ICS 35.040
L80

中华人民共和国国家标准

GB/T —XXXX

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

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

(ISO/IEC 27018:2019,MOD)

（征求意见稿）

（本稿完成日期：2020-06-19）

-XX-XX 发布 XXXX-XX- 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目　　次

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。

本文件使用重新起草法修改采用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的技术性差异及其原因如下：

——本文件与 ISO 27018:2019 相比在结构上有较多调整，附录 B 中列出了本文件与 ISO 27018:2019 的章条编号对照一览表。

——关于规范性引用文件，本文件做了具有技术性差异的调整，以适应我国的技术条件，调整的情况集中反应在第 2 章“规范性引用文件”中，具体调整如下：

- 用等同采用国际文件的 GB/T 22081－2016，代替了 ISO/IEC 27002:2013（见第 4 章至第 18 章）；
- 增加引用了 GB/T 35273－2020（见第 3 章、附录 C）。

——使用术语和定义“个人信息”（3.2）代替术语和定义“个人可识别信息（PII）”（见 ISO/IEC 27018：2019 3.2），以适应我国的技术条件；

——用“个人信息”代替 ISO/IEC 27018:2019 中的“个人可识别信息（PII）”，与我国的相关术语表述一致，便于标准的执行；

——使用术语和定义“个人信息控制者”（3.3）代替术语和定义“PII 控制者”（见 ISO/IEC 27018：2019 3.3），与我国的相关术语表述一致，便于标准的执行；

——使用术语和定义“个人信息主体”（3.4）代替术语和定义“PII 主体”（见 ISO/IEC 27018：2019 3.4），与我国的相关术语表述一致，便于标准的执行；

——使用术语和定义“个人信息处理者”（3.5）代替术语和定义“PII 处理者”（见 ISO/IEC 27018：2019 3.5），同时说明“个人信息处理者”在我国也称为“受委托者”（见 3.5 注），与我国的相关术语表述一致，便于标准的执行；

——使用术语“个人信息处理”（3.6）代替术语“PII 处理”（见 ISO/IEC 27018：2019 3.6），与我国的相关术语表述一致，便于标准的执行。

本文件做了下列编辑性修改：

——改正印刷错误 A.10.13 为 A.10.3（见 9.4.1 注，ISO/IEC 27018:2019 9.4.1 注）；

——改正印刷错误 A.10.13 为 A.10.3（见 11.2.7 注，ISO/IEC 27018:2019 11.2.7 注）；

——增加了资料性附录 C，提供了 GB/T 35273－2020《信息安全技术 个人信息安全规范》中的个人信息安全基本原则与本文件遵循的隐私原则的对比分析，阐明了彼此的对应关系。

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、同程艺龙控股有限公司、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（安徽省信息安全测评中心）。

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、张轩铭、王利强、王爱义、杨帆、石磊、黄磊、王理东、王法中、许立前、范正翔、于秀彦、刘堪伪。

引　言

0.1　背景和环境

在云服务场景下，云服务商通常需要依据与客户签订的合同，以双方均遵守个人可识别信息（在本文件中用“个人信息”代替）保护相关法律法规的方式提供服务。云服务商与客户之间的责任和责任划分方式会因法律管辖区或合同条款有所不同。有关如何处理(即收集、使用、转让和删除)个人信息的法律有时被称为数据保护法；个人信息有时也被称为个人可识别信息或个人数据。个人信息处理者履行的义务因法律管辖区而异，这使得提供云计算服务的企业在跨国运营中面临挑战。

当公有云服务商按照云服务客户的指示处理个人信息时，公有云服务商充当 “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可以是一个自然人(即在云中处理自身个人信息的“个人信息主体”)，也可以是一个组织(即处理多个“个人信息主体”信息的“个人信息控制者”)。云服务客户可以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的合同中约定的可用服务。在这种场景下，需要注意的是，云服务客户拥有处理和使用数据的权限。个人信息控制者和个人信息处理者的区别在于，公有云个人信息处理者除了执行云服务客户要求的个人信息处理操作和为实现云服务客户目的而进行的必要操作外，不能有其他数据处理操作。

注：公有云个人信息处理者在处理云服务客户的账户数据时，可以充当个人信息控制者。本文件不包括此类活动。

本文件旨在创建一组通用的安全类别和控制，与GB/T 22081中的信息安全目标和控制结合使用，由充当个人信息处理者的公有云服务商来实施。本文件有以下目标：

——帮助公有云服务商在充当个人信息处理者时履行适用的义务，无论直接的义务还是合同约定的由个人信息处理者承担的义务；

——使得公有云个人信息处理者在相关事务上透明，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；

——为云服务客户行使审计权力和履行符合性义务提供一种机制，以避免单个云服务客户在技术上无法对托管在多方虚拟化服务器（云）环境中的数据进行审计，以及可能增加的物理和逻辑网络安全控制方面的风险。

本文件可以为公有云服务商，特别是那些跨国运营的公有云服务商，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

本文件可供组织在基于GB/T 22080的云计算信息安全管理系统实施过程中选择个人信息保护控制时参考，也可作为公有云个人信息处理者实施普遍接受的个人信息保护控制的指导性文件。特别是，本文件以GB/T 22081为基础，并考虑了作为个人信息处理者的公有云服务商的个人信息保护要求所产生的特定风险环境。

通常来说，实施GB/T 22080的组织是出于保护自身信息资产的目的。但是，当公有云服务商作为个人信息处理者来保护个人信息时，组织其实是在保护客户委托给它的信息资产。公有云个人信息处理者实施GB/T 22081中的控制，既适合于该目的，也是必要的。本文件增强了GB/T 22081中的控制，以适应

