国 际 电 信 联 盟

ITU-T X.1058

(03/2017)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

安全应用和服务 – 安全管理

信息技术 – 安全技术 – 个人可识别信息保护行为准则

ITU-T X.1058 建议书

国际电信联盟

ITU-T X 系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
报文处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	**X.1050–X.1069**
生物测定安全	X.1080–X.1099
安全应用和服务	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
计算网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1339
PKI 相关建议书	X.1340–X.1349
物联网（IoT）安全	X.1360–X.1369
智能交通系统（ITS）安全	X.1370–X.1379
网络安全信息交换	
网络安全概述	X.1500–X.1519
脆弱性/状态信息交换	X.1520–X.1539
事件/事故/探索法信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
探索法和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和导则	X.1640–X.1659
云计算安全的落实工作	X.1660–X.1679
其他云计算安全问题	X.1680–X.1699

欲了解更详细信息，请查阅 ITU-T建议书目录。

国际标准 ISO/IEC 29151
ITU-T X.1058建议书

信息技术 – 安全技术 – 个人可识别信息保护行为准则

摘要

处理个人可识别信息（PII）组织的数量在不断增加，经这些组织处理的PII数量也有增无减。同时，对于个人可识别信息保护和个人数据安全的社会期望也在不断提高。许多国家正致力于完善其法律，加大对愈发猖獗的资料外泄事件的打击力度。

本规范制定了控制目标、控制手段，并为实施控制制定相应指南，以期满足在对个人可识别信息（PII）保护进行风险和影响评估时出现的各项要求。特别是，本规范基于ISO/IEC 27002，对有关指南进行规定，考虑到了处理PII的要求，可用于应对组织信息安全面临的各项风险环境。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1058	2017-03-30	17	11.1002/1000/13182

关键词

实施规程、控制、实施指南、PII。

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一识别码，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

引言

处理个人可识别信息（PII）组织的数量在不断增加，经这些组织处理的PII数量也有增无减。同时，对于个人可识别信息保护和个人数据安全的社会期望也在不断提高。许多国家正致力于完善其法律，加大对愈发猖獗的资料外泄事件的打击力度。

随着PII外泄事件不断增加，为降低机密信息发生外泄的风险，并减轻机密信息外泄对有关组织和个人的影响，负责收集或处理PII的组织对制定PII保护指南的诉求愈发强烈。本规范因而应运而生。

本规范为PII控制者就信息安全和PII保护控制（通常应用于各个处理PII保护的组织）的方方面面进行指导。下文列举的其他ISO/IEC系列标准对整个PII保护进程的其他方面进行了指导或提出了相关要求：

– ISO/IEC 27001规定了信息保护管理进程和相关要求，为PII保护奠定了基础。

– ISO/IEC 27002为组织的信息安全标准和信息安全管理实践提供指南，包括控制选择、控制实施和控制管理，该标准还涉及组织的信息安全风险环境。

– ISO/IEC 27009规定了具体领域（现场、领用领域或市场）的ISO/IEC 27001使用需要。该标准考虑了未计入ISO/IEC 27001的其他需求，以及如何对ISO/IEC 27001的需求进行完善，并列明未计入ISO/IEC 27001附件A的其他控制或控制设备。

– ISO/IEC 27018为采用云服务等处理工具处理PII的组织提供相关指导。

– ISO/IEC 29134为认定、分析和评价隐私风险提供指南，而ISO/IEC 27001和ISO/IEC 27005为认定、分析和评价安全风险提供方法。

控制方法的选择应该以风险分析认定的风险为准，从而制定一套全面的、连贯的控制系统。控制方法应依具体的PII处理情况进行调整。

本规范包括两部分 — 1）由第1至第18条构成的标准主体；及2）规范性附录。该结构体现了对ISO/IEC 27002进行有针对性扩充的标准做法。

本规范的主体结构（包括条款标题）与ISO/IEC 27002的主体部分一致。本标准引言部分和第1至4条介绍了本规范的使用背景。第5至18条的标题与ISO/IEC 27002一致，这体现了本规范是在ISO/IEC 27002的指导下制定的，增加了许多针对PII保护的新控制方法。就PII控制方而言，ISO/IEC 27002中的许多控制无需扩增。然而，在一些情况下人们需要新增操作指南，本标准中与ISO/IEC 27002标题（和条款编号）一致的相关标题项下已给出该等新增指南。

本标准的规范性附件包括PII保护控制的扩增内容，对ISO/IEC 27002的已有内容进行补充。据此，该等新增PII保护控制及其相关指南共分为12个门类，对应于ISO/IEC 29100的保密政策和11项保密原则：

– 同意和选择；

– 目的、合法性和规范；

– 收集限制；

– 资料最小化；

– 使用、保留和披露限制；

– 准确度和质量；

– 开放性、透明性和注意；

– 个人参与和访问；

– 问责制；

– 信息安全；

– 隐私合规。

图1描述了本规范与ISO/IEC系列国际标准之间的关系

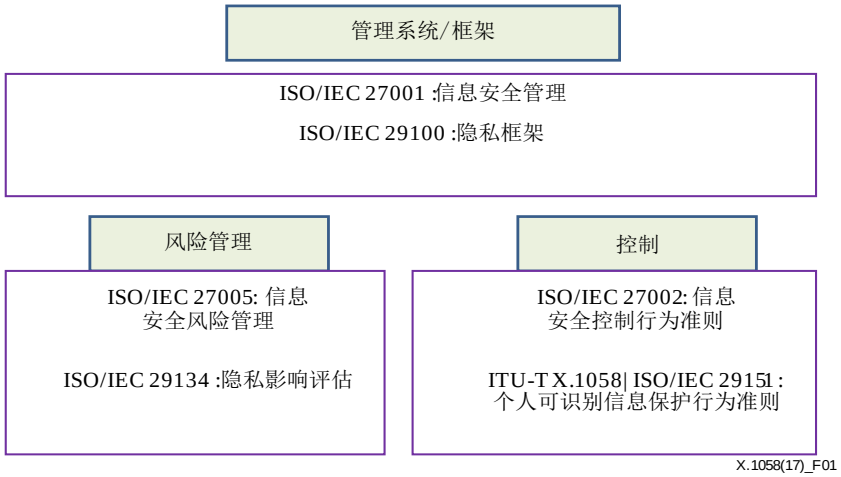

图1 – 本规范与ISO/IEC系列国际标准之间的关系

本规范的各项指南以ISO/IEC 27002为准，并且为解决在处理PII的过程中出现的隐私保护要求而进行必要调整。

a) 各类不同的处理域包括：
   - 公共云服务；
   - 社会网络应用；
   - 家庭联网设备；
   - 搜索，分析；
   - 为实现广告宣传或类似目的而处理PII；
   - 大数据分析项目；
   - 雇用处理；
   - 销售服务业务管理（企业资源规划、客户关系管理）；

b) 各类不同处理位置包括：
   - 个人信息处理平台（如智能卡、智能手机及其各类应用、智能电表、可穿戴设备）；
   - 数据传输和收集网络（如网络处理最初创建手机定位数据的位置，该数据在某些辖区可被视为PII）；
   - 组织自身拥有的处理基础设施；
   - 第三方处理平台；

c) 收集特征包括：
   - 一次性的数据收集（如一项注册服务等）；
   - 持续性的数据收集（如，可不断检测身体各项参数的佩戴式或体内传感器、可进行多次数据收集的非接触式支付卡支付方式，以及智能电表数据收集系统等）。

注 – 持续性的数据收集可能包括或产生有关行为的、有关位置的和其他类型的PII。在这些情况下，由于PII保护控制允许在同意的情况下对访问和收集进行管理，并允许PII当事人对该访问或收集进行适当控制，据此，需要考虑采用该PII保护控制。

国际标准
ITU-T建议书

信息技术 — 安全技术 — 个人可识别信息保护行为准则

1 范围

本建议书|国际标准制定了控制目标、控制手段，并为实施控制制定相应指南，以期满足在对个人可识别信息（PII）保护进行风险和影响评估时出现的各项要求。

特别是，本建议书|国际标准基于ISO/IEC 27002，对有关指南进行规定，考虑到了处理PII的要求，可用于应对组织信息安全面临的各项风险环境。

本建议书|国际标准适用于负责控制PII的各类组织（定义见ISO/IEC 29100），包括负责处理PII的各个上市公司、私人企业、政府实体以及非营利组织。

2 规范性参考文献

下列ITU-T建议书和国际标准所包含的条款，通过在本建议书 | 国际标准中的引用而构成本建议书 | 国际标准的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献都面临修订，使用本建议书 | 国际标准的各方应探讨使用下列建议书和其他参考文献最新版本的可能性。国际电工委员会（IEC）和国际标准化组织（ISO）的成员负责维护当前有效的国际标准的注册。国际电信联盟电信标准化局负责维护当前有效的ITU-T建议书的注册。

– ISO/IEC 27002:2013，信息技术 – 安全技术 – 信息安全控制实施规程

– ISO/IEC 29100:2011，信息技术 – 安全技术 – 隐私框架。

3 定义和缩略语

3.1 定义

本建议书|国际标准中，术语和定义规定在ISO/IEC 27000:2016、ISO/IEC 29100中且以下适用。

ISO在线浏览平台、IEC电子百科及国际电联术语和定义为用于标准化工作的术语数据库。

3.1.1 首席隐私官（chief privacy officer）：组织中负责保护个人可识别信息（PII）的高级管理人员

3.1.2 去身份识别进程（de-identification process）：采用去身份识别技术移除一系列识别数据与数据当事人之间关联的进程。

3.2 缩略语

本规范中，以下缩略语系指：

BCR 企业约束规则

CCTV 闭路电视

CPO 首席隐私官

PBD 通过设计保护隐私

PDA 个人数字助理

PET 隐私增强技术

PIA 隐私影响评估

PII 个人可识别信息

RFID 射频识别

USB 通用串行总线

4 概述

4.1 PII保护的目的

本规范规定了一组PII控制方法。PII保护的目的是促使各组织落实一套控制机制，作为其整体PII保护计划的一部分。他们可依照ISO/IEC 29100规定的隐私原则，在隐私框架内用于增强人们的隐私意识，以严格遵守有关隐私的法律法规，管理隐私风险，以及用于满足PII当事人，监管人和客户的期望。

4.2 PII保护要求

组织应该明确其PII保护要求。ISO/IEC 29100的隐私原则可用于明确该要求。PII保护要求有三大主要来源：

– 关于PII保护的法律、法定、法规和合同要求，如某组织、其贸易伙伴、承包商和服务提供商必须遵守的PII要求；

– 对组织和PII当事人进行风险评估（即安全风险和隐私风险评估），评估时考虑该组织的整体经营策略和目标；

– 企业政策：组织也可以自行选择是否遵循先前的要求准则。

组织同样应考虑用于助力PII保护的PII处理原则（如ISO/IEC 29100中界定的隐私原则）、目标和业务要求。

应根据风险评估选择PII保护控制（包括安全控制）。如ISO/IEC 29134所述，隐私影响评估（PIA）的评估结果将为PII保护的风险管理以及风险防控控制的实施提供指南，并为之规定妥善的处理方法，明确了优先级。

ISO/IEC 29134等文件的PIA规范可为隐私风险评估提供指南，包括为风险评估、风险处理方案、风险接受和风险审查等提供相关建议等。

4.3 控制

隐私风险评估可以帮助各个组织确定在模拟PII当事人权利遭非法处理和削弱而造成的隐私泄露风险。组织应该选择并实施相关控制，以便处理风险影响程序发现的各项风险。随后，应对该等控制和处理方法进行记录，最好在独立的风险登记册中分开记录。

4.4 选择控制

本规范中的控制方法可供人们选择（按引用包括ISO/IEC 27002规定的控制，这为人们提供了一套参考控制集）。需要时，也可从其他控制集中选择控制，新控制也可以用来满足某些具体需要（这要视情况而定）。

控制的选择取决于组织依风险处理和一般风险管理标准所做的决定，该等决定适用于该组织，通过有关合约也适用于其客户和供应商。控制的选择还应以国家和国际上适用的法律法规为准。

