



中华人民共和国国家标准

GB/T 41574—2022

信息技术 安全技术 公有云中个人信息保护实践指南

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

(ISO/IEC 27018:2019, Information technology—Security techniques—
Code of practice for protection of personally identifiable information(PII) in
public clouds acting as PII processors, MOD)

2022-07-11 发布

2023-02-01 实施

国家市场监督管理总局 发布
国家标准化管理委员会

目 次

前言 V

引言 VII

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 概述 2

4.1 本文件的结构 2

4.2 控制类别 3

5 信息安全策略 3

5.1 信息安全管理指导 3

5.1.1 信息安全策略 3

5.1.2 信息安全策略的评审 4

6 信息安全组织 4

6.1 内部组织 4

6.1.1 信息安全的角色和责任 4

6.1.2 职责分离 4

6.1.3 与职能机构的联系 4

6.1.4 与特定相关方的联系 4

6.1.5 项目管理中的信息安全 4

6.2 移动设备和远程工作 4

7 人力资源安全 4

7.1 任用前 4

7.2 任用中 5

7.2.1 管理责任 5

7.2.2 信息安全意识、教育和培训 5

7.2.3 违规处理过程 5

7.3 任用的终止和变更 5

8 资产管理 5

9 访问控制 5

9.1 访问控制的业务要求 5

9.2 用户访问管理 5

9.2.1 用户注册和注销 6

9.2.2 用户访问供给 6

9.2.3 特许访问权管理 6

9.2.4 用户的秘密鉴别信息管理 6

9.2.5 用户访问权的评审 6

9.2.6	访问权的移除或调整	6
9.3	用户责任	6
9.3.1	秘密鉴别信息的使用	6
9.4	系统和应用访问控制	6
9.4.1	信息访问限制	6
9.4.2	安全登录规程	6
9.4.3	口令管理系统	6
9.4.4	特权实用程序的使用	7
9.4.5	程序源代码的访问控制	7
10	密码	7
10.1	密码控制	7
10.1.1	密码控制的使用策略	7
10.1.2	密钥管理	7
11	物理和环境安全	7
11.1	安全区域	7
11.2	设备	7
11.2.1	设备安置和保护	7
11.2.2	支持性设施	7
11.2.3	布缆安全	7
11.2.4	设备维护	8
11.2.5	资产的移动	8
11.2.6	组织场所外的设备与资产安全	8
11.2.7	设备的安全处置或再利用	8
11.2.8	无人值守的用户设备	8
11.2.9	清理桌面和屏幕策略	8
12	运行安全	8
12.1	运行规程和责任	8
12.1.1	文件化的操作规程	8
12.1.2	变更管理	8
12.1.3	容量管理	8
12.1.4	开发、测试和运行环境的分离	8
12.2	恶意软件防范	9
12.3	备份	9
12.3.1	信息备份	9
12.4	日志和监视	9
12.4.1	事态日志	9
12.4.2	日志信息的保护	9
12.4.3	管理员和操作员日志	10
12.4.4	时钟同步	10
12.5	运行软件控制	10
12.6	技术方面的脆弱性管理	10
12.7	信息系统审计的考虑	10

13	通信安全	10
13.1	网络安全管理	10
13.2	信息传输	10
13.2.1	信息传输策略和规程	10
13.2.2	信息传输协议	10
13.2.3	电子消息发送	10
13.2.4	保密或不披露协议	10
14	系统获取、开发和维护	11
15	供应商关系	11
16	信息安全事件管理	11
16.1	信息安全事件的管理和改进	11
16.1.1	责任和规程	11
16.1.2	报告信息安全事态	11
16.1.3	报告信息安全弱点	11
16.1.4	信息安全事态的评估和决策	11
16.1.5	信息安全事件的响应	11
16.1.6	从信息安全事件中学习	11
16.1.7	证据的收集	12
17	业务连续性管理的信息安全方面	12
18	符合性	12
18.1	符合法律和合同要求	12
18.2	信息安全评审	12
18.2.1	信息安全独立评审	12
18.2.2	符合安全策略和标准	12
18.2.3	技术符合性评审	12
附录 A (资料性)	本文件与 ISO/IEC 27018:2019 结构编号对照情况	13
附录 B (规范性)	公有云个人信息处理者保护个人信息的扩展控制措施集	15
附录 C (资料性)	云服务提供者、云服务客户和云服务用户的关系	21
参考文献		22

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件修改采用 ISO/IEC 27018:2019《信息技术 安全技术 个人可识别信息(PII)处理者在公有云中保护 PII 的实践指南》。

本文件与 ISO/IEC 27018:2019 相比,在结构上有较多调整。两个文件之间的结构编号变化对照一览表见附录 A。

本文件与 ISO/IEC 27018:2019 的技术差异及其原因如下:

- 将术语“个人可识别信息(PII)”更改为“个人信息”,并更改了定义,与 GB/T 35273—2020 的术语和定义保持一致(见 3.1,ISO/IEC 27018:2019 的 3.2);
- 将术语“PII 控制者”更改为“个人信息控制者”,并更改了定义,与 GB/T 35273—2020 的术语和定义保持一致(见 3.2,ISO/IEC 27018:2019 的 3.3);
- 将术语“PII 主体”更改为“个人信息主体”,并更改了定义,与 GB/T 35273—2020 的术语和定义保持一致(见 3.3,ISO/IEC 27018:2019 的 3.4);
- 将术语“PII 处理者”更改为“个人信息处理者”,并更改了定义,与 GB/T 35273—2020 的术语和定义保持一致(见 3.4,ISO/IEC 27018:2019 的 3.5);
- 将术语“PII 处理”更改为“个人信息处理”,并更改了定义,与 GB/T 35273—2020 的术语和定义保持一致(见 3.5,ISO/IEC 27018:2019 的 3.6);
- 将表题中的 ISO/IEC 27002 更改为 GB/T 22081(见表 1,ISO/IEC 27018:2019 的表 1);
- 增加处理者委托分包商处理个人信息的建议,与 GB/T 35273—2020 中 9.1 c) 2) 关于受委托者的要求保持一致(见 5.1.1);
- 删除“公有云 PII 保护其他信息”中法律法规对处理者和控制者不同要求的表述,以符合我国标准化文件的起草规则(见 ISO/IEC 27018:2019 的 5.1.1);
- 删除“公有云 PII 保护其他信息”中法律法规对处理者处罚的要求,以符合我国标准化文件的起草规则(见 ISO/IEC 27018:2019 的 7.2.2);
- 增加采用密码技术解决机密性、完整性、真实性、不可否认性需求的要求(见 10.1.1);
- 增加处理者转让个人信息的建议,与 GB/T 35273—2020 的相关条款保持一致(见 B.2.3);
- 增加处理者向境外提供个人信息的建议,以适应我国的技术条件,便于本文件的应用(见 B.4.1、B.7.14);
- 增加处理者委托代理商处理个人信息的建议,与 GB/T 35273—2020 中 9.1 c) 2) 关于受委托者的要求保持一致(见 B.7.1);
- 增加数据恢复日志包含信息的建议(见 B.7.3);
- 删除“公有云 PII 保护实现指南”中关于处理者告知义务的相关法律表述,以符合我国标准化文件的起草规则(见 ISO/IEC 27018:2019 的 A.10.1)。

本文件做了下列编辑性改动:

- 为与现有标准系列一致,将标准名称更改为《信息技术 安全技术 公有云中个人信息保护实践指南》;
- 更改附录 B 中新增控制措施的分类原则,与我国的个人信息保护原则保持一致(见 B.1,ISO/IEC 27018:2019 的 A.1);