风险的分布式特性，以及云服务客户与公有云个人信息处理者之间存在的合同关系。本文件以两种方式增强了GB/T 22081：

——为GB/T 22081中的某些控制提供了适用于公有云个人信息保护的实施指南；
——附录 A 提供了一组额外控制和相关指南，用于 GB/T 22081 中的控制集未解决的公有云个人信息保护要求。

本文件中的大多数控制和指南也适用于个人信息控制者。需要注意的是，在大多数情况下，个人信息控制者还需履行本文件未说明的额外义务。

0.3 个人信息保护要求

组织必须确定其对个人信息的保护要求。这些要求有三个主要来源，如下所述：

a) 法律、法规、监管和合同要求：组织及其贸易伙伴、承包商和服务商必须满足法律、法规、监管和合同的要求及义务，以及它们的社会文化责任和运营环境。需要指出的是，个人信息处理者作出的法律、法规和合同承诺可能强制选择特定的控制措施，也可能需要特定的文件来实施这些控制。这些要求可能因司法管辖区而异。
b) 风险：评估组织中的个人信息面临的风险时，要考虑组织的整体业务战略和目标。通过风险评估，可以识别威胁、评估脆弱性和发生的可能性、估计潜在影响。ISO/IEC 27005 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) 公司政策：尽管公司政策已经涵盖了法律和社会文化要求的诸多义务，但组织也可自愿选择超越 a）要求的文件。

0.4 云计算环境下控制的选择和实施

可以从本文件中选择云计算环境下的控制(包括参考GB/T 22081中的控制创建的针对特定行业或应用的组合参考控制集)。如果需要，还可以从其他控制集中选择控制，或者设计新的控制以满足特定要求。

注：公有云个人信息处理者提供的个人信息处理服务可以被视为一种云计算应用，而不是其自身的一个部门。然而，本文件中仍然使用术语“特定行业”，是因为该术语是ISO/IEC 27000系列文件中的常规术语。

控制的选择取决于组织的决策，这些决策是基于风险接受文件、风险处理选项、以及适用于组织与其有合同关系的客户和供应商约定的一般风险管理方法作出的，并且还受到国家和国际相关法律法规的约束。 如果未选择本文件中的控制，则需要记录在册并说明未选择的理由。

此外，控制的选择和实施取决于公有云提供商在整个云计算参考架构中的实际角色（见ISO/IEC 17789）。许多不同的组织可以在云计算环境中提供基础设施服务和应用服务。在某些情况下，所选择的控制对于云计算参考架构的特定服务类别来说可能是唯一的。在其他情况下，它们在实施安全控制时可以共享角色。合同协议需要明确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。

本文件中的控制可视为指导原则，适用于大多数组织。下文将给出详细解释，并提供实施指南。如果在公有云个人信息处理者的信息系统、服务和操作的设计中考虑了保护个人信息的要求，那么实施控制将会更简单。这种考虑通常被称为“隐私设计”(参见参考文献[9])。

0.5 制定额外指南

本文件可视为制定个人信息保护指南的起点。本实践指南中的控制和实现指南并不一定都是适用的。此外，可能还需要本文件未包含的额外控制和实现指南。当开发包含额外指南或控制的文档时，本文件包含的交叉引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

个人信息具有从创建和生成到存储、处理、使用、传输，直至最终销毁的自然生命周期。个人信息在生命周期的各个阶段可能面临不同的风险，但保护个人信息在生命周期的各个阶段都很重要。

个人信息保护需考虑现有的和新的信息系统，并进行全生命周期管理。

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

1　范围

本文件根据 ISO/IEC 29100 中的隐私原则，为在公有云计算环境中实施个人信息保护建立了普遍接受的控制目标、控制和指南。

特别是，基于 GB/T 22081 并考虑了公有云服务商所处信息安全风险环境的监管要求，本文件给出了个人信息保护指南。

本文件适用于所有类型和规模的组织，包括公共和私营公司、政府机构和非营利组织。组织作为个人信息处理者，按照合同约定通过云计算向其他组织提供信息处理服务。

本文件中的实现指南也与个人信息控制者有关。但是，个人信息控制者可能还要遵守额外的个人信息保护法律法规和义务，而这些法律法规和义务不适用于个人信息处理者。本文件无意涵盖此类额外义务。

注：本文件中使用“个人信息”代替“个人可识别信息（PII）”。

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　信息安全管理系统　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。

ISO 和 IEC 在以下地址维护用于标准化的术语数据库：

——ISO 在线浏览平台：http://www.iso.org/obp

——IEC 电子百科：http://www.electropedia.org/

3.1

数据泄露　data breach

由于安全防护不足导致受保护数据在传输、存储或处理过程中被意外或非法的破坏、丢失、篡改、

未经授权披露或访问。

[来源：ISO/IEC 27040:2015，3.7]

3.2

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：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、通信通讯联系方式、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。

[来源：GB/T 35273－2020，3.1，做了修改：删除注 2 和注 3]。

3.3

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]。

3.4

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]。

3.5

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：个人信息处理者在我国也称为受委托者，受委托者见GB/T 35273－2020 9.1。

3.6

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、咨询、披露、匿名化、假名化、传播或以其他方式提供、删除或销毁。

3.7

公有云服务商 public cloud service provider

根据公有云模型提供云服务的一方。

4 概述

4.1 文件结构

本文件的结构与 GB/T 22081 类似。GB/T 22081 中规定的目标和控制适用于本文件，且无需补充其他额外信息时，本文件仅给出了对 GB/T 22081 的引用。附录 A 给出了适用于云计算服务商的个人信息保护的额外控制和相关实现指南。

