ICS 33.030
CCS M 42

中华人民共和国国家标准

GB/T 43506—2023

电信和互联网服务　用户个人信息保护技术要求

Telecom and internet service—User personal information protection requirements

2023-12-28 发布　　2024-04-01 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。

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。

本文件由工业和信息化部提出。

本文件由全国通信服务标准化技术委员会(SAC/TC 543)归口。

本文件起草单位：中国信息通信研究院、深圳市腾讯计算机系统有限公司、北京奇虎科技有限公司、阿里巴巴云计算(北京)有限公司、中移互联网有限公司、中国联合网络通信集团有限公司、中国电信集团有限公司、北京捷兴信源信息技术有限公司、北京卓易讯畅科技有限公司、北京百度网讯科技有限公司、浙江鹏信信息科技股份有限公司、中发数安科技(北京)有限公司、北京京东叁佰陆拾度电子商务有限公司、维沃移动通信有限公司、上海寻梦信息技术有限公司。

本文件主要起草人：汤立波、常浩伦、臧磊、李成、于润东、郭文双、李鑫、李宗祥、顾伟、黄晓林、葛雨明、张雪丽、马峰、黎伟健、胡莉琼、高枫、王兰芳、杨澄宇、刘淼、张屹、周群、陈学宝、贾科、张航、朱政、陈鑫、张亚男。

引　言

近年来，伴随大数据、云计算等新一代信息通信技术的快速发展，数据资产已经成为电信和互联网企业不可或缺的重要财富，用户个人信息已经成为数据资产的重中之重。然而，企业个人信息保护意识参差不齐，电信和互联网服务个人信息保护违规事件不断发生，用户个人信息和权益受到侵害。电信和互联网服务用户个人信息保护已经被行业主管部门列为重要监管工作，个人信息和权益保护相关标准是行业管理、企业自律的重要依据。

本文件依据《中华人民共和国个人信息保护法》《中华人民共和国网络安全法》《全国人民代表大会常务委员会关于加强网络信息保护的决定》《电信和互联网用户个人信息保护规定》等法律法规要求进行编写。

现有《电信和互联网服务　用户个人信息保护》系列行业标准在电信和互联网服务行业广泛应用，有效促进了电信和互联网服务行业在个人信息和权益保护方面的健康发展。为进一步保证电信和互联网服务的规范性和安全性，避免用户个人信息和权益受到侵害，根据现有行业标准完善形成本文件，进一步加强对用户个人信息和权益保护的广泛适用性。

电信和互联网服务　用户个人信息保护技术要求

1　范围

本文件界定了电信和互联网服务用户个人信息和权益保护的术语和定义，规定了保护范围、信息分类、分级对象、分级方法和保护要求。

本文件适用于电信业务经营者和互联网信息服务提供者在提供服务过程中的用户个人信息和权益保护。

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

电信和互联网服务用户个人信息　telecom and internet service user personal information

电信业务经营者和互联网信息服务提供者在提供服务过程中以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

注：以下简称用户个人信息。

3.2

电信和互联网服务用户个人信息处理　telecom and internet service user personal information processing

电信业务经营者和互联网信息服务提供者对个人信息进行的收集、存储、使用、加工、传输、提供、公开、删除等活动。

4　缩略语

下列缩略语适用于本文件。

IMEI：移动设备国际身份码（International Mobile Equipment Identity）

IMSI：国际移动用户识别码（International Mobile Subscriber Identification Number）

MAC：介质访问控制（Media Access Control）

SIM：用户身份识别模块（Subscriber Identity Module）

5　用户个人信息保护范围

用户个人信息保护范围包括电信和互联网服务运营主体及其提供的服务在业务筹备、办理、注册、开展、终止等全生命周期过程中所收集、存储、使用、加工、传输、提供、公开、删除的以电子或者其他方式

