ICS 03.080.01
CCS A 12

中华人民共和国国家标准

GB/T XXXXX—XXXX/ISO 31700-1

产品和服务设计中的消费者隐私保护 第1部分：高阶要求

Consumer protection — Privacy by design for consumer goods and services —

Part 1: High-level requirements

（ISO 31700-1，IDT）

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－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。

本文件等同采用ISO 31700-1:2023《产品和服务设计中的消费者隐私保护 第1部分：高阶要求》。

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。

本文件由全国服务标准化技术委员会（SAC/TC 264）提出并归口。

本文件起草单位：中国标准化研究院等。

本文件主要起草人：暂略。

引 言

消费者信任和个人隐私需求满足是数字经济关注的焦点，主要涉及组织及数字商品（服务）如何处理消费者的个人身份信息和其他数据。如果个人身份信息由于疏忽、丧失时效性或隐私惯例遭受损害，对个人可能产生严重影响。此外，消费者对数字产品的信任受到损害时，对企业可能产生潜在的法律或声誉影响。

隐私设计是在产品设计和开发过程中考虑到保护消费者隐私的方法，涉及整个产品生命周期（从产品投放市场之前，到消费者购买和使用，再到产品最终停止使用的时间）。这意味着产品具有默认的面向消费者的隐私控制和设置，可提供适当的隐私级别，不会给消费者带来不必要的负担。

“隐私设计”最初由加拿大安大略省信息和隐私专员使用。目的是减少个人在使用消费品时争取隐私保护的负担。

设计隐私可通过以下三个指导原则来描述：

（1）授权和透明度

对隐私声明、隐私尽职调查方法以及处理个人身份信息软件系统的设计和操作的透明度和问责制要求不断增长。其目的是促进企业更注重隐私设计、赢得消费者信任并满足消费者隐私保护需求，展示法律和监管合规性。隐私设计通过分析消费者的观点、背景、需求以及与消费者沟通处理隐私问题的方法，创新隐私设计方案。

（2）制度化与责任

在整个生态系统中建立健全隐私规范时，隐私设计侧重于消费者的观点。隐私设计考虑了消费者对产品消费行为以及消费者在产品生命周期中的隐私需求。有关消费者隐私需求的决策将更加一致和系统化，并与其他利益相关者的利益构成一项功能需求。

隐私设计注重问责制、责任感和领导力等因素，其对于隐私设计及规范化至关重要。领导者应在产品设计过程中为实现隐私设计的规范化做出承诺。

（3）生态系统和生命周期

隐私设计的方法可应用于更广泛的信息生态系统。该方法应有助于隐私和消费者保护，同时应进一步考虑背景因素，如消费者类型及其使用产品的意图。

隐私设计适用于所有使用个人身份信息的产品，无论是实物商品，还是服务（如软件服务），旨在适应不同国家和部门的各种需求。

在产品生命周期的任何阶段，包括在开发阶段或消费者使用后，都可能发现额外的隐私问题和相关控制需求。隐私设计方法应支持产品的更新换代，在初始设计阶段之后设计和部署补充隐私增强功能。

（4）本文件受众群体

本文件的主要受众群体是负责消费品和服务的设计、制造、运维、测试和处置的组织人员和第三方。

产品和服务设计中的消费者隐私保护 第1部分：高阶要求

1 范围

本文件规范了产品和服务设计中的消费者隐私保护的通则、消费者沟通要求、风险管理要求、开发、部署和操作设计的隐私控制要求和个人身份信息生命周期结束要求等。

本文件适用于产品和服务设计中的消费者隐私保护高阶管理。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

消费者 consumer

出于私人目的而购买或使用资金、产品的个人。

注1：“消费者”(包含老人、儿童和残疾人)包括消费者和潜在消费者。消费品可一次性购买，也可长期合同约定购买。

注2：本术语仅适用于自然人，不适用于法人实体。

注3：消费者购买或使用的资金、产品或服务(3.4)，不仅用于私人目的（如自备设备），也可用于专业。

[来源：GB/T 36000—2015，3.19]

[来源：ISO/IEC 指南 14:2018，3.2，有修改]

3.2

个人身份信息 personal identified information

个人信息 personal information

个人信息可用于该信息与涉及相关信息的自然人之间建立联系，也可与自然人直接或间接建立联系。

注1：为确定个人身份信息主体是否可识别，应考虑持有数据的隐私利益相关者或其他方为建立个人身份信息集与自然人之间联系所使用的方法。

注2：公共云**个人身份信息处理者**(3.20）通常无法明确知晓其处理的信息所属类别，除非云服务客户将其透明化。

[来源：ISO/IEC 19944-1:2020，3.3.1，有修改]

3.3

隐私泄露 privacy breach

在违反一项或多项相关隐私保护**要求**(3.9）的情况下处理**个人身份信息**(3.2）。

[来源：ISO/IEC 29100:2011，2.13]

3.4

服务 service

为满足消费者（3.1）的利益或需求而提供的一项或多项活动。

注1：服务通常是无形的。

注2：服务是指在与消费者互动过程中了解其需求，并在服务交付时提供相应的活动。这些服务可能涉及到银行、会计或公共组织（如学校或医院）等机构的持续交互关系。

注3：提供服务可能涉及以下方面：

——对消费者提供有形产品进行的活动；

——对消费者提供无形产品进行的活动；

——无形产品的交付。

注4：服务通常由消费者享有。

[来源：GB/T 24620—2022，3.11]

3.5

隐私设计 privacy by design

在涉及**个人身份信息**(3.2)的产品或**服务**(3.4)的初始设计阶段和整个生命周期中应考虑隐私的设计方法，包括考虑产品**报废**(3.15）和**删除**(3.26）任何相关的个人身份信息。

注：生命周期还包括更新改造期间。

3.6

消费者可配置的隐私设置 consumer-configurable privacy setting

消费者隐私设置 consumer privacy setting

消费者隐私控制 consumer privacy control

个人身份信息(3.2）负责人出于特定目的处理个人身份信息作出的具体选择。

[来源：ISO/IEC 29100:2011，2.17，有修改]

3.7

处理个人身份信息 processing of personally identifiable information

对**个人身份信息**(3.2）进行的一系列操作。

注：个人身份信息处理包括但不限于收集、存储、更改、检索、咨询、披露、匿名化、假名化、传播或以其他方式提供、删除或销毁个人身份信息。

[来源：ISO/IEC 29100:2011，2.23]

3.8

要求 requirement

以明确的方式翻译或表达需求及其相关**约束**(3.9）和**条件**(3.10）的陈述。

注1：要求存在于系统结构的不同层次。

注2：要求总是与系统、软件、**服务**(3.4）等相关。

[来源：ISO/IEC/IEEE 29148:2018，3.1.19，有修改]

3.9

约束 constraint

为确保符合特定的标准或要求，对系统的各个方面和过程进行外部监管和控制。

注：约束是强制或强迫加在解决方案上的因素，会限制或修改设计。

[来源：ISO/IEC/IEEE 29148:2018，3.1.7]

3.10

条件 condition

需要满足可测量的定性或定量属性的特定要求，这些**属性**(3.11)表明要求适用的特定情况或事件。

[来源：ISO/IEC/IEEE 29148: 2018，3.1.6]

3.11

属性 attribute

一个实体的固有性质或特征，可通过一定方法从定性或定量上加以区分。

注：ISO 9000区分两种类型的属性：固有存在于某物中的永久特性；以及产品、过程或系统的指定特征(如产品的价格、产品的所有者）。指定的特性不是该产品、过程或系统的固有质量特性。

[来源：ISO/IEC 25000:2014，4.1，有修改]

3.12

第三方 third party

独立于组织之外的个人或机构。

注1：所有商业伙伴都是第三方，但并非所有第三方都是商业伙伴。

注2：第三方可以是**个人身份信息控制者**(3.19）或**个人身份信息处理者**(3.20），或两者兼而有之。

3.13

消费品 consumer product

主要但不限于为个人或家庭使用而设计和生产的商品或服务，包括其组件、零件、附件、使用说明以及包装。

[来源：ISO 10377:2013，2.2，有修改]

3.14

个人身份信息生命周期 personally identifiable information lifecycle

从**个人身份信息**(3.2）的创建、收集、存储、使用和转移到最终处置的整个期间。

[来源：ISO/IEC 29151:2017，4.6，修改]

3.15

报废 retirement

运维机构决定撤回对现有系统的主动支持，并计划将部分或全部系统替换为新系统，或者安装升级后的系统。

注1：从其运行环境中移除系统或组件。

注2：从组织角度定义的使用结束或产品生命周期结束，即组织停止营销、销售或提供产品的零件、**服务**（3.4）或软件更新。

[来源：ISO/IEC/IEEE 15288:2015，4.1.39，有修改]

3.16

隐私控制 privacy control

降低**隐私风险**(3.18）发生的可能性或产生后果的控制措施。

注：隐私控制包括组织层面、物理层面和技术层面的措施，如政策、程序、指南、法律合同、管理实践等。

[来源：ISO/IEC 29100:2011，有修改]

3.17

信息安全 information security

保持信息的机密性、完整性和可用性。

注：信息安全还可能涉及其他属性如真实性、可问责性和可靠性。

[来源：ISO/IEC 27000:2018，3.28]

3.18

隐私风险 privacy risk

不确定性对隐私的影响。

注1：不确定性是指与某个事件、事件结果或发生可能性相关的，信息不完全、理解不透彻或知识不全面的状态。

注2：隐私风险可能是**个人身份信息**(3.2）的滥用或**消费者**(3.1）因个人身份信息处理不当造成的。

[来源：ISO/IEC 29100:2011，2.19，有修改]

3.19

个人身份信息控制者 personally identifiable information controller

能够决定处理个人身份信息目的和方式的隐私利益相关者，而不是将数据用于个人目的的自然人。

[来源：ISO/IEC 29100:2011，2.10，有修改]