“公有云个人信息保护实现指南”标题下给出了适用于云计算服务商个人信息保护的额外指南。“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，这些特定行业指南和信息包含在 GB/T 22081 定义的类别中。与 GB/T 22081 中条款号

对应的本文件条款号见表 1。

本文件应与 GB/T 22080 结合使用。附录 A 中给出的额外控制应作为基于 GB/T 22080 的信息安全管理体系实施过程的一部分被考虑采用。

表1　为实施 GB/T 22081 中的控制而提供的特定行业指南和其他信息的位置

章节号	标题	备注
5	信息安全策略	提供了特定行业的实现指南和其他信息。
6	信息安全组织	提供了特定行业的实现指南。
7	人力资源安全	提供了特定行业的实现指南和其他信息。
8	资产管理	没有提供额外的特定行业实现指南或其他信息。
9	访问控制	提供了特定行业的实现指南，同时交叉引用了附录 A 中的控制。
10	密码	提供了特定行业的实现指南。
11	物理和环境安全	提供了特定行业的实现指南，同时交叉引用了附录 A 中的控制。
12	运行安全	提供了特定行业的实现指南。
13	通信安全	提供了特定行业的实现指南，同时交叉引用了附录 A 中的控制。
14	系统获取、开发和维护	没有提供额外的特定行业实现指南或其他信息。
15	供应商关系	没有提供额外的特定行业实现指南或其他信息。
16	信息安全事件管理	提供了特定行业的实现指南。
17	业务连续性管理的信息安全方面	没有提供额外的特定行业实现指南或其他信息。
18	符合性	提供了特定行业的实现指南，同时交叉引用了附录 A 中的控制。

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，可被用于实现该控制目标。

控制的描述结构如下：

控制

为满足控制目标，给出了定义特定控制的陈述。

公有云个人信息保护实现指南

为支持该控制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或不足以在所有情况下适用，也不一定满足组织的特定控制要求。因此，替代的或额外的控制，或其他形式的风险处理（规避、转移或接受风险）可能是适当的。

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 5.1中给出的目标适用。

5.1.1　信息安全策略

GB/T 22081 5.1.1中给出的控制、相关实现指南和其他信息适用。以下特定行业指南也适用。

公有云个人信息保护实现指南

宜通过一项声明增强信息安全策略，该声明支持并承诺遵守适用的个人信息保护法规及公有云个人信息处理者与客户（云服务客户）达成的合同条款。

合同协议宜在考虑云服务类型（例如IaaS模式、PaaS模式或SaaS模式）的前提下，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。例如应用层控制责任划分取决于公有云个人信息处理者是提供SaaS服务，还是提供可供云服务客户搭建自身应用的PaaS服务或IaaS服务。

公有云个人信息保护其他信息

在某些司法管辖区，公有云个人信息处理者直接受个人信息保护法规的约束。在其他司法管辖区，个人信息保护立法仅适用于个人信息控制者。

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机制，确保公有云个人信息处理者有义务支持和管理符合性要求。合同可以要求云服务客户接受符合性要求的独立审计。例如通过实施本文件和GB/T 22081中的相关控制。

5.1.2 信息安全策略的评审

GB/T 22081 5.1.2中给出的控制和相关实现指南适用。

6 信息安全组织

6.1 内部组织

GB/T 22081－2016 6.1中给出的目标适用。

6.1.1 信息安全的角色和责任

GB/T 22081 6.1.1 中的控制、相关实现指南和其他信息适用。以下特定行业指南也适用。

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点，供云服务客户根据合同处理个人信息时使用。

6.1.2 职责分离

GB/T 22081 6.1.2 中给出的控制、相关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 6.1.3 中给出的控制、相关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 6.1.4 中给出的控制、相关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 6.1.5 中给出的控制、相关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 6.2中给出的目标和内容适用。

7 人力资源安全

7.1 任用前

GB/T 22081－2016 7.1中给出的目标和内容适用。

7.2 任用中

GB/T 22081－2016 7.2中给出的目标适用。

7.2.1 管理责任

GB/T 22081 7.2.1中给出的控制、相关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 7.2.2中给出的控制、相关实现指南和其他信息适用。以下特定行业指南也适用。

公有云个人信息保护实现指南

宜采取措施使相关人员了解违反隐私或安全规则及程序，尤其是违反个人信息处理安全规则及程序可能对公有云个人信息处理者造成的影响（例如法律后果、业务损失、品牌或声誉损害），对员工造成的影响（例如纪律后果），对个人信息主体造成的影响（例如身体、物质和情感后果）。

公有云个人信息保护其他信息

在某些司法管辖区，公有云个人信息处理者可能会受到法律制裁，包括直接受到当地个人信息保护机构的巨额罚款。在其他司法管辖区，使用本文件建立公有云个人信息处理者和云服务客户之间的合同，宜有助于为违反安全规则和程序的合同制裁奠定基础。

7.2.3 违规处理过程

GB/T 22081 7.2.3中给出的控制、相关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 7.3中给出的目标和内容适用。

8 资产管理

GB/T 22081－2016 第8章给出的目标和内容适用。

9 访问控制

9.1 访问控制的业务要求

GB/T 22081－2016 9.1中给出的目标和内容适用。

9.2 用户访问管理

GB/T 22081－2016 9.2中给出的目标适用。以下特定行业指南也适用于本条中所有控制的实现。

公有云个人信息保护实现指南

在云计算参考架构的服务类别的环境中，云服务客户可能负责其控制下的云服务用户的部分或全部访问管理。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下的云服务用户的