记录的用户个人信息，以及在服务过程中的用户权益保护。

电信和互联网服务提供者和运营者应按照保护范围，依据本文件要求对用户个人信息和权益进行保护。

6 用户个人信息分类

6.1 分类概述

综合考虑用户个人信息的属性和类型特征，将电信和互联网用户个人信息分为用户身份和鉴权信息、用户数据和服务内容信息、用户服务相关信息三类。

a) 用户身份和鉴权信息：能够单独或与其他信息结合，对用户自然人身份进行识别，或代替用户自然人身份属性在电信和互联网服务中使用的虚拟身份信息，也包括用于验证身份的鉴权相关信息。

b) 用户数据和服务内容信息：电信和互联网服务过程中收集的具有用户隐私属性的数据和内容信息。

c) 用户服务相关信息：电信和互联网服务过程中，所收集的服务使用情况及服务相关辅助类信息。

6.2 用户身份和鉴权信息

用户身份和鉴权信息包括用户自然人身份和标识信息、用户虚拟身份和鉴权信息两个子类，具体描述见表1。

表1 用户身份和鉴权信息子类和范围

子类	范围(包括但不限于)	信息举例
A1：用户自然人身份和标识信息	A1-1：用户基本资料	姓名、证件类型及号码、年龄、性别、职业、工作单位、地址、民族、国籍等
	A1-2：身份证明	身份证、军官证、护照、驾照、社保卡等证件影印件
	A1-3：生物特征	指纹、声纹、虹膜、脸谱等
A2：用户虚拟身份和鉴权信息	A2-1：普通服务身份标识和鉴权信息	电话号码、账号、邮箱地址、用户个人数字证书以及服务涉及的密码、口令、密码保护答案等
	A2-2：交易类服务身份标识和鉴权信息	各类交易账号和相应的密码、密码保护答案等

6.3 用户数据和服务内容信息

用户数据和服务内容信息包括用户服务内容和资料数据、用户社交内容信息两个子类，具体描述见表2。

表 2　用户数据和服务内容信息子类和范围

子类	范围(包括但不限于)	信息举例
B1:用户服务内容和资料数据	B1-1:服务内容信息	电信网服务内容信息,如通话内容、短信、彩信等; 互联网服务内容信息,如即时通信内容、互联网传输的涉及个人信息的数据文件、邮件内容等
	B1-2:联系人信息	通讯录、好友列表、群组列表等用户资料数据
	B1-3:用户私有资料数据	用户云存储、终端、存储卡等存储的用户文字、多媒体、剪切板内容等资料数据信息
B2:用户社交内容信息	B2-1:私密社交内容	对特定用户群体发布的社交信息,如群组内发布内容、设置权限社交平台内容等

6.4　用户服务相关信息

用户服务相关信息包括服务使用信息、设备信息两个子类,具体描述见表 3。

表 3　用户服务相关信息子类和范围

子类	范围(包括但不限于)	信息举例
C1:用户服务使用信息	C1-1:业务订购、订阅关系	业务订购信息、业务注册时间、修改、注销状况信息等
	C1-2:服务记录和日志	服务详单:如语音、短信、彩信等电信业务服务详单,可能包含主叫号码、主叫位置、被叫号码、开始通信时间、时长、流量信息等; 互联网或移动互联网业务使用情况等,如小型文本数据(Cookie)内容、服务访问记录(网址、业务日志、网购记录、浏览记录等)
	C1-3:消费信息和账单	停开机、入网时间、在网时间、积分、预存款、信用等级、信用额度、缴费情况、付费方式等; 账单:如出账的固定费用、通信费用、数据费用、代收费用、余额等
	C1-4:位置信息	用户所在的经纬度、地区代码、小区代码、基站号等
C2:用户设备信息	C2-1:设备信息	硬件型号、唯一设备识别码 IMEI、设备 MAC 地址、SIM 卡 IMSI 信息等

