BS ISO/IEC 29151:2017

INTERNATIONAL STANDARD

ISO/IEC 29151

First edition
2017-08

Information technology — Security techniques — Code of practice for personally identifiable information protection

Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour la protection des données à caractère personnel

Reference number
ISO/IEC 29151:2017(E)

COPYRIGHT PROTECTED DOCUMENT

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

CONTENTS

Foreword

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

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

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

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

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

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*, in collaboration with ITU-T. The identical text is published as ITU-T Recommendation X.1058.

Introduction

The number of organizations processing personally identifiable information (PII) is increasing, as is the amount of PII that these organizations deal with. At the same time, societal expectations for the protection of PII and the security of data relating to individuals are also increasing. A number of countries are augmenting their laws to address the increased number of high profile data breaches.

As the number of PII breaches increases, organizations collecting or processing PII will increasingly need guidance on how they should protect PII in order to reduce the risk of privacy breaches occurring, and to reduce the impact of breaches on the organization and on the individuals concerned. This Specification provides such guidance.

This Specification offers guidance for PII controllers on a broad range of information security and PII protection controls that are commonly applied in many different organizations that deal with protection of PII. The remaining parts of the family of ISO/IEC standards, listed here, provide guidance or requirements on other aspects of the overall process of protecting PII:

- ISO/IEC 27001 specifies an information security management process and associated requirements, which could be used as a basis for the protection of PII.
- ISO/IEC 27002 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls, taking into consideration the organization's information security risk environment(s).
- ISO/IEC 27009 specifies the requirements for the use of ISO/IEC 27001 in any specific sector (field, application area or market sector). It explains how to include requirements additional to those in ISO/IEC 27001, how to refine any of the ISO/IEC 27001 requirements, and how to include controls or control sets in addition to Annex A of ISO/IEC 27001.
- ISO/IEC 27018 offers guidance to organizations acting as PII processors when offering processing capabilities as cloud services.
- ISO/IEC 29134 provides guidelines for identifying, analysing, and assessing privacy risks, while ISO/IEC 27001 together with ISO/IEC 27005 provides a methodology for identifying, analysing, and assessing security risks.

Controls should be chosen based on the risks identified as a result of a risk analysis to develop a comprehensive, consistent system of controls. Controls should be adapted to the context of the particular processing of PII.

This Specification contains two parts: 1) the main body consisting of clauses 1 to 18, and 2) a normative annex. This structure reflects normal practice for the development of sector-specific extensions to ISO/IEC 27002.

The structure of the main body of this Specification, including the clause titles, reflects the main body of ISO/IEC 27002. The introduction and clauses 1 to 4 provide background on the use of this Specification. Headings for clauses 5 to 18 mirror those of ISO/IEC 27002, reflecting the fact that this Specification builds on the guidance in ISO/IEC 27002, adding new controls specific to the protection of PII. Many of the controls in ISO/IEC 27002 need no amplification in the context of PII controllers. However, in some cases, additional implementation guidance is needed, and this is given under the appropriate heading (and clause number) from ISO/IEC 27002.

The normative annex contains an extended set of PII protection-specific controls that supplement those given in ISO/IEC 27002. These new PII protection controls, with their associated guidance, are divided into 12 categories, corresponding to the privacy policy and the 11 privacy principles of ISO/IEC 29100:

- consent and choice;
- purpose, legitimacy and specification;
- collection limitation;
- data minimization;
- use, retention and disclosure limitation;
- accuracy and quality;
- openness, transparency and notice;
- individual participation and access;
- accountability;
- information security; and
- privacy compliance.

Figure 1 describes the relationship between this Specification and the family of ISO/IEC standards.