访问。例如通过提供管理权限管理或终止访问。

9.2.1 用户注册和注销

GB/T 22081 9.2.1中给出的控制、相关实现指南和其他信息适用。以下特定行业指南也适用。

公有云个人信息保护实现指南

宜制定用户注册和注销程序，处理用户访问控制受到破坏的情况。例如密码或其他用户数据受损。

注：个别司法管辖区可能会对未使用身份验证凭据的检查频率提出特定要求。在这些司法管辖区运营的组织有责任遵守这些要求。

9.2.2 用户访问供给

GB/T 22081 9.2.2中给出的控制、相关实现指南和其他信息适用。

9.2.3 特许访问权管理

GB/T 22081 9.2.3中给出的控制、相关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 9.2.4中给出的控制、相关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 9.2.5中给出的控制、相关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 9.2.6中给出的控制、相关实现指南和其他信息适用。

9.3 用户责任

GB/T 22081－2016 9.3中给出的目标适用。

9.3.1 秘密鉴别信息的使用

GB/T 22081 9.3.1中给出的控制和相关实现指南适用。

9.4 系统和应用访问控制

GB/T 22081－2016 9.4中给出的目标适用。

9.4.1 信息访问限制

GB/T 22081 9.4.1中给出的控制和相关实现指南适用。

注：有关信息访问限制的额外控制和指南见A.10.3。

9.4.2 安全登录规程

GB/T 22081 9.4.2中给出的控制、相关实现指南和其他信息适用。以下特定行业指南也适用。

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为云服务客户控制的云服务用户的任何账户提供安全登录过程。

9.4.3 口令管理系统

GB/T 22081 9.4.3中给出的控制、相关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 9.4.4中给出的控制、相关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 9.4.5中给出的控制、相关实现指南和其他信息适用。

10 密码

10.1 密码控制

GB/T 22081－2016 10.1中给出的目标适用。

10.1.1 密码控制的使用策略

GB/T 22081 10.1.1中给出的控制、相关实现指南和其他信息适用。以下特定行业指南也适用。

公有云个人信息保护实现指南

公有云个人信息处理者宜向云服务客户提供其使用加密技术保护其处理的个人信息的情况。公有云个人信息处理者还宜向云服务客户提供任何可以帮助其应用自身加密保护技术的功能信息。

注：在某些司法管辖区，可能需要使用加密技术来保护特定类型的个人信息。例如有关个人信息主体的健康数据、居民注册号、护照号和驾驶执照号。

10.1.2 密钥管理

GB/T 22081 10.1.2中给出的控制、相关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 11.1中给出的目标和内容适用。

11.2 设备

GB/T 22081－2016 11.2中给出的目标适用。

11.2.1 设备安置和保护

GB/T 22081 11.2.1中给出的控制和相关实现指南适用。

11.2.2 支持性设施

GB/T 22081 11.2.2中给出的控制、相关实现指南和其他信息适用。

11.2.3 布缆安全

GB/T 22081 11.2.3中给出的控制和相关实现指南适用。

11.2.4 设备维护

GB/T 22081 11.2.4中给出的控制和相关实现指南适用。

11.2.5 资产的移动

GB/T 22081 11.2.5中给出的控制、相关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 11.2.6中给出的控制、相关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 11.2.7中给出的控制、相关实现指南和其他信息适用。以下特定行业指南也适用。

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，对于可能包含个人信息的存储介质，宜视为包含个人信息的存储介质进行处理。

注：有关安全处置或再利用设备的额外控制和指南见A.10.3。

11.2.8 无人值守的用户设备

GB/T 22081 11.2.8中给出的控制和相关实现指南适用。

11.2.9 清理桌面和屏幕策略

GB/T 22081 11.2.9中给出的控制、相关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 12.1中给出的目标适用。

12.1.1 文件化的操作规程

GB/T 22081 12.1.1中给出的控制和相关实现指南适用。

12.1.2 变更管理

GB/T 22081 12.1.2中给出的控制、相关实现指南和其他信息适用。

12.1.3 容量管理

GB/T 22081 12.1.3中给出的控制、相关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 12.1.4中给出的控制、相关实现指南和其他信息适用。以下特定行业指南也适用。

公有云个人信息保护实现指南

个人信息用于测试目的时，宜进行风险评估。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 12.2中给出的目标和内容适用。

12.3 备份

GB/T 22081－2016 12.3中给出的目标适用。

12.3.1 信息备份

GB/T 22081 12.3.1中给出的控制、相关实现指南和其他信息适用。以下特定行业指南也适用。

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，确保数据处理操作的连续性，并提供在发生破坏性事件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（可以在信息处理系统本身内）创建或维护多个数据副本。

个人信息在这方面的特定责任可能由云服务客户承担。如果公有云个人信息处理者明确地向云服务客户提供备份和恢复服务，那么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云服务客户数据能力的明确信息。

注1：某些司法管辖区可能对备份频率作出特别规定。在这些司法管辖区内运营的组织有责任遵守这些规定。

宜制定程序保证在破坏性事件发生后的指定记录期内对数据进行恢复操作。

备份和恢复程序宜按规定的记录频率进行审查。

注2：某些司法管辖区可能对备份和恢复程序的审核频率作出特别规定。在这些司法管辖区内运营的组织有责任遵守这些规定。

本文件中对分包处理个人信息的控制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。本文件中的控制也涵盖了进行物理介质传输的情况。