3.20

个人身份信息处理者 personally identifiable information processor

代表并按照**个人身份信息控制者**(3.19）的指示处理**个人身份信息**(3.2）的隐私利益相关方。

[来源：ISO/IEC 29100:2011，2.12]

3.21

以人为本的设计 human-centred design

系统设计和开发的方法，注重人类对系统的使用，运用人为因素、人体工程学和可用性等方面的知识和技术，以提高交互式系统的可用性。

注1：术语“以人为本的设计”而非“以消费者为中心的设计”用于强调设计影响许多利益相关者，而不仅仅是那些通常被认为是**消费者**(3.1）的利益相关者。但在实践中它们通常是同义词。

注2：可用系统可以提供许多好处，包括提高生产率、增强消费者福祉、避免压力、增加可访问性和降低危害风险。

[来源：ISO/IEC 25063:2014，3.6，有修改]

3.22

应用案例 use case

描述**消费者**(3.1）和消费品之间的交互关系，用于帮助识别、理清和满足**要求**(3.8），以支持特定的业务目标。

[来源：ISO/TR 14872:2019，3.9，有修改]

3.23

消费者脆弱性 consumer vulnerability

由于个人和市场环境因素的影响，个人在与产品提供方的交易中可能会处于不利地位或面临遭受损害的风险。

注1：任何人都可能随时受到攻击。脆弱性可以是暂时的，也可以是永久的。

注2：导致消费者脆弱性的因素可以是个人因素(如疾病、伤害、残疾等）或环境因素(如失业、丧亲等）。

注3：组织的流程和程序可以减少或加剧消费者的脆弱性。

注4：自身利益容易受损害的消费者有以下几种：

——在与服务提供者交易时面临更高的负面影响风险；

——提升自身利益的能力有限；

——难以获得或收集信息；

——购买、选择或获得适合服务的能力较差；

——更容易受到某些营销手段的影响。

注5：市场环境因素包括但不限于：人口因素、生态因素、经济因素、社会文化因素、政治和法律因素、国际环境、技术因素。

[来源：ISO/IEC指南76:2020，3.14，有修改]

3.24

责任人 accountable person

委派人员完成指定任务并承担责任的人。

[来源：ISO 24134:2006，3.9，有修改]

3.25

责任方 responsible party

完成委托任务或指定交付物的人员。

注1：责任方可以是个人，也可以是组织或项目的代表，也可以是发布任务的一方。

注2：责任方通常指派或拥有负责监督产品隐私设计项目的责任人。

注3：责任方通常指派或拥有一名责任人，其职责是对产品设计的隐私参数的行动、决策和性能负责。

3.26

删除 deletion

改变**个人身份信息**(3.2），使其不再存在、可识别或可用，并且只能通过耗费更多努力才能重建。

注1：“删除”包括以下内容：处理机制、擦除、销毁、数据存储介质的销毁。

注2：“删除”是指消除位模式或类似的做法，而不是简单地标记或移动要隐藏的数据。因此，考虑到所有可能合理使用的手段，例如现有的技术水平、人力和技术资源、成本和时间，重建个人身份信息十分困难。

注3：选择删除方法应考虑基于风险的方法，包括个人身份信息的敏感性和可能使用的取证工具。所需措施可能随着时间的推移而改变，这取决于技术水平和其他因素。

注4：个人身份信息也可通过应用不可逆的去识别技术来改变。此类数据通常不受隐私立法的约束。

注5：去识别技术见 ISO/IEC 20889。

3.27

隐私风险评估 privacy risk assessment

在组织更广泛的风险管理框架内确定、分析、评估、咨询、沟通和规划处理个人身份信息(3.2）的过程。

注：该过程可以通过各种方式形成文件，包括隐私影响评估。

[来源：ISO/IEC 29100:2011，2.20，有修改]

3.28

文件化信息 documented information

文件 document

人工制品 artefact

一个组织及其所包含的媒介需要控制和维护的信息。

注1：文件化信息可以是任何形式、任何媒介、任何来源。

注2：文件化信息可指：

——管理体系，包括相关过程；

——为组织运作而创造的信息(文件）；

——取得成果的证据(记录）。

[来源：ISO/IEC 27000:2018，3.19]

3.29

信息安全管理 information security management

管理信息的保密性、完整性和可用性。

[来源：ISO/IEC TR 27016:2014，3.12]

3.30

弱势消费者 vulnerable consumer

由于年龄、文化水平(包括技术知识）、身体状况的限制，或无法获取产品安全信息，亦或由于精神、情感、社会或身体原因，可能永久或暂时无法代表自己的利益，从而限制自身意愿和知情决定能力的**消费者**(3.1）。

[来源：ISO 10377:2013，2.30，有修改]

3.31

变更管理 change management

对产品或服务进行改变或提议改变的手段。

[来源：ISO/IEC/IEEE 24765:2017]

3.32

个人身份信息负责人 personally identifiable information principal

与个人身份信息相关的自然人。

[来源：ISO/IEC 29100:2011，有修改]

3.33

使用结束 end of use

消费者不再需要和使用产品。

注：终止使用的原因包括但不限于：产品损坏、无法正常运行、无法满足消费者需求、消费者死亡或丧失行为能力、产品已被回收或销毁或消费者通过二手市场将其转移给其他消费者。

3.34

网络安全 cybersecurity

保护IT系统不受硬件、软件或信息的攻击或损坏，也不受其提供服务的中断或误导。

[来源：ISO/TR 22100- 4:18 8，3.10，有修改]

3.35

风险 risk

不确定性对目标的影响。

[来源：ISO/IEC指南73:2009，1.1，有修改]

4 通则

4.1 概述

4.1.1 为实现在消费品设计中保护消费者隐私的目的，服务供应商应满足一些要求。在定义消费品隐私要求时，消费者的隐私权和偏好发挥着重要的信息作用。

4.1.2 个人身份信息存在生命周期，即从创建开始，经过收集、存储、使用和转移到最终处置（安全销毁）结束。个人身份信息的价值和对消费者的相关风险在生命周期各个阶段可能不同，但保护消费者隐私是同等重要的。

4.1.3 信息系统也存在生命周期，即从构思开始，经过设计、开发、测试到实现、使用和维护，并于最终退出服务和处置，此过程的每个阶段均可考虑个人身份信息的保护。同时结合考虑当前和预计的隐私、信息安全风险及可能发生的实际事件，新系统的开发和对现有系统的更改为组织提供了更新、改进安全和隐私控制的机会。

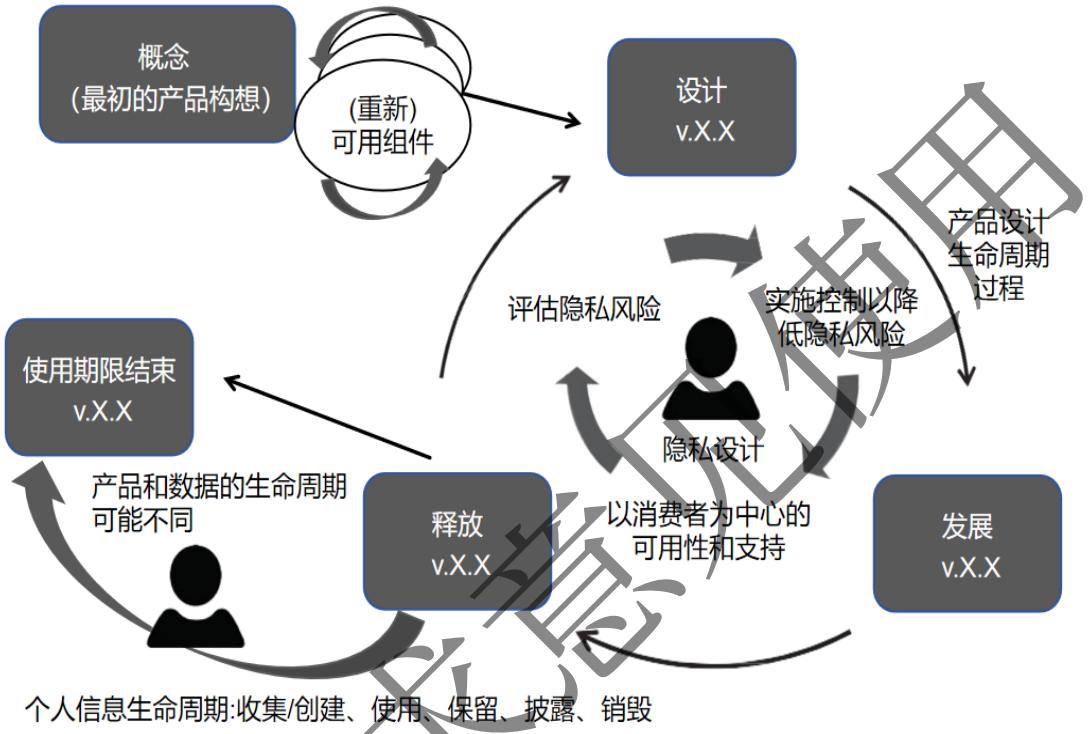

图1 个人身份信息和产品生命周期

4.2 设计消费者行使隐私权的功能

4.2.1 要求

应设计可使消费者执行其隐私权和特权的功能。

注1：方式包括但不限于对产品特征、产品设计的处理以及产品的有效性。

注2：前提是符合消费品销售地的有关法规和要求。

4.2.2 说明

4.2.2.1 关于消费者个人身份信息处理的诸多决策不仅取决于身份信息控制者，其相关决定也受到法律法规、合同、经济因素以及技术控制的约束。

4.2.2.2 消费者购买和使用产品的行为使身份信息控制者有保护隐私权的义务。身份信息控制者应了解消费者在其履行义务时所起到的作用，否则可能会浪费大量资源且无法履行其义务。

4.2.2.3 由于消费者隐私需求对身份信息控制者持续提供符合要求的产品的能力存在影响，因此将其纳入组织审查相关方的过程非常重要。消费者授权包括扮演参与性角色的能力，以及在产品处理个人身份信息生命周期中行使有效隐私权的能力。