控制的选择和实施还取决于组织在基础设施或服务供应方面所起到的作用。各个组织也许已开始供应基础设施或服务了。在某些情况下，所选控制也许仅适用于某一组织。或者，各组织在实施控制时应共同承担某种责任。比如，合约应该明确规定，一切提供或使用上述服务的组织应承担保护PII的责任。

本规范中的控制可供负责处理PII的组织进行参考，并且可适用于所有负责控制PII的组织。负责处理PII的组织应按照负责控制PII的组织的指导行事。负责控制PII的组织应保证，其负责处理PII的组织能够根据PII处理目标落实PII处理协议规定的一切必要的控制方法。二者均可使用云服务。负责控制PII的组织可以通过审查ISO/IEC 27018来确认拟实施的相关控制。

5-18节对于本规范中的控制以及相关实施指南提供了更加详细的论述。如果组织的信息系统、服务和运行在设计阶段就已经考虑到了PII保护的各项要求，上述控制也许就会更加易于实施。该考虑是一种通常被称为“通过设计保护隐私（PBD）”的概念。关于控制选择及相关风险处理选择的更多信息可参阅ISO/IEC 29134。其他参考资料见参考文献列表。

4.5 制定组织专用指南

本规范可被视为拉开了制定组织专用指南的序幕。本规范中的控制和指南并非适用于所有组织。

此外，未收录于本规范的新增控制和指南可能也不可或缺。当制定了包含新指南或控制的文件后，可能有必要在本规范中新增对这些条款的交叉引用（如适用），该功能可能为审计员和业务伙伴的合规性检查工作提供帮助。

4.6 生命周期考量

PII的自然生命周期如下：创建或初创、收集、存储、使用、转让到最终处理（如安全销毁）。PII的重要性和面临的风险在其生命周期的各阶段可能并不相同，但从某种程度而言，PII保护的重要性在其生命周期的每时每刻都不容忽视。

信息系统也存在生命周期，即信息系统的构想、规定、设计、开发、测试、实施、使用、维护、最终淘汰和处理。同样，在上述每个阶段都不应忽视PII保护。通过研究现实情况，模拟信息安全风险和隐私风险，人们可开发新系统并取代现有系统，从而为各组织更新并完善安全控制和PII保护控制提供良机。

4.7 本规范的结构

本规范的其余部分包含两大规范性部分。

本规范的第一部分由第5至第18小节构成，为ISO/IEC 27002规定的某些现有控制增添相关指南和其他信息。本部分各小节使用的标题和编号与ISO/IEC 27002中的小节标题一致，以方便与其进行交叉参考。

本规范的第二部分即附录A，对某个PII保护控制集进行详细描述。该部分采用的格式与ISO/IEC 27002相同，规定了控制目标（见方框内文字），并在方框下方列举可供使用的一个或多个控制方法。控制说明的结构如下：

控制

该标题下的案文界定旨在满足控制目标的具体控制语句。

PII保护的实施指南

该标题下的案文提供更加详尽的信息，以助力有关控制的实施，帮助实现控制目标。本规范规定的指南也许不能完全或充分适用于各类情况，可能也无法满足组织特定的控制要求。因此，可以选择其他控制方法替代，或者利用其他形式的风险处理方法（风险规避或风险转移等）。

关于PII保护的其他信息

该标题下的案文进一步提供可能需要考虑的其他信息，如考虑法律因素和参考其他标准。

5 信息安全政策

5.1 信息安全的管理方向

5.1.1 引言

以ISO/IEC 27002:2013第5.1条规定的内容为准。

5.1.2 信息安全规则

以ISO/IEC 27002项下第5.1.1条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

信息安全规则应该包括适当的PII保护安全措施声明。PII保护的详情可查阅ISO/IEC 27002:2013的18.1.4节。

在设计、实施和审查信息安全规则时，各个组织不应忽视ISO/IEC 29100规定的隐私保护要求。

各组织应规定与安全无关的PII保护内容，作为一项独立的隐私政策。请参见A.2节中的导则。

5.1.3 信息安全政策审查

以ISO/IEC 27002中第5.1.2条规定及相关实施指南为准。

6 信息安全组织

6.1 内部组织

6.1.1 引言

以ISO/IEC 27002中第6.1条规定的内容为准。

6.1.2 信息安全的作用和功能

以ISO/IEC 27002中第6.1.1条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

我们需要对PII保护的作用和功能进行明确界定、妥善记录和正确传达。具体如下：

a) 应从组织内明确选定负责PII保护的资深人员（有时系指首席隐私官（CPO））；

b) 应从组织内明确选定负责配合信息安全部门工作的个人或群体（即PII保护部门）；以及

c) 所有参与PII处理的个人（包括用户和支持人员）的工作职责中应包含相应的PII保护要求。

已经确立的PII保护部门应与其他PII处理部门、信息安全部门（该部门负责落实PII保护法等规定的安全要求）以及法律部门（该部门负责解释法律、法规和合同条款，同时负责处理数据泄露事故）开展密切合作。

组织应该考虑是否需要，并依情况而定设立跨部门理事会或委员会，该理事会或委员会的成员应从负责处理PII的职能部门中选定。PII保护需多学科辅助，该委员会可让人们立即有机会完善PII保护，以便发现执行隐私影响评估（PIA）的新风险和新领域，并可帮助人们设计信息泄露事故的预防措施、检测措施和应对措施等。本标准建议，该委员会应定期召开会议，会议主席应为负责PII保护的人员（即上文a)所指人员）。

负责控制PII的组织应该要求其负责处理PII的组织指定一个联络人或联络部门，以便收发PII处理合同项下关于PII处理的各项问题。

负责PII保护部门的相关人员应该向首席隐私官发出报告，目的是确保该等人员有足够权限履行其职责。

6.1.3 职责划分

以ISO/IEC 27002中第6.1.2条规定及相关实施指南为准。以下新增指南同样适用。

PII保护实施指南

PII保护的职责和责任范围应与信息安全的职责和责任范围无关。尽管人们认为PII保护的信息安全十分重要，但仍需将PII保护的职责和责任范围与信息安全的职责和责任范围尽量分离。必要时或需要时，出于对完善PII保护的考虑，各组织应增进负责信息安全人员之间的协调合作。

组织应本着职责划分原则来分配PII处理的访问权限，在对于高风险处理工作而言尤应如此。

本着职责划分原则，人员在访问正在进行处理的PII时，不得同时访问有关该等处理的记录文件。

为答复PII当事人的要求而访问PII收集信息的人员，不得进行其他任何形式的PII访问。该访问权限仅限于负责答复PII当事人要求的人员所有。

6.1.4 联系有关部门

以ISO/IEC 27002中第6.1.3条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

适用时，组织应制定好相关规程，规定隐私泄露事故、处理明细或其他事项的汇报时间和汇报对象（如向数据保护部门等进行汇报）。

6.1.5 联系特殊利益集团

以ISO/IEC 27002中第6.1.4条规定及相关实施指南和其他信息为准。

6.1.6 项目管理中的信息安全

以ISO/IEC 27002中第6.1.5条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

任何新项目启动时，应就确定是否需要开展隐私影响评估进行至少一次临界分析。应注意，“项目”一词系指与组织实施或变更的现有或新技术、产品、服务、程序、信息系统、流程或项目有关的一切事项。

进一步指导参见ISO/IEC 29134中规定的隐私影响评估。

6.2 移动设备和电子办公

6.2.1 引言

以ISO/IEC 27002:2013中第6.2条规定的内容为准。

6.2.2 移动设备规则

以ISO/IEC 27002中第6.2.1条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

由于笔记本电脑、手机、通用串行总线（USB）设备和个人数字助理（PDA）等便携和移动设备面临的泄密风险通常比非便携设备（如办公室里的公用电脑）高，因此各组织应根据风险评估严格限制通过上述设备访问PII。

各组织应根据风险评估严格限制远程访问PII，如果远程访问无法避免，要确保远程访问通信能够得到加密、信息认证，其完整性也应得到保护。

6.2.3 电子办公

以ISO/IEC 27002中第6.2.2条规定及相关实施指南和其他信息为准。

7 人力资源安全

7.1 雇佣前

7.1.1 引言

以ISO/IEC 27002:2013中第7.1条规定的内容为准。

7.1.2 筛选

以ISO/IEC 27002中第7.1.1条规定及相关实施指南和其他信息为准。

7.1.3 雇佣期限和条件

以ISO/IEC 27002中第7.1.2条规定及相关实施指南和其他信息为准。

7.2 雇佣期间

7.2.1 引言

以ISO/IEC 27002:2013中第7.2条规定的内容为准。

7.2.2 管理责任

以ISO/IEC 27002中第7.2.1条规定及相关实施指南和其他信息为准。

7.2.3 信息安全意识、教育和培训

以ISO/IEC 27002中第7.2.2条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

应采取措施，让相关人员认识到违反隐私或安全规程，尤其是违反关于PII处理的相关规程可能带来的后果。例如，负责控制PII的组织可能会承担法律责任，其业务出现亏损，或者品牌与声望遭到损害，员工可能会遭到处分，PII当事人则可能遭受身体、物质和精神损害。

各个组织在增强全员信息安全意识、开展信息安全教育和培训的同时，还应就PII保护和PII处理开展相关培训和教育活动。

7.2.4 处分程序

以ISO/IEC 27002中第7.2.3条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

各个组织应采取规范性的惩处办法。若发生隐私泄露事件，各组织应向受影响方明确通知相关惩处办法。惩处办法应适用于全部隐私泄露事件。

7.3 雇佣的终止和变更

7.3.1 引言

以ISO/IEC 27002:2013中第7.3条规定的内容为准。

7.3.2 雇佣责任的终止或变更

以ISO/IEC 27002中第7.3.1条规定及相关实施指南和其他信息为准。

8 资产管理

8.1 资产责任

8.1.1 引言

以ISO/IEC 27002:2013中第8.1条规定的内容为准。

8.1.2 资产清单

以ISO/IEC 27002中第8.1.1条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

各个组织应按ISO/IEC 29134规定，使用PIA报告（如有）等提供的信息，来创建、维护和更新资产清单。资产清单应囊括PII资产和负责处理PII的全部系统。

在对资产清单进行创建和维护时，各个组织应从关于PII信息处理系统的PIA报告中提取以下信息。以下清单仅为举例，最终实施清单可能会有增删：

a) 明确各个系统的名称和缩略语；

b) 经该等系统处理的PII类型；

c) 对PII的所有类型进行分类（参见第8.2.2条），包括个人信息和信息系统内的信息。

d) 对PII当事人和组织而言，PII泄漏事件的潜在影响等级；

e) 收集PII的目的；

f) PII可否外包给其他PII处理组织进行处理；

g) PII是否传送给其他负责控制PII的组织，若如此，请指明接收方（单方或多方）；

h) PII的保存期；

i) 对该PII进行收集或处理的地理区域；

j) 是否存在跨境数据传输。

各个组织应定期向PII保护员提供PII清单的更新版本，从而为所有PII信息处理系统（新版或升级版）创建相关安全控制。

8.1.3 资产所有权

以ISO/IEC 27002中第8.1.2条规定及相关实施指南和其他信息为准。

8.1.4 资产可接受使用

以ISO/IEC 27002中第8.1.3条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

各个组织应需保护的资产，可让PII免于遭受未授权访问、未授权修改、未授权移除、损失或损坏、错误和非法处理等。

8.1.5 资产归还

以ISO/IEC 27002中第8.1.4条规定及相关实施指南和其他信息为准。

8.2 信息分类

8.2.1 引言

以ISO/IEC 27002:2013中第8.2条规定的内容为准。

8.2.2 信息分类

以ISO/IEC 27002中第8.2.1条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

组织应采用现有的分类类别（ISO/IEC 27002中称为信息组别）或新设的分类类别对包含PII的全部信息进行分类。新分类类别应包括但不限于敏感性PII和非敏感性PII等一般数据。数据类别还可更加细化，如可分为个人健康信息（PHI）、个人财务信息（PFI）。如果各组织创建了新分类类别，则也应规定这些类别的保护水平。实际使用的分类方法也将取决于如下要素：相关数据保护立法和法规界定的要求、其他法律义务（如契约责任）、信息的性质和敏感性，以及信息泄露事件可能引起的损害风险。