公有云个人信息处理者宜制定一项政策，规定信息备份要求以及擦除备份信息中包含的个人信息的任何进一步要求（例如合同和（或）法律要求）。

12.4 日志和监视

GB/T 22081－2016 12.4中给出的目标适用。

12.4.1 事态日志

GB/T 22081 12.4.1中给出的控制、相关实现指南和其他信息适用。以下特定行业指南也适用。

公有云个人信息保护实现指南

宜建立一个流程，按照规定的周期审查事件日志，识别违规之处并提出补救措施。

可能时，事件日志宜记录个人信息是否因某个事件而更改（添加、修改或删除），以及由谁更改。多个服务商提供不同类别的服务时，可能在实施本指南时充当不同或共享的角色。

公有云个人信息处理者宜定义关于是否、何时，以及如何向云服务客户提供或使用日志信息的准则。这些流程宜提供给云服务客户。

如果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只能访问与该云服务客户相关的活动，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 12.4.2中给出的控制、相关实现指南和其他信息适用。以下特定行业指南也适用。

公有云个人信息保护特殊实现指南

为安全监控和操作诊断等目的而记录的日志信息可能包含个人信息。宜采取措施，如控制访问（见9.2.3），确保记录的信息仅用于预期目的。

宜建立一个程序，最好是自动程序，确保在规定的和记录期限内删除记录。

12.4.3 管理员和操作员日志

GB/T 22081 12.4.3中给出的控制、相关的实现指南和其他信息适用。

12.4.4 时钟同步

GB/T 22081 12.4.4中给出的控制、相关的实现指南和其他信息适用。

12.5 运行软件控制

GB/T 22081－2016 12.5 中给出的目标和内容适用。

12.6 技术方面的脆弱性管理

GB/T 22081－2016 12.6 中给出的目标和内容适用。

12.7 信息系统审计的考虑

GB/T 22081－2016 12.7中给出的目标和内容适用。

13 通信安全

13.1 网络安全管理

GB/T 22081－2016 13.1中给出的目标和内容适用。

13.2 信息传输

GB/T 22081－2016 13.2中给出的目标适用。

13.2.1 信息传输策略和规程

GB/T 22081 13.2.1中给出的控制、相关实现指南和其他信息适用。以下特定行业指南也适用。

公有云个人信息保护实现指南

使用物理介质进行个人信息传入和传出信息传输时，宜建立一个系统来记录所用物理介质的相关信息，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。可能时，宜要求云服务客户采取额外措施（例如加密），确保只能在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 13.2.2中给出的控制、相关实现指南和其他信息适用。

13.2.3 电子消息发送

GB/T 22081 13.2.3中给出的控制、相关实现指南和其他信息适用。

13.2.4 保密或不泄露协议

GB/T 22081 13.2.4中给出的控制、相关实现指南和其他信息适用。

注：有关保密或保密协议的额外控制和指南可在A.10.1中找到。

14 系统获取、开发和维护

GB/T 22081－2016 第14章中给出的目标和内容适用。

15 供应商关系

GB/T 22081－2016 第15章中给出的目标和内容适用。

注：有关供应商关系管理的更多信息可从ISO/IEC 27036-4获得。

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 16.1中给出的目标适用。以下特定行业指南也适用于本条中所有控制的实现。

公有云个人信息保护实现指南

在整个云计算参考架构的背景下，信息安全事件的管理和改进可能存在共享角色。可能需要公有云个人信息处理者与云服务客户合作实现本条中的控制。

16.1.1 责任和规程

GB/T 22081 16.1.1中给出的控制、相关实现指南和其他信息适用。以下特定行业指南也适用。

公有云个人信息保护实现指南

信息安全事件宜触发公有云个人信息处理者的审查，该活动可作为信息安全事件管理的一部分，以确定是否发生了涉及个人信息的数据泄露（见A.9）。

信息安全事态不会造成任何实际的或可能产生影响的对个人信息及其存储个人信息的公有云个人信息处理者设备设施的非授权访问。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嗅探。

16.1.2 报告信息安全事态

GB/T 22081 16.1.2中给出的控制、相关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 16.1.3中给出的控制、相关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 16.1.4中给出的控制、相关实现指南适用。

16.1.5 信息安全事件的响应

GB/T 22081 16.1.5中给出的控制、相关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 16.1.6中给出的控制、相关实现指南和其他信息适用。

16.1.7 证据的收集

GB/T 22081 16.1.7中给出的控制、相关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 第17章中给出的目标和内容适用。

18 符合性

18.1 符合法律和合同要求

GB/T 22081－2016 18.1中给出的目标和内容适用。

注：符合法律和合同要求的额外控制和相关指南见A.11。

18.2 信息安全评审

GB/T 22081－2016 18.2中给出的目标适用。

18.2.1 信息安全独立评审

GB/T 22081 18.2.1中给出的控制、相关实现指南和其他信息适用。以下特定行业指南也适用。

公有云个人信息保护实现指南

如果个别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，证明信息安全保护是按照公有云个人信息处理者的策略和流程实施和操作的。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法。只要提供足够的透明度，它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 符合安全策略和文件

GB/T 22081 18.2.2中给出的控制、相关实现指南和其他信息适用。

18.2.3 技术符合性评审

GB/T 22081 18.2.3 中给出的控制、相关实现指南和其他信息适用。

附 录 A
（规范性）
公有云个人信息处理者用于个人信息保护的扩展控制集

A.1 总则

本附录给出了新的控制和相关实现指南，并结合GB/T 22081中的增强控制和指导（见第5章至第18章）构成了扩展控制集，以满足作为个人信息处理者的公有云服务商保护个人信息的要求。