- 增加对“脱链”的解释说明,以提高条款的易读性,便于本文件的应用(见 B.2.3 注 1);
- 增加对“消磁”的解释说明,以提高条款的易读性,便于本文件的应用(见 B.2.3 注 2);
- 增加附录 A(资料性)“本文件与 ISO/IEC 27018:2019 结构编号对照情况”;
- 增加附录 C(资料性)“云服务提供者、云服务客户和云服务用户的关系”;
- 删除 ISO/IEC 27018:2019 的 9.2.1 注;
- 删除 ISO/IEC 27018:2019 的 10.1.1 注;
- 删除 ISO/IEC 27018:2019 的 12.3.1 注 1 和注 2;
- 删除 ISO/IEC 27018:2019 的 A.6.1 示例;
- 删除 ISO/IEC 27018:2019 的 A.11.3 注的第 1 句;
- 将本项控制措施和指南可归入的其他原则改为“公开透明”原则,与我国的个人信息保护原则保持一致(见 B.2.3 注 3,ISO/IEC 27018:2019 的 A.10.3 注);
- 更改“公有云 PII 保护实现指南”中涉及 PII 收集和使用所遵循原则的表述,与我国的个人信息保护原则保持一致(见 B.3.1,ISO/IEC 27018:2019 的 A.3.1);
- 更改“公有云 PII 保护实现指南”中的“PII 控制者”为“云服务客户”,以提高易读性,便于本文件的应用(见 B.8.1,ISO/IEC 27018:2019 的 A.2.1)。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)归口。

本文件起草单位:山东省标准化研究院、杭州拓深科技有限公司、中国网络安全审查技术与认证中心、陕西省网络与信息安全测评中心、艺龙网信息技术(北京)有限公司、中电长城网际系统应用有限公司、北京钱袋宝支付技术有限公司、国家工业信息安全发展研究中心、腾讯云计算(北京)有限责任公司、陕西省信息化工程研究院、中电数据服务有限公司、上海市信息安全行业协会、上海安言信息技术有限公司、安徽省电子产品监督检验所、山东中测信息技术有限公司。

本文件主要起草人:王庆升、尤其、党斌、闵京华、兰安娜、柳彩云、王永霞、张勇、张博、周亚超、孙岩、张轩铭、靳倩、王利强、赵首花、王爱义、杨帆、石磊、黄磊、王理冬、赵倩倩、马卓元、贾梦妮、闫育芸、秦峰、杨向东、王法中、许立前、范正翔、于秀彦、刘勘伪、吴博。

引 言

0.1 背景和环境

近年,越来越多的云服务客户使用云服务提供者的服务,委托其进行个人信息处理。GB/T 35273—2020 中规定了对接受委托处理一方(GB/T 35273—2020 中 9.1 称为“受委托者”,本文文件中的“处理者”即“受委托者”)的要求。本文件按照 GB/T 35273—2020 对处理者的要求,提供了一种在公有云中保护个人信息的通用合规框架,指导处理者开展公有云中个人信息处理操作。

公有云服务提供者通常需要依据与云服务客户签订的合同,并在双方均遵守个人信息保护法律法规相关要求的前提下开展服务。对于个人信息保护的这些要求,云服务提供者与云服务客户是依据法律法规和它们之间的合同来确定的。

当公有云服务提供者按照云服务客户的要求处理个人信息时,公有云服务提供者充当“个人信息处理者”的角色。与公有云个人信息处理者有合同关系的云服务客户是“个人信息控制者”。在云计算环境下,个人信息控制者掌握个人信息的控制权,其也具有处理和使用个人信息的权限。个人信息控制者与个人信息处理者均可处理个人信息,但个人信息处理者作为受委托的一方,只能执行个人信息控制者要求的个人信息处理操作和为实现个人信息控制者目标而进行的必要操作。同时,云服务客户也可授权一个或多个云服务用户使用其服务,但这些服务仅限于云服务客户与公有云个人信息处理者签订合同中约定的可用服务。

本文件旨在创建一组通用的控制类别和控制措施,与 GB/T 22081 中的信息安全控制目标和控制措施结合使用,由个人信息处理者来实现。本文件的目的如下:

- 帮助公有云个人信息处理者履行相应义务,这些义务包括法律法规规定的直接义务及合同约定的其他义务;
- 使公有云个人信息处理者在相关事务上保持透明,便于云服务客户选择管理良好的基于云的个人信息处理服务;
- 协助云服务客户和公有云个人信息处理者签订合同协议;
- 在单个云服务客户无法对托管在多方或虚拟化服务器(云)中的数据进行审计,或者此类审计可能增加现有物理和逻辑网络安全控制风险的情况下,为云服务客户行使审计权力和承担符合性责任提供一种机制。

本文件可为公有云服务提供者,特别是跨国运营的公有云服务提供者,提供一种通用的合规框架。

0.2 公有云计算服务的个人信息保护控制

在基于 GB/T 22080 实施云计算信息安全管理的过程中,公有云个人信息处理者可参考本文文件选择个人信息保护控制措施。本文件也可作为公有云个人信息处理者实施通用的个人信息保护控制措施的指导文件。尤其是,本文件在 GB/T 22081 的基础上,考虑了个人信息处理者所面临的特定风险环境。

通常来说,组织实施 GB/T 22080 是为了保护自身的信息资产。然而,公有云个人信息处理者保护的个人信息,实际上是云服务客户的信息资产。因此,由公有云个人信息处理者实施 GB/T 22081 中的

控制措施是合理的,也是必要的。同时,为适应公有云计算环境中风险分散的特点,并符合云服务客户与公有云个人信息处理者之间的合同要求,本文件增强了 GB/T 22081 中的控制措施。本文件通过以下 2 种方式增强了 GB/T 22081:

- 为 GB/T 22081 中的某些控制措施提供了适用于公有云个人信息保护的实现指南;
- 附录 B 提供了一组新的控制措施和相关指南,以解决 GB/T 22081 中的控制措施集未能满足的公有云个人信息保护要求。

0.3 个人信息保护要求

组织确定其对个人信息的保护要求。这些要求有以下 3 个主要来源。

- a) 法律、法规、监管和合同要求:一个来源是组织及其贸易伙伴、承包商和服务商满足的法律、法规、监管和合同要求或义务,以及社会文化责任和运营环境要求。需要注意的是,法律、法规和合同可能强制要求个人信息处理者选择特定的控制措施,也可能要求其制定具体的准则来实现这些控制措施。
- b) 风险:另一个来源是,考虑组织整体业务战略和目标的基础上,组织对个人信息相关的评估风险。组织通过风险评估识别威胁、评估脆弱性和发生的可能性、估计潜在影响。GB/T 31722 提供了信息安全风险管理指南,包括风险评估、风险接受、风险沟通、风险监视和风险审查的建议。ISO/IEC 29134 提供了有关隐私影响评估的指南。
- c) 组织政策:尽管组织政策涵盖了来自法律和社会文化的诸多义务,但组织仍可自愿选择超出 a) 的要求。

0.4 云计算环境下控制措施的选择和实现

组织可能从本文件中选择控制措施(包括引用的 GB/T 22081 中的控制措施,以及面向具体应用创建的组合参考控制措施集)。若需要,组织还可能从其他控制措施集中选择控制措施,或者设计新的控制措施以满足特定要求。

控制措施的选择取决于组织的决策。这些决策是基于风险接受程度、风险处理方案,以及适用于组织与其有合同关系的客户、供应商的一般风险管理方法作出的。控制措施的选择还受国内外法律法规的约束。若未选择本文件中的控制措施,则需说明并记录未选择的理由。