在某国被归类为非敏感信息的信息在其他国家可能被归类为敏感信息，这应以当地适用的数据保护法为准。

对PII的某一部分进行分类时，若涉及一个或多个附加属性，则可能需要进行重新评价和修改。相关指南和规程应得到落实。

8.2.3 标记信息

以ISO/IEC 27002中第8.2.2条规定及相关实施指南和其他信息为准。以下新增导则也适用：

PII保护实施指南

如果某个组织未将PII归为某个分类类别，那么该组织应确保其所辖人员应知晓PII的定义及如何识别信息是否属于PII。

8.2.4 处理资产

以ISO/IEC 27002中第8.2.3条规定及相关实施指南和其他信息为准。以下新增导则也适用：

PII保护实施指南

如果相关组织允许其所辖人员不对PII相关分类类别进行信息标记，那么他们应使其所辖人员将所有包含PII的信息作为指定分类类别的信息处理。

8.3 媒介处理

8.3.1 引言

以ISO/IEC 27002：2013中第8.3条规定的内容为准。

8.3.2 可移动媒介管理

以ISO/IEC 27002中第8.3.1条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

一些管辖地区也许要求对包含PII的可移动媒介进行加密。不论法律是否做出加密要求，加密始终是降低PII泄漏风险的推荐方法。

若需着重确保数据的机密性或完整性，则应使用密码技术保护可移动媒介的PII。应开展风险分析，以明确所需保护等级，这反过来有助于人们确认拟用密码算法的所需类型、强度和品质。

关于使用密码控制的新增指南参见第10.1节。

8.3.3 媒介处置

以ISO/IEC 27002中第8.3.2条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

包含PII媒介的安全处置规程应与信息的敏感性，以及信息不当处理造成的影响之等级呈正比例关系。一些管辖地区可能会为包含PII或具体PII类型（例如健康数据、财务数据等）的媒介的处置规程设定标准。

8.3.4 物理媒介传输

以ISO/IEC 27002中第8.3.3条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

不论何时，但凡用物理媒介进行信息传输，皆应采取措施记录不断传入、传出的含PII物理媒介，所需记录的有：物理媒介的类型、识别号（例如序列号或存货标签号）、未授权发送方/接收方、日期和时间、物理媒介的数量以及所包含的PII类别，并检查有哪些物理媒介丢失。同时还应记录的有：传输的目的和范围、传输授权方和传输的法律/契约基础。还应考虑对数据最小化原则的明确引用。

9 访问控制

9.1 访问控制的业务要求

9.1.1 引言

以ISO/IEC 27002：2013中第9.1条规定的内容为准。

9.1.2 访问控制方法

以ISO/IEC 27002中第9.1.1条规定及相关实施指南和其他信息为准。

9.1.3 网络和网络服务访问

以ISO/IEC 27002中第9.1.2条规定及相关实施指南和其他信息为准。

9.2 用户访问管理

9.2.1 引言

以ISO/IEC 27002：2013中第9.2条规定的内容为准。

9.2.2 用户注册和注销

以ISO/IEC 27002中第9.2.1条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

用户注册注销规程以及用户生命周期管理应针对（因疏忽泄密引起的）用户访问控制损坏、密码或其他用户注册数据损坏设计解决措施。

9.2.3 用户访问调配

以ISO/IEC 27002中第9.2.2条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

各组织应根据ISO/IEC 29100中规定的数据最小化原则，授权用户访问PII信息处理系统。

各组织应根据ISO/IEC 29100中规定的数据最小化原则，仅将PII信息处理系统的访问权限授予需要实施具体处理任务的个人，且人数越少越好。

各组织应就某些PII和PII处理（即健康数据）实施严格的授权方法。

9.2.4 特许访问权限管理

以ISO/IEC 27002中第9.2.3条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

对PII的批量处理（例如批量查询、批量修改、批量导出和批量删除等）会增加信息批量泄露风险。各组织在转让该等特权操作的访问权时应该承担注意义务。为防止PII遭到滥用，应对访问PII处理（特别是高风险PII处理）的特许权限转让进行严格限定。转让时，还应降低两人或多人相互勾结行泄密之事的风险。相关日志文件应对该特许权限的转让和使用进行记录。所有转让应明确规定访问许可期限，各组织应定期对全部访问许可进行审查，并依情况而定更新、撤销或终止该等访问许可。

9.2.5 用户秘密认证信息管理

以ISO/IEC 27002中第9.2.4条规定及相关实施指南和其他信息为准。

9.2.6 用户访问权限审查

以ISO/IEC 27002中第9.2.5条规定及相关实施指南和其他信息为准。

9.2.7 移除或调整访问权限

以ISO/IEC 27002中第9.2.6条规定及相关实施指南和其他信息为准。

9.3 用户责任

9.3.1 引言

以ISO/IEC 27002：2013中第9.2条规定的内容为准。

9.3.2 用户秘密认证信息

以ISO/IEC 27002中第9.3.1条规定及相关实施指南和其他信息为准。

9.4 系统和应用访问控制

9.4.1 引言

以ISO/IEC 27002：2013中第9.2条规定的内容为准。

9.4.2 信息访问限制

以ISO/IEC 27002中第9.4.1条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

组织应提前审查是否有必要利用查询语言处理PII，随后方可允许操作员和管理员等人士使用该语言在内含PII的数据库中自动批量检索PII。

如果对查询语言的使用符合保护要求，组织应采取技术性措施对该等语言的使用设限，仅为实现特定目的所必须时使用，使用范围越小越好。

据此，访问限制将查询语言的使用权限仅限于数据记录中少数经预定义的敏感领域。

如果有人要求访问通常不予授权访问的区域（如操作区域），则应通过更加严格的审批机制进行批准。组织应将审批程序记录在案并加以保存。

9.4.3 安全登录程序

以ISO/IEC 27002中第9.4.2条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

如果PII想PII控制方请求账户，PII应根据风险分析结果对这些账户设置安全登录程序。

9.4.4 密码管理系统

以ISO/IEC 27002中第9.4.3条规定及相关实施指南和其他信息为准。

9.4.5 对特许使用程序的使用

以ISO/IEC 27002中第9.4.4条规定及相关实施指南和其他信息为准。

9.4.6 对程序源代码的访问控制

以ISO/IEC 27002中第9.4.5条规定及相关实施指南和其他信息为准。

10 密码技术

10.1 加密控制

10.1.1 引言

以ISO/IEC 27002：2013中第10.1条规定的内容为准。

10.1.2 加密控制的使用方法

以ISO/IEC 27002中第10.1.1条规定及相关实施指南和其他信息为准。

10.1.3 密钥管理

以ISO/IEC 27002中第10.1.2条规定及相关实施指南和其他信息为准。

11 物理和环境安全

11.1 安全区域

11.1.1 引言

以ISO/IEC 27002：2013中第10.1条规定的内容为准。

11.1.2 物理安全边界

以ISO/IEC 27002中第11.1.1条规定及相关实施指南和其他信息为准。

11.1.3 物理登录控制

以ISO/IEC 27002中第11.1.2条规定及相关实施指南和其他信息为准。

11.1.4 办公室、房间和设施安全

以ISO/IEC 27002中第11.1.3条规定及相关实施指南和其他信息为准。

11.1.5 规避外部和环境威胁

以ISO/IEC 27002中第11.1.4条规定及相关实施指南和其他信息为准。

11.1.6 安全工作区域

以ISO/IEC 27002中第11.1.5条规定及相关实施指南和其他信息为准。

11.1.7 发送和载入区

以ISO/IEC 27002中第11.1.6条规定及相关实施指南和其他信息为准。

11.2 设备

11.2.1 引言

以ISO/IEC 27002：2013中第11.2条规定的内容为准。

11.2.2 设备选址和保护

以ISO/IEC 27002中第11.2.1条规定及相关实施指南和其他信息为准。

11.2.3 支援设施

以ISO/IEC 27002中第11.2.2条规定及相关实施指南和其他信息为准。

11.2.4 电缆安全

以ISO/IEC 27002中第11.2.3条规定及相关实施指南和其他信息为准。

11.2.5 设备维护

以ISO/IEC 27002中第11.2.4条规定及相关实施指南和其他信息为准。

11.2.6 资产移除

以ISO/IEC 27002中第11.2.5条规定及相关实施指南和其他信息为准。

11.2.7 （企业）外部设备和资产的安全保护

以ISO/IEC 27002中第11.2.6条规定及相关实施指南和其他信息为准。

11.2.8 设备安全处理或重新使用

以ISO/IEC 27002中第11.2.7条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

为实现安全处理或重新使用的目的，应按照业已界定和记录的方法使用经批准的技术（而非标准的删除或格式功能），销毁内含储存媒介（可能含有PII）的设备，或者销毁、删除或覆盖PII，让原始PII无法恢复。如果设备储存媒介内含已加密PII，则对解密密钥或密钥持有物（智能卡等）实施有效破坏也许就足够了。

11.2.9 自动化用户设备

以ISO/IEC 27002项下第11.2.8条规定及相关实施指南和其他信息为准。

11.2.10 清洁桌面和屏幕规则

以ISO/IEC 27002中第11.2.9条规定及相关实施指南和其他信息为准。

12 操作安全

12.1 操作方法和责任

12.1.1 引言

以ISO/IEC 27002:2013中第11.2条规定的内容为准。

12.1.2 操作方法记录

以ISO/IEC 27002中第12.1.1条规定及相关实施指南和其他信息为准。

12.1.3 变更管理

以ISO/IEC 27002中第12.1.2条规定及相关实施指南和其他信息为准。

12.1.4 能力管理

以ISO/IEC 27002中第12.1.3条规定及相关实施指南和其他信息为准。

12.1.5 开发、测试和操作环境分离

以ISO/IEC 27002中第12.1.4条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

开发、测试和操作环境在逻辑上和（如可能）在实际上应是分离的。应实施有效的访问控制，以确保访问权仅为被正式授权的一方所有。如果测试、研发网络或设备要求访问操作网络，则应实施更加严格的访问控制。

组织应评估包含PII的可移动媒体和无线设备在各类环境中的使用风险。

若未经法律许可或未经PII当事人明确同意，不得在PII当事人未匿名的情况下为研发和测试之目的使用PII。

12.2 恶意软件防护

12.2.1 引言

以ISO/IEC 27002:2013中第12.2条规定的内容为准。

12.2.2 防控恶意软件

以ISO/IEC 27002中第12.2.1条规定及相关实施指南和其他信息为准。

12.3 备份

12.3.1 引言

以ISO/IEC 27002:2013中第12.3条规定的内容为准。

12.3.2 信息备份

以ISO/IEC 27002中第12.3.1条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

PII信息处理系统应采用附加或备用机制，如保护PII数据免遭丢失的异地数据备份，这可确保PII处理操作的连续性，并且在极为必要的情况下，可保证PII处理操作在破坏性事件发生后进行储存备份。

注 – 数据备份和恢复操作间存在一定时间间隔。储存于备份文件中的PII在进行恢复评估时已非最新信息，任何基于非最新PII的操作都可能导致出现不正确的结果并带来隐私泄漏风险。

12.4 记录和监控

12.4.1 引言

以ISO/IEC 27002:2013中第12.4条规定的内容为准。

12.4.2 事件日志记录

以ISO/IEC 27002中第12.4.1条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

如可能，事件日志应记录如下信息：受到评估的PII类型、对该PII的处理方式（如读取、打印、增补、修改、删除等）、处理时间和处理方等，对特定类别的PII（如健康数据）而言尤应如此。如果有多个服务提供商提供服务，各方在实施该指南时发挥的作用可能相同也可能不同。

应采取措施，制定明确的书面审查周期对系统日志进行审查，以便发现故障并提出补救措施。

PII控制方应就管理员为实现特定目的（如进行安全监控或运行诊断）是否需要使用、何时使用及如何使用日志信息进行规定。

12.4.3 日志信息保护

以ISO/IEC 27002中第12.4.2条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

旨在实现安全监控和运行诊断等目的而记录的日志信息也许内含PII。应采取访问控制（参见第9.2.3条）等措施，以便确保日志信息仅用于实现预期目的。还应采取措施确保日志文件的完整性。