4.2.3 指南

4.2.3.1 组织应遵循隐私信息管理体系。ISO/IEC 27701 和 NIST 隐私框架为其提供了更多解释。

4.2.3.2 组织应识别与消费者隐私权有关的产品影响因素，包括法律要求、文化规范、合同、经济和可用技术等，并在执行时邀请专家参与。

4.2.3.3 组织应确定其是否属于某一法定角色（个人身份信息控制者或处理者），因为此类角色可能对消费者施加特定的法律义务。

4.2.3.4 组织应实施供应链隐私最佳措施，以允许消费者行使其权利和特权。

4.2.3.5 对个人身份信息的访问应仅授予有数据业务需求（由隐私政策确定）的授权员工。

4.2.3.6 在通过设计框架和保护机制确定产品特性和隐私时，组织应考虑可用性和整体消费者体验。

4.2.3.7 组织应提供一份简短且完整的隐私声明，以清晰简单的术语说明消费者如何行使其隐私权，见 ISO/IEC 29184。

4.2.3.8 设计消费品时应仅获取、收集、使用、披露、转移或存储产品所需的最少信息以满足所确定的组织目的。

4.2.3.9 在新产品或修改后的产品中配置消费者隐私设置时，应审查公司承诺（隐私政策或公开声明）并进行更新，以确保没有违反公司对消费者的承诺以及适用的法律和监管要求。

4.2.3.10 当消费者提出请求时，组织应能定位所有相关的个人身份信息，并以可扩展、及时和安全的方式执行必要的操作（如硬删除、导出、限制、纠正）。

4.2.3.11 在符合适用法律或合同要求的情况下，产品报废后，组织应仅处理法律、法规或合同要求的最少个人身份信息。

4.3 开发确定消费者隐私偏好的功能

4.3.1 要求

在设计和开发产品时，组织应确定与个人身份信息有关的消费者需求。

4.3.2 说明

4.3.2.1 个人身份信息的处理使产品能够正常使用，并使组织能够在产品生命周期中为消费者提供支持。只有组织对消费者隐私偏好有清晰认识时，才能设计出既能保护消费者隐私又能使组织履行其义务的产品。此外，当曾经被认作机器数据或遥测数据的 IP 地址、MAC 地址和其他类型信息可以合理地链接到消费者的设备时，此类信息被许多司法管辖区视作个人身份信息。

4.3.2.2 消费者对现有和新兴的“网络”（通信网络、社交网络、个人网络等）、信息通信技术和其他数字产品之间的关联性有不同的了解。计算技术的进步对消费者隐私的保护存在一定影响，例如一组似乎无法识别消费者的信息，当与其他信息集相联系时，可能允许识别消费者并泄露其个人信息，或者可能通过添加虚假信息扭曲消费者的个人信息。

4.3.2.3 消费者具有脆弱性，这将影响他们与产品和隐私控制进行交互的方式。除非组织非常了解其消费者，否则无法确定隐私控制的设置是否会按照原设计的方式运行。

4.3.3 指南

4.3.3.1 在定义消费品隐私要求时，消费者隐私偏好和需求应发挥重要的信息作用。

4.3.3.2 为确保产品的隐私控制按设计运行，消费者的观点和偏好应作为产品设计过程的一部分，从而为消费者提供有益的用户体验。

4.3.3.3 组织应了解消费者如何进行隐私控制，以便产品的隐私控制在消费者采取或不采取行动的情况下仍能保持稳健。

4.3.3.4 组织应将其现有和未来的消费者视为产品生命周期中的关键资源，并通过一种正规的方式接触这些消费者，例如从反馈机制的简单分析到由专业研究人员部署严格的研究方法，从而进行最彻底的用户研究。

4.3.3.5 如果产品具有可由消费者操作的隐私控制，消费者应被告知如何进行具体的操作，以防止在有意或无意中发生错误。这些错误包括但不限于以下内容：

——违背消费者意愿的数据处理；

——消费者不知情地点击错误的选项；

——消费者不了解启用或禁用特定设置或控制对处理个人信息的影响或含义；

——消费者位置被产品默认跟踪等。

4.3.3.6 组织应清楚地了解消费者的隐私偏好，否则很难设计出既能保护消费者隐私又能使组织履行其义务的产品以同时满足这些偏好。

4.4 为隐私设计人机界面

4.4.1 要求

组织应考虑消费者的能力及其潜在缺陷，设计可由消费者配置的隐私设置和管理措施。

4.4.2 说明

4.4.2.1 使用以人为本的设计和开发方法，不仅有利于消费者，而且对组织有实质性的经济价值。高可用性的系统、服务和商品往往在技术和商业上都更成功。

4.4.2.2 授权消费者管理个人数据、隐私控制和偏好是防止滥用和误用个人身份信息的关键。消费者了解产品如何处理个人身份信息并进行控制是透明度和信任的基础。

4.4.2.3 如果消费者对产品进行隐私控制，则需要在用例中对其进行定义和记录，并在产品的设计中考虑消费者体验、人为因素以及与产品功能相关的各种潜在消费者能力、体验和残疾等因素。

4.4.2.4 用例描述了消费者对产品的使用情况，并对消费者的隐私风险进行分析。定义中心用例允许产品设计人员探索其他用例以及滥用或误用的用例。用例可用于识别由消费者交互、已知技术和消费者漏洞引起的消费者隐私需求。

4.4.3 指南

4.4.3.1 在消费者可配置隐私设置的设计中，消费者的控制和选择应清晰明了。

4.4.3.2 设计消费者可配置隐私设置时应采用隐私工程技术。

4.4.3.3 产品设计可传达个人身份信息处理的语境。产品开发团队应避免妨碍透明度、利用模糊性以及在使用个人身份信息时创造负面消费者体验的设计实践，即需要在所有产品开发阶段（包括消费者体验和系统设计）仔细考虑隐私控制，以确保消费者不会无意中共享个人身份信息，并防止因其管理方式不当而泄露个人身份信息的情况发生。

4.5 分配相关角色和权限

4.5.1 要求

组织应指派并维护特定的角色与职责，至少需要一名员工负责管理个人身份信息以及产品生命周期，并在整个生命周期中保持对隐私风险的控制。

4.5.2 说明

产品和个人身份信息生命周期中的角色和权限应为风险管理提供信息，并设置与产品相关的隐私控制问责制。

4.5.3 指南

4.5.3.1 责任人的职责应涵盖对隐私状况的控制。该角色可以在产品及其处理个人身份信息的生命周期中发挥作用，以确保所有产品隐私控制的效力。负责人员可包括但不限于：事件反馈协调员、生产经理和消费者沟通人员。

4.5.3.2 应明确界定责任和职责，提供充足的资源并定期审查其有效性。

4.6 建立多功能职责

4.6.1 要求

组织应指定一名负责人参与隐私控制的设计和管理，并负责对产品个人身份信息的处理。

4.6.2 说明

4.6.2.1 负责人对产品隐私控制的整体有效性负责，但设计和操作通常需要来自多个职能部门的协助。有时团队是由多个职能部门合并而成，这些团队由来自不同职能领域的专家组成，他们为实现组织目标而协同工作。

4.6.2.2 保护隐私是设计过程中不可或缺的一部分，需要集合多领域的专业知识。为实现这一目标，集成设计团队要求工程师与其他非技术领域的专家进行合作，例如法律和消费者研究领域，这有助于在通常关注安全性的技术专家之间嵌入强有力的隐私规范。

4.6.2.3 隐私风险不仅来自与网络安全相关的事件，还来自授权的个人身份信息处理过程，开发团队可同时邀请安全隐私专家参与消费品隐私保护的设计过程。

4.6.2.4 隐私安全和信息安全是密切相关的整体。隐私原则包括信息安全和个人身份信息的合理保障要求。健全的道德规范、原则、实践和组织政策可以提供指导性决策。治理机制可以支持、维护和发展这些规范、原则和实践。信息安全旨在保护个人和企业的活动和资产，使其免受保密性、完整性和可用性的损失。

4.6.3 指南

4.6.3.1 每个职能部门和组织中为隐私控制的设计或操作贡献专业知识的高级职位应被指定为这些贡献的代表并承担责任。

4.6.3.2 为确保隐私的重要性可恰当地与其他优先事项一起纳入，职务应足够高级。

4.7 培养隐私知识、技能和能力

4.7.1 要求

应为负责设计和操作隐私控制的人员提供必要的培训，以确保团队具备有效履行其职责的知识、技能和能力。

4.7.2 说明

通过设计、了解隐私并将其应用于产品和服务的能力是隐私工作人员（包括责任人和相关方）的重要技能。

4.7.3 指南

4.7.3.1 组织应根据培训目标，设计针对责任方的隐私培训方案。

4.7.3.2 组织应实时监控培训效果，确保其长期有效性，并及时审查和更新培训内容，使其保持最新状态。

4.7.3.3 培训应涵盖个人身份信息生命周期的各个方面。

示例：例如个人身份信息的范围、所处理数据的类型和分类；实际应用场景；员工设备上的数据；共享数据的工具；公司提供工具（如电子邮件）的数据政策；以及在后续出现问题时如何联系隐私团队。