这些额外控制按照ISO/IEC 29100中的11个隐私原则进行分类。在多数情况下，控制可能归入多个隐私原则。此时，应将这些控制归入最相关的原则。

A.2 同意和选择

A.2.1 关于个人信息主体权利的合作义务

控制

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，以便于个人信息主体能够访问、纠正、删除与其有关的个人信息。

公有云个人信息保护实现指南

个人信息控制者在这方面的义务可能通过法律、法规或合同来约定，这些义务可能包括云服务客户使用个人信息处理者提供的服务。例如及时纠正或删除个人信息。

个人信息控制者在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，相关信息或技术措施宜在合同中明确。

A.3 目的合法性和规范

A.3.1 公有云个人信息处理者的目的

控制

根据合同约定处理个人信息时，不宜独立于云服务客户的指示进行任何其他用途的处理操作。

公有云个人信息保护实现指南

这些指示可以包含在公有云个人信息处理者和云服务客户的合同中。例如服务达到的目标和完成时间。

为实现云服务客户的目标，从技术角度考虑，由公有云个人信息处理者按照云服务客户的通用指令，而不是明确指令，来决定处理个人信息的方法是合理的。例如为了有效地利用网络或处理能力，有必要根据个人信息主体的某些特性来分配特定的处理资源。公有云个人信息处理者关于处理方法的决定涉及个人信息的收集和使用等活动时，公有云个人信息处理者宜遵守ISO/IEC 29100中规定的相关隐私原则。

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，便于云服务客户确认公有云个人信息处理者符合目的规范和限制原则的要求，并确认公有云个人信息处理者或者其分包商没有出于独立于公有云客户指示的其他目处理个人信息的情形。

A.3.2 公有云个人信息处理者的商业用途

控制

未经明确同意，公有云个人信息处理者不得将合作处理的个人信息用于营销和广告。此类同意不宜成为接受服务的条件。

注：此控制是对A.3.1的补充，不可替换或取代。

A.4 收集限制

没有额外控制与此隐私原则相关。

A.5 数据最小化

A.5.1 安全删除临时文件

控制

宜在规定的时间或记录周期内擦除或销毁临时文件和文档。

公有云个人信息保护实现指南

关于个人信息擦除的实现指南见A.10.3。

信息系统可以在其正常操作过程中创建临时文件。此类文件面向系统或应用，但可包括与数据库更新和其他应用程序软件操作相关的文件系统回滚日志和临时文件。相关信息处理任务完成后，不需要留存临时文件，但有些情况下可能也不会删除它们。这些文件的留存时间是不确定的，但“垃圾收集”程序宜识别相关文件并确定自上次使用以来的时间。

个人信息处理系统宜实施定期检查，删除超出规定期限的未被使用的临时文件。

A.6 使用、保存和披露限制

A.6.1 个人信息披露通知

控制

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，向云服务客户通报由执法机构提出的任何具有法律约束力的披露个人信息的请求，禁止披露的信息除外。

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保证：

——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咨询云服务客户；

——接受云服务客户授权的任何合同约定的个人信息披露请求。

示例：根据刑法，禁止披露可能是为了保护执法调查的机密性。

A.6.2 个人信息披露记录

控制

宜记录向第三方的个人信息披露，包括披露的内容，向谁披露，以及披露时间。

公有云个人信息保护实现指南

在正常的操作处理过程中，个人信息可能被披露。这些披露宜被记录（见12.4.1）。向第三方的任何其他披露，例如核发调查或外部审计产生的披露，也宜被记录。记录宜包括披露的来源和作出披露的

权利来源。

A.7 准确性和质量

没有其他控制与此隐私原则相关。

A.8 公开、透明和通知

A.8.1 分包个人信息处理控制的披露

控制

公有云个人信息处理者使用分包商处理个人信息前，宜告知相关云服务客户。

公有云个人信息保护实现指南

使用分包商处理个人信息的规定宜在公有云个人信息处理者和云服务客户的合同中公开透明。合同宜明确，只有在服务开始获得云服务客户一般同意的前提下，才可委托分包商进行处理操作。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拒绝此类变更或终止合同。

披露的信息宜包括使用分包合同的事实和相关分包商名称，可不包括特定业务的细节。披露的信息还宜包括分包商可以在哪个国家处理数据（见A.12.1）或者分包商有义务履行或超过公有云个人信息处理者义务的方式（见A.11.12）。

如果评估认为分包商信息的公开披露增加了安全风险并超出了可接受的范围，则宜根据保密协议和（或）应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可用的。

A.9 个人参与和访问

没有额外控制与此隐私原则有关。

A.10 责任

A.10.1 包含个人信息数据泄露的通告

控制

在未经授权访问个人信息或未经授权访问个人信息处理设备设施，导致个人信息丢失、泄露或更改时，公有云个人信息处理者宜立即通知相关云服务客户。

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括个人信息数据泄露通知的条款。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有关机构的告知义务。此告知义务不包括由云服务客户、个人信息主体或其负责的系统组件引起的数据泄露。合同还宜规定包含个人信息的数据泄露通知的最迟时间。

如果发生涉及个人信息的数据泄露，则记录宜包括事件描述、时间段、事件后果、报告者姓名、事件报告对象，解决事件采取的步骤（包括负责人和覆盖的数据）以及事件造成的损失，披露或变更的事实。