12.4.4 管理员和操作员日志

以ISO/IEC 27002中第12.4.3条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

各组织应监控（系统管理员或操作员的）PII特许访问权限以及该等人员随后进行的PII处理。该监控行为应构成对PII信息处理系统进行全面监控的一部分。

各组织应对异常活动状况进行明确，并且应实施自动化程序向该组织内的有关人员汇报该等异常活动。

12.4.5 时钟同步

以ISO/IEC 27002中第12.4.4条规定及相关实施指南和其他信息为准。

12.5 操作软件控制

12.5.1 引言

以ISO/IEC 27002:2013中第12.5条规定的内容为准。

12.5.2 在操作系统上安装软件

以ISO/IEC 27002中第12.5.1条规定及相关实施指南和其他信息为准。

12.6 技术缺陷管理

12.6.1 引言

以ISO/IEC 27002:2013中第12.6条规定的内容为准。

12.6.2 技术缺陷管理

以ISO/IEC 27002中第12.6.1条规定及相关实施指南和其他信息为准。

12.6.3 软件安装限制

以ISO/IEC 27002中第12.6.2条规定及相关实施指南和其他信息为准。

12.7 信息系统审计考量

12.7.1 引言

以ISO/IEC 27002:2013中第12.7条规定的内容为准。

12.7.2 信息系统审计控制

以ISO/IEC 27002中第12.6.2条规定及相关实施指南和其他信息为准。

13 通信安全

13.1 网络安全管理

13.1.1 引言

以ISO/IEC 27002:2013中第13.1条规定的内容为准。

13.1.2 网络控制

以ISO/IEC 27002中第13.1.1条规定及相关实施指南和其他信息为准。

13.1.3 网络服务安全

以ISO/IEC 27002中第13.1.2条规定及相关实施指南和其他信息为准。

13.1.4 网络分离

以ISO/IEC 27002中第13.1.3条规定及相关实施指南和其他信息为准。

13.2 信息转移

13.2.1 引言

以ISO/IEC 27002:2013中第13.1条规定的内容为准。

13.2.2 信息转移规则和方法

以ISO/IEC 27002中第13.2.1条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

应采取适当措施降低信息转移时的PII泄漏风险。通常，实施加密可以解决这一问题，其他主要措施包括去身份识别、掩蔽或模糊法。

13.2.3 信息转移协议

以ISO/IEC 27002中第13.2.2条规定及相关实施指南和其他信息为准。

13.2.4 电子消息

以ISO/IEC 27002中第13.2.3条规定及相关实施指南和其他信息为准。

13.2.5 保密或不可泄露协议

以ISO/IEC 27002中第13.2.1条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

各组织应对PII的外部处理条件进行规定。这些条件应构成有关协议的一部分（如合同、保密协议或不可泄露协议）。

14 系统采集、研发和维护

14.1 信息系统安全要求

14.1.1 引言

以ISO/IEC 27002:2013中第14.1条规定的内容为准。

14.1.2 信息安全要求分析和规范

以ISO/IEC 27002中第14.1.1条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

对PII信息处理系统进行重大变更时，应进行隐私影响评估（PIA）。隐私影响评估的实施指南参见ISO/IEC 29134。PIA评估结果应用来确定，应采用何种控制方法来控制PIA处理过程中出现的风险。

14.1.3 保护公用网络应用服务

以ISO/IEC 27002中第14.1.2条规定及相关实施指南和其他信息为准。

14.1.4 保护应用服务交易

以ISO/IEC 27002中第14.1.3条规定及相关实施指南和其他信息为准。

14.2 研发和支持进程安全

14.2.1 引言

以ISO/IEC 27002:2013中第14.2条规定的内容为准。

14.2.2 安全研发规则

以ISO/IEC 27002中第14.2.1条规定及相关实施指南和其他信息为准。

14.2.3 系统变更控制方法

以ISO/IEC 27002中第14.2.2条规定及相关实施指南和其他信息为准。

14.2.4 变更操作平台后进行应用技术审查

以ISO/IEC 27002中第14.2.3条规定及相关实施指南和其他信息为准。

14.2.5 软件包变更限制

以ISO/IEC 27002中第14.2.4条规定及相关实施指南和其他信息为准。

14.2.6 安全系统工程原理

以ISO/IEC 27002中第14.2.5条规定及相关实施指南和其他信息为准。

14.2.7 安全研发环境

以ISO/IEC 27002中第14.2.6条规定及相关实施指南和其他信息为准。

14.2.8 研发外包

以ISO/IEC 27002中第14.2.7条规定及相关实施指南和其他信息为准。

14.2.9 系统安全测试

以ISO/IEC 27002中第14.2.8条规定及相关实施指南和其他信息为准。

14.2.10 系统验收测试

以ISO/IEC 27002中第14.2.9条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

系统验收测试还应包括隐私保护要求测试。

14.3 测试数据

14.3.1 引言

以ISO/IEC 27002:2013中第14.3条规定的内容为准。

14.3.2 测试数据保护

以ISO/IEC 27002中第14.3.1条规定及相关实施指南和其他信息为准。

以下新增指南同样适用。

PII保护实施指南

通常，内含PII的操作数据不得用于研发和测试。在这些环境中使用真实的PII会增加信息泄漏风险。但是，各组织可以使用综合数据或采取措施（如掩蔽、模糊、去身份识别等方法）来“隐藏”任何拟使用的真实PII。

15 供应商关系

15.1 供应商关系信息安全

15.1.1 引言

以ISO/IEC 27002:2013中第15.1条规定的内容为准。

15.1.2 供应商关系信息安全政策

以ISO/IEC 27002中第15.1.1条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

若某一组织需要某PII处理方提供服务，该组织应评估该处理方的经验、可信度，以及其是否能够满足适用法律、法规、合同或其他法定协议规定的PII保护要求。

充当PII控制方的组织应和充当PII处理方的组织签署一份书面合同，该合同应清楚列明PII控制方和PII处理方的各项任务和职责，同时该合同应内含关于PII保护的条款，规定PII处理方在进行处理工作时所应承担的责任。

PII控制合同至少应包括以下内容：

– 关于合同项下PII处理之规模、性质和目的有关声明；
– 规定PII处理方有授予PII当事人PII访问权和审查权的义务，以及有处理PII当事人提起的任何投诉的义务。（参见A.10节）；
– 各组织为满足法律法规要求而采取的其他措施；
– 授权PII控制方对PII处理方处所进行审计；
– 出现数据泄露、未授权处理或其他违反合同条款和条件的情况时，该合同有义务进行报告，并应明确双方的联系人；
– PII控制方向PII处理方提出的指导方法；
– 合同终止时应采取的相关措施，特别是为安全删除（企业）内部PII或返还PII和物理媒介时应采取的相关措施。

PII控制方应确保，未经其事先批准，PII处理方不得对处理工作进行进一步分包（即，使用分处理器）。PII处理方应遵守与此相关的一切法律法规。

PII控制方应确保，PII处理方除为实现本合同或其他法定协议规定的目的而处理PII外，不为其他任何目的处理PII。

PII控制方应确保，PII处理方能够根据PII控制方的政策或其他指示对PII进行安全处理。（如根据特定机构的要求进行处理）

15.1.3 解决供应商协议中的安全问题

以ISO/IEC 27002中第15.1.2条规定及相关实施指南和其他信息为准。

15.1.4 信息和通信技术供应链

以ISO/IEC 27002中第15.1.3条规定及相关实施指南和其他信息为准。

15.2 供应商服务交付管理

15.2.1 引言

以ISO/IEC 27002:2013中第15.2条规定的内容为准。

15.2.2 供应商服务监控和审查

以ISO/IEC 27002中第15.2.1条规定及相关实施指南和其他信息为准。

15.2.3 供应商服务变更管理

以ISO/IEC 27002中第15.2.2条规定及相关实施指南和其他信息为准。

16 信息安全事件管理

16.1 信息安全事件管理和完善

16.1.1 引言

以ISO/IEC 27002:2013中第16.1条规定的内容为准。

16.1.2 责任和方法

以ISO/IEC 27002中第16.1.1条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

各组织应能够对隐私泄漏事件进行（并准备进行）有组织的且有效的回应。据此，各组织应制定并实施隐私泄漏事件应急预案。

隐私泄漏事件应急预案应包括以下内容：

a) 隐私泄漏事件的定义及隐私泄露事件回应的范围；

b) 建立跨部门的隐私泄漏事件应对小组，由该小组制定、实施、测试、执行和审查隐私泄漏事件应急预案（该计划应由组织内的高级管理人员批准实施）；

c) 明确隐私泄漏事件应对小组每位组员的任务、责任和权利；

d) 若出现跨境隐私泄漏事件，则该预案应负责解释与境外组织开展合作所需的各项法律依据；

e) 确保受内部隐私政策管辖的人员（如雇员、承包商等）能够依照组织内泄密管理指导方案，及时向信息安全员和PII保护员（有时系指首席隐私官（CPO））汇报隐私泄漏事件；

f) 进行事件影响评估（任务），以便确定受影响方或组织将似遭受的潜在或实际损害的性质和程度（如因之而产生的窘境、不便或不公等）；

g) 采取必要措施，减轻上述损害，降低损害性事件再度发生的可能性。

h) 确定是否需要向受影响人员和其他指定实体（如管理者）发送通知，确定通知发送的时间和通知的形式，适当时，还需要提供该通知。

各组织可以选择将隐私泄漏事件应急预案和安全事件应急预案结合在一起，也可以让二者相互独立。根据信息安全事件管理程序，信息安全事件发生时，PII控制方需要对其进行审查，以确定是否发生了PII数据泄漏事件。

信息安全事件发生时，PII控制方可能不会展开审查。信息安全事件包括但不限于：对防火墙或边缘服务器的Ping命令攻击或其他广播攻击、端口扫描、不成功登录、拒绝服务攻击和数据包嗅探。信息安全事件并不必然导致PII出现可能或实际的泄漏，或导致PII处理设备或设施出现可能或实际的信息泄漏。

16.1.3 报告信息安全事件

以ISO/IEC 27002中第16.1.2条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

PII遭到泄漏时，只有立即采取措施才能保护PII当事人的权利和利益。

各管辖地区可规定PII安全事件（如未授权处理、违约等行为）报告或通知的具体要求（如立法或制定法规等）。PII安全事件发生时，应尽快向有关部门通知事件明细，包括组织提出的应急预案（应急预案披露时需考虑某些限制性因素）。上述有关部门包括数据保护部门、执法机关和受该事件影响的企业等。

