虚拟化服务器（云）环境中托管的单个云服务客户对托管数据进行技术审计，在技术上不切实际的情况下行使审计、合规权利和责任的机制，并可增加风险以使这些物理和逻辑网络安全控制到位。

本文件为公有云服务提供商，特别是在跨国市场运营的云服务提供商，提供了一个通用的合规框架。