4.7.3.4 负责数据处理工作的员工应接受隐私意识的教育和培训，以履行符合组织政策、流程、程序和隐私价值观的相关职责。

4.7.3.5 为确保组织操作流程符合其对消费者的义务，相关员工也应接受培训并具备足够的能力。

示例：如保障消费者能够行使隐私权或偏好。

4.7.3.6 为确保工作的高效性，参与产品设计和执行的员工应认识到他们的隐私责任，并对提供专业知识的员工进行培训。

4.7.3.7 与第三方的合同和服务水平协议中，应包含培养隐私知识、技能和能力的内容，包括涉及个人身份信息转移的第三方。

4.7.3.8 培训应分享最佳实践，并将其扩展到第三方贡献者，包括涉及个人身份信息转移的第三方。

4.8 确保了解隐私控制

4.8.1 要求

为负责设计和操作隐私控制的人员提供必要的培训，以确保团队充分了解产品的隐私要求和组织的隐私政策和程序。

4.8.2 说明

4.8.2.1 若组织想让参与产品及其数据生命周期设计和开发的员工更好地掌握隐私知识，组织自身首先需要具备隐私专业知识。这些专业知识可来自组织内部，也可从外部获取。在项目开始之前和进行过程中，产品隐私控制和组织隐私政策的知识传播是必不可少的，这样员工才能将专业知识与他们的核心技能相结合，在产品开发过程中确定实现隐私控制的最佳方法，并确保其与组织的隐私目标保持一致。同时，组织还应为员工提供适当的资源，以确保他们在整个产品开发阶段、进行阶段以及个人身份信息生命周期中能够按需解决问题。

4.8.2.2 根据以下要求，负责人可以了解并确保其团队具备足够的技能和知识来进行相应的控制。

4.8.2.3 合规和管理控制，包括隐私意识和培训、隐私影响评估、治理和隐私计划、处理活动记录、同意文本、数据处理协议、具有约束力的公司规则、第三方控制或协议。

4.8.2.4 技术控制。包括物理设备控制，生存时间（一种限制计算机或网络数据有效期的机制），个人身份信息加密（传输和暂停），去标识化和匿名化，访问控制，其他隐私增强技术。

4.8.2.5 隐私增强服务，包括但不限于许可工具包或框架，个人身份信息删除、导出以及加密服务，去标识化或匿名化工具、最新个人身份信息库存、消费者个人身份信息定位器。

4.8.2.6 负责人需要得到各种隐私专家的支持，以完成以下任务：

——基于法律、政策、规定和隐私风险评估的合规控制建议；

——建议并标准化在实施控制过程中的技术控制、工具和其他支持，识别平台的隐私差距并领导平台控制；

——维护整个组织的隐私计划和项目；

——确保跟踪技术控制并确定其优先级，以便在整个组织内取得进展并实施，例如整个组织内数据的保留，数据清单项目，数据导出或删除项目。

4.8.3 指南

4.8.3.1 为确保以结构化、透明的方式将良好实践纳入产品，每个提供专业知识的责任方均应接受隐私培训。

4.8.3.2 为确保良好的隐私实践以结构化的方式纳入产品，提供专业知识的各责任方应具备适当的隐私专业知识并理解流程。

4.8.3.3 与产品相关的法律法规义务以及组织选用的自愿隐私政策应构成产品隐私控制目标的来源，并指导设计和开发人员隐私设计控制。

4.9 文件化信息管理

4.9.1 要求

为验证隐私控制的设计和运行的有效性，组织应建立并管理文件信息。

4.9.2 说明

4.9.2.1 如果产品隐私控制的设计和操作将嵌入至产品生命周期中，那么设计阶段的文件将捕获关键信息以供组织员工和第三方使用。文件化的信息通常采用活动文件的形式，并随使用隐私控制的详细信息、测试信息以及生命周期后期的操作而更新。

4.9.2.2 组织应维护文件化信息（如政策、程序、应遵循的说明），并存储记录以便跟踪所执行的活动。这将有助于员工开展活动，因为员工需要了解政策、程序和指示，并审查以前的任务或类似活动的记录。消费品隐私设计的文件化信息包括以下内容：

——隐私风险评估；

——个人身份信息/数据流或地图；

——产品和服务的功能性和非功能性隐私要求；

——在产品和服务中实施的隐私控制；

——测试结果、验收决定和交付授权；

——与消费者就隐私问题进行沟通。

4.9.3 指南

4.9.3.1 应管理经相关部门批准的文件化信息，并供所有预期接收者阅读和使用。

注：有关使用隐私信息管理系统或信息安全管理系统所形成文件化信息的更多资料，请参见ISO/IEC 27701、ISO/IEC 27001和ISO/IEC 27002。

4.9.3.2 应控制文件化信息以确保其在需要的时间和地点可用并适合使用，并得到充分的保护（如防止丢失机密性、不当使用或丧失完整性）。

4.9.3.3 为控制文件化信息，组织应进行下列活动：

——分发、获取、检索和使用；

——存储和保存，包括保持可读性；

——变更控制（如版本控制）；

——保留和处置。

4.9.3.4 组织应适当识别并控制策划和运行隐私控制所需的外部文件化信息。

5 消费者沟通要求

5.1 概述

5.1.1 接触过隐私信息产品的消费者希望在身份信息收集时或做出影响隐私的决策时获得信息，这些信息应包含产品关于个人身份信息处理和隐私管理的具体方法、解释和承诺。目的是促进消费者在购买或使用之前做出正确的决策。此外，消费者还希望知晓处理个人身份信息方式中因意外或错误使用个人隐私面临风险的时间和个人身份信息处理目的发生变化的时间。

5.1.2 个人身份信息的透明度和消费者沟通支持问责制度，可使消费者和其他人能够将个人身份信息的实际处理细节与制度中的解释和承诺进行比较，从而在必要时采取行动（即提出投诉或停止使用产品）并向负责人提出质疑。消费者沟通采用多种形式，从消费者界面、帮助文件和产品文件，到包装、销售内容和消费者服务手册，再到常见问题解答、通知和政策。

5.1.3 负责人应对消费者负责，创建以隐私为中心的产品信息文件。

5.2 提供隐私信息

5.2.1 要求

5.2.1.1 组织应告知用户关于产品的消费者可配置隐私设置。

5.2.1.2 为便于根据隐私要求配置产品，组织应维护并向其他用户提供有关产品隐私设置或功能的信息。

5.2.2 说明

5.2.2.1 当产品发布给消费者后，组织改变其控制的能力就会受到限制。除非测试产品控制操作的预发布过程是可靠的，否则可能会发布无法适当管理其隐私风险的产品。

5.2.2.2 为便于消费者在使用或购买处理个人身份信息的产品时做出正确决定，消费者应了解产品处理个人身份信息的过程。通常可采用产品隐私设置、功能手册、隐私声明、产品文件的形式，说明处理个人身份信息的过程、合同和服务协议、发送支持与投诉的方式；还可采用用户界面标签、包装和营销声明的形式。

注：ISO/IEC 29184提供有关在线隐私声明内容的更多信息。

5.2.2.3 在产品支持期间，应使消费者了解隐私风险的变化有助于他们有效地管理风险。如果这种沟通设计未达预期效果，消费者可能会发现该产品使他们面临重大的剩余隐私风险。

5.2.2.4 支持可包括对软件或硬件的技术修复，这些修复可改变产品在开发期间内置的隐私控制。

5.2.2.5 消费者通常需要通过支持来了解如何安装、设置、操作产品以及如何处理可能遇到的问题或投诉。

5.2.2.6 消费者通常需要通过支持，了解安装、设置和操作产品的方式，以及他们是否存在问题或投诉。消费者产品通常涉及由不同提供者提供的服务，为便于消费者后续联系负责人，应明确告知消费者提供者的信息，确保消费者知晓获得支持的方式，其保护隐私的支持活动有助于维持消费者对第三方的信任和信心。

5.2.3 指南

5.2.3.1 以隐私为重点的通知和文件的来源信息应包括：

——对产品隐私设置或功能的简要、连贯概述，包括从默认隐私保护设置重新配置的结果；

——解释产品处理个人身份信息的隐私声明和产品文件的方式，包括已处理的个人身份信息、处理个人身份信息的目的、与谁共享数据；

——合同和服务协议；

——请求支持或发送投诉的说明以及消费者行使可用隐私权的方式；

——启用的控件作为产品设计的一部分，可保护个人身份信息和消费者免受不公平和未经授权的个

人身份信息访问和使用；

——机器学习透明度，例如在模型中，明确哪个版本的模型正在使用、模型使用目的、模型创建者目的；在数据集中，应明确个人身份信息如何被收集、是否被清理、以及偏差是否检查；在可追溯性方面，查找在算法决策期间使用了哪个模型（包括版本）以及哪些数据集和个人身份信息；

——负责决定处理个人身份信息，以及为事件和隐私泄露管理通知响应的实体。

5.2.3.2 当收集数据并传递给第三方用于商业目的时，应确定商业模式。

5.2.3.3 不仅在沟通策略应考虑残疾人使用的产品所收集数据的敏感性和消费者需求的多样性（如听觉、视觉或触觉），而且在制定隐私披露、通知和产品其他控制时也应考虑这些因素。

5.2.3.4 组织应指定适当的岗位维护此类文件。

5.2.3.5 联系信息应包括组织的名称、地址和联系方式，以及消费者可收到回复的信息的时间。

5.2.3.6 如果消费者死亡，组织应计划、设计并操作控制消费者的数字遗产，并将这些信息传达给相关消费者。

5.2.3.7 组织应确保沟通概述他们对用户数字遗产的隐私控制进行计划、设计和操作的方式，并指导消费者实施这些控制的方法。

5.2.3.8 团队应确定一个预退出期，在此期间将产品的退出计划通知消费者。

5.2.3.9 产品使用寿命终止时的消费者信息应包括以下内容：

——实体产品的最佳保质期；

——消费者选择是否继续使用该产品；

——替代消费品；

——产品寿命终止情况给消费者带来意外困难时，消费者的反馈机制；

——组织将继续保留/处理个人身份信息的事实；

——产品寿命结束后保留/处理个人身份信息的目的；

——个人身份信息的类型；

——保留期（或用于确定保留期的标准）。

5.3 提供隐私信息的责任

5.3.1 要求

为便于消费者了解其个人身份信息在整个个人身份信息生命周期中的处理情况，负责人应确保向消费者的责任方提供隐私通知或文件。

5.3.2 说明

提供隐私信息的责任可确保处理个人身份信息的产品在设计时经过充分考虑，并确保此类产品的消费者能够访问有关个人身份信息在此类产品中被处理的信息。在某些情况下，面向消费者的负责人与负责设计产品的负责人是相同的。