如果发生涉及个人信息的数据泄露，则记录还宜包括受损数据的描述（如果已知）；如果执行了通知，则记录还宜包括通知云服务客户或监管机构采取的步骤。

在某些司法管辖区，相关法律或法规可能要求公有云个人信息处理者将涉及个人信息的数据泄露，直接通知相应的监管机构（例如个人信息保护机构）。

注：可能存在其他需要通知的违规行为。例如未经许可或其他授权进行采集，未经授权使用等。

A.10.2 行政安全政策和指南的保留期

控制

在替换（包括更新）安全策略和操作程序时，宜保留副本一段时间。

公有云个人信息保护实现指南

在解决客户争议和个人信息保护机构调查时，可能需要审查当前和以往的政策、程序。在法律或合同没有明确要求的情况下，安全策略和操作程序的最短保留期为五年。

A.10.3 个人信息返回、传输和处置

控制

公有云个人信息处理者宜制定适用于云服务客户个人信息返回、传输和处置的政策。

公有云个人信息保护实现指南

在某个时间，可能需要以某种方式处理个人信息。这可能涉及将个人信息返回给云服务客户；将个人信息转移至另一个公有云个人信息处理者或个人信息控制者；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宜提供必要的信息，以允许云服务客户确保根据合同处理的个人信息（由公有云个人信息处理者及其任何分包商）从存储的任何位置删除，包括备份和业务连续性的目的，只要它们不再是云服务客户的特定目的所必需的。宜以合同形式提供处置机制（脱链、覆盖、消磁、销毁或其他形式的擦除）和（或）使用的商业文件的性质。

公有云个人信息处理者宜制订并实施有关个人信息处置的策略，并宜将此策略提供给云服务客户。

政策宜涵盖合同终止后个人信息销毁前的保留期，避免云服务客户因合同意外失效而丢失个人信息。

注：该控制和指南与“使用、保留和公开限制”原则的保留要素相关（见A.6）。

A.11 信息安全

A.11.1 机密或保密协议

控制

在公有云个人信息处理者控制下访问个人信息的自然人宜遵守保密协议。

公有云个人信息保护实现指南

公有云个人信息处理者及其员工、代理之间任何形式的保密协议，都宜确保员工和代理不会披露与云服务客户的指示无关的个人信息（见A.3.1）。保密义务宜履行至相关合同终止。

A.11.2 创建硬拷贝材料的限制

控制

宜限制显示个人信息的硬拷贝材料的创建。

公有云个人信息保护实现指南

硬拷贝材料包括打印的材料。

A.11.3 数据恢复的控制和记录

控制

宜有数据恢复的程序和日志。

公有云个人信息保护实现指南

注：上述控制使适用于某些法律管辖区的以下要求成为通用要求。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。

A.11.4 存储介质离开场所的数据保护

控制

存储介质上的个人信息离开组织场所宜遵守授权程序，除授权人员外，任何其他人员不得访问（例如加密相关数据）。

A.11.5 未加密便携式存储介质和设备的使用

控制

除非不可避免，不宜使用便携式物理介质和不支持加密的便携式设备，并且宜记录此类便携式介质和设备的使用情况。

A.11.6 公用数据传输网络传输个人信息的加密

控制

通过公共数据传输网络传输的个人信息宜在传输之前进行加密。

公有云个人信息保护实现指南

在某些情况下，为了有效传输，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业务数据。例如电子邮件的交换。

如果多个云服务商提供不同服务类别（来自云计算参考框架）的服务，那么实施本指南时可能充当不同角色或共享角色。

A.11.7 硬拷贝材料的安全处置

控制

销毁硬拷贝材料时，宜使用横切、粉碎、焚烧、碎片化等将其彻底销毁。

A.11.8 用户ID的独立用法

控制

如果多人访问存储的个人信息，则每个人都宜具有不同的用户ID，以便进行识别、身份验证和授权。

A.11.9 授权用户的记录

控制

宜保留已授权访问信息系统的用户或用户配置文件的最新记录。

公有云个人信息保护实现指南

公有云个人信息处理者宜维护所有授权访问用户资料。用户资料由用户的数据集组成，包括用户ID，用于实现提供对信息系统的授权访问的技术控制。

A.11.10 用户ID 管理

控制

不宜将停用或过期的用户ID授权给其他人。

公有云个人信息保护实现指南

在云计算参考框架下，云服务客户可能部分负责或全部负责其控制下的云服务用户ID的管理工作。

A.11.11 合同措施

控制

云服务客户与公有云个人信息控制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和个人信息保护义务可能直接源自适用的法律。否则，合同宜约定与公有云个人信息处理者相关的个人信息保护义务。

本文件中的控制与GB/T 22081中的控制旨在提供一种控制措施参考目录，以帮助签订关于个人信息处理的合同。签订合同签订，公有云个人信息处理者宜将保护个人信息的服务材料告知云服务客户。

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，云服务客户最终有责任确保公有云个人信息处理者实施的措施符合其义务。

A.11.12 分包的个人信息处理

控制

公有云个人信息处理者与处理个人信息的任何分包商之间的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和个人信息保护义务。代理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

使用分包商存储副本的情况包含在本控制中（见A.8.1）。

A.11.13 预使用数据存储空间数据的访问

控制

公有云个人信息处理者宜确保无论何时将数据存储空间分配给云服务客户，以前驻留在该存储空间上的任何数据都不会被该云服务客户看到。

公有云个人信息保护实现指南

云服务用户删除信息系统中保存的数据时，出于保持系统性能的考虑，显式删除数据是不切实际的。这种风险宜通过具体的技术措施予以避免。

实施该控制的过程中，没有适合处理所有情况的具体指南。但是，可举个例子，如果某云服务用户尝试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无。