此外,控制措施的选择和实现还取决于组织在整个云计算参考架构中的实际角色(见 GB/T 32399)。在云计算环境中,可能存在多个组织参与提供基础设施服务和应用服务的情况。在某些情况下,所选控制措施对于云计算参考架构中的特定服务类别来说可能是唯一的。而在其他情况下,实现安全控制措施可能共享角色。合同协议需要规定提供或使用云服务的所有组织承担的个人信
息保护责任。这些组织包括公有云个人信息处理者及其分包商、云服务客户。

本文件中的控制措施可视为一种指导原则,适用于大多数组织。下文将给出这些控制措施的详细说明和实现指南。若公有云个人信息处理者在设计信息系统、服务和操作的过程中预先考虑了保护个人信息的要求,那么这些控制措施的实现将会更加简单。这是“隐私设计”(参见参考文献[9])的一部分。

0.5 制定额外指南

本文件可看作开发个人信息保护指南的起点。对于保护个人信息而言,本文件中的控制措施和实现指南可能并非都是适用的,并且可能还需要本文件未包含的额外控制措施和实现指南。在开发包含

额外控制措施或指南的文件时,交叉引用本文件中的适用条款可有助于审计人员和业务合作伙伴进行合规性检查。

0.6 生命周期的考虑

个人信息有其固有的生命周期,即从创建和生成,经过存储、处理、使用、传输到最终销毁或消失。个人信息在生命周期中面临不同的风险,但在生命周期的各个阶段保护个人信息仍很重要。

个人信息保护需结合现有的和新的信息系统进行考虑,并进行全生命周期管理。

信息技术 安全技术

公有云中个人信息保护实践指南

1 范围

本文件给出了在公有云中实施个人信息保护的控制目标和控制措施,在 GB/T 22081 基础上给出了公有云个人信息保护指南。

本文件适用于作为个人信息处理者的所有类型和规模的组织,包括公有和私营公司、政府机构和非营利组织。

本文件也可能适用于作为个人信息控制者的组织。但是,个人信息控制者可能还受额外的个人信息保护法律法规和义务的约束,而这些法律法规和义务不适用于个人信息处理者。本文件不涵盖此类额外义务。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 22081—2016 信息技术 安全技术 信息安全控制实践指南(ISO/IEC 27002:2013,IDT)

GB/T 29246 信息技术 安全技术 信息安全管理体系 概述和词汇(GB/T 29246—2017, ISO/IEC 27000:2016,IDT)

GB/T 32400 信息技术 云计算 概览与词汇(GB/T 32400—2015,ISO/IEC 17788:2014,IDT)

GB/T 35273—2020 信息安全技术 个人信息安全规范

3 术语和定义

GB/T 29246 和 GB/T 32400 界定的以及下列术语和定义适用于本文件。

3.1

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

注 1: 个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注 2: 关于个人信息的判定方法和类型参见 GB/T 35273—2020 中附录 A。

注 3: 个人信息控制者通过个人信息或其他信息加工处理后形成的信息,例如,用户画像或特征标签,能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的,属于个人信息。

[来源:GB/T 35273—2020,3.1]。

3.2

个人信息控制者 personal information controller

有能力决定个人信息处理目的、方式等的组织或个人。

[来源:GB/T 35273—2020,3.4]。

3.3

个人信息主体 **personal information principal**

个人信息所标识或者关联的自然人。

[来源:GB/T 35273—2020,3.3]。

3.4

个人信息处理者 **personal information processor**

代表并根据个人信息控制者的要求处理个人信息的组织或个人。

注：对于处理个人信息而言，个人信息处理者与 GB/T 35273—2020 中 9.1 提到的“受委托者”履行的义务相同，两者可以等同使用。

3.5

个人信息处理 **processing of personal information**

对个人信息执行的操作或操作集。

注：个人信息处理操作包括但不限于收集、存储、变更、恢复、查阅、披露、匿名化、假名化、传播或以其他方式提供、删除或销毁个人信息。

3.6

公有云服务提供者 **public cloud service provider**

根据公有云模型提供云服务的参与方。

3.7

数据失陷 **data breach**

导致受保护数据在传输、存储或处理过程中被意外或非法销毁、丢失、变更，以及未经授权披露或访问的安全危害。

[来源:ISO/IEC 27040:2015,3.7]

4 概述

4.1 本文件的结构

本文件的结构与 GB/T 22081 类似。当无需补充其他信息，GB/T 22081 中规定的控制目标和控制措施适用于本文件时，本文件仅给出对 GB/T 22081 相应条款的引用。附录 B 给出了适用于公有云个人信息处理者保护个人信息的额外控制措施和相关实现指南。

“公有云个人信息保护实现指南”标题下给出了适用于公有云服务提供者保护个人信息的额外指南。“公有云个人信息保护其他信息”标题下给出了增强这些额外指南的更多相关信息。

如表 1 所示，面向特定应用的指南和其他信息包含在 GB/T 22081 定义的控制类别中。本文件的条款号与 GB/T 22081 中的条款号一致，见表 1。

本文件应与 GB/T 22080 结合使用，并将附录 B 给出的额外控制措施作为实施基于 GB/T 22080 的信息安全管理体系的组成部分。

表 1 实现 GB/T 22081 中定义的控制措施所需的特定指南和其他信息在本文件中的位置

条款号	标题	备注
5	信息安全策略	提供了特定应用的实现指南和其他信息
6	信息安全组织	提供了特定应用的实现指南
7	人力资源安全	提供了特定应用的实现指南和其他信息

表 1 实现 GB/T 22081 中定义的控制措施所需的特定指南和其他信息在本文件中的位置（续）

条款号	标题	备注
8	资产管理	没有提供额外的特定应用实现指南或其他信息
9	访问控制	提供了特定应用的实现指南,同时交叉引用了附录 B 中的控制措施
10	密码	提供了特定应用的实现指南
11	物理和环境安全	提供了特定应用的实现指南,同时交叉引用了附录 B 中的控制措施
12	运行安全	提供了特定应用的实现指南
13	通信安全	提供了特定应用的实现指南,同时交叉引用了附录 B 中的控制措施
14	系统获取、开发和维护	没有提供额外的特定应用实现指南或其他信息
15	供应商关系	没有提供额外的特定应用实现指南或其他信息
16	信息安全事件管理	提供了特定应用的实现指南
17	业务连续性管理的信息安全方面	没有提供额外的特定应用实现指南或其他信息
18	符合性	提供了特定应用的实现指南,同时交叉引用了附录 B 中的控制措施

4.2 控制类别

根据 GB/T 22081,每一个主要控制类别包括:

- a) 一个控制目标,声明要实现什么;
- b) 一个或多个控制措施,可被用于实现该控制目标。

控制措施的描述结构如下:

控制措施

为满足控制目标,给出了定义特定控制措施的陈述。

公有云个人信息保护实现指南

为支持该控制措施的实现并满足控制目标,提供更详细的信息。该指南不一定完全适用于所有情况,也不一定满足组织的特定控制要求。因此,可能需要替代的或额外的控制措施,或其他形式的风险处理方式(例如,规避、转移或接受风险)。

公有云个人信息保护其他信息

提供需要考虑的更多信息。例如,法律方面的考虑和对其他文件的参考。

5 信息安全策略

5.1 信息安全管理指导

GB/T 22081—2016 中 5.1 规定的目标适用。

5.1.1 信息安全策略

GB/T 22081—2016 中 5.1.1 规定的控制措施、实现指南和其他信息适用。以下特定应用指南也适用。

公有云个人信息保护实现指南

宜通过发表声明增强信息安全策略。该声明应承诺遵守适用的个人信息保护法规,以及公有云个人信息处理者与云服务客户达成的合同条款。

合同协议宜明确划分公有云个人信息处理者、其分包商和云服务客户之间的责任,且在划分责任时宜考虑所提供的云服务类型(例如,IaaS模式、PaaS模式或SaaS模式)。例如,公有云个人信息处理者提供SaaS、PaaS或IaaS等不同的服务类型时,应用层控制的责任划分也不同。