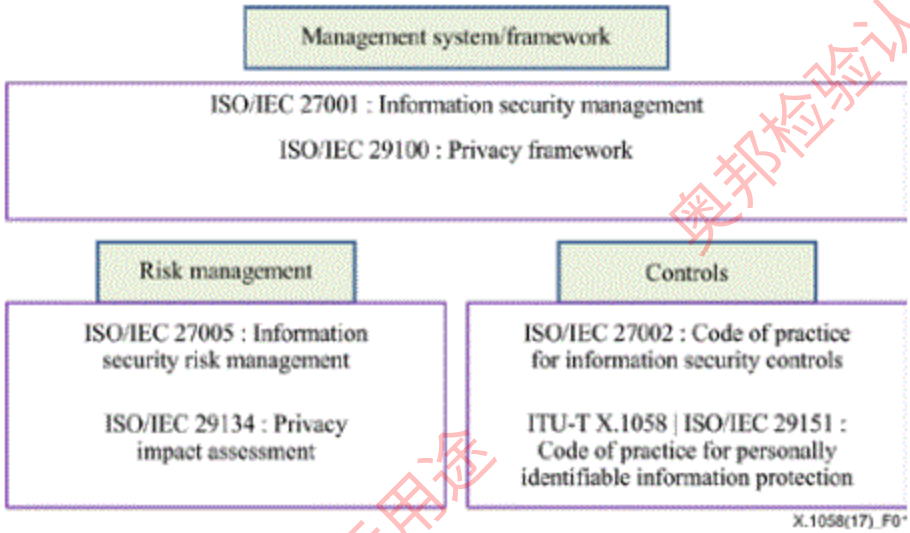

Figure 1 – The relationship of this Specification and the family of ISO/IEC standards

This Specification includes guidelines based on ISO/IEC 27002, and adapts these as necessary to address the privacy safeguarding requirements that arise from the processing of PII:

a) In different processing domains such as:
   - public cloud services,
   - social networking applications,
   - internet-connected devices in the home,
   - search, analysis,
   - targeting of PII for advertising and similar purposes,
   - big data analytics programmes,
   - employment processing,
   - business management in sales and service (enterprise resource planning, customer relationship management);

b) In different locations such as:
   - on a personal processing platform provided to an individual (e.g., smart cards, smart phones and their apps, smart meters, wearable devices),
   - within data transportation and collection networks (e.g., where mobile phone location data is created operationally by network processing, which may be considered PII in some jurisdictions),
   - within an organization's own processing infrastructure,
   - on a third party's processing platform;

c) For the collection characteristic such as:
   - one-time data collection (e.g., on registering for a service),
   - ongoing data collection (e.g., frequent health parameter monitoring by sensors on or in an individual's body, multiple data collections using contactless payment cards for payment, smart meter data collection systems, and so on).

NOTE – Ongoing data collection can contain or yield behavioural, locational and other types of PII. In such cases, the use of PII protection controls that allow access and collection to be managed based on consent and that allow the PII principal to exercise appropriate control over such access and collection, need to be considered.

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

Information technology – Security techniques – Code of practice for personally identifiable information protection

1 Scope

This Recommendation | International Standard establishes control objectives, controls and guidelines for implementing controls, to meet the requirements identified by a risk and impact assessment related to the protection of personally identifiable information (PII).

In particular, this Recommendation | International Standard specifies guidelines based on ISO/IEC 27002, taking into consideration the requirements for processing PII that may be applicable within the context of an organization's information security risk environment(s).

This Recommendation | International Standard is applicable to all types and sizes of organizations acting as PII controllers (as defined in ISO/IEC 29100), including public and private companies, government entities and not-for-profit organizations that process PII.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

– ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls*.
– ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework*.

3 Definitions and abbreviated terms

3.1 Definitions

For the purposes of this Recommendation | International Standard, the terms and definitions that are given in ISO/IEC 27000:2016, ISO/IEC 29100 and the following apply.

The ISO *Online browsing platform*, IEC *Electropedia* and ITU *Terms and definitions* are terminological databases for use in standardization.

3.1.1 chief privacy officer (CPO): Senior management individual who is accountable for the protection of personally identifiable information (PII) in an organization.