A.12 隐私符合性

A.12.1 个人信息的地理位置

控制

公有云个人信息处理者宜指定并记录可能存储个人信息的国家/地区。

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，还宜包括使用分包处理个人信息产生的国家身份。如果存在适用于数据国际转让的特定合同，如示范合同条款、约束性公司规则、跨境隐私规则，则宜识别这些合同及适用这些合同的国家及情况。公有云个人信息处理者宜将这方面的任何可能变更及时通知云服务客户，以便云服务客户能够拒绝此类变更或终止合同。

A.12.2 个人信息的预定目的地

控制

宜提供有效手段确保通过网络传输的个人信息到达预定目的地。

附 录 B
（资料性）
本文件与 ISO/IEC 27018:2019 相比的结构变化情况

表B.1 本文件与 ISO/IEC 27018:2019 的章条编号对照情况

本文件章条编号	对应的ISO/IEC 27018:2019章条编号
0.1	0.1
0.2	0.2
0.3	0.3
0.4	0.4
0.5	0.5
0.6	0.6
3.1	3.1
3.2	—
3.3	—
3.4	—
3.5	—
3.6	—
—	3.2
—	3.3
—	3.4
—	3.5
-	3.6
3.7	3.7
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

表 B.1　本文件与 ISO/IEC 27018:2019 的章条编号对照情况（续）

本文件章条编号	对应的ISO/IEC 27018:2019章条编号
附录A	附录A
附录B	—
附录C	—

附 录 C
（资料性）
本文件与 GB/T 35273－35273 个人信息保护原则的对照情况

本文件根据ISO/IEC 29100 中提出的隐私原则，建立了云计算环境下普遍接受的控制目标、控制和指南，以保护个人信息安全。ISO/IEC 29100中的隐私原则源自一些政府、国家和国际组织制定的现有原则，是信息通信技术（ICT）系统保护隐私的通用原则，用于指导信息技术系统隐私政策和隐私控制的设计、开发和实施。个人信息处理者、个人信息控制者作为ICT系统中的重要角色亦遵守该原则。这些隐私原则包括：

——同意和选择。除非在个人信息主体不能拒绝或适用法律明确允许未经自然人同意可处理个人信息的情况，都应向个人信息主体给出是否允许处理其个人信息的选择。

——目的合法性和规范。处理个人信息的目的应遵守适用法律的规定。

——收集限制。收集的个人信息应限制在实现个人信息控制者指定（合法）的目的所必需的范围内。

——数据最小化。严格限制处理个人信息的行为。

——使用、保留和披露限制。将个人信息的使用、保留和披露（包括转让）限制在实现指定、合法的目的所必要的范围内。

——准确性和质量。保证个人信息准确、完整、可靠。

——公开、透明和通知。向个人信息主体告知处理个人信息的程序、目的，以及发生的重大变化。

——个人参与和访问。赋予个人信息主体访问和审查其个人信息的能力，允许修改、删除其个人信息。

——责任。处理个人信息应承担保护个人信息的责任。

——信息安全。在授权范围内保护个人信息，确保个人信息的完整性、机密性和可用性，以及在整个生命周期内免受未经授权访问、破坏、使用、修改、披露或损失之类的风险。

——隐私符合性。建立适当的内部控制和独立监督机制，确保个人信息处理活动符合数据保护和隐私安全要求。

GB/T 35273主要针对个人信息面临的安全问题，规范个人信息控制者在收集、存储、使用、共享、转让、公开披露等信息处理环节中的相关行为，同时要求个人信息控制者开展个人信息处理活动应遵循合法、正当、必要的原则，具体包括：

——权责一致。采取技术和其他必要的措施保障个人信息的安全，对其个人信息处理活动对个人信息主体合法权益造成的损害承担责任。

——目的明确。具有明确、清晰、具体的个人信息处理目的。

——选择同意。向个人信息主体明示个人信息处理目的、方式、范围等规则，征求其授权同意。

——最小必要。只处理满足个人信息主体授权同意的目的所需的最少个人信息类型和数量。目的达成后，应及时删除个人信息。

——公开透明。以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则等，并接受外部监督。

——确保安全。具备与所面临的安全风险相匹配的安全能力，并采取足够的管理措施和技术手段，保护个人信息的保密性、完整性、可用性。

——主体参与。向个人信息主体提供能够查询、更正、删除其个人信息，以及撤回授权同意、注销账户、投诉等方法。

由此可见，本文件遵循的隐私原则与GB/T 35273－2020规定的个人信息安全基本原则相协调，只是表述形式有差异。表C.1给出了本文件遵循的隐私原则与GB/T 35273－2020规定的个人信息安全基本原则的一种映射关系，但映射关系可能会因不同应用场景会有所不同。

表C.1　本文件与 GB/T 35273－2020 个人信息保护原则对照情况

本文件的隐私保护原则	对应的GB/T 35273－2020的个人信息安全基本原则
同意和选择	4 c)选择同意
目的合法性和规范	4 b)目的明确
收集限制	4 d)最小必要
数据最小化	4 d)最小必要
使用、保留和披露限制	4 d)最小必要
准确性和质量	4 a)权责一致
公开、透明和通知	4 e)公开透明
个人参与和访问	4 g)主体参与
责任	4 a)权责一致
信息安全	4 f)确保安全
隐私符合性	4 f)确保安全

参 考 文 献

[1] GB/T 22080 信息技术 安全技术 信息安全管理系统 要求

[2] GB/T 31722 信息技术 安全技术 信息安全风险管理

[3] GB/T 32399 信息技术 云计算 参考架构

[4] ISO/IEC 27035 Information technology—Security techniques—Information security incident management

[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] NISA.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)