分包商接受个人信息处理者的再次委托处理个人信息时,个人信息处理者应事先征得个人信息控制者的授权(见GB/T 35273—2020中9.1)。

公有云个人信息保护其他信息

云服务客户和公有云个人信息处理者之间的合同提供了一种确保公有云个人信息处理者支持和管理符合性的机制。通过实施本文件和GB/T 22081中的相关控制措施,公有云个人信息处理者可能在合同中要求云服务客户接受独立的符合性审计。

5.1.2 信息安全策略的评审

GB/T 22081—2016中5.1.2规定的控制措施和实现指南适用。

6 信息安全组织

6.1 内部组织

GB/T 22081—2016中6.1规定的目标适用。

6.1.1 信息安全的角色和责任

GB/T 22081—2016中6.1.1规定的控制措施、实现指南和其他信息适用。以下特定应用指南也适用。

公有云个人信息保护实现指南

公有云个人信息处理者宜指定一个联系人,负责与云服务客户的协调工作。

6.1.2 职责分离

GB/T 22081—2016中6.1.2规定的控制措施、实现指南和其他信息适用。

6.1.3 与职能机构的联系

GB/T 22081—2016中6.1.3规定的控制措施、实现指南和其他信息适用。

6.1.4 与特定相关方的联系

GB/T 22081—2016中6.1.4规定的控制措施、实现指南和其他信息适用。

6.1.5 项目管理中的信息安全

GB/T 22081—2016中6.1.5规定的控制措施、实现指南和其他信息适用。

6.2 移动设备和远程工作

GB/T 22081—2016中6.2规定的目标和内容适用。

7 人力资源安全

7.1 任用前

GB/T 22081—2016中7.1规定的目标和内容适用。

7.2 任用中

GB/T 22081—2016 中 7.2 规定的目标适用。

7.2.1 管理责任

GB/T 22081—2016 中 7.2.1 规定的控制措施、实现指南和其他信息适用。

7.2.2 信息安全意识、教育和培训

GB/T 22081—2016 中 7.2.2 规定的控制措施、实现指南和其他信息适用。以下特定应用指南也适用。

公有云个人信息保护实现指南

宜采取措施使相关人员,特别是个人信息处理人员,了解违反隐私和安全规则造成的影响,包括对公有云个人信息处理者的影响(例如,法律后果、业务损失、品牌或声誉损害),对员工的影响(例如,纪律处分)以及对个人信息主体的影响(例如,身体上、物质上和情感上的后果)。

公有云个人信息保护其他信息

公有云个人信息处理者和云服务客户依据本文件签订合同,宜有助于为违反安全规则的制裁奠定合同基础。

7.2.3 违规处理过程

GB/T 22081—2016 中 7.2.3 规定的控制措施、实现指南和其他信息适用。

7.3 任用的终止和变更

GB/T 22081—2016 中 7.3 规定的目标和内容适用。

8 资产管理

GB/T 22081—2016 中第 8 章规定的目标和内容适用。

9 访问控制

9.1 访问控制的业务要求

GB/T 22081—2016 中 9.1 规定的目标和内容适用。

9.2 用户访问管理

GB/T 22081—2016 中 9.2 规定的目标适用。以下特定应用指南也适用于本条中所有控制措施的实现。

公有云个人信息保护实现指南

对于云计算参考架构中定义的不同服务类别,云服务客户可能对其控制的云服务用户具有不同的访问管理权限。在适当的情况下,公有云个人信息处理者宜使云服务客户能够管理其控制的云服务用户的访问。例如,公有云个人信息处理者向云服务客户提供管理权限去管理或终止用户访问。

注:云服务客户、云服务用户的关系见附录 C。

9.2.1 用户注册和注销

GB/T 22081—2016 中 9.2.1 规定的控制措施、实现指南和其他信息适用。以下特定应用指南也适用。

公有云个人信息保护实现指南

用户注册和注销程序宜解决用户访问控制受损的情况,例如,口令或其他用户注册数据受损。

9.2.2 用户访问供给

GB/T 22081—2016 中 9.2.2 规定的控制措施、实现指南和其他信息适用。

9.2.3 特许访问权管理

GB/T 22081—2016 中 9.2.3 规定的控制措施、实现指南和其他信息适用。

9.2.4 用户的秘密鉴别信息管理

GB/T 22081—2016 中 9.2.4 规定的控制措施、实现指南和其他信息适用。

9.2.5 用户访问权的评审

GB/T 22081—2016 中 9.2.5 规定的控制措施、实现指南和其他信息适用。

9.2.6 访问权的移除或调整

GB/T 22081—2016 中 9.2.6 规定的控制措施、实现指南和其他信息适用。

9.3 用户责任

GB/T 22081—2016 中 9.3 规定的目标适用。

9.3.1 秘密鉴别信息的使用

GB/T 22081—2016 中 9.3.1 规定的控制措施和实现指南适用。

9.4 系统和应用访问控制

GB/T 22081—2016 中 9.4 规定的目标适用。

9.4.1 信息访问限制

GB/T 22081—2016 中 9.4.1 规定的控制措施和实现指南适用。

注:有关信息访问限制的额外控制措施和指南见 B.7.13。

9.4.2 安全登录规程

GB/T 22081—2016 中 9.4.2 规定的控制措施、实现指南和其他信息适用。以下特定应用指南也适用。

公有云个人信息保护实现指南

需要时,公有云个人信息处理者宜向云服务客户控制下的云服务用户请求的任何账户提供安全登录程序。

9.4.3 口令管理系统

GB/T 22081—2016 中 9.4.3 规定的控制措施、实现指南和其他信息适用。

9.4.4 特权实用程序的使用

GB/T 22081—2016 中 9.4.4 规定的控制措施、实现指南和其他信息适用。

9.4.5 程序源代码的访问控制

GB/T 22081—2016 中 9.4.5 规定的控制措施、实现指南和其他信息适用。

10 密码

10.1 密码控制

GB/T 22081—2016 中 10.1 规定的目标适用。

10.1.1 密码控制的使用策略

GB/T 22081—2016 中 10.1.1 规定的控制措施、实现指南和其他信息适用。以下特定应用指南也适用。

公有云个人信息保护实现指南

公有云个人信息处理者宜将其使用密码保护所处理个人信息的相关信息提供给云服务客户。公有云个人信息处理者还宜向云服务客户提供功能信息,这些功能可能帮助云服务客户应用其自身的密码保护。