5.3.3 指南

5.3.3.1 提供隐私的通知或文件应在产品销售或许可之前提供给消费者，贯穿产品和个人身份信息生命周期。

5.3.3.2 多功能团队应通知消费者、销售人员和支持人员，由于停止销售、支持或组织处理产品数据而可能需要采取的隐私保护措施。

注：ISO/IEC 29184提供了更多关于良好实践的解释，鼓励参考该文件提供通知。

5.4 回应消费者询问和投诉

5.4.1 要求

为有效回应消费者对其个人身份信息处理的询问或投诉，责任方应向消费者提供相应的资源和升级手段。

5.4.2 说明

当出现问题并需要解释时，责任人有义务为消费者一方提供支持。

5.4.3 指南

此类资源应包括：

——消费者和技术支持活动说明的培训和文件（包括在支持操作期间维护隐私）；

——与产品内的隐私控制相关的技术问题和消费者使用问题的常见问题解答；

——在投诉无法直接解决的情况下，可供消费者使用的独立替代机制；

——关于消费者寻求帮助的地点与方式。

5.5 与不同消费者群体进行沟通

5.5.1 要求

组织可以通过产品设计市场中的各种渠道与消费者进行沟通，以确保消费者能够充分了解产品的特点、隐私设置以及个人身份信息处理方式。这样的沟通方式应该是不受限的，以帮助消费者更好地理解产品的各个方面。

5.5.2 说明

5.5.2.1 确保消费者能够理解文件内容，并知晓能够满足自身需求的支持方式和活动。

5.5.2.2 作为隐私设计的一部分，设计产品的组织应安排保障机制，确保购买或使用产品的消费者可通过该机制与转售商或制造组织就隐私问题或投诉进行沟通，直至产品报废、寿命终止或支持终止。

5.5.3 指南

5.5.3.1 隐私设置和隐私管理措施应考虑目标消费者的特征，包括目标群体中的弱势消费者，尤其应考虑未成年人、老年人和信息技术素养较低的人。

5.5.3.2 组织应通过合同或内部服务协议确保面向消费者的负责人为产品消费者提供提问、投诉、寻求支持或解决其隐私权的手段。

5.5.3.3 应编写清晰易懂的文件，并使消费者易于获取，应考虑弱势消费者以及推广该产品或服务所在国家的语言。文件内容可以包括隐私设置和控制、个人身份信息处理及个人身份信息保护措施。

5.5.3.4 应通过多种沟通渠道与消费者进行沟通。

5.5.3.5 为确保这些渠道是否为产品消费者提供可接受的消费者体验，应对渠道的有效性进行监控、审查和修订。

5.6 数据泄露沟通

5.6.1 要求

为便于在隐私泄露后与利益相关者进行沟通，组织应创建、测试并维护能够与利益相关者进行沟通的安排。

5.6.2 说明

数据被泄露的情况下，与消费者进行沟通，对于确保受影响的消费者有权管理剩余隐私风险十分重要。此外，监管机构还可能为组织设置报告数据泄露的最后期限。

注：请参阅ISO/IEC27035-1、ISO/IEC27035-2。

5.6.3 指南

5.6.3.1 组织应考虑包括：

——通信中包含哪些内容（如原因、数据泄露类型、消费者可以采取的行动、组织采取的行动、获得进一步信息的联系方式）；

——使用的沟通渠道与个人沟通方式；

——组织未获取联系方式情况下的处理；

——由谁及何时发出通知；

——以何种语言编制通知书；

——由谁来结束通信；

5.6.3.2 此沟通应提前准备，并作为隐私泄露管理准备工作的一部分。

6 风险管理要求

6.1 引言

6.1.1 风险管理方法能够帮助处理个人身份信息与其他运营风险。隐私设计能够积极有效地管理和降低隐私风险，防止隐私泄露。在这种情况下，风险管理的目的是管理消费者所面临的隐私风险问题。

6.1.2 有关生态系统的信息可能会导致隐私风险。组织应建立验收标准，根据该标准评估风险并确定隐私风险的重要性，从而为后续的风险处理做出决策提供帮助。此外，组织还可以与个人身份信息负责人和其他利益相关者针对标准进行沟通，在直接沟通不可行的情况下可采用反馈机制。

6.1.3 与消费产品相关的隐私风险可将隐私事件考虑为个人可能会遇到的潜在问题,这些问题由系统、产品或服务对数据的操作产生，无论是数字形式还是非数字形式，从数据收集到处置，都贯穿了整个生命周期。

6.1.4 对于评估期间应考虑的隐私风险来源，组织可参考内部来源和外部来源。

6.1.5 任何与消费品相关的个人身份信息的使用，无论消费者是否直接使用该产品，都可通过设计纳入隐私。

6.1.6 出现在全球范围内的文件和标准中的隐私风险管理指南和资源，可由各种数据保护机构授权。

6.2 进行隐私风险评估

6.2.1 要求

组织应采取结构化的隐私风险评估方法,证明隐私风险在个人身份信息的整个生命周期隐私控制的设计和操作中充分考虑了隐私风险。

6.2.2 说明

6.2.2.1 隐私风险评估有助于识别产品产生的隐私风险，对其进行优先排序并确定适当的风险管理方法，可处理各种风险。根据既定的风险标准，采取相应的风险处理措施或接受风险，但由于权力或资源

的限制，一些已识别的风险可能需要上报或委托给负责人之外的其他人进行决策。这个过程可以通过各种方式进行记录，包括进行隐私影响评估。

6.2.2.2 为进行隐私风险评估，可以投入多种资源。其中包括深入了解产品的运行生态系统、建立评估风险的标准、选择适当的评估方法，以及更具体的资源投入，如数据图表、产品用例以及与产品相关的隐私要求。

6.2.2.3 文件化信息为已知的隐私风险评估提供了背景、过程和边界的基础，并支持后续的风险管理。文件化信息包括功能性和非功能性隐私要求的明确文件。与组织隐私相关文件（如隐私政策、隐私培训材料、隐私咨询人员文件）可构成更大组织范围的隐私信息管理方法。

6.2.3 指南

6.2.3.1 为衡量个人身份信息处理的好处与风险，隐私风险评估应进行风险等级排序，并确定适当的响应措施。

6.2.3.2 组织应在生产或发布消费品之前进行隐私风险评估。

6.2.3.3 应制作数据图和加工活动记录，可有效说明个人身份信息处理的背景和流程，包括特定建议流程的潜在结果，例如通过公共标识符意外连接日志数据，或在共享存储容器中意外混合数。数据图和加工活动记录也可采用不同的方式说明，包含基于组织需求的不同级别的详细信息。数据地图可以包括操作环境、组件的所有者或运营商、跨个人身份信息生命周期的特定处理类型，以及跨消费产品生命周期处理的个人身份信息的特定元素。

6.2.3.4 最初应从各种来源获得与产品相关的隐私需求，包括法律环境(如法律、法规、合同）、组织政策、文化价值观、相关标准和隐私原则。信息越敏感或个人权利的风险越高，组织在设计和实施中越有义务采取保护数据的措施。这些要求根据隐私风险评估的结果进行更新或扩展。

6.2.3.5 组织应评估使用第三方引入的隐私风险，包括在产品生命周期中转移个人身份信息的第三方。

6.2.3.6 应考虑产品和整个产品生态系统中的个人身份信息的退出隐私风险。

6.2.3.7 组织应评估在产品退出后和消费者使用结束后保留与产品相关的个人身份信息的风险。

6.2.3.8 新技术纳入产品时，其潜在隐私风险也应作为隐私风险评估的输入。

6.2.3.9 消费者隐私需求可以作为隐私风险评估的有用输入。组织应评估消费者对隐私的期望，并在合理范围内满足消费者的需求。

6.3 评估第三方的隐私能力

6.3.1 要求

在尽职调查中，组织应该考虑评估设计或操作隐私控制的第三方的隐私风险管理能力。

6.3.2 说明

6.3.2.1 消费品对个人身份信息的获取较为复杂，尤其在涉及多个利益相关者时。每个组件可在多个生命周期内运行，例如，“虚拟助理”包括在内部运行的产品或系统（家庭设备），以及在外部运行的系统（组织服务器）。除了消费产品的物理实体生命周期之外，还可以涉及其他生命周期，如个人身份信息生命周期、组织服务器生命周期、系统开发生命周期等，每个生命周期都可能会涉及质量检查和认证等多功能协作活动。因此，涉及复杂利益相关者网络和需求的消费品的运营，需要识别、调整和协调生态系统中利益相关者的角色和责任。

6.3.2.2 在第三方为支持产品生命周期而处理个人身份信息的情况下，可在建立个人身份信息生命周期和相关隐私控制时考虑其处理。这表明，由于第三方在产品生命周期开始之前或结束之后处理个人身份信息（包括个人身份信息转移的对象），个人身份信息生命周期被延长。

6.3.3 指南

6.3.3.1 第三方的隐私能力应通过适当的尽职调查、风险评估和协议进行评估，其中协议规定了其义务、责任和绩效审查，包括审计和审查。

6.3.3.2 第三方和收购方在此过程中的作用至关重要。第三方和收购方特定的隐私风险和隐私控制，可能会对产品带来的隐私风险产生重大影响。因此，第三方应提供信息使组织能够应对这些风险，这种信息共享应构成与第三方(包括个人身份信息接收方）签订的合同或服务水平协议的一部分。

