ICS 35.080
L 77

中华人民共和国国家标准

GB/T 33770.2—2019

信息技术服务　外包
第2部分：数据保护要求

Information technology service—Outsourcing—
Part 2：Data protection requirements

2019-08-30 发布　　2020-03-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 33770《信息技术服务　外包》分为6个部分：

——第1部分：服务提供方通用要求；

——第2部分：数据保护要求；

——第3部分：交付中心要求；

——第4部分：非结构化数据管理与服务要求；

——第5部分：发包方项目管理要求；

——第6部分：服务需方通用要求。

本部分为GB/T 33770的第2部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本部分起草单位：大连软件行业协会、大连华信计算机技术股份有限公司、东软集团股份有限公司、成都市大数据中心、北京护航科技股份有限公司、广州赛宝认证中心服务有限公司、中国电子技术标准化研究院、金税信息技术服务股份有限公司、上海北宙企业管理咨询有限公司、上海有孚网络股份有限公司、北京信城通数码科技有限公司、广州番禺职业技术学院、上海三零卫士信息安全有限公司、神州数码系统集成服务有限公司、上海宝信软件股份有限公司、昆明东电科技有限公司、东软睿道教育信息技术有限公司、江苏润和软件股份有限公司、文思海辉技术有限公司。

本部分主要起草人：郎庆斌、尹宏、刘宏、高昕、陈锡民、赵振文、但强、于浩、梁晓雁、丁宗安、熊健淞、职亮亮、刘颋、张树玲、刘亭杉、杜远、唐百惠、王伟、邬敏华、李阳、郑义、王斌斌、万啟东、徐瑶、谢尚飞、韩沫、邵峰、董雷、宋悦、王鑫。

引　言

本部分内涵和外延均较宽泛，存在易于混淆、多义性的概念、理解，需予以说明，以便于标准条文的解释和标准的应用。

0.1　基准

本部分考虑个人信息与商业数据具有类同的特质，在收集、处理、使用中，其安全要求、安全机制、安全策略等是同等的，可以采用同一的管理方式，适于 IT 服务外包组织共同遵守和应用，也可为其他行业提供借鉴。

0.2　数据

“数据”是一个广义的概念，本部分中，代指涉及个人信息、商业数据的相关信息。

知识产权涉及面广、构成复杂，且已有相关法规，然而，与知识产权相关信息的保护存在法律空白。由于这部分信息与商业数据的特质类同。因此，本部分将知识产权相关信息归入商业数据。

0.3　商业数据

“商业数据”亦是一个广义的概念，内涵宽泛。本部分中，特指敏感的商业秘密或其他需要保护的数据。

0.4　综合数据库

本部分限定综合数据库是由结构化、非结构化个人信息、商业数据（包括自动处理和非自动处理）分别构成的逻辑数据库。

0.5　数据管理

数据保护是针对数据及相关资源、环境、管理体系等的管理活动或行为之一，因而，本部分采用“数据管理”涵盖“数据保护”。本部分数据管理涉及个人信息管理、商业数据管理。

数据管理包含数据收集、处理、使用的整个生命周期。

0.6　数据安全性

本部分涉及的数据安全性，是指个人信息、商业数据的保密性、完整性、准确性、可用性、真实性、可控性和不可抵赖性。

0.7　数据管理体系

指具有特定功能、由相互关联的若干要素构成的有机整体，通过整合、协调资源，聚焦管理要素，实

现预定目标。要素与要素、要素与体系、体系与环境等之间相互作用又相互影响。

本部分为个人信息管理、商业数据管理提供了基本的规则和要求，以构建数据管理体系，充分保障数据主体的权利，保障相关业务的稳定、有效运行。

0.8 标准架构和体例

本部分以管理为主线，以数据生命周期为导向，构建数据管理标准架构，并不同于质量管理体系的标准体例，以便于集聚、整合管理要素，完善、改进、可控数据管理体系，以策数据安全。

0.9 标准兼容性

本部分与国际、国内信息安全标准及其他相关标准协调一致，并与这些标准相互配合或相互整合实施和运行。

0.10 业务连续性

本部分在提供安全指导的同时，需基于数据的合理流通，保证业务的连续性。

0.11 标准适用性

IT 服务外包组织与各类组织的数据安全属性、特征基本一致，其安全机制、安全策略是类同的，因而，本部分具有普适性：

a) 本部分规范的数据管理规则，既是 IT 服务管理的基础，亦可为 IT 服务的发展建立数据管理基准；

b) 本部分规范的数据管理规则，具有共性的特征，可以依据组织的特征解释、剪裁；

c) IT 服务外包组织与各类组织的特征区别是组织的业务和管理，其所涉数据（含合同管理），亦为本部分范畴；

d) 本部分不仅适用于 IT 服务外包组织，其他机关、企业、事业、社会团体等各类组织，可以参照执行。

信息技术服务　外包
第2部分:数据保护要求

1　范围

GB/T 33770的本部分规定了信息技术外包服务中数据保护所涉及的数据生命周期、数据主体权利、数据管理者、数据管理、管理机制、数据获取、数据处理、安全管理、过程管理、应急管理等方面的基本规则和要求。

本部分适用于选择和提供IT服务、评价和认定IT服务提供能力的组织等。其他组织可参照执行。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 22080　信息技术　安全技术　信息安全管理体系　要求

GB/T 22081　信息技术　安全技术　信息安全管理实用规则

3　术语和定义

下列术语和定义适用于本文件。

3.1

介质　medium

承载数据的载体。

3.2

媒介　mediation

存储、传输数据的载体。

3.3

媒体　media

生产、传播数据的媒介。

3.4

数据　data

描述个人信息、商业数据的形态、属性等,并便于保存、处理、使用。

3.5

个人信息　personal information

依附于个人,并可描述个人基本形态的信息,包括通过听觉、视觉、触觉等感官直接识别个人的信息,如声音、数字、文字、图像、影像等;借助各种手段间接识别个人的信息,如与个人相关各种信息对照、参考、分析等。