采用密码技术解决机密性、完整性、真实性、不可否认性需求的,应遵循相关密码国家标准和行业标准。

10.1.2 密钥管理

GB/T 22081—2016 中 10.1.2 规定的控制措施、实现指南和其他信息适用。

11 物理和环境安全

11.1 安全区域

GB/T 22081—2016 中 11.1 规定的目标和内容适用。

11.2 设备

GB/T 22081—2016 中 11.2 规定的目标适用。

11.2.1 设备安置和保护

GB/T 22081—2016 中 11.2.1 规定的控制措施和实现指南适用。

11.2.2 支持性设施

GB/T 22081—2016 中 11.2.2 规定的控制措施、实现指南和其他信息适用。

11.2.3 布缆安全

GB/T 22081—2016 中 11.2.3 规定的控制措施和实现指南适用。

11.2.4 设备维护

GB/T 22081—2016 中 11.2.4 规定的控制措施和实现指南适用。

11.2.5 资产的移动

GB/T 22081—2016 中 11.2.5 规定的控制措施、实现指南和其他信息适用。

11.2.6 组织场所外的设备与资产安全

GB/T 22081—2016 中 11.2.6 规定的控制措施、实现指南和其他信息适用。

11.2.7 设备的安全处置或再利用

GB/T 22081—2016 中 11.2.7 规定的控制措施、实现指南和其他信息适用。以下特定应用指南也适用。

公有云个人信息保护实现指南

出于安全处置或再利用的目的,可能包含个人信息的存储介质宜视为包含个人信息的设备。

注:有关设备安全处置或再利用的额外控制措施和指南见 B.7.13。

11.2.8 无人值守的用户设备

GB/T 22081—2016 中 11.2.8 规定的控制措施和实现指南适用。

11.2.9 清理桌面和屏幕策略

GB/T 22081—2016 中 11.2.9 规定的控制措施、实现指南和其他信息适用。

12 运行安全

12.1 运行规程和责任

GB/T 22081—2016 中 12.1 规定的目标适用。

12.1.1 文件化的操作规程

GB/T 22081—2016 中 12.1.1 规定的控制措施和实现指南适用。

12.1.2 变更管理

GB/T 22081—2016 中 12.1.2 规定的控制措施、实现指南和其他信息适用。

12.1.3 容量管理

GB/T 22081—2016 中 12.1.3 规定的控制措施、实现指南和其他信息适用。

12.1.4 开发、测试和运行环境的分离

GB/T 22081—2016 中 12.1.4 规定的控制措施、实现指南和其他信息适用。以下特定应用指南也适用。

公有云个人信息保护实现指南

出于测试目的使用个人信息时,宜进行风险评估,且宜实施技术措施和组织措施降低已识别的风险。

12.2 恶意软件防范

GB/T 22081—2016 中 12.2 规定的目标和内容适用。

12.3 备份

GB/T 22081—2016 中 12.3 规定的目标适用。

12.3.1 信息备份

GB/T 22081—2016 中 12.3.1 规定的控制措施、实现指南和其他信息适用。以下特定应用指南也适用。

公有云个人信息保护实现指南

基于云计算模型的信息处理系统为异地备份引入了额外或替代机制,以防止数据丢失,并确保数据处理操作的连续性以及提供在发生破坏性事态后恢复数据处理操作的能力。为了备份和(或)恢复,宜在不同的物理和(或)逻辑位置上(可以在自身信息处理系统内)创建或维护多个数据副本。

云服务客户可能承担备份和(或)恢复责任,但当公有云个人信息处理者明确向云服务客户提供备份和恢复服务时,公有云个人信息处理者宜向云服务客户提供其备份和恢复服务的明确信息。

宜制定备份和恢复程序,保证在破坏性事态发生后的规定时间内恢复数据。

宜按规定的频率评审备份和恢复程序。

本文件中适用于分包处理个人信息的控制措施涵盖了使用分包商存储所处理数据复制副本或备份副本的情况。本文件中的控制措施也涵盖了使用物理介质传输个人信息的情况。

公有云个人信息处理者宜制定策略,以满足信息备份及擦除备份信息中包含的个人信息的其他要求[例如,合同和(或)法律规定的要求]。

12.4 日志和监视

GB/T 22081—2016 中 12.4 规定的目标适用。

12.4.1 事态日志

GB/T 22081—2016 中 12.4.1 规定的控制措施、实现指南和其他信息适用。以下特定应用指南也适用。

公有云个人信息保护实现指南

宜建立流程,按规定的周期评审事态日志,识别违规行为并提出补救措施。

在可能的情况下,事态日志宜记录个人信息是否因某个事态而更正(添加、修改或删除),以及由谁更正。若多个云服务提供者提供云计算参考架构中定义的不同类别的服务,则在实现本文件时可能会出现不同的角色或共享的角色。

公有云个人信息处理者宜制定关于是否、何时,以及如何向云服务客户提供日志信息的规则。同时,这些规则宜对云服务客户有效。

若允许云服务客户访问由公有云个人信息处理者控制的日志记录,则公有云个人信息处理者宜确保云服务客户仅能访问与其相关的活动,而不能访问其他云服务客户的日志记录。

12.4.2 日志信息的保护

GB/T 22081—2016 中 12.4.2 规定的控制措施、实现指南和其他信息适用。以下特定应用指南也适用。

公有云个人信息保护实现指南

因安全监控和运行诊断等目的而记录的日志信息可能包含个人信息。宜采取诸如控制访问(见

9.2.3)的措施,确保日志信息仅用于预期目的。

宜建立程序,最好是自动化程序,确保在规定的期限内删除日志信息。

12.4.3 管理员和操作员日志

GB/T 22081—2016 中 12.4.3 规定的控制措施、实现指南和其他信息适用。

12.4.4 时钟同步

GB/T 22081—2016 中 12.4.4 规定的控制措施、实现指南和其他信息适用。

12.5 运行软件控制

GB/T 22081—2016 中 12.5 规定的目标和内容适用。

12.6 技术方面的脆弱性管理

GB/T 22081—2016 中 12.6 规定的目标和内容适用。

12.7 信息系统审计的考虑

GB/T 22081—2016 中 12.7 规定的目标和内容适用。

13 通信安全

13.1 网络安全管理

GB/T 22081—2016 中 13.1 规定的目标和内容适用。

13.2 信息传输

GB/T 22081—2016 中 13.2 规定的目标适用。

13.2.1 信息传输策略和规程

GB/T 22081—2016 中 13.2.1 规定的控制措施、实现指南和其他信息适用。以下特定应用指南也适用。

公有云个人信息保护实现指南

使用物理介质传输信息时,宜建立一个系统记录传入传出物理介质的相关信息。这些信息包括物理介质的类型、被授权的发送方/接收方、日期和时间,以及物理介质的数量。在可能的情况下,宜要求云服务客户采取额外措施(例如,加密),确保只能在传输的目的地而非传输过程中访问数据。

13.2.2 信息传输协议

GB/T 22081—2016 中 13.2.2 规定的控制措施、实现指南和其他信息适用。

13.2.3 电子消息发送

GB/T 22081—2016 中 13.2.3 规定的控制措施、实现指南和其他信息适用。

13.2.4 保密或不披露协议

GB/T 22081—2016 中 13.2.4 规定的控制措施、实现指南和其他信息适用。

注:保密或不披露协议的额外控制措施和指南可在 B.7.1 中找到。

14 系统获取、开发和维护

GB/T 22081—2016 中第 14 章规定的目标和内容适用。

15 供应商关系

GB/T 22081—2016 中第 15 章规定的目标和内容适用。

注：有关供应商关系管理的更多信息见 ISO/IEC 27036-4。

16 信息安全事件管理

16.1 信息安全事件的管理和改进

GB/T 22081—2016 中 16.1 规定的目标适用。以下特定应用指南也适用于本条中所有控制措施的实现。

公有云个人信息保护实现指南

云计算参考架构下，信息安全事件的管理和改进活动中可能存在共享的角色。公有云个人信息处理者可能需要与云服务客户合作实现本条中的控制措施。

16.1.1 责任和规程

GB/T 22081—2016 中 16.1.1 规定的控制措施、实现指南和其他信息适用。以下特定应用指南也适用。

公有云个人信息保护实现指南

作为信息安全事件管理过程的一部分，信息安全事件宜触发对公有云个人信息处理者的评审，以确定是否违规处理了包含个人信息的数据（见 B.2.1）。

信息安全事态不宜触发此类评审。信息安全事态是指不会导致未经授权实际访问或极可能访问个人信息以及存储个人信息的公有云个人信息处理者设备设施的事件。信息安全事态包括但不限于：对防火墙或边缘服务器的点对点攻击和其他广播攻击、端口扫描、登录尝试失败、拒绝服务攻击和数据包侦听。