PII当事人在受到隐私泄漏事件影响后，有关组织应采取有效的补救措施进行补救，例如对错误信息进行纠正或删除。

16.1.4 报告安全漏洞

以ISO/IEC 27002中第16.1.3条规定及相关实施指南和其他信息为准。

16.1.5 信息安全事件评估和决策

以ISO/IEC 27002中第16.1.4条规定及相关实施指南和其他信息为准。

16.1.6 应对信息安全事件

以ISO/IEC 27002中第16.1.5条规定及相关实施指南和其他信息为准。

16.1.7 从信息安全事件中获取经验

以ISO/IEC 27002中第16.1.6条规定及相关实施指南和其他信息为准。

16.1.8 证据收集

以ISO/IEC 27002中第16.1.7条规定及相关实施指南和其他信息为准。

17 业务连续性管理的信息安全视角

17.1 信息安全连续性

17.1.1 引言

以ISO/IEC 27002:2013中第17.1条规定的内容为准。

17.1.2 设计信息安全连续性

以ISO/IEC 27002中第17.1.1条规定及相关实施指南和其他信息为准。

17.1.3 实施信息安全连续性

以ISO/IEC 27002中第17.1.2条规定及相关实施指南和其他信息为准。

17.1.4 验证、审查和评估信息安全连续性

以ISO/IEC 27002中第17.1.3条规定及相关实施指南和其他信息为准。

17.2 信息冗余

17.2.1 引言

以ISO/IEC 27002:2013中第17.2条规定的内容为准。

17.2.2 信息处理设施的可用性

以ISO/IEC 27002中第17.2.1条规定及相关实施指南和其他信息为准。

18 合规性

18.1 遵守法律和合约要求

18.1.1 引言

以ISO/IEC 27002:2013中第18.1条规定的内容为准。

18.1.2 明确适用立法和合约要求

以ISO/IEC 27002中第18.1.1条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

各组织应明确对其适用的、关于PII保护的法律和法规。如果已经明确，那么各组织应针对这些要求采取必要措施。以下情况为此类要求的示例。

a) 某些PII种类（例如身份证号码、护照号码或信用卡号码）如果需要额外保护，则应对其使用加密技术。应选取所需加密算法的类型、强度和品质。

与该要求有关的安全控制规定在10.1.2节。

b) 各辖区可规定包含PII信息的最低备份次数，以及最低备份检查和恢复次数。

与该要求有关的安全控制规定在12.3.2节。

各组织应开展隐私影响评估，实施隐私处理方案，从而帮助确保各项涉及PII处理的项目和服务符合隐私保护要求。进一步指导参见ISO/IEC29134。

各组织应制定审计方案，以便核实PII处理是否遵循相关的隐私保护要求。审计方案应规定审计工作的拟实施频率。

审计工作可以由组织开展（如通过组织内部的审计部门开展），此外，审计工作还可由有资格的独立第三方开展。

关于PII保护的其他信息

在许多管辖地区，尽管正是PII控制方对确保合规承担最终责任，但是PII处理工作的全部参与者均应积极面对并努力识别法律或其他因素引起的相关隐私保护要求。

PII控制方和PII处理方签署的合同对创建合规机制作出规定，该机制确保PII处理方对相关合规进行支持管理。合同要求有关方面以PII处理方接受的方式对合规性进行独立审计，即通过本规范、ISO/IEC 27002和ISO IEC 27018中规定的相关控制进行操作。

18.1.3 知识产权

以ISO/IEC 27002中第18.1.2条规定及相关实施指南和其他信息为准。

18.1.4 记录保护

以ISO/IEC 27002中第18.1.3条规定及相关实施指南和其他信息为准。

18.1.5 隐私和个人可识别信息保护

以ISO/IEC 27002中第18.1.4条规定及相关实施指南和其他信息为准。

18.1.6 加密控制规则

以ISO/IEC 27002中第18.1.5条规定及相关实施指南和其他信息为准。

18.2 信息安全审查

18.2.1 引言

以ISO/IEC 27002:2013中第18.2条规定的内容为准。

18.2.2 信息安全独立审查

以ISO/IEC 27002中第18.2.1条规定及相关实施指南和其他信息为准。以下新增指南同样适用。

PII保护实施指南

如果有关方面进行的审计工作并非切实可行，或者可能增加安全事故风险，组织应在合同签署前向未来的有关方面提供相关证据，证明信息安全是按PII控制方的政策和方法实施操作的。通常，PII控制方选择的相关独立审计应允许有关方面对PII控制方的处理操作进行审查，只要透明度得到了保证，该审计就能够为有关方面所接受。

18.2.3 遵守安全政策和标准

以ISO/IEC 27002中第18.2.2条规定及相关实施指南和其他信息为准。

18.2.4 技术合规审查

以ISO/IEC 27002中第18.2.3条规定及相关实施指南和其他信息为准。

附件A

个人可识别信息（PII）保护补充控制

（本附录构成本建议|国际标准书中的一部分）

A.1 总则

本附录对新目标、新控制以及新实施指南进行了定义。这些新目标、新控制以及新实施指南构成一个补充控制，以满足PII保护方面的特殊要求。

本规范中的指南以国际标准化组织（ISO）29100:2011中的指南为基础，并假定ISO中的指南已经得以执行。

A.2节描述了PII保护总政策，而后续条款则反映了国际标准化组织（ISO）/国际电工委员会（IEC）29100中的隐私权原则。

A.2 PII应用与保护总政策

目标：依据商业要求及相关法律法规，为PII保护提供管理方向与支持。

控制

涉及PII处理的组织应当在PII应用与保护方面建立一项政策。

PII保护实施指南

隐私规则应该包括有关声明（关于独立的隐私政策或对现有政策进行补充的声明），支持并承诺让人们严格遵守适用的PII保护法、各项合同要求和内部规则。

隐私政策和安全政策虽然密切相关，但其涵盖的议题或有不同。信息安全政策和隐私政策二者应该处理信息的机密性、完整性和可用性。此外，隐私政策应处理同意和个人访问等问题。

ISO/IEC 29100为隐私权的实施框架提供了指南。PII保护政策应当满足以下几点：

– 切合组织目的；
– 使组织搜集、整理PII 的过程公开透明；
– 为设立PII保护目标提供框架；
– 针对PII保护方面的问题决策确立规则；
– 为隐私风险接受确立标准（也可见ISO/IEC29134的6.3.1节）；
– 包含一项承诺，满足目前适用的隐私权保护要求；
– 包含一项持续改进的承诺；
– 组织的成员之间保持通讯联系；
– 可酌情对利益相关方发挥作用。

A.3 许可与选择

A.3.1 许可

目标：除另有法律法规的限制，否则应通过组织有意义的、消息灵通的、自由给予许可的活动来使PII当事人积极参与PII处理进程。

控制

除PII当事人不能自由拒绝许可，或适用法律明确允许未经当事人同意进行PII处理，否则组织应当提供必要手段，使PII当事人能够获取有意义的、消息灵通的、清楚的、自由给予的许可。

PII保护实施指南

组织应当做到如下几点：

a) 为确保在任何处理开始前获得许可，应确立并实施实用手段，以得到PII当事人的许可及进行案例（即所选实用手段无法投入使用的案例）分析，在必要情况下，确立替代解决方案；

b) 为确保在任何处理开始前获得许可，在可行的、合适的或法律允许的情况下，组织应当提供手段使PII当事人提供许可。处理过程包括：PII收集、存储、变更、检索、磋商、公开、去身份识别、匿名化处理、传播或对PII进行适当的删除或销毁处理；

c) 若许可是由一个法定代理人（例如代表儿童或经法律认定丧失能力的人）提供的，组织应当储存许可记录；

d) 在必要的情况下，通知所有将PII转移至第三方的当事人，并提供适当手段使PII当事人为这种转移提供他们的许可。

e) 在可行的、合适的或法律允许的情况下，在使用和公开以前收集的PII之前，先得到PII当事人的许可，并保证这些许可是在任何进一步处理开始前获取的；

f) 确保许可是在PII处理目的为人所知、公开透明的情况下获取，并保证获得这种许可是有特殊目的；

g) 提高公众意识，获得公众许可（例如通过更新公众通知的方式）；

h) 为PII当事人提供一个机制，以便他们修改许可范围。任何对许可的修改都应当及时进行，并且人们应当依据修订后的许可，对处理进程进行修改或终止；

i) 确保许可遵循所有适用法律要求，包括在适当情况下对敏感PII的明确许可的要求；

j) 在适当情况下，允许默认同意。当PII当事人已对处理过程有清楚认识且未提出反对意见时，这种情形也许表明当事人同意；

k) 在所有处理操作实施前先给出通知；

l) 在有需要的情况下，对PII当事人或其授权代理人的身份进行核实，向处理进程提交许可。得到的用于证明的信息应按照相应的目的的最低要求标准被保留，只有信息有必要用于相应的目的时才能得以保留，不被需要时应得到安全处置。

关于PII保护的其他信息

组织应当依据适用法律，通过可选择式或默认同意的方式获得许可。可选择式许可是首选方式，但并不是一直可行。可选择式许可要求PII当事人用平权法案允许组织收集或使用PII。当人们通过使用电子媒介来收集许可时，组织应当考虑，是需要单向确认还是双重选择性加入。

有了选择性退出机制，除非PII当事人用平权法案来告知，否则组织可假设PII当事人已经明确允许对他们的PII进行处理。

默认同意通常可经一个人的作为或不作为进行推断。举一个默认同意的例子：顾客将收货地址告知网上零售商，零售商便会在为顾客送货时按照惯例地用到这个地址信息。

当收集到国家身份编号（例如社会保险号码、居民登记号码、护照号码）时，组织应当实施实用手段来获得PII当事人的独立许可。

组织也许提供，例如， PII当事人的项目选择（这些项目选择是关于PII当事人是否愿意在一些情况下被取得联系）。在此种情况下，组织建立许可机制来保障组织运作尽可能遵照PII当事人的项目选择。

许可可为电子版或打印版，这取决于适用的法律法规要求和实际情况。

当PII被传至另一个组织或从另一个组织传来时，组织应当建立程序来更新他们的记录，以反映由PII当事人产生的内容更新与许可变更（例如修改、吊销），并确保这些更新/变更被传至与该组织分享PII的组织。只有少量信息（这些信息对确保正确记录的更新来说有必要）应当从PII当事人那里收集并与其他机构分享。组织应当定期地审查进程，以确保它们没有处理无关紧要的PII。

A.3.2 选择

目标：当选择不允许处理他们的PII，拒绝或撤回许可，或抵制一种特殊类型的处理时，组 织在适当的、可行的情况下告知PII当事人，并向PII当事人解释同意或拒绝许可带来的影响。

控制

除非PII当事人不能自由地拒绝给出许可， 或适用法律特意允许未经PII当事人许可进行PII处理，否则组织应当为PII当事人提供清晰明了、不可或缺、通俗易懂、便于使用、价格合理的机制，让他们对自己的PII处理做出选择。

PII保护实施指南

组织应当做到如下几点：

a) 确保在任何处理进行之前，PII当事人对他们的PII处理做出的选择能够奏效；

b) 当PII当事人提供与该服务有关的PII时，组织为该当事人提供服务；

c) 在相关法律法规允许的情况下，组织应当制定并实施一些措施，使PII当事人能够有权反对个人PII被处理，并给予PII当事人多种方法（例如邮寄信件、电子邮件、电话联系）保障他们对权利的行使；

d) 组织收到异议声明后，应当在适用法律或组织政策中规定的期限内告知已收到；

e) 当所选的实用手段不可使用时，组织应当对此情况进行分析，并确定备份解决方案，在有必要的情况下，允许PII当事人继续及时行使权利反对PII处理；

f) 组织应确保PII的归类、标签、存储有利于PII当事人行使权利反对PII处理，并确保PII当事人能够及时免费行使反对权；

g) 对PII当事人或其授权代理人的身份进行核实，向处理进程提交异议。得到的用于证明的信息应按照相应的目的的最低要求标准被保留，只有信息有必要用于相应的目的时才能得以保留，不被需要时应得到安全处置；[在以上内容中有所重复]

h) 如果反对权的行使要求法律依据，确保PII当事人在提供合理异议依据时行使反对权。组织对任何异议的回绝，都应当详述理由，即为何PII管理者认为这些异议依据不合法；

i) 确保与该组织分享PII的组织能够意识到PII当事人提交的异议，并且确保这些组织能够接受有价值的异议；以及

j) 在可能的情况下，使PII当事人有能力选择反对PII处理的某些方面，而不是让他们全盘接受或否决处理过程。

关于PII保护的其他信息

在很多情况下，根据适用法律，提供一个机制让组织在收集公开信息时做出选择，这种做法没有必要，而且行不通。例如，在从公众记录或报纸上收集PII当事人的姓名和地址时，没有必要提供一个可选择机制。

A.4 目的合法性与规范

A.4.1 目的合法性

目标：确保PII的处理目的遵守适用法律，且有法律依据。

控制

组织应当采取恰当措施，以确保PII的处理目的遵守适用法律，且有法律依据。

PII保护实施指南

组织应当做到如下几点：

a) 组织应当确定决议处理是否除了经许可之外，还可以在法律依据（例如法律实施、公共安全、PII管理者的法律义务或正当利益）的基础上进行；

b) 确定是否通过法律依据（例如法律实施、公共安全或法律义务）来管理决议处理，这些法律依据禁止PII当事人在关于对他们的PII处理方面做出选择；

注 – 如果在国际上进行PII处理或收集，所需的许可和进行方式可能因各地区法律制度而异。

c) 确定法律权力（依据）允许PII处理，这种法律权力（依据）可以是概括性的，或支持一项特定程序或信息系统；

d) 包含一些程序，以确保PII处理依照所有适用法律法规及主管机关对法律法规的解释。当确定处理目的的合法性时，应考虑处理进程的大致背景，包括PII管理者与PII当事人之间潜在关系的类型、科技发展水平，以及社会与文化态度变化。