6.3.3.3 组织应实施第三方治理技术机制和操作流程，以治理数据共享和隐私风险。

6.3.3.4 组织与第三方（包括个人身份信息转移给的第三方）的关系应基于合同或其他措施。

6.3.3.5 组织应在与第三方签订的合同中加入条款，在消费者对个人信息行使任何权利或产品报废时定义第三方义务。

6.3.3.6 应通过适当的方式定期评估第三方的绩效，并采取适当的措施。

6.3.3.7 与第三方进行评审不接受配合时，应根据需要进行补救。

6.4 制定与记录隐私控制要求

6.4.1 要求

组织应制定并记录将决定个人身份信息生命周期中隐私控制设计和操作的要求。

6.4.2 说明

6.4.2.1 隐私要求为设计或选择隐私控制提供了基础。工程活动涉及的识别隐私控制要求可以满足隐私目标和处理隐私风险，该要求更侧重于后者。

6.4.2.2 组织选择管理隐私风险的控制措施各不相同。因此，消费者通常需要访问信息，这些信息解释了管理产品中隐私的方法，以及在给定产品中有权访问隐私控制的操作方法，直至退出。

6.4.2.3 许多管理、技术、质量、安全和其他与信息相关的标准都包括隐私控制。任何相关来源的隐私控制都可以纳入产品的设计过程。

6.4.3 指南

6.4.3.1 应根据隐私风险评估结果制定要求。

6.4.3.2 隐私风险评估的结果可能会导致与产品相关的初始隐私控制集的更改。

6.4.3.3 应对范围内产品所依赖的隐私控制进行一致性审查。

6.4.3.4 风险评估的输出应按照隐私控制的最新文件要求。

6.4.3.5 在制定隐私控制要求时，还应考虑评估的消费者隐私需求和偏好。

6.4.3.6 多功能团队应识别在产品销售或支持停止后继续使用组织处理资源的消费者。

6.5 监测和更新风险评估

6.5.1 要求

产品投放市场后，为满足隐私要求，组织应监控正在使用的产品的隐私风险，并在必要时更新隐私控制的设计和操作。

6.5.2 说明

产品或组织环境的变化可能会引发新的隐私风险,作为隐私风险管理的一部分,需要更新文件信息、隐私风险评估、隐私要求和实施的控制措施。更新内容包括：

——用于隐私风险评估的输入；
——更新隐私风险和风险应对处理或接受决定；
——更新隐私控制实施，包括重新评估隐私控制的适用性以及开发新隐私控制的可能性。当将设计过程应用于产品生命周期的报废阶段时，可将产品通过二手市场出售，或者直接报废。

6.5.3 指南

6.5.3.1 组织应在设计阶段对产品的使用进行设计，并评估当产品出现故障时它是否继续满足隐私要求。

6.5.3.2 在产品生命周期中，对文件信息、隐私风险评估、隐私要求和隐私控制操作的更新应该是迭代的。

6.5.3.3 组织应确保产品所有发布的内容，确保以防止隐私控制失效的方式管理隐私风险。

6.5.3.4 组织应评估新出现的隐私风险，包括消费者的反馈和投诉。监控可直接涉及产品的变更和相关的个人身份信息处理，也可以是产品的外部监控，例如组织目标或法律法规环境。发布后的产品更新可能需要与消费者进行新的沟通。

6.5.3.5 组织应确保对产品功能或其他设置的更改不会损失隐私控制操作的有效性，也不会增加额外的隐私风险，且无需考虑其他或新的补偿控制或控制改进。

6.6 将隐私风险纳入网络安全弹性设计

6.6.1 要求

组织应在其信息安全政策和程序中考虑个人身份信息的风险。

注：考虑因素包括中断对隐私控制弹性的影响。

6.6.2 说明

6.6.2.1 组织适应性是组织在不断变化的环境中吸收和适应的能力。组织的运营和产品供应链可能会受到日常干扰。如果要持续运行控制，则需要做好防止、检测和恢复造成个人身份信息中断的准备。

6.6.2.2 可组合性是处理组件相互关系的系统设计原则。将系统嵌入到产品中并将产品用作更大系统的组件时，隐私受到保护的可能性低。因此，在网络安全弹性规划的背景下隐私设计时，了解系统内的隐私风险以及其他系统的组件至关重要。

6.6.3 指南

关于组织适应性的指导可参见ISO 22316[48]。

7 开发、部署和操作设计的隐私控制

7.1 引言

7.1.1 隐私控制应贯穿于产品的整个生命周期，包括设计、开发、部署、管理和操作，以确保这些控制能够在产品中持续实现预期的隐私目标。同时，这些控制不应降低标准或以非常规的方式运行。

7.1.2 消费者隐私需求或偏好也可能在产品生命周期内设计和实施新的隐私控制需求。

7.1.3 采用协调的方法设计、开发、部署、管理、操作和改进产品的隐私控制，有助于提高隐私设计的效率、有效性和持续性。

7.1.4 若将隐私控制的开发、部署、管理和操作集成到组织的开发、部署、管理、操作和演进控制的总方法中，可提高有效性和效率。

7.1.5 隐私控制的管理可成为 ISO 20000-1 中规定的组织服务管理体系的一部分。

注：ISO 20000-1规定了组织建立、实施、保持和持续改进组织服务管理体系的要求。需求包括服务的规划、设计、转换、交付和改进，以满足服务需求并交付价值。

7.2 将隐私控制的设计和操作应用到产品开发和管理生命周期中

7.2.1 要求

组织应将消费品隐私控制的设计和操作应用到产品的开发和管理生命周期中。

7.2.2 说明

隐私控制的设计和操作是为了实现产品的预期隐私目标，以及采用相关的管理实践、流程和策略来确保达到产品隐私目标。具体的开发和管理方法以及隐私控制的工作会因产品的性质和设计使用的环境而有所不同。在设计和构建、部署及操作新的或变更的的隐私控制过程中，需要满足如下要求：

——隐私要求和控制说明；

——支持要求和控制的管理信息系统和工具；

——隐私控制技术架构；

——支持隐私控制的行政和其他管理流程；

——描述已开发的控制、其部署和运行性能的测量方法和指标。

7.2.3 指南

7.2.3.1 组织应保持关于所有隐私控制的一致性和准确信息的单一来源性，这些信息可广泛提供给有权限的访问者。

7.2.3.2 为满足隐私要求，组织应提供所有当前和计划的隐私控制，通过不断的协商、审批、监察、报告和审查，并采取行动纠正或改善。

7.2.3.3 组织应通过管理可能影响服务的风险来确保隐私控制的持续运行，从而确保与连续性相关的最低服务水平。

7.2.3.4 组织应确保隐私控制的机密性、完整性和可用性，与确定的隐私保护目标保持一致。

7.2.3.5 组织应确保与第三方签订的所有合同和协议均支持产品的隐私要求，且所有第三方均履行其合同承诺。

7.2.3.6 为确保第三方完整参与了个人身份信息的生命周期，组织应与提供专业知识的第三方人员密切联系。

7.2.3.7 第三方应提供信息，使组织能够在出现隐私问题时解释这类问题，这种信息共享应成为与第三方签订合同和服务水平协议的一部分。

7.3 设计隐私控制

7.3.1 要求

为满足隐私风险评估产生的要求，组织应设计隐私控制。

7.3.2 说明

7.3.2.1 通过设计控制满足要求，控制是基于风险和期望的结果或实施控制的目标所设计，将实施的控制组合起来创建隐私功能。

7.3.2.2 产品和相关个人身份信息处理的隐私控制包括但不限于以下内容：

——基于组织初始知识的隐私控制，例如同意管理和隐私偏好管理；

——满足隐私风险评估要求的隐私控制。

7.3.3 指南

7.3.3.1 为满足消费者在整个个人身份信息生命周期中的隐私要求和需求，组织应设计隐私控制。

7.3.3.2 组织应设计隐私控制以满足隐私风险评估中产生的风险。

7.4 实施隐私控制

7.4.1 要求

为满足隐私要求，组织应设计、开发、测试、验证和实施隐私控制，并在整个个人身份信息生命周期内监视其有效性。

7.4.2 说明

隐私控制的工程、开发、测试和验证可确保产品及其相关的个人身份信息处理和已实现的隐私控制满足组织的隐私目标和需求。

7.4.3 指南

7.4.3.1 组织应在整个产品生命周期和个人身份信息生命周期内设计、开发、实施和操作控制，以满足要求。

7.4.3.2 隐私控制实施应与组织的企业架构及相关的安全和隐私架构保持一致。

7.4.3.3 组织在实施控制时应采用最佳实践，包括隐私工程方法、概念和原则。

7.4.3.4 关于成本、收益和风险权衡，风险评估应指导并告知使用不同技术或政策进行操作控制。

7.4.3.5 应对隐私控制进行测试，以确保其满足隐私要求。

7.4.3.6 实施建议的隐私控制的可行性应包括在潜在新产品的选项评估过程中。当评估可行性表明产品不能满足隐私要求时，可能会对产品进行审查或放弃。

7.4.3.7 输出应是一组已实施的隐私控制，这些控制应满足已确立的要求，并准备好向服务过渡。

7.5 设计隐私控制测试

7.5.1 要求

为确保隐私控制在整个人身份信息生命周期中预期运行的有效性，组织应进行控制测试并制定验收标准。

7.5.2 说明

为了确保隐私控制的有效性，需要对每个待测试的隐私控制的设计和操作进行全面的测试，包括使用和误用案例以及回归测试。在产品开发期间，需要对控件的设计进行测试；在发布前、整个支持期直至退出期间，需要对控件的操作进行测试；在某些情况下，需要在退出后进行测试。