16.1.2 报告信息安全事态

GB/T 22081—2016 中 16.1.2 规定的控制措施、实现指南和其他信息适用。

16.1.3 报告信息安全弱点

GB/T 22081—2016 中 16.1.3 规定的控制措施、实现指南和其他信息适用。

16.1.4 信息安全事态的评估和决策

GB/T 22081—2016 中 16.1.4 规定的控制措施、实现指南适用。

16.1.5 信息安全事件的响应

GB/T 22081—2016 中 16.1.5 规定的控制措施、实现指南和其他信息适用。

16.1.6 从信息安全事件中学习

GB/T 22081—2016 中 16.1.6 规定的控制措施、实现指南和其他信息适用。

16.1.7 证据的收集

GB/T 22081—2016 中 16.1.7 规定的控制措施、实现指南和其他信息适用。

17 业务连续性管理的信息安全方面

GB/T 22081—2016 中第 17 章规定的目标和内容适用。

18 符合性

18.1 符合法律和合同要求

GB/T 22081—2016 中 18.1 规定的目标和内容适用。

注：符合法律和合同要求的额外控制措施和相关指南见 B.2。

18.2 信息安全评审

GB/T 22081—2016 中 18.2 规定的目标适用。

18.2.1 信息安全独立评审

GB/T 22081—2016 中 18.2.1 规定的控制措施、实现指南和其他信息适用。以下特定应用指南也适用。

公有云个人信息保护实现指南

若单个云服务客户的审计不切实际或可能增加安全风险(见 0.1),则公有云个人信息处理者宜在签订合同前和合同期内向潜在的云服务客户提供独立证据,证明信息安全符合公有云个人信息处理者的策略和规程。通常情况下,公有云个人信息处理者选择的独立审计是一种可接受的方式。在保证足够透明的前提下,独立审计可以满足云服务客户评审公有云个人信息处理者处理操作的要求。

18.2.2 符合安全策略和标准

GB/T 22081—2016 中 18.2.2 规定的控制措施、实现指南和其他信息适用。

18.2.3 技术符合性评审

GB/T 22081—2016 中 18.2.3 规定的控制措施、实现指南和其他信息适用。

附 录 A
(资料性)

本文件与 ISO/IEC 27018:2019 结构编号对照情况

表 A.1 给出了本文件与 ISO/IEC 27018:2019 结构编号对照一览表。

表 A.1 本文件与 ISO/IEC 27018:2019 结构编号对照情况

本文件结构编号	ISO/IEC 27018:2019 结构编号
1	1
2	2
3	3
3.1	3.2
3.2	3.3
3.3	3.4
3.4	3.5
3.5	3.6
3.6	3.7
3.7	3.1
4	4
5	5
6	6
7	7
8	8
9	9
10	10
11	11
12	12
13	13
14	14
15	15
16	16
17	17
18	18
附录 A	—
附录 B	附录 A
B.1	A.1
B.2	—

表 A.1 本文件与 ISO/IEC 27018:2019 结构编号对照情况 (续)

本文件结构编号	ISO/IEC 27018:2019 结构编号
B.2.1	A.10.1
B.2.2	A.10.2
B.2.3	A.10.3
B.3	—
B.3.1	A.3.1
B.3.2	A.3.2
B.4	—
B.4.1	A.8.1
B.5	—
B.5.1	A.5.1
B.6	—
B.6.1	A.6.1
B.6.2	A.6.2
B.7	—
B.7.1	A.11.1
B.7.2	A.11.2
B.7.3	A.11.3
B.7.4	A.11.4
B.7.5	A.11.5
B.7.6	A.11.6
B.7.7	A.11.7
B.7.8	A.11.8
B.7.9	A.11.9
B.7.10	A.11.10
B.7.11	A.11.11
B.7.12	A.11.12
B.7.13	A.11.13
B.7.14	A.12.1
B.7.15	A.12.2
B.8	—
B.8.1	A.2.1
附录 C	—

附录 B

(规范性)

公有云个人信息处理者保护个人信息的扩展控制措施集

B.1 总则

本附录给出了新的控制措施和实现指南并构成扩展控制措施集,与文件正文中的增强控制措施和指南结合使用,以满足个人信息处理者保护个人信息的要求。

这些新的控制措施按照 GB/T 35273—2020 中的个人信息保护原则进行分类。在多数情况下,控制措施可能归入多个原则,但应将这些控制措施归入其中最相关的原则。

B.2 权责一致

B.2.1 包含个人信息的数据失陷告知

控制措施

若未经授权访问个人信息或处理个人信息的设备设施导致个人信息丢失、泄露或变更,则公有云个人信息处理者宜立即告知相关云服务客户。

公有云个人信息保护实现指南

公有云个人信息处理者与云服务客户之间的合同宜包含涉及个人信息的数据失陷告知条款。合同宜规定公有云个人信息处理者应如何向云服务客户提供必要的信息,以便云服务客户履行向监管机构告知的义务。此告知义务不适用于因云服务客户、个人信息主体或其负责的系统组件引起的数据失陷。合同还宜规定涉及个人信息的数据失陷告知的最迟时间。

若发生涉及个人信息的数据失陷事件,则宜记录事件描述、发生时间、事件后果、报告者姓名、向谁报告了事件,处理事件所采取的步骤(包括负责人和恢复的数据)以及事件造成的损失、泄露或变更个人信息的事实。

若发生涉及个人信息的数据失陷事件,则还宜记录违规数据的描述(若已知);若已通知个人信息控制者,则宜将采取的步骤告知云服务客户和(或)监管机构。

注:本条并未涵盖其他要求告知的数据失陷事件,例如,未经同意或其他授权收集、未经授权使用等。

B.2.2 行政安全策略和指南的保留期

控制措施

安全策略和操作规程副本宜在规定的替换(包括更新)周期内保留。

公有云个人信息保护实现指南

客户争议处理和配合个人信息保护机构调查时,可能需要评审当前和以往的策略和规程。若法律或合同无明确要求,则安全策略和规程的最短保留期宜为五年。

B.2.3 个人信息返回、转让和处置

控制措施

公有云个人信息处理者宜制定个人信息返回、转让和(或)处置的策略,并对云服务客户有效。

公有云个人信息保护实现指南

在某个时间点,公有云个人信息处理者可能需要以某种形式处理个人信息。这些处理包括将个人信息返回给云服务客户,将个人信息转让给其他个人信息处理者或个人信息控制者(例如,合并),将个

人信息安全地删除或以其他方式销毁、匿名化或归档。

公有云个人信息处理者转让个人信息时,宜向云服务客户告知并征得同意。

若云服务客户不再需要个人信息,包括出于备份和业务连续性目的保存的数据,则公有云个人信息处理者宜提供必要的信息,以使云服务客户能够确保擦除(由公有云个人信息处理者及其分包商擦除)保存于任何位置的个人信息。合同中宜约定具体的个人信息处置方式(例如,脱链、覆盖、消磁、销毁或其他形式的擦除)和(或)适用的商业标准。

注 1: 脱链是一种个人信息处置方法,使用技术手段使信息与自然人脱离链接。

注 2: 消磁是一种数据销毁方法,是指使用强磁场将保存在硬盘、磁盘、磁带等磁介质上的数据彻底清除。

公有云个人信息处理者宜制定并实施处置个人信息的策略,并对云服务客户有效。

该策略宜涵盖合同终止到个人信息销毁的保留期,以保护云服务客户不会因合同意外失效而丢失个人信息。

注 3: 该控制措施和指南也与“公开透明”原则相关(见 B.6)。

B.3 目的明确

B.3.1 公有云个人信息处理者的目的

控制措施

不宜独立于云服务客户指示的任何其他目的处理合同约定的个人信息。

公有云个人信息保护实现指南

这些指示可能包含在公有云个人信息处理者和云服务客户的合同中,例如,服务要实现的目标和完成时限。

为达到云服务客户的目的,公有云个人信息处理者可能从技术角度决定处理云服务客户个人信息的方式。这些决定符合云服务客户的通用指示,但没有云服务客户的专用指示。例如,为有效利用网络能力或处理能力,可能有必要根据个人信息主体的某些特性来分配处理资源。公有云个人信息处理者确定的个人信息处理方法涉及个人信息的收集和使用,公有云个人信息处理者宜遵循GB/T 35273—2020 中规定的个人信息保护原则。