组织应当设立一些程序，以确保PII的处理方式不违背且不存在违背法律义务（包括法律条文、习惯法或合同条款）的可能。

如果组织拥有一个劳资联合委员会或工会，根据适用法律，组织可能会在建立目的的合法性时，与该类团体进行协商，以保障职员的权益。

关于PII收集的任何项目或活动的授权，项目官员应与负责PII保护的人员（有时称作CPO）或资格相当的法律顾问进行商议。有关PII收集的授权应当备有证明文件。

A.4.2 目的规范

目标：在收集PII之前，明确提出收集PII的目的，并对原有目的的后续落实进行限制。

控制

组织应向PII当事人传达PII收集和处理的目的。如果之前未向PII当事人传达过有关PII收集和处理的目的，那么应在收集PII时（或之前），以及处理PII之前向PII当事人传达有关消息。

PII保护实施指南

在信息首次被收集或用于一个新的目的之前，组织应当向PII当事人传达这项（或这些）目的，用清晰且适用于实际情况的语言书就规范细则，并对处理敏感PII的需要给予充分解释。

通常，法律措词对具体的PII收集和使用进行明确批准。当法律措词书就得很宽泛并涉及翻译时，组织应当与CPO和法律顾问进行商议，以确保有关PII收集的概括授权和明确授权之间有清晰的关联。

一旦明确了具体目的，组织应当在相关的用于PII收集的隐私合规性文件中，或以其它形式写明目的。为进一步避免未经批准收集或使用PII的行为，PII管理人员应接受由组织部门给予的有关PII收集方面的培训。

组织应当做到如下几点：

a) 明确规定PII仅用于各项业务流程；

b) 以合理的方式，将用于各项业务流程的PII进行区分；

c) 依据业务流程（包括薪资管理、休假申请管理以及职业晋升）管理访问权限，并为处理最敏感PII的系统创建一个专用的IT环境；

d) 定期证实PII是被有效区分，且接受器与互连未被添加。

A.5 收集限制

目标：将PII的收集限制在适用法律的范围内，这对于特定的PII收集目的非常必要。

控制

组织应当实施有效措施，将PII的收集类型与收集数量限定在通知（见A.9.1）中规定的目的的最小元素，并限定在适用的法律法规范围内。

PII保护实施指南

组织应当做到如下几点：

a) 经PII当事人许可，将PII的收集限定在通知（见A.9.1）中规定的目的的最小元素；

b) 未经法律授权或许可，不得进行敏感PII收集；

c) 对直接或间接（间接方式包括：通过网络日志、系统日志等方式获得）从PII当事人处收集的信息进行限制。

组织应当明确PII处理的目的，识别出哪些PII对实现目的是有用的，哪些信息是不必要收集的，并证实仅收集必要信息。

在收集PII之前，组织应当慎重考虑需要收集哪些PII来达到一个特殊目的，而不是盲目收集。

组织应当定期审查收集PII的目的，以保证这些信息的有效性。组织也应定期审查他们收集的PII，以确保这些信息仍然是目的的最低要求标准。

除经法律授权或得到明确许可，否则组织不得进行敏感PII（例如身份证号码）收集。

有关PII 保护的其他信息

一些管辖区域也许会将一定类别的PII（例如族源、政治见解、宗教或其他信仰、个人健康数据、性生活或犯罪记录等）定义为敏感PII。这些管辖区域会对这类PII的收集进行限制，因此组织在考虑收集哪些PII信息时应考虑这些限制因素。

A.6 数据最小化

目标：令PII数据最小化，使其仅满足PII管理者的正当利益，并使PII的公开仅涉及最少数量的隐私利益相关者。

控制

组织应当实施有效措施使处理的PII数据的数量降到最低，使其仅满足PII管理者的正当利益。例如，一个组织可能会以正当方式增大它的PII处理量和存储量，以增加或拓展其经营活动。

PII保护实施指南

组织应当做到如下几点：

a) 确保采用“须知原则”，例如，一个人只能在PII处理正当目的的框架内访问PII，且该PII对其执行公务是有必要的；

b) 使用或提供违约选择权，在可能的情况下，进行合作或交易，只要不涉及PII当事人的身份证明即可；

c) 对所收集的PII的链接性进行限制；

d) 对组织保存的PII实行初步评审，并建立、遵循一个计划表，以便定期审查，确保只收集通知当中规定的PII，且这些PII继续对完成当前商业目的有必要；

e) 限制含有PII的电子文件的传送，使其仅能提供给最少数的利益相关者，这些利益相关者会在他们的工作中用到PII；

f) 根据实际情况确定哪些PII应当是匿名的或去识别化的、PII的储存方法（例如数据库域或文本节选）、以及识别到的风险；

g) 将一些数据和已识别到的风险去识别化，这些数据要求这种去识别化，且这种去识别化建立在需要被去识别化的数据形式（例如数据库和文字记录）的基础上。

h) 只要PII处理的初衷不复存在，如果法律不要求保留这些PII或只要可以如此行事，则应删除或销毁PII；以及

i) 考虑是否使用、使用何种隐私增强技术（PET）。

要求支持特殊组织业务流程的PII元素的最小集合，也许是组织被授权采集的PII的子集。

PII应分为强制性收集的PII和选择性收集的PII。组织收集的强制性PII应仅用于提供服务，在收集选择性PII时，应得到适当的选择性加入许可。在PII当事人拒绝给出选择性PII时，组织也应为PII当事人提供服务。

CPO与法律顾问应当要求项目官员证明提议PII处理的合理性，以确保信息系统或实现合法授权的目的的活动对PII处理的需求程度最低。

注1 – ISO/IEC 29100中将匿名化定义为一个流程，在此流程中，通过PII管理者单独操作或与任何一方合作的方式，使用一种方法，令PII的更改不可逆转，PII当事人再也不能直接或间接被识别。这种流程必定会导致（不可逆转的）信息丢失。在一些情况下，简单地对数据进行部分删除可能会达到理想目标。

注2 – 未来准备制定一份国际标准来描述一种隐私-增强数据去识别化技术，这种技术用来根据ISO/IEC 29100中的隐私原则描绘和制定去识别化措施。通常来说，为使去识别化流程遵从法律，去识别化通过属性删除和属性泛化及严格的组织和技术措施来实现。

注3 – 当出于某种目的对PII进行处理时，应将PII处理范围最小化，使其仅用于该种目的，切勿过多泄露关于PII当事人的信息。例如，如果需要交通调查申请者的地理区域信息，可以考虑仅收集附近的地标信息，而不是收集确切的地址信息。

注4 – 通常，在分析匿名资料时，如果输出结果只是小型数据集，可能会暴露PII当事人的身份。针对此种情况，一个比较妥当的做法是，当记录的数量低于阈值数（10个记录）时，阻止结果输出。阈值应当在数据分布模式的基础上谨慎达到。

在适当情况下，组织也应减少PII存储量，以减轻隐私与安全风险。组织应在可行的情况下，尽最大可能对他们持有的PII进行初步审查和随后审查，以确保数据栈的准确性、相关性、及时性和完整性。

组织也应当使持有的PII尽可能少用于备案的组织商业目的。组织应当制定并推广一个计划表，以定期检查数据栈，对初步审查进行补充。

组织通过定期评估来减小风险，以确保仅收集通知中指定的数据，并确保所收集的数据的相关性和必要性。

A.7 使用、保留与公开限制

A.7.1 使用、保留与公开限制

目标：对用于具体的、明确的、合法目的的PII使用与保留进行限制，实现声明目的或配合适用法律后，不应再保留这些PII。

控制

组织应当实施合理措施，对用于合法、预期目的的PII的处理进行限制，当实现声明目的或配合适用法律后，不应再保留这些PII。

PII保护实施指南

组织应当做到如下几点：

a) 对PII的使用、保留与公开（包括转移）进行限制，使其仅为实现具体的、明确的、合法目的的；

b) 设置PII信息系统，以便在PII收集、创建、更新PII时记录数据，以及在批准的记录保留计划中对PII进行删除或存档时记录数据。

PII保护使用实施指南

组织应当做到如下几点：

a) 当声明目的已完成但适用法律要求保留PII时，对PII进行封锁（即存档、保障安全、不再进行进一步处理）；

b) 使用恰当的技术或方法，以确保安全删除或销毁PII（包括原版、副本以及存档记录）；

c) 仅将PII用于批准的目的，或在PII收集时（或之前）告知PII当事人，并在任何用于新用途的处理开始之前，在必要的情况下，在处理PII之前征得当事人的同意；

d) 外部第三方仅在极为必要且被正式授权的情况下才可访问组织系统和PII。若有商业原因确实需访问组织系统和PII，应遵循恰当的批准程序；

e) 证实经允许与组织系统连接的第三方系统已在经允许连接之前采取了恰当的保护措施；

f) 定期审查第三方实施的保护措施，以确保它们符合组织的安全要求。若审查结果显示第三方的保护措施不合格，则中断第三方与组织系统的连接，直到其安全措施得以恢复；

g) 如果PII访问是通过远程接口进行的，应建立合适的访问认证机制。对PII访问日志进行记录；

h) 如果所收集到的PII在安全监控过程中发生变化，要发出通知以告知公众。

PII保护保留实施指南

可能会出现这种情况：特殊商业目的已完成，但法律仍要求保留PII结果。那么组织应当：

a) 只在授权时间期限内保留PII，以达到法律和组织的要求，或实现通知中指定的目的，并在保留期满后立即删除PII；

b) 当完成特殊商业目的后，如果仍要求保留PII，应实施一些有效措施（例如通过去识别化对PII实行保护）；

c) 确定PII的保留期限，使其具有时间限制，并且适合某个处理目的；

d) 证实信息系统能发现保留期已满；

e) 确保经允许的保留期限得以落实，并依据保留期限对PII进行处置；

f) 赋予系统自动化功能，使其能够将保留期满的PII删除。这种删除应当在可行的情况下立即进行；

g) 根据实际情况、PII存储形式（包括数据库域或文本节选）以及识别出的风险，确定对哪些内容进行去识别化；

h) 将一些数据和已识别到的风险去识别化，这些数据要求这种去识别化，且这种去识别化建立在需要被去识别化的数据形式（例如数据库和文字记录）的基础上；

i) 如果那些数据不能被去识别化，则选择所需的工具（包括部分删除、散列法、密钥散列及指数）来保护PII。

PII保护公开实施指南

组织应当做到如下几点：

a) 除非有相关法律法规允许，否则在PII当事人不知情和未同意的情况下，组织不得将PII向第三方公开。如果向组织内部有须知原则的人士（例如职员）公开PII，可能不需PII当事人的知情和许可；

b) 当进行PII转移时，组织应提供强有力的保护机制（包括数据加密和完整性保护）。

职员PII的处理（即安全删除或存档）也应当根据相关的法律法规，并根据组织处理政策，在适当的情况下，应征得职员的同意。

A.7.2 临时文件的安全删除

目标：为特定时期内删除临时文件提供技术措施。

控制

应在指定的、备有证明文件的期限内，对含有PII的临时文件和文档进行处理。

PII保护实施指南

信息系统在它们正常运行时产生含有PII的临时文件。这类文件具有系统和应用特性，但也许包括带有回滚能力的文件系统，以及临时文件，这些临时文件与数据库更新和其他应用软件的运行相关联。当相关的信息处理任务完成后，通常不再需要临时文件，但在某些情况下，这些临时文件不会自动删除。这些文件的使用时间长短是不确定的，但一个“垃圾收集”程序应识别出相关的临时文件，并确定它们距离最后一次被使用已有多长时间。