3.1.2 de-identification process: Process of removing the association between a set of identifying data and the data principal, using de-identification techniques.

3.2 Abbreviated terms

For the purposes of this Specification, the following abbreviations apply.

BCR	Binding Corporate Rule
CCTV	Closed-Circuit Television
CPO	Chief Privacy Officer
PBD	Privacy By Design
PDA	Personal Digital Assistant
PET	Privacy Enhancing Technology

国际标准

ISO/IEC 29151

初版 2017 年 8 月

信息技术 - 安全技术 - 个人身份信息保护实施规范

Reference number ISO/IEC 29151:2017(E)

受版权保护的文件

国际标准化组织版权办公室

瑞士日内瓦韦尔尼耶市布兰东内街 8 号 401 室，
邮编：1214 电话：+41 22 749 01 1

传 真：+41 22 749 09 47 邮
箱：copyright@iso.org

www.iso.org

目录

前言

国际标准化组织（ISO）和国际电工委员会（IEC）构成了全球标准化的专业体系。作为 ISO 或 IEC 成员的各国机构通过各自组织设立的专门技术委员会参与国际标准的制定工作，这些技术委员会负责处理特定领域的技术活动。ISO 和 IEC 的技术委员会在共同感兴趣的领域开展合作。其他国际组织，无论是政府的还是非政府的，在与 ISO 和 IEC 保持联络的情况下，也参与相关工作。在信息技术领域，ISO 和 IEC 共同成立了联合技术委员会 ISO/IEC JTC 1。

本文件的编制程序以及其后续维护所采用的程序在 ISO/IEC 指令第 1 部分中有描述。尤其应注意不同类型的文件所需的不同批准标准。本文件是依据 ISO/IEC 指令第 2 部分的编辑规则起草的（见 www.iso.org/directives）。

请注意，本文件中的某些内容可能受专利保护。国际标准化组织（ISO）和国际电工委员会（IEC）不对任何此类专利的识别负责。在文件编制过程中所识别出的任何专利权详情将在引言部分和/或国际标准化组织收到的专利声明清单中列出（见 www.iso.org/patents）。

本文件中使用的任何商标名称均为方便用户而提供，不构成任何背书。

有关标准的自愿性质、与合格评定相关的 ISO 特定术语和表达的含义，以及 ISO 在技术性贸易壁垒（TBT）方面遵循世界贸易组织（WTO）原则的信息，请访问以下网址：www.iso.org/iso/foreword.html 。

负责本文件的委员会是国际标准化组织/国际电工委员会第 1 联合技术委员会（ISO/IEC JTC 1）下属的信息技术安全技术分技术委员会（SC 27），并与国际电信联盟电信标准化部门（ITU-T）合作。相同文本已作为 ITU-T 建议 X.1058 发布。

介绍

处理个人身份信息（PII）的组织数量在增加，这些组织所处理的个人身份信息量也在增加。与此同时，社会对个人身份信息保护以及与个人相关数据安全的期望也在提高。许多国家正在加强相关法律，以应对日益增多的重大数据泄露事件。

随着个人身份信息（PII）泄露事件数量的增加，收集或处理个人身份信息的组织将越来越需要有关如何保护个人身份信息的指导，以降低隐私泄露事件发生的可能性，并减轻泄露事件对组织和相关个人的影响。本规范提供了此类指导。

本规范为处理个人身份信息（PII）保护的各类组织提供了广泛的信息安全和个人身份信息保护控制措施方面的指导。此处列出的 ISO/IEC 标准系列的其余部分，就保护个人身份信息的整个流程的其他方面提供了指导或要求：