公有云个人信息处理者宜及时向云服务客户提供所有相关信息,以便云服务客户确保公有云个人信息处理者的操作遵循目的规范和限制原则,同时确保公有云个人信息处理者或者其分包商没有独立于公有云客户指示处理个人信息。

B.3.2 公有云个人信息处理者的商业使用

控制措施

未经明确同意,公有云个人信息处理者不宜将合同约定处理的个人信息用于营销和广告。此类同意不宜成为使用其服务的条件。

注: 该控制措施是对通用控制措施 B.3.1 的补充,不可替换。

B.4 选择同意

B.4.1 个人信息分包处理的披露

控制措施

公有云个人信息处理者使用分包商处理个人信息前,宜向相关云服务客户披露。

公有云个人信息保护实现指南

宜在公有云个人信息处理者和云服务客户的合同中约定使用分包商处理个人信息的条款。合同宜规定,只有在服务开始即取得云服务客户同意的前提下,才可委托分包商处理个人信息。公有云个人信息处

理者宜将这方面的任何可能变更及时通知云服务客户,以便云服务客户能够选择拒绝此类变更或终止合同。

披露的信息宜包括使用分包的事实和分包商名称,但不包括具体业务细节。披露的信息还宜包括分包商可能在哪些国家处理数据(见 B.7.14),以及分包商通过哪些方式达到或超出公有云个人信息处理者义务的要求(见 B.7.12)。

若评估认为公开披露分包商的信息增加了安全风险并超出了可接受的范围,则宜根据不披露协议和(或)云服务客户的要求进行披露。宜让云服务客户意识到该信息是有用的。

B.5 最小必要

B.5.1 安全擦除临时文件

控制措施

宜在规定的时间周期内擦除或销毁临时文件和记录。

公有云个人信息保护实现指南

个人信息擦除的实现指南见 B.2.3。

信息系统运行中可能产生临时文件。此类文件与具体系统或应用有关,但可能包括文件系统回滚日志,以及与数据库更新和其他应用程序操作相关的临时文件。信息处理任务完成后,无需留存临时文件,但也有不能删除这些文件的情形。这些文件的留存时间是不确定的,宜使用“垃圾收集”程序识别这些文件并计算自上次使用以来的时间间隔。

个人信息处理系统宜执行周期性检查,确保删除超出规定期限的未使用的临时文件。

B.6 公开透明

B.6.1 个人信息披露告知

控制措施

公有云个人信息处理者与云服务客户之间的合同宜要求公有云个人信息处理者按照约定的程序和时间,将法律规定的个人信息披露请求告知云服务客户。禁止披露的情形除外。

公有云个人信息保护实现指南

公有云个人信息处理者宜在合同中承诺:

- 拒绝任何不具有法律约束力的个人信息披露请求;
- 披露任何个人信息前,在法律允许的情况下征求云服务客户意见;
- 接受任何合同约定并经相应云服务客户授权同意的个人信息披露请求。

B.6.2 个人信息披露记录

控制措施

宜记录向第三方披露个人信息的情况,包括披露的内容、向谁披露及披露时间。

公有云个人信息保护实现指南

个人信息的正常处理过程中,可能披露个人信息,宜记录这些披露(见 12.4.1)。向第三方的任何其他披露也宜被记录,例如,合法调查或外部审计引起的披露。记录宜包括请求披露的来源和授权披露的来源。

B.7 确保安全

B.7.1 保密或不披露协议

控制措施

公有云个人信息处理者控制的个体访问个人信息时,宜履行保密义务。

公有云个人信息保护实现指南

公有云个人信息处理者与其员工、代理商之间任何形式的保密协议,均宜确保员工和代理商不会独立于云服务客户的指示披露个人信息(见 B.3.1)。保密义务宜在合同终止后继续有效。

代理商接受个人信息处理者的再次委托处理个人信息时,个人信息处理者宜事先征得个人信息控制者的授权。

B.7.2 创建硬拷贝材料的限制

控制措施

宜限制生成显示个人信息的硬拷贝材料。

公有云个人信息保护实现指南

硬拷贝材料包括印刷材料。

B.7.3 数据恢复的控制和记录

控制措施

宜有数据恢复工作的程序和日志。

公有云个人信息保护实现指南

数据恢复日志宜包含负责人、恢复数据的说明和手动恢复的数据。

B.7.4 存储介质离开场所的数据保护

控制措施

介质上的个人信息离开组织场所宜遵守授权规程。除授权人员外,任何人员不宜访问这些信息(例如,通过加密相关数据)。

B.7.5 未加密便携式存储介质和设备的使用

控制措施

除非必要,不宜使用未加密的便携式物理介质和便携式设备。若使用,则宜记录此类便携式介质和设备的使用情况。

B.7.6 公共数据传输网络传输个人信息的加密

控制措施

宜在传输之前加密通过公共数据传输网络传输的个人信息。

公有云个人信息保护实现指南

某些情况下,例如电子邮件交互,公共数据传输网络系统的固有特性可能需要公开一些包头或流量数据,以保证传输的有效性。

若多个服务提供者提供云计算参考架构中定义的不同类别的服务,则在实现本文件时可能出现角色变化或角色共享的情形。

B.7.7 硬拷贝材料的安全处置

控制措施

销毁硬拷贝材料时,宜采用安全的销毁方式。例如,剪切、粉碎、焚烧、制浆等。

B.7.8 用户 ID 的唯一使用**控制措施**

若存在多个个体访问存储的个人信息的情形,则个体应具有不同的用户 ID,以便进行识别、认证和授权。

B.7.9 授权用户的记录**控制措施**

宜保存授权访问信息系统的用户或用户资料的最新记录。

公有云个人信息保护实现指南

公有云个人信息处理宜维护所有授权访问用户的资料。用户资料是用户的数据集合,包括用户 ID。这些资料对于通过技术手段控制信息系统的授权访问是必需的。

B.7.10 用户 ID 管理**控制措施**

不宜将停用或过期的用户 ID 授权给其他用户。

公有云个人信息保护实现指南

在完整的云计算参考架构下,云服务客户可能使用不同的权限管理其控制的云服务用户的 ID。

B.7.11 合同措施**控制措施**

云服务客户与公有云个人信息处理者之间的合同宜规定最低限度的技术措施和组织措施,以确保合同约定的安全措施落实到位,并且不会出现未经个人信息控制者授权而处理数据的情况。公有云个人信息处理者不宜单方面削弱这些措施。

公有云个人信息保护实现指南

公有云个人信息处理者的信息安全要求和个人信息保护义务可能直接源自适用的法律。若没有适用的法律,则宜在合同中约定公有云个人信息处理者的个人信息保护义务。

本文件和 GB/T 22081 中的控制措施旨在提供一种措施的参考目录,以帮助云服务客户与公有云个人信息处理者签订个人信息的处理合同。签订合同之前,公有云个人信息处理者宜将其个人信息保护能力告知潜在的云服务客户。