PII处理信息系统应当进行定期检查，确保将用过的临时文件在超过指定期限后删除。

A.7.3 PII公开通知

目标：确保PII处理者将有关PII公开的法律约束要求告知PII管理者。

控制

除非另有法律禁止这种PII公开，否则PII管理者与PII处理者之间的合同应要求PII处理者按照合同中约定的程序和时间，将法律或其他权威机构规定的有关PII公开的法律约束要求告知PII管理者。

PII保护实施指南

组织应当实施措施（例如合同义务）确保：

a) 除非另有法律禁止这种PII公开，否则在接受有关PII公开的法律约束要求之前，PII处理者应征求相关的PII管理者的意见；

b) 除非另有法律禁止，否则PII处理者应接受由相关PII管理者授权的任何有关PII公开的合同约定要求。

A.7.4 PII公开情况记录

目标：确保对PII向第三方公布的情况进行记录。

控制

PII向第三方公布的情况应当有记录，包括公布开内容、向谁公开、公开时间以及公开目的。

PII保护实施指南

PII可能在系统正常运行期间被公开，这些公开情况应有记录。任何向第三方公开PII的情况（例如为了合法调查与外部审计）都应有记录。这些记录当中应包括将PII进行公开的原因，以及向哪些机构公开了PII信息。

A.7.5 分包PII处理公开

目标：确保PII处理者向PII管理者公开任何使用分包商的情况。

控制

在PII处理者使用分包商进行PII处理之前，应将这种使用情况告知PII管理者。

PII保护实施指南

PII处理者和PII管理者应在合同中写明有关使用分包商处理PII的条款。合同中应当指明，经PII管理者事先授权后，PII处理者才可使用分包商。PII处理者应当及时将预期变化告知PII管理者，以便PII管理者可以反对这些变化或终止许可。

公开的信息应当包含使用分包的事实以及相关的分包商的名字，但不是业务具体细节；还应包括国家（分包商可能在哪个国家进行数据处理），以及分包商使用哪些方法来完成或超出PII处理者的义务。

当公开有关使用分包商的信息被认定会将安全风险增大到无法接受的程度时，应在保密协议和/或PII管理者的要求下进行公开。PII管理者应当知道所使用分包商的信息是可用的。

A.8 准确性与质量

目标：保障处理的PII对于使用目的来说具有准确性、完整性、最新性、适用性和相关性。

控制

组织应当采取恰当的措施，确保无论是直接地还是间接地从PII当事人那里采集到的PII，质量都能过关。

PII保护实施指南

达到数据质量，即处理的PII对于使用目的来说具有足够的准确性、完整性、最新性、适用性和相关性。

组织应当做到如下几点：

a) 建立PII收集程序，以帮助保障准确性与质量；

b) 收集PII时使用一种方法，以便在PII离开权威性数据源后，PII发生的任意变更仍能被发现；

c) 在收集和创建PII时，如果可行，尽最大可能证实PII的准确性、相关性、及时性和完整性；

d) 在处理PII之前，保障PII的可靠性，这些PII是从权威性数据源和PII当事人那里收集的；

e) 在适当的情况下，在对PII做出改变之前，通过恰当的方法证实PII当事人所提出的修正要求的正确性与合法性；

f) 定期检查，在必要的情况下，对于程序或系统所使用的错误的或过期的PII进行纠正；

g) 制定相应指南，并尽最大可能确保所传播信息的准确性、完整性、适当性和相关性。组织应当采取合理的步骤证实PII的准确性。这些步骤可能包括，例如，当收集到地址，或地址进入信息系统时，使用自动地址验证查找工具——应用程序接口（APIs），对地址进行编辑，并使其生效。

当PII具有足够敏感的属性，例如，当其用于一个纳税人的经常性收益收入的年度确认时，组织应当将机制并入信息系统，并确立相应的程序解决如下问题：信息多久更新一次，用什么方法更新信息。

尽可能将数据错误的范围缩至最小，PII应由PII当事人直接录入信息系统，而不需要别人对数据进行转录。但在有些情况下PII转录在所难免。组织应当使PII当事人能够证实转录的PII。这有利于在间接损害发生前纠正错误，这些间接损害由错误PII的处理导致。

关于PII保护的其他信息

保护数据质量所采取的方法类型可能取决于PII的属性与实际情况，即PII的使用方法和获得途径。证实敏感PII的准确性所采取的措施，要比证实敏感性较低的PII所采取的措施更加全面。如果PII是从除了PII当事人或PII当事人的授权代理人以外的地方获得的，那么需要使用额外的程序证实PII的准确性。

A.9 公开、透明与通知

A.9.1 隐私权通知

目标：确保使用简明语言书写带有适当程度细节的隐私权通知，使其通俗易懂。

控制

组织应当采取恰当措施，适时告知PII当事人PII处理的目的。

PII保护实施指南

组织应当做到如下几点：

a) 有效地将以下内容告知PII当事人：对PII当事人隐私造成影响的活动（包括但不限于PII的收集、分享、安全保护、以及安全处置）；PII的收集授权；对选择做出判断，依据是，组织如何使用PII以及落实或不落实这些选择可能带来的结果；具备向PII处理提出反对意见的能力；

b) 提供量身定制的通知与许可机制，以满足组织运转需要；

c) 在实践或政策发生变化之前，或发生后在可行的情况下尽快对通知进行修订，以反映这些变化，因为这些变化会影响PII或改变PII的活动，影响到隐私；

d) 确保通知的完整性，并确保通知适用于目标受众，这些目标受众以PII属性、通知所采取的实用手段、以及PII管理者和PII当事人之间的关系属性为基础；

e) 以清晰的方式呈现信息，使不熟悉信息技术、互联网或法律术语的人也能理解；

f) 确保在PII收集时或收集之前发出通知；

g) 确保在通知发出后再进行PII采集；

h) 当实用手段不发挥作用时，确定备选解决方案；

i) 在可能的情况下，使用一种方法证实通知已发布；

j) 若隐私权通知是以物质手段呈现的，组织应将通知张贴在PII当事人能够看到的地方，或要求对通知或文件进行签字或草签；

k) 为有关标志或符号的条款出台一项政策，这些标志或符号用于告知PII当事人相关的技术[即闭路电视（CCTV）系统、WiFi以及射频识别（RFID）]的使用。

在可能的条件下，应将通知置于明显的PII收集点（例如置于组织的网站或实际位置），而不用由PII当事人作出具体要求。

A.9.2 公开透明

目标：关于对PII的处理，组织应向PII当事人呈现清晰易懂的信息，信息内容包括PII管理政策、程序以及实践。

控制

组织应当采取恰当的措施，针对PII的处理，向PII当事人呈现清晰易懂的信息，信息内容包括PII管理政策、程序以及实践。

PII保护实施指南

组织应当做到如下几点：

a) 关于对PII的处理，组织应向PII当事人呈现清晰易懂的信息，信息内容包括PII管理政策、程序以及实践；

b) 将选择与手段进行公开，这些选择与手段由PII管理者提供给PII当事人，目的是限制信息处理，以及为了访问、收集和消除PII当事人的信息。

此外，组织应当对以下内容进行说明：

a) 组织所收集的PII，以及收集PII信息的目的；

b) 组织内部如何使用PII；

c) 组织是否同第三方分享PII，如果分享，应说明第三方组织的类别，以及分享的原因；

d) PII当事人是否有能力对PII的特殊用途或分享给予许可，有以及如何给予这类许可；

e) PII要被保留多久；

f) 组织是出售数据，还是依据数据分析组织与PII风险详细资料对数据进行进一步加工；

g) 在适当的情况下，PII当事人怎样访问PII，以对PII进行修改和校正；

h) 提供恰当的信息，即如何保护PII；

i) 确保PII当事人能够访问有关其隐私活动的信息，并能够与其CPO取得联系；

j) 如果收到请求，组织应当提供信息，这些信息是关于隐私泄露已经或可能带来的请求者PII泄露；组织也应同时为请求者提供一些相关措施，以减轻隐私泄露带来的额外风险。

组织也应当采取不同的机制，以告知公众有关它们的隐私保护实践，这些实践包括但不限于PIA报告、隐私保护报告、公共网页、电子邮件分布、博客以及定期出版物（例如季报）。组织还应当向公众开放电子邮箱和/或公众热线，使公众能够针对隐私保护行动，向隐私保护署递交反馈意见或直接提出问题。

A.10 PII当事人参与及访问

A.10.1 PII当事人访问

目标：使PII当事人有能力访问、审核他们的PII，并质疑PII的准确性和完整性。

控制

组织应当采取恰当措施，使PII当事人能够访问自己的PII，并对PII进行修正或删除。

PII保护实施指南

组织应当做到如下几点：

a) 组织应当确定可行措施来允许PII当事人行使访问权（在适用法律允许的情况下）。个人应当能够及时行使访问权，且行使权利的方式应当简便快捷，且与最初收集PII的手段（例如通过平信或电子邮件）相似；

b) 当出现所选方法不奏效的情况时，对情况进行分析，如有必要，应确定备份解决方案；

c) 使PII当事人能够访问组织持有的PII，以检查其准确性，在必要情况下进行修正；

d) 在收到请求时，回复的方式尽可能与对方提出请求所使用的方式相同，例如，如果收到的请求是以平信书就的，那么组织也应使用平信给予回复；

e) 出台规章制度，即PII当事人可能怎样要求对系统中的记录进行访问；

f) 允许PII当事人直接地或间接地质疑PII的准确性与完整性，并在特殊情况下对PII进行适当的、合理的修改、校正或移除；

g) 设立程序，使PII当事人能够简便、迅速、高效地行使这些权利，并且不存在无故延误或花费（例如，应当依据适用法律法规或组织政策来回应）；

h) 组织应当设定一项流程，以告知PII当事人关于当事人发出的请求所处的状态，以及必要PII处理的情况（例如，通过信件或电子邮件告知PII当事人，组织已收到请求，并告知当事人组织将在何时进行回复）。如果PII管理者告知PII当事人递交有关请求处理的时间表，并已经提出了合理的回复时间，储存档案中记录的回复日期可能就存在时间偏差；

i) 在法律允许的最大范围内，确保PII当事人能够经常行使访问权；

j) 确保只有与PII信息相关的个人或其授权代理人才能访问PII。这就要求，请求访问的个人要用符合要求的方式识别并证明其身份的真实性。适用法律法规可能会对身份识别与证实的要求进行定义；

k) 除非法律法规另有规定，否则当要求对请求者的身份真实性进行识别和证实时，应确定识别和证实方式。组织应当要求仅将最少量的信息用于确保身份的准确性。这种信息应得到妥善保护，并仅在必要的时候才能被留存；

l) 确保仅将PII发送至相关的PII当事人，并以安全的方式发送；

m) 确保当PII当事人请求得到信息时，组织能够将信息提供给当事人，同时也要保护其他PII当事人的PII；

n) 在一些管辖区域的法律允许的情况下，如果组织要征收访问费用，应通过隐私公告来告知；

o) 要求PII处理者支持PII管理者，以促进PII当事人行使权利来对数据进行访问、纠正或删除；

通过访问，PII当事人可对组织系统中有关他们的PII记录进行审查。当事人可及时访问数据，且数据访问过程简便，访问价格合理。受物资、法律要求及其他因素影响，组织允许当事人进行记录访问的流程可能会有不同。

A.10.2 纠正及参与

目标：若组织向PII处理者和第三方公布了数据，那么应向他们提供数据的修正、校对或移除。

控制

除非有相关法律法规禁止，否则组织应采取恰当的措施，使PII当事人能够对组织持有的PII进行纠正、修改或删除。组织也应当建立一项机制，以将数据的纠正、修改或删除告知PII处理者，并尽可能告知获取PII的第三方。