- ISO/IEC 27001 规定了信息安全管理体系流程及相关要求，可作为保护个人身份信息（PII）的基础。
- ISO/IEC 27002 提供了组织信息安全标准和信息安全管理体系实践的指导方针，包括控制措施的选择、实施和管理，同时考虑组织的信息安全风险环境。
- ISO/IEC 27009 规定了在任何特定领域（行业、应用领域或市场领域）使用 ISO/IEC 27001 的要求。它说明了如何纳入超出 ISO/IEC 27001 要求的内容，如何细化 ISO/IEC 27001 中的任何要求，以及如何在 ISO/IEC 27001 附录 A 之外增加控制措施或控制集。
- ISO/IEC 27018 为作为个人身份信息（PII）处理方的组织在以云服务形式提供处理能力时提供了指导。
- ISO/IEC 29134 提供了识别、分析和评估隐私风险的指南，而 ISO/IEC 27001 与 ISO/IEC 27005 则共同提供了一种识别、分析和评估安全风险的方法。

应根据风险分析所识别的风险来选择控制措施，以建立全面、一致的控制体系。控制措施应适应特定个人数据处理的实际情况。

本规范包含两部分：1）由第 1 条至第 18 条组成的主体部分；2）一个规范性附录。这种结构反映了针对 ISO/IEC 27002 开发特定领域扩展的常规做法。

本规范正文的结构，包括各条款标题，反映了 ISO/IEC 27002 的正文结构。引言和第 1 至 4 条提供了关于本规范使用的背景信息。第 5 至 18 条的标题与 ISO/IEC 27002 相同，这表明本规范是在 ISO/IEC 27002 的指导基础上构建的，并增加了针对个人身份信息（PII）保护的特定控制措施。在个人身份信息控制者的背景下，ISO/IEC 27002 中的许多控制措施无需进一步说明。然而，在某些情况下，需要额外的实施指导，这些指导在 ISO/IEC 27002 相应的标题（及条款编号）下给出。

规范性附录包含了一套扩展的个人身份信息（PII）保护专用控制措施，对 ISO/IEC 27002 中给出的控制措施进行了补充。这些新的 PII 保护控制措施及其相关指南被划分为 12 个类别，分别对应隐私政策以及 ISO/IEC 29100 中的 11 项隐私原则：

- 同意与选择；
- 目的、合法性和具体规定；
- 收集限制；
- 数据最小化；
- 使用、保留和披露限制；
- 准确性和质量；
- 公开性、透明度和通知；
- 个人参与和获取；
- 问责制；责任追究制
- 信息安全；以及
- 隐私合规。