签订合同期间,公有云个人信息处理者宜保持其能力的透明性。但是,云服务客户仍对确保公有云个人信息处理者实施措施是否满足保护要求承担最终责任。

B.7.12 个人信息的外包处理**控制措施**

公有云个人信息处理者与分包商签订的个人信息处理合同宜规定最低限度的技术措施和组织措施,以满足公有云个人信息处理者的信息安全要求和个人信息保护义务。分包商不宜单方面削弱这些措施。

公有云个人信息保护实现指南

本控制措施涵盖了使用分包商存储备份副本的情况(见 B.4.1)。

B.7.13 已用数据存储空间上数据的访问**控制措施**

公有云个人信息处理者宜确保云服务客户不会看到驻留在该存储空间上的任何往期数据。

公有云个人信息保护实现指南

出于性能的考虑,云服务用户删除信息系统中保存的数据时,可能无法显示地擦除这些数据。这可能导致其他用户读取这些数据。宜通过具体的技术措施避免这种风险。

没有具体指南适用于实现该控制措施的所有情况。但是,可参照以下示例处理:若云服务用户读取尚未被其自身数据覆盖的存储空间,则云基础设施、平台或应用程序将返回零。

B.7.14 个人信息的地理位置

控制措施

公有云个人信息处理者宜指定和记录可能存储个人信息的国家。

公有云个人信息保护实现指南

宜向云服务客户提供可能存储个人信息的国家身份,还宜包括因使用分包处理个人信息而产生的国家身份。若具体的合同协议适用于国际间的数据转让,例如,示范合同条款、约束性公司规则、跨境隐私规则,则也宜识别这些协议及适用这些协议的国家或情况。公有云个人信息处理者宜将这方面的任何可能变更及时告知云服务客户,以便云服务客户能够选择拒绝此类变更或终止合同。

B.7.15 个人信息传输目的地

控制措施

使用数据传输网络传输个人信息宜受适当控制,以确保数据到达指定的目的地。

B.8 主体参与

B.8.1 配合个人信息主体行使权利的义务

控制措施

公有云个人信息处理者宜向云服务客户提供使其履行义务的手段,以便个人信息主体能够行使访问、纠正和(或)擦除与其有关的个人信息的权利。

公有云个人信息保护实现指南

云服务客户在这方面的义务可能由法律、法规或合同约定。这些义务可能通过使用公有云个人信息处理者提供服务的方式来履行,例如,由公有云个人信息处理者及时纠正或删除个人信息。

云服务客户使用公有云个人信息处理者提供的信息或技术措施,帮助个人信息主体行使权利时,宜在合同中明确规定这些信息或技术措施。

附录 C
(资料性)

云服务提供者、云服务客户和云服务用户的关系

云服务提供者(见 GB/T 32400—2015 中 3.2.15)、云服务客户(见 GB/T 32400—2015 中 3.2.11)和云服务用户(见 GB/T 32400—2015 中 3.2.17)都是云计算环境下的不同角色。云服务提供者是提供云服务的参与方;云服务客户是为使用云服务而处于一定业务关系中的参与方;云服务用户是云服务客户中使用云服务的自然人或实体代表。

云服务提供者作为云服务的提供方,向云服务客户提供云服务。本文件中提到的云服务提供者指的是公有云服务提供者。当云服务提供者按照云服务客户的要求处理个人信息时,云服务提供者被称为“个人信息处理者”。

云服务客户是云服务提供者的服务对象。云服务客户按照从事活动的不同,可包括云服务用户、云服务管理者、云服务业务管理者、云服务集成者等子角色。云服务用户是云服务客户的一个子角色。云服务用户是自然人,或代表自然人的实体。

- 注 1: 云服务管理者是云服务客户的一个子角色。云服务管理者的主要目的是保证用户使用云服务时运行稳定,同时保证云服务与客户已有的 ICT 系统 and 应用之间运行良好。云服务管理者监控所有与使用云服务相关的操作流程,并承担云服务客户与云服务提供者之间技术交互的切入点。
- 注 2: 云服务业务管理者是云服务客户的一个子角色,其目的是通过经济有效的方式获取和使用云服务,满足云服务客户的业务目标。云服务业务管理者的主要职责是关注使用云服务时的财务和法律方面,包括批准,持续的所有权和责任。
- 注 3: 云服务集成者是云服务客户的一个子角色,负责云服务与云服务客户现有 ICT 系统的集成,包括应用功能和数据的集成。

云服务提供者、云服务客户和云服务用户的关系如图 C.1 所示。

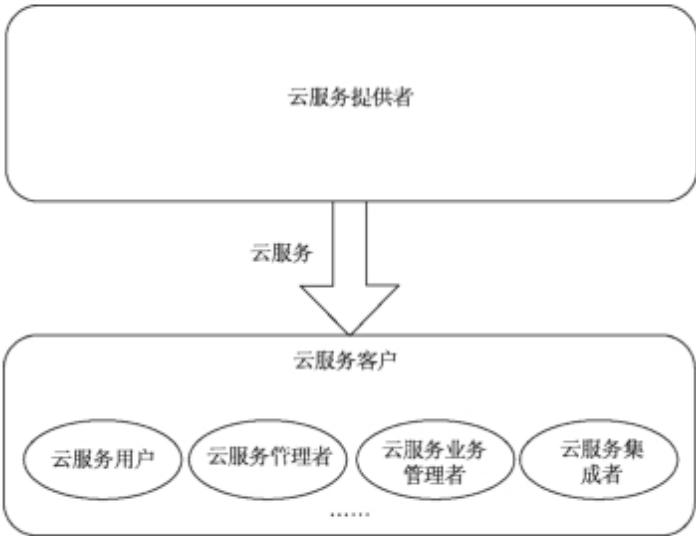


图 C.1 云服务提供者、云服务客户和云服务用户的关系图

参 考 文 献

- [1] GB/T 20985(所有部分) 信息技术 安全技术 信息安全事件管理
 - [2] GB/T 22080 信息技术 安全技术 信息安全管理系统 要求
 - [3] GB/T 31722 信息技术 安全技术 信息安全风险管理
 - [4] GB/T 32399 信息技术 云计算 参考架构
 - [5] ISO/IEC 27036-4 Information technology—Security techniques—Information security for supplier relationships—Part 4:Guidelines for security of cloud services
 - [6] ISO/IEC 27040 Information technology—Security techniques—Storage security
 - [7] ISO/IEC 29100:2011 Information technology—Security techniques—Privacy framework
 - [8] ISO/IEC 29101 Information technology—Security techniques—Privacy architecture framework
 - [9] ISO/IEC 29134 Information technology—Security techniques—Guidelines for privacy impact assessment
 - [10] ISO/IEC 29191 Information technology—Security techniques—Requirements for partially anonymous,partially unlinkable authentication
 - [11] ISO/IEC JTC1/SC27,WG5 Standing Document 2—Part 1:Privacy References List.Latest Version,available at <http://www.jtc1sc27.din.de/sbe/wg5sd2>
 - [12] BS 10012:2009 Data protection.Specification for a personal information management system
 - [13] JIS Q 15001:2006 Personal information protection management systems—Requirements
 - [14] NIST SP 800-53rev4,Security and Privacy Controls for Federal Information systems and Organizations, April 2013 (<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>)
 - [15] NIST SP 800-122,Guide to Protecting the Confidentiality of Personally Identifiable Information(PII),April2010(<http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>)
 - [16] NIST SP 800-144,Guidelines on Security and Privacy in Public Cloud Computing, December 2011(<http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf>)
 - [17] ENISA.Report on Cloud Computing: Benefits,risks and recommendations for information security, November2009 (http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport)
 - [18] European Union,Article 29 Working Party, Opinion 05/2012 on Cloud Computing,adopted July 2012;(http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion_recommendation/files/2012/wp196_en.pdf)
-

