信息安全技术　个人信息安全规范

GB/T 35273—2020
代替 GB/T 35273—2017

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 35273—2017《信息安全技术　个人信息安全规范》，与 GB/T 35273—2017 相比，除编辑性修改外主要技术变化如下：

——增加了“多项业务功能的自主选择”（见 5.3）；

——修改了“征得授权同意的例外”（见 5.6，2017 年版的 5.4）；

——增加了“用户画像的使用限制”（见 7.4）；

——增加了“个性化展示的使用”（见 7.5）；

——增加了“基于不同业务目所收集个人信息的汇聚融合”（见 7.6）；

——修改了“个人信息主体注销账户”（见 8.5，2017 年版的 7.8）；

——增加了“第三方接入管理”（见 9.7）；

——修改了“明确责任部门与人员”（见 11.1，2017 年版的 10.1）；

——增加了“个人信息安全工程”（见 11.2）；

——增加了“个人信息处理活动记录”（见 11.3）；

——修改了“实现个人信息主体自主意愿的方法”（见附录 C，2017 年版的附录 C）。

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这些专利的责任。

本标准由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本标准起草单位：中国电子技术标准化研究院、北京信息安全测评中心、颐信科技有限公司、四川大学、清华大学、中国信息通信研究院、公安部第一研究所、中国网络安全审查技术与认证中心、深圳腾讯计算机系统有限公司、上海国际问题研究院、阿里巴巴（北京）软件服务有限公司、中电长城网际系统应用有限公司、阿里云计算有限公司、华为技术有限公司、强韵数据科技有限公司。

本标准主要起草人：洪延青、何延哲、杨建军、钱秀槟、陈兴蜀、刘贤刚、上官晓丽、高林、邵正强、金涛、胡影、赵冉冉、韩煜、陈湉、高磊、张晓梅、张志强、葛鑫、周晨炜、秦小伟、邵华、蔡晓丹、黄晓林、顾伟、黄劲、李媛、许静慧、赵章界、孔耀晖、范红、杜跃进、杨思磊、张亚男、叶晓俊、郑斌、闵京华、鲁传颖、周亚超、杨露、王海舟、王建民、秦颂、姚相振、葛小宇、王道奎、沈锡镛。

本标准所代替标准的历次版本发布情况为：

——GB/T 35273—2017。

引　言

近年，随着信息技术的快速发展和互联网应用的普及，越来越多的组织大量收集、使用个人信息，给人们生活带来便利的同时，也出现了对个人信息的非法收集、滥用、泄露等问题，个人信息安全面临严重威胁。

本标准针对个人信息面临的安全问题，根据《中华人民共和国网络安全法》等相关法律，规范个人信息控制者在收集、存储、使用、共享、转让、公开披露等信息处理环节中的相关行为，旨在遏制个人信息非法收集、滥用、泄漏等乱象，最大程度地保障个人的合法权益和社会公共利益。

对标准中的具体事项，法律法规另有规定的，需遵照其规定执行。

信息安全技术　个人信息安全规范

1　范围

本标准规定了开展收集、存储、使用、共享、转让、公开披露、删除等个人信息处理活动的原则和安全要求。

本标准适用于规范各类组织的个人信息处理活动，也适用于主管监管部门、第三方评估机构等组织对个人信息处理活动进行监督、管理和评估。

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 25069—2010　信息安全技术　术语

3　术语和定义

GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

个人信息　personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

注 1：个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注 2：关于个人信息的判定方法和类型参见附录 A。

注 3：个人信息控制者通过个人信息或其他信息加工处理后形成的信息，例如，用户画像或特征标签，能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的，属于个人信息。

3.2

个人敏感信息　personal sensitive information

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

注 1：个人敏感信息包括身份证件号码、个人生物识别信息、银行账户、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14 岁以下(含)儿童的个人信息等。

注 2：关于个人敏感信息的判定方法和类型参见附录 B。

注 3：个人信息控制者通过个人信息或其他信息加工处理后形成的信息，如一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的，属于个人敏感信息。

3.3

个人信息主体　personal information subject

个人信息所标识或者关联的自然人。

3.4

个人信息控制者　personal information controller

有能力决定个人信息处理目的、方式等的组织或个人。

3.5

收集 collect

获得个人信息的控制权的行为。

注1：包括由个人信息主体主动提供、通过与个人信息主体交互或记录个人信息主体行为等自动采集行为，以及通过共享、转让、搜集公开信息等间接获取个人信息等行为。

注2：如果产品或服务的提供者提供工具供个人信息主体使用，提供者不对个人信息进行访问的，则不属于本标准所称的收集。例如，离线导航软件在终端获取个人信息主体位置信息后，如果不回传至软件提供者，则不属于个人信息主体位置信息的收集。

3.6

明示同意 explicit consent

个人信息主体通过书面、口头等方式主动作出纸质或电子形式的声明，或者自主作出肯定性动作，对其个人信息进行特定处理作出明确授权的行为。

注：肯定性动作包括个人信息主体主动勾选、主动点击"同意""注册""发送""拨打"、主动填写或提供等。

3.7

授权同意 consent

个人信息主体对其个人信息进行特定处理作出明确授权的行为。

注：包括通过积极的行为作出授权（即明示同意），或者通过消极的不作为而作出授权（如信息采集区域内的个人信息主体在被告知信息收集行为后没有离开该区域）。

3.8

用户画像 user profiling

通过收集、汇聚、分析个人信息，对某特定自然人个人特征，如职业、经济、健康、教育、个人喜好、信用、行为等方面作出分析或预测，形成其个人特征模型的过程。

注：直接使用特定自然人的个人信息，形成该自然人的特征模型，称为直接用户画像。使用来源于特定自然人以外的个人信息，如其所在群体的数据，形成该自然人的特征模型，称为间接用户画像。

3.9

个人信息安全影响评估 personal information security impact assessment

针对个人信息处理活动，检验其合法合规程度，判断其对个人信息主体合法权益造成损害的各种风险，以及评估用于保护个人信息主体的各项措施有效性的过程。

3.10

删除 delete

在实现日常业务功能所涉及的系统中去除个人信息的行为，使其保持不可被检索、访问的状态。

3.11

公开披露 public disclosure

向社会或不特定人群发布信息的行为。

3.12

转让 transfer of control

将个人信息控制权由一个控制者向另一个控制者转移的过程。

3.13

共享 sharing

个人信息控制者向其他控制者提供个人信息，且双方分别对个人信息拥有独立控制权的过程。

3.14

匿名化 anonymization

通过对个人信息的技术处理，使得个人信息主体无法被识别或者关联，且处理后的信息不能被复原的过程。