7.5.3 指南

7.5.3.1 所有隐私控制的设计和操作测试都应提前设计，以便根据预先确定的计划对其进行健全性测试并由管理层进行批准。

7.5.3.2 验收准则也应事先设计和批准。

7.5.3.3 验收准则的制定应遵循明确的方法。

示例：通过设计过程定义隐私的预期结果(即对评估风险的有效保护）；为提供有效的风险保障，界定应实施的隐

私规定（例如目的限制、资料最小化、透明度等）；确定有效实现设计原则的技术或流程(例如数据匿名化、可访问用户界面设计等）。

7.5.3.4 检测应符合验收准则，才可认定控制的有效性。

7.5.3.5 为确保有效地满足每个标准，应定义测试方法 。

示例：确保数据最小化的差异隐私，确保视觉界面可用性的用户体验设计方法。

7.5.3.6 如果测试表明控制无效，则应审查、修订和重新测试其设计和操作，然后才能将其视为有效管理隐私风险。

7.5.3.7 组织应根据隐私和数据风险相关测试场景进行隐私威胁建模；可行的情况下，考虑增加现有的开发安全威胁建模流程。

7.5.3.8 为确保隐私控制的可行性和相关性，组织应每年审核隐私控制测试计划。

7.5.3.9 如果发生可能对隐私控制产生影响的更改，应重复进行测试。

7.5.3.10 软硬件产品和业务流程应采取隐私、安全和测试措施。

7.6 管理隐私控制的过渡

7.6.1 要求

组织应确保产品在向新的、经过修改的或已废止的隐私控制过渡的过程持续满足隐私要求。

7.6.2 说明

在产品战略和生命周期设计阶段，组织需要确保新的、经过修改的或已废止的隐私控制能够满足所记录的目标。这个阶段还需要负责产品从一个生命周期状态过渡到另一个生命周期状态（从设计到开发，从开发到运营，从运营到生命结束），同时控制风险并支持组织做出决策。

7.6.3 指南

7.6.3.1 为确保顺利和成功地过渡新的、更改的或失效的控制，组织应确保所有相关的隐私控制过渡计划都已到位，并管理相关的隐私控制支持和协调活动。

7.6.3.2 变更过程负责控制所有产品变更的生命周期，在基于对信息技术的产品造成最低破坏的情况下，实现有益的变更。组织应确保系统地管理变更，以优化隐私风险暴露，最小化隐私影响，并在第一次尝试时保证成功实施，及时通知所有利益相关者。第二个过程，即变更管理，负责控制所有变更的生命周期，使得在对信息技术服务的干扰最小的情况下进行有益的变更。

7.6.3.3 组织应确保交付隐私控制所需的信息技术资产得到适当控制，并确保在需要的时间和地点能够获得准确、可靠的资产信息。这些信息应详细到如何配置资产以及处理它们之间的关系。

7.6.3.4 为交付已部署产品所需的新隐私功能，同时保护现有隐私服务的完整性，组织应负责计划、调度和控制隐私产品版本的构建、测试和部署。

7.6.3.5 组织应确保现有、新的或更改的隐私控制符合设计规范。验证是控制解决方案的“质量保证”部分。在实时产品生产环境中提供的隐私控制的最终效用（适宜性）和保证（适用性）反映了验证过程的效率和有效性。虽然验证确保满足业务需求，但测试关注的是满足规范。

7.6.3.6 组织应提供一致和标准化的方法，确定隐私控制变更对业务结果以及现有和拟议的隐私控制可能产生的影响。此类信息使变更管理能够在隐私目标的背景下做出适当的决定。

7.6.3.7 组织应确保系统地收集、分类和存储与隐私控制设计、开发和实施之间过渡相关的数据、信息和知识。这些步骤能够在恰当的时间、恰当的地点获得信息和数据，支持未来正确决策，并通过减少重新创建或重新交流现有知识来提高效率。

7.7 管理隐私控制的运行

7.7.1 要求

组织应确保影响隐私的服务和控制有效且高效地运行，包括满足消费者请求、解决服务故障、解决问题和执行日常运营任务。

7.7.2 说明

隐私控制操作旨在协调并执行所需的活动和流程，以确保在约定的服务水平下，向内部组织用户和外部消费者提供并管理隐私控制。此外，控制操作还应用于提供和支持隐私控制的技术。在这个阶段，隐私控制的真正价值是由业务、消费者和用户共同实现的。因此，这个阶段还需要负责根据消费者的需求来维护、改进并不断优化主动隐私控制。

7.7.3 指南

7.7.3.1 组织应确保对消费者使用产品过程中影响隐私的事件进行监视、检测和补救，对事件进行解释和理解，确定所需的控制措施和补救措施。

7.7.3.2 为确保保持约定的隐私控制服务质量水平，组织应制定有效的隐私事件管理政策和程序。

7.7.3.3 为减少对组织运营和消费者隐私的不利影响，组织应在发现影响隐私事件后尽快恢复正常隐私控制运行。

7.7.3.4 组织应为消费者提供渠道，请求和接收隐私控制方面的标准信息，并支持存在预定义的授权和资格流程的隐私控制。它还向消费者提供有关隐私控制服务补救的可用性以及获取这些服务的程序的信息。

7.7.3.5 组织应管理所有产品的生命周期，从最初的识别到进一步的调查、记录和最终消除这些问题。努力将支持产品基础设施中的底层设计、开发或操作错误可能导致的隐私事件和问题对消费者隐私的不利影响降到最低，并主动防止与这类错误相关的隐私事件再次发生。

7.7.3.6 组织应负责允许组织用户适当使用影响 IT 服务、数据或其他资产的隐私。访问管理确保只有经过授权的用户才能访问或修改资产，从而帮助保护资产的机密性、完整性和可用性。访问管理在隐私支持流程中实现信息安全管理策略，有时也称为权限管理或身份管理。

7.8 准备和管理隐私泄露

7.8.1 要求

组织应与相关第三方一起设计、实施和运行控制措施，以预防、检测和从事件中恢复因运营中断和隐私泄露而导致的正常运营，并与利益相关者进行沟通。

7.8.2 说明

组织可能无法完全防范隐私泄露，但运营中断和对消费者的影响并非如此。隐私泄露管理是组织弹性安排的一部分，以确保采用无缝的方法预防、检测、恢复业务，并就隐私泄露进行沟通。

7.8.3 指南

7.8.3.1 演练隐私泄露程序、事件分类、向高级管理层汇报以及试用与消费者的沟通计划是组织弹性安排的核心。请参考 ISO/IEC 27035-1 和 ISO/IEC 27035-2，ISO/IEC 29180:2012 和 ISO 22316。

7.8.3.2 在设计网络安全弹性时，应识别并纳入个人身份信息风险。

7.9 在个人身份信息生命周期中为所依赖的流程和产品操作实施隐私控制

7.9.1 要求

为持续满足隐私要求，组织应与第三方一起，在支持产品的服务中设计和实施隐私控制。

注：用于支持产品的特定过程将根据特定产品的需求和市场细分(以及其他因素）而有所不同。

7.9.2 说明

组织通常在产品支持过程中设计和运行隐私控制。当数据迁移时，产品可以采用一种模式，避免在销售点进行数据存储（除非设备损坏）。通过服务注册、独立工作或以匿名方式与服务交互等方式，隐私设计可以避免数据收集的需求。在产品的整个生命周期中，产品需要以多种方式处理个人身份信息，这些处理过程对于产品的销售、营销、分销、支持和退出是必要的。有些处理过程是预先存在的，有些则根据产品的隐私设计方法重新设计和实现。重要的是，与个人身份信息处理相关的流程应更加简洁，以保护与产品交互的人员或其个人身份信息由产品处理的人员的隐私。

7.9.3 指南

7.9.3.1 应对范围所依赖的产品的隐私要求进行一致性审查，因为只有在整个产品生态系统中处理隐私风险，对隐私的设计承诺才会加大。

7.9.3.2 营销和销售材料应反映产品的实际功能。

7.9.3.3 分销和销售点人员应接受培训，能够告知消费者并减轻相关的隐私风险。

示例：在支持产品注册、安装和激活时。

8 个人身份信息生命周期结束要求

8.1 引言

8.1.1 消费品与个人身份信息二者的生命周期不完全相同。产品在生命周期结束时可能会被召回、淘汰或停止支持。消费者在组织结束支持后可处置、转让、销售或继续使用产品，而消费品生命周期的结束也可能是由于消费者死亡，即消费者的使用结束并不意味着个人身份信息生命周期的结束。个人身份信息生命周期的结束与产品设计同样重要。设计隐私可在考虑和计划删除个人身份信息方面体现。

8.1.2 消费者在产品生命周期及其相关隐私风险方面发挥着关键作用。如果消费者在该阶段有自由裁量权，那么在继续使用产品时，应告知他们管理自己和他人的隐私。个人身份信息的责任在供应商对产品结束支持后也可继续。

8.2 设计退出和终止使用的隐私控制

8.2.1 要求

应与第三方合作设计和运行隐私控制，管理产品退出时、退出后以及消费者使用结束时个人身份信息的风险。

8.2.2 说明

组织有责任确保在个人身份信息的整个生命周期内实施隐私控制，即使在产品报废后仍需对消费者的个人身份信息进行长期管理。产品的使用寿命并不一定意味着相关个人身份信息的生命周期结束。实际上，消费者的个人身份信息可能需要在产品退出后仍继续处理。因此，组织在开发产品时应考虑隐私风险，并且在产品的官方使用寿命内仍然实施隐私控制。各种可能出现的退出案例也必须被考虑在内。如果在这段时间内没有适当管理隐私风险，消费者的个人身份信息可能会面临无限期延长风险。

8.2.3 指南

8.2.3.1 在设计产品时，应考虑产品的寿命终止，包括消费者通过二手市场将产品传递给其他消费者的情况，如果消费者死亡，则停止销售产品，取消产品支持。

8.2.3.2 只要消费者与产品相关的个人身份信息得到处理，隐私控制就应发挥作用。

8.2.3.3 如果发现隐私风险发生变化，则应采用与产品开发期间相同的方式设计、测试和运行隐私控制的变化。

8.2.3.4 产品应具有允许消费者安全删除存储在产品上的个人身份信息的功能。

8.2.3.5 个人身份信息的收集和保留应根据组织的需求来确定，并在技术和组织流程层面上实施。前提是该组织必须遵守相关的法律义务，才能进行个人身份信息的收集和保留。