图 1 描述了本规范与 ISO/IEC 标准族之间的关系。

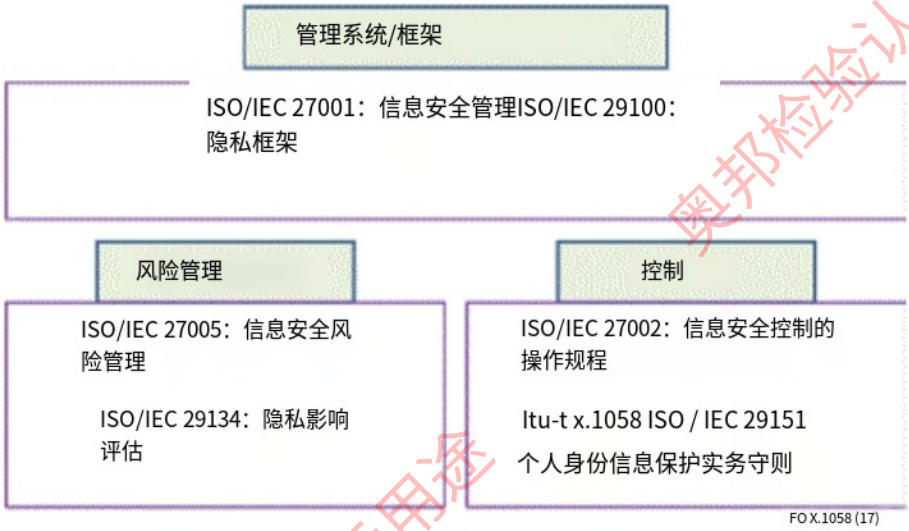

图 1 - 本规范与 ISO/IEC 标准族的关系

本规范包含基于 ISO/IEC 27002 的指南，并根据需要对其进行调整，以满足处理个人身份信息（PII）所产生的隐私保护要求：

a) 在诸如以下的不同处理领域中：

- 公共云服务
- 社交网络应用程序
- 家庭中的联网设备
- 搜索，分析
- 针对个人身份信息（PII）进行广告宣传及类似用途的定向操作
- 大数据分析项目
- 就业手续办理。
- 销售与服务中的业务管理（企业资源规划、客户关系管理）

b) 在不同的地点，例如：

- 在提供给个人的个人处理平台上（例如智能卡、智能手机及其应用程序、智能电表、可穿戴设备）
- 在数据传输和收集网络中（例如，移动电话位置数据由网络处理在运营过程中生成，在某些司法管辖区可能被视为个人身份信息），
- 在组织自身的处理基础设施内，
- 在第三方的处理平台上；

c) 对于诸如以下的收集特征：

- 一次性数据收集（例如，在注册服务时）
- 持续的数据收集（例如，通过佩戴在或植入人体的传感器频繁监测健康参数、使用非接触式支付卡进行多次支付数据收集、智能电表数据收集系统等等）。

注意：持续进行的数据收集可能包含或产生行为、位置及其他类型的个人身份信息。在这种情况下，需要考虑采用个人身份信息保护控制措施，这些措施应基于同意来管理访问和收集，并允许个人身份信息主体对这种访问和收集进行适当控制。

INTERNATIONAL STANDARD ITU-T RECOMMENDATION

信息技术 - 安全技术 - 个人身份信息保护实施规范

1 范围

本国际标准建议书确立了控制目标、控制措施以及实施控制的指南，以满足与个人身份信息（PID）保护相关的风险和影响评估所确定的要求。

特别是，本建议书 | 国际标准基于 ISO/IEC 27002 规定了相关指南，同时考虑了组织的信息安全风险环境中可能适用于处理个人身份信息（PII）的要求。

本建议书 | 国际标准适用于所有类型和规模的组织，只要其作为个人身份信息（PII）控制器（如 ISO/IEC 29100 中所定义）处理个人身份信息，包括公共和私营公司、政府实体以及非营利组织。

2 规范性引用文件

以下建议书和国际标准包含通过本文件中的引用而成为本建议书 | 国际标准组成部分的条款。在出版时，所列版本有效。所有建议书和标准均可能修订，基于本建议书 | 国际标准达成协议的各方应考虑采用以下所列建议书和标准的最新版本。国际电工委员会（IEC）和国际标准化组织（ISO）的成员保存现行有效的国际标准的登记册。国际电信联盟电信标准化局保存现行有效的 ITU-T 建议书清单。

ISO/IEC 27002:2013《信息技术 安全技术 信息安全控制实施指南》

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

就本建议书 | 国际标准而言，适用 ISO/IEC 27000:2016、ISO/IEC 29100 中给出的术语和定义以及以下术语和定义。

国际标准化组织在线浏览平台、国际电工委员会电工术语在线词典和国际电信联盟术语和定义是用于标准化工作的术语数据库。

3.1.1 首席隐私官（CPO）：在组织中负责保护个人身份信息（PID）的高级管理人员。

3.1.2 去标识化过程：使用去标识化技术移除一组标识数据与数据主体之间关联的过程。

3.2 缩略语

就本规范而言，以下缩写适用。

BCR	约束性公司规则
中央电视台	闭路电视
CPO	首席私隐主任
PBD	Privacy By Design
掌上电脑	个人数码助理
宠物	增强私隐科技

私增强技术

如需获取全文，请联系奥邦检验认证集团客户服务部门：

1）通过邮件提出申请。请发送到邮箱：**17312273399@163.com**

2）也可通过客服电话咨询 **025-85307007**。