PII保护实施指南

组织应当做到如下几点：

a) 确保当事人能经常行使权纠正的权利；

b) 当出现所选方法不奏效的情况时，对情况进行分析，如有必要，应确定备份解决方案；[在以上内容中有所重复]

c) 在相关法律法规允许的最大范围内，确保PII当事人能够行使权利进行修改；

d) 若收到纠正请求，应确保修正后的数据的准确性；

e) 确保PII当事人在递交请求后能得到确认；

f) 如果第三方可能得到PII，组织应确保告知第三方纠正后的信息；

g) 仅允许PII当事人访问他们需要纠正、修改或删除的PII；

A.10.3 投诉管理

目标：建立有效的内部投诉处理与纠正程序，以供PII当事人使用。

控制

组织应采取有效措施，以有效处理来自PII当事人的投诉。

PII保护实施指南

组织应当设立一项投诉管理流程，并设置一个联络点，对PII当事人针对组织隐私保护实践产生的投诉、关心的事项或提出的问题进行接收和回应。

组织应当建立易于PII当事人接受、便于PII当事人使用的投诉机制，包括所有能够成功应对投诉的信息（包括CPO或其他官员专门用来接收投诉的联络信息）。

组织投诉管理流程应当包括跟踪机制，以确保接收到的所有投诉都经审查，并得到了及时的解决。投诉管理也应当包括由投诉触发的更正功能。

关于PII保护的其他信息

PII当事人产生的投诉、关心的事项以及提出的问题都可作为外部输入的重要资源，能够最大程度地改进操作模式、技术使用、数据处理方面的实践，并增强对隐私的保护，提升安全系数。

A.11 问责制

A.11.1 管理

目标：有效管理PII处理。

控制

组织应当采取有效措施，针对PII处理建立有效的管理制度。

PII保护实施指南

组织应当做到如下几点：

a) 通过程序或信息系统，任命专人负责制定、实施并维护全组织的管理与隐私保护程序，使PII处理遵从法律法规。任命的专人可被确定为CPO。另一种选择是，在分包工程的一名专门人员的支持下，一位董事会专门成员来承担问责制；

b) 确保指定的专人具备监督PII处理所需的必要知识技能；

c) 确保指定的专人参与有关PII保护的所有事项，并能够及时地、直接向高级管理汇报情况；

d) 为指定的专人提供其为完成工作所需的人员、场所、设备及其他资源；

e) 设定一个流程来发现隐私法和隐私政策中发生的变化，这些变化会影响PII保护程序；

f) 制定、传播并实施可行的PII保护政策与流程，这些政策与流程可以为涉及PII的程序、信息系统或技术提供PII保护以及安全控制管理；

g) 定期更新PII保护计划、政策与程序；

h) 定期对组织运行中的PII保护情况进行记录。一个高级管理代表或董事会成员应对PII保护情况的定量指标、奉献与漏洞等方面进行可视化管理。这种定期审查是出于需要，而非外界触发。

A.11.2 隐私风险评估

目标：设立隐私风险评估流程，如有必要，进行隐私风险评估。

控制

当一个组织进行PII处理时，应当设立用于隐私风险评估的必要流程。

PII保护实施指南

隐私风险评估通常由一个组织进行，这个组织严肃履行职责，并对PII当事人给予足够重视。在一些管辖区域，一个隐私风险评估须符合法律法规要求。ISO/IEC 29134可能会被作为隐私风险评估的指南。

组织在进行隐私风险评估时，应考虑资产、威胁、漏洞及安全保护（现有的和提议的）。组织应当记录如下内容：

a) 隐私风险评估的结果应包括，但不限于正在进行处理的PII；

b) 识别出的隐私风险；

c) 提议的缓和措施。

A.11.3 针对承包商与PII处理者的隐私保护要求

目标：通过合同契约或其他手段（例如强制性内部政策），确保接收PII的第三方也要提供至少同等水平的PII保护。

控制

组织应当采取恰当措施，确保承包商与PII处理者已对PII实行同等水平的保护。

PII保护实施指南

组织应当做到如下几点：

a) 在服务水平协议中记录PII保护要求，这些PII保护要求是PII处理者需要达到的；

b) 对承包商落实要求的状况进行监督和审核；

c) 为承包商与PII处理者安排PII保护任务，并让其承担相应的责任；

d) 通过合同确定服务的主题和时间框架，PII处理者处理PII的程度、方式和目的，以及所处理的PII的类型；

e) 说明在何种情况下，PII处理者应于服务完成时、管理协议终止时或PII管理者有要求时对PII进行归还或安全处理；

f) 在PII提供者与可能访问PII的职员之间确立保密条款；

g) 除非合同中有特殊允许，否则应确保服务提供商不将PII告知第三方，也不可将PII交给第三方保存；

h) 组织应明确服务提供商的责任，以在出现数据漏洞对PII造成影响时告知PII管理者；

i) 合同中应明确规定，服务提供商应将一些变化告知PII管理者，这些变化与服务相关，例如启用附加功能；

j) 在适当的情况下，记录并传播所有与PII保护相关的政策、程序以及实践。

组织应当向法律顾问、CPO、合同官咨询可能对实施控制产生影响的适用法律、指令、政策或规章。

注 – 也实行条款15.1.2的附加实施指南。

关于PII保护的其他信息

承包商与PII处理者可能包含但不限于服务局、信息提供者、信息处理者以及其他的组织，这些组织设置信息系统，提供技术服务及其他外包应用。

A.11.4 隐私保护监督与审查

目标：对PII保护控制以及内部PII保护政策的有效性进行监督和审查。

控制

组织应当采取恰当的措施，定期对PII保护控制以及内部PII保护政策的有效性进行监督和审查。

PII保护实施指南

组织应当做到如下几点：

a) 定期监督和审查PII处理运行，尤其是涉及敏感PII的处理运行，确保运行符合适用法律法规以及合同条款；

b) 定期监督和审查PII保护控制，确保其符合适用法律法规以及合同条款；

c) 确保审查由具备资格的、独立的一方（无论是组织内部还是组织外部的）来进行；

d) 如果用内部资源进行审查，组织应当定期让外部的一方进行审查，以进行独立评估。

A.11.5 PII保护认知与培训

目标：为将要访问PII的PII管理人员提供PII保护认知与培训。

控制

组织应当采取恰当措施为PII管理人员提供PII保护认知与培训。

PII保护实施指南

组织应当做到如下几点：

a) 实施并坚持一项综合的培训与认知战略，以确保PII管理人员了解PII保护职责与程序；

b) 在具有监管权的、合同约定的以及技术的环境中创造机制，以定期更新PII管理人员的PII保护职责，这种环境可能会影响组织的隐私合规；

c) 定期（例如每年一次）或根据需要（例如发生事件之后）进行基本的、有针对性的、基于角色的PII保护培训。这对于仅在罕见情况下进行PII处理的活动来说，尤为重要。

d) 确保PII管理人员定期证实（人工证实或电子证实）对PII保护要求责任的接受。

A.11.6 PII 保护报告

目标：对PII保护报告进行撰写、传播及更新。

控制

在适当情况下，为实施带有特殊法定和规定的PII保护程序的授权问责制，组织应当向高级管理以及其他负有监督PII保护责任的人撰写、传播、更新报告（例如，关于漏洞、调查、审查的报告）。

PII保护实施指南

组织应当通过内外部PII保护报告，在组织PII保护运行方面加强问责制与透明度。报告也促使组织设立程序，以符合PII保护要求和PII保护控制，比较组织的运行情况，发现政策与实施的漏洞和差距，并发现成功模式。

A.12 信息安全

目标：确保根据风险评估结果对PII实行适当保护。

控制

组织应当根据威胁风险评估或隐私影响评估结果，用适当的控制对组织关注和监管的PII 进行保护。

PII保护实施指南

组织应当做到如下几点：

a) 在可操作的、功能的、战略的水平上，用适当的控制对PII进行保护，确保PII的完整性、机密性以及可用性，并保护PII免受风险，这些风险诸如未授权访问、破坏、使用、修正、泄露或其生命周期的损耗；

b) 选择PII处理者以及合适的合同，合同可为PII处理提供组织的、物理的、技术的控制，确保PII处理符合这些控制模式；

c) 以适用法律要求、安全标准、ISO 31000中的系统安全风险评估结果、以及费用效益分析结果为基础，设立安全控制；

d) 对PII 访问进行限制，只有需要通过访问PII来完成任务的人，才可以访问，并且这些人只能访问他们为完成任务所需要的PII内容；

e) 解决隐私风险评估和审查程序发现的风险和漏洞；

f) 在进行的安全风险管理程序中，对控制进行定期审查与重新估计。

有时一些数据隐私法中对安全要求有规定，在这种情况下，安全要求应在数据安全功能中得以实施。

设计与实施安全控制时，应采用尽职调查。

A.13 隐私合规

A.13.1 合规

目标：避免与隐私和隐私保护要求相关的法律、法令、法规、隐私权政策或合同义务上的漏洞。

控制

组织应当采取恰当措施，确保PII处理符合要求。

PII保护实施指南

为保护个人可识别信息（PII），组织应做到如下几点：

a) 撰写年度报告，详述现存风险，说明合规的位置，并包括一个关于突出行动的总结；

b) 遵从定义明确的漏洞回应程序，在一些管辖区域，这些程序可包括一些要求，以告知PII当事人和其他管理机构（例如数据保护管理机构）。

A.13.2 一些管辖区域的跨国界数据转移管制

目标：在个人可识别信息（PII）跨国界转移时对其进行保护。

控制

组织应当采取恰当措施，确保任何PII的跨国界转移都要符合相关要求。

PII保护实施指南

当PII需要被传送至其当前所在领土以外的国家时，一些管辖地区的数据隐私法会对PII传送进行管制，管制的情况通常是以下的一项或几项：

a) 通知数据保护管理机构；

b) 获得数据保护管理机构的许可，尤其是当数据为敏感数据时；

c) 进行适当的尽职调查，确保PII跨国界传送时得到的保护程度与其在原来的国家得到的保护程度相同；

d) 实施特定数据传送法规，例如《标准合同条款》或《结合企业规则（BCR）》。

组织应当实施恰当措施，在传送数据之前检查特殊管制要求是否被应用于计划的数据传送，以及是否符合要求。

参考资料

- BSI 10012, *Specification for a personal information management system.*
- European Commission, *Evaluation report on the data retention directive (Directive 2006/24/EC)*, 2011.
- ISO/IEC 27000:2016, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.
- ISO/IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements*.
- ISO/IEC 27005, *Information technology – Security techniques – Information security risk management*.
- ISO/IEC 27009, *Information technology – Security techniques – Sector-specific application of ISO/IEC 27001 – Requirements*.
- ISO/IEC 27018, *Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*.
- ISO/IEC 29134, *Information technology – Security techniques – Guidelines for privacy impact assessment*.
- IEC *Electropedia*. Available (viewed 2017-07-06) at: http://www.electropedia.org/.
- ISO *Online* browsing *platform*. Available (viewed 2017-07-06) at: http://www.iso.org/obp.
- ITU *Terms and definitions*. Available (viewed 2017-07-07) at: http://www.itu.int/ITU-R/go/terminology-database.
- KCS, *Personal information management system*, December, 2011.
- NIST Special Publication 800-53 Appendix J, *Security and privacy controls for federal information systems and organizations*, July, 2011.
- NIST Special Publication 800-122, *Guide to protecting the confidentiality of personally identifiable information (PII)*, April 2010.

ITU-T 建议书系列

系列A	ITU-T工作的组织
系列D	资费及结算原则和国际电信/ICT的经济和政策问题
系列E	综合网络运行、电话业务、业务运行和人为因素
系列F	非话电信业务
系列G	传输系统和媒介、数字系统和网络
系列H	视听及多媒体系统
系列I	综合业务数字网
系列J	有线网络和电视、声音节目及其他多媒体信号的传输
系列K	干扰的防护
系列L	环境与ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列M	电信管理，包括TMN和网络维护
系列N	维护：国际声音节目和电视传输电路
系列O	测量设备的技术规范
系列P	电话传输质量、电话设施及本地线路网络
系列Q	交换和信令
系列R	电报传输
系列S	电报业务终端设备
系列T	远程信息处理业务的终端设备
系列U	电报交换
系列V	电话网上的数据通信
系列X	**数据网、开放系统通信和安全性**
系列Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列Z	用于电信系统的语言和一般软件问题

瑞士印刷
2018年，日内瓦