8.2.3.6 在产品支持和产品使用结束后，个人身份信息的保留和处理只能出于有效的组织目的进行。

8.2.3.7 如果不再需要组织保留的个人身份信息，并且个人身份信息已达到其生命周期的末尾，则数据的破坏程度应取决于数据的敏感性。

注：NIST[58]包括对存储设备进行消毒和销毁数据的建议，包括通过覆盖数据来清除数据，以及销毁物理介质。

8.2.3.8 应将产品支持结束后产品数据的保留和处理情况通知消费者。

8.2.3.9 当个人身份信息不再需要满足特定合法组织或法律要求时，应安全销毁或匿名化个人身份信息[51][59]。

8.2.3.10 在淘汰任何产品之前，对拟议的隐私控制的更改应该成为授权过程的一部分。

8.2.3.11 应考虑产品支持结束后的消费者产品使用情况，同时持续监测市场，并通过纠正措施解决任何可能导致重大消费者隐私风险的已识别威胁或漏洞。

8.2.3.12 消费者寿命终止用例应包括：消费者停止使用（消费者死亡、产品处置或回收）或重复使用，例如通过二手市场转让产品。

8.2.3.13 如果消费者对产品淘汰后的使用有自由裁量权，他们应该被告知其在任何产品淘汰后使用中管理自己和他人隐私风险的责任。

8.2.3.14 多功能团队应在产品寿命结束时通知消费者、销售和支持人员，他们可以采取哪些行动来保护个人身份信息的隐私，因为个人身份信息的销售、支持或其他组织处理结束了。

8.2.3.15 产品退出可能在发布几年后发生，因此自进行初始隐私风险评估以来，情况发生了变化。在产品退出之前，应重新审查产品的隐私风险评估，并在必要时进行更新。

参 考 文 献

[1]International Conference on Data Protection and Privacy Commissioners (32nd October 2010） Resolution on Privacy by Design. https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf.

[2]EDPS Preliminary Opinion on Privacy by Design, May 31, 2018. https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-designen.

[3]Privacy by Design, The 7 Foundational Principles. January 2011. https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

[4]The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf

[5]EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (https://edpb .europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en） .

[6]ISO 26000:2010, Guidance on social responsibility.

[7]ISO/IEC 29151 :2017, Information technology—Security techniques—Code of practice for personally identifiable information protection.

[8]UNCTAD, Data Protection and Privacy Legislation Worldwide. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

[9]OECD Privacy Framework http://www.oecd.org/sti/ieconomy/oecd_privacy framework.pdf

[10]REGULATION, (EU） 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation）.

[11]APEC privacy framework principles https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015）.

[12]ISO/IEC 29100:2011 Information technology-Security techniques-Privacy framework https://www.iso.org/standard/45123.html.

[13]ISO 15944 - 8:2012 Information technology-Business operational view-Part 8: Identification of privacy protection requirements as external constraints on business transactions https://www.iso.org/standard/51544.html.

[14]GAPP Generally accepted privacy principles (GAPP） in privacy policy development. https://www.cpacanada.ca/en/business-and-accounting-resources/other-general-business-topics/information-management-and-technology/publications/business-and-organizational-privacy-policy-resources/gapp-in-privacy-policy-development.

[15]ISO/IEC 27701:2019, Security techniques-Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management-Requirements and guidelines.

[16]NIST PRIVACY FRAMEWORK, A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT, VERSION 1.0 January 16, 2020.

[17]ISO/IEC 29184:2020 Information technology— Security techniques-Online privacy notices and consent.

[18]ISO/DIS 22458 Consumer vulnerability – Requirements and guidelines for the design and delivery of inclusive service.

[19]ISO/IEC Guide 76:2020 Development of service standards-Recommendations for addressing consumer issues.

[20]Future of Privacy Forum. The Internet of Things and Persons with Disabilities. 2019. https://fpf .org/2019/01/31/iot-devices-should-deal-with-privacy-impacts-for-people-with-disabilities/.

[21]ISO/IEC 27556 User-centric framework for the handling of personally identifiable information (PII） based on privacy preferences.

[22]OASIS, Privacy Management Reference Model and Methodology (PMRM） Version 1.0, Committee Specification 02. 17 May 2016. http://docs.oasis-open.org/pmrm/PMRM/v1.0/cs02/PMRM-v1.0 -cs02.html.

[23]IEC 62559-2, Use case methodology-Part 2: Definition of the templatesfor use cases, actor list And requirements list.

[24]ISO/IEC/TR 27550, Information technology-Security techniques-Privacy engineering for system life cycle processes.

[25]ISO/IEC 27001, Information security, cybersecurity and privacy protection-Information security management systems-Requirements.

[26]ISO/IEC 27002, Information security, cybersecurity and privacy protection-Information security Controls.

[27]ISO 30401, Knowledge management systems-Requirements.

[28]ISO 9001, Quality management systems-Requirements.

[29]ISO/IEC/IEEE 15288:2015, Systems and software engineering-System life cycle processes

[30]OASIS Privacy by Design for Software Engineers https://www.oasis-open.org/committees/tchome.php?wg abbrev=pbd-se.

[31]van der Nagel E., Arnold M., Nansen B., Gibbs M., Kohn T., Bellamy C. et al.,Death and the Internet: Consumer issues for planning and managing digital legacies.Australian Communications Consumer Action Network, Sydney, Second Edition, 2017.

[32]IEC/IEEE 82079-1, Preparation of informationfor use (instructionsfor use） of products-Part 1: Principles and general requirements.

[33] ISO COPOLCO, 2016, Identification of current consumer issues in privacy and protection of personal data – Document N211/2016 Annex 1.

[34]ANEC Principles for Digital Devices https://www.anec.eu/publications/other-publications/588-anec-consumer- representatives- guidance-domestic-privacy-and-the-privacy-of-digitally-connected-devices.

[35]Securing consumer trust in the Internet of Things. Principles & recommendations 2017’ ANEC,BEUC, CI, ICRT.

[36]ISO/IEC 27035-1, Information technology-Security techniques-Information security incident management-Part 1: Principles of incident management.

[37]ISO/IEC 27035-2, Information technology-Security techniques-Information security incident management-Part 2: Guidelines to plan and preparefor incident response.

[38]ISO 31000, Risk management-Guidelines.

[39]ISO/IEC 27557, Information security, cybersecurity and privacy protection-Application of ISO 31000:2018for organizational privacy risk management.

[40]OWASP Foundation https://owasp.org/.

[41]NIST source: https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources.

[42]NIST privacy risk model:NISTIR 8062.Introduction to Privacy Engineering and Risk Managementin Federal Systems 2017.http://csrc.nist.gov/publications/drafts/nistir-8062/ nistir_8062_draft.pdf.

[43]NIST,National Institute of Standards and Technology (2019） NIST Privacy Risk Assessment Methodology(PRAM）.https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/ resources.

[44]CNIL privacy risk model: CNIL PIA manual 1- methodology: how to carry out a PIA. June 2015 Edition. https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf.

[45]ISO/IEC 29134:2017, Information technology-Securitytechniques —Guidelines for privacy impact assessment.

[46]NIST Special Publication 800-30, Revision 1, Guide for Conducting Risk Assessments,https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

[47]DistriNet Research Group. https://www.linddun.org/.

[48]ISO 22316, Security and resilience-Organizational resilience-Principles and attributes.

[49]NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Information.Systems and Organizations. September 2020
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[50]ISO/IEC 20000-1, Information technology-Service management-Part 1: Service management system requirements.

[51]ISO/IEC 20889:2018, Privacy enhancing data de-identification terminology and classification of Techniques.

[52]ISO/IEC/TS 27570:2021, Privacy protection-Privacy guidelinesfor smart cities.

[53]ISO COPOLCO 39th meeting – An outline description of the proposed new standard for privacy by design of consumer goods and services, April 2017 – Annex B of Document N283.

[54]ISO 10377:2013, Consumer product safety-Guidelinesfor suppliers.

[55]Operationalizing Privacy by Design https://collections.ola.org/mon/26012/320221.pdf.

[56]ISO/IEC 27005, Information security,cybersecurityand privacy protection—Guidanceon managing information security risks.

[57]ISO/IEC 29180:2012, Information technology-Telecommunications and information exchange.
between systems-Security framework for ubiquitous sensor networks.

[58]NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization. Feb 2015
https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization.

[59]ISO/IEC 27555:2021, Information security, cybersecurity and privacy protection-Guidelines on personally identifiable information deletion.

[60]ISO/IEC Guide 14:2018, Products and related services-Informationfor consumers.

[61]ISO/IEC 19944-1:2020, Cloud computing and distributed platforms ─ Data flow, data categories and data use-Part 1: Fundamentals.

[62]ISO 9000:2015, Quality management systems-Fundamentals and vocabulary.

[63]ISO/IEC/IEEE29148:2018,Systems and software engineering-Lifecycle processes-Requirements engineering.

[64]ISO/IEC 25000:2014,Systems and software engineering-Systems and software Quality Requirements and Evaluation (SQuaRE）-Guide to SQuaRE.

[65]ISO/IEC 27000:2018, Information technology-Security techniques-Information security management systems-Overview and vocabulary.

[66]ISO/IEC 25063:2014, Systems and software engineering-Systems and software product Quality Requirements and Evaluation (SQuaRE）-Common Industry Format (CIF） for usability: Context of use description.

[67]ISO/TR 14872:2019, Health informatics-Identification of medicinal products-Core principles for maintenance of identifiers and terms.

[68]ISO/IEC 29100:2011/Amd.1:2018, Information technology -Security techniques-Privacy framework-Amendment 1: Clarifications.

[69]ISO/IEC/TR 27016:2014, Information technology-Security techniques-Information security management-Organizational economics.

[70]ISO/IEC/IEEE 24765:2017, Systems and software engineering-Vocabulary.

[71]ISO Guide 73:2009, Risk management-Vocabulary.

[72]ISO/TR 31700-2, Consumer protection-Privacy by design for consumer goods and services-Part 2: Use cases.

[73]GB/T 19000—2016 质量管理体系基础和术语

[74]GB/T 36000—2015 社会责任指南