7　用户个人信息保护分级及保护要求

7.1　分级概述

用户个人信息保护分级对象为特定的电信和互联网服务,该服务包含用于信息交互的各类硬件、软件及相关应用逻辑和业务流程。

用户个人信息保护分级的目标是根据服务所处理用户个人信息的敏感性,对电信和互联网服务进

行用户个人信息保护级别划分。

本文件将用户个人信息保护级别由高到低划分为5级—1级，服务所处理的用户个人信息（即分级要素）敏感性越高，该服务的用户个人信息保护级别就越高。

7.2 分级方法

7.2.1 第5级服务的分级方法

如果电信业务经营者和互联网信息服务提供者在提供服务过程中处理第5级分级要素，则该服务的用户个人信息保护级别为5级。第5级服务分级要素主要包括以下内容。

a) A1-2（身份证明）：包括但不限于身份证、军官证、护照、驾照、社保卡等影印件。

b) A1-3（生物特征）：包括但不限于指纹、声纹、虹膜、脸谱等。

c) A2-2（交易类服务身份标识和鉴权信息）：包括但不限于各类交易账号和相应的密码、密码保护答案等。

7.2.2 第4级服务的分级方法

如果电信业务经营者和互联网信息服务提供者在提供服务过程中未处理第5级服务分级要素，但处理第4级服务分级要素，则该服务的用户个人信息保护级别为4级。第4级服务分级要素主要包括以下内容。

a) A1-1（用户基本资料）：包括但不限于姓名、证件类型及号码、年龄、性别、职业、工作单位、地址、民族、国籍等。

b) A2-1（普通服务身份标识和鉴权信息）：包括但不限于电话号码、账号、邮箱地址、用户个人数字证书以及服务涉及的密码、口令、密码保护答案等。

c) B1-2（联系人信息）：包括但不限于通讯录、好友列表、群组列表等用户资料数据。

d) C1-4（位置信息）：包括但不限于用户所在的经纬度、地区代码、小区代码、基站号等。

7.2.3 第3级服务的分级方法

如果电信业务经营者和互联网信息服务提供者在提供服务过程中未处理第4级、第5级服务分级要素，但处理第3级服务分级要素，则该服务的用户个人信息保护级别为3级。第3级服务分级要素主要包括以下内容。

a) B1-1（服务内容信息）：包括电信网和互联网中的服务数据。包括但不限于电信网服务内容信息，如通话内容、短信、彩信等互联网服务内容信息，如即时通信内容、互联网传输的涉及个人信息的数据文件、邮件内容等。

b) B1-3（用户私有资料数据）：包括但不限于用户云存储、终端、存储卡等存储的用户文字、多媒体、剪切板内容等资料数据信息。

c) B2-1（私密社交内容）：包括但不限于对特定用户群体发布的社交信息，如群组内发布内容、设置权限社交平台内容等。

d) C1-2（服务记录和日志）：包括但不限于以下内容。

   1) 服务详单：如语音、短信、彩信等电信业务服务详单，可能包含主叫号码、主叫位置、被叫号码、开始通信时间、时长、流量信息等。

   2) 互联网或移动互联网业务使用情况：如Cookie内容、服务访问记录，如网址、业务日志、网购记录、浏览记录等。

e) C2-1（设备信息）：包括但不限于硬件型号、唯一设备识别码IMEI、设备MAC地址、SIM卡IMSI信息等。

7.2.4 第2级服务的分级方法

如果电信业务经营者和互联网信息服务提供者在提供服务中未处理第3级、第4级、第5级服务分级要素，但处理第2级服务分级要素，则该服务的用户个人信息保护级别为2级。第2级服务分级要素主要包括以下内容。

C1-3(消费信息和账单)：包括但不限于停开机、入网时间、在网时间、积分、预存款、信用等级、信用额度、缴费情况、付费方式、出账的固定费用、通信费用、数据费用、代收费用、余额等。

7.2.5 第1级服务的分级方法

如果电信业务经营者和互联网信息服务提供者在提供服务过程中未处理第2级、第3级、第4级、第5级服务分级要素，但处理第1级服务分级要素，则该服务的用户个人信息保护级别为1级。第1级服务分级要素主要包括以下内容。

C1-1(业务订购、订阅关系)：包括但不限于业务订购信息、业务注册时间、修改、注销状况信息等。

7.3 保护要求

7.3.1 基本保护要求

电信业务经营者和互联网信息服务提供者在提供服务过程中遵循以下基本保护要求。

a) 遵循正当、必要和诚信原则，不应通过误导、欺诈、胁迫等方式处理个人信息或让用户使用其服务。

b) 处理个人信息具有明确、合理的目的，并与处理目的直接相关，采取对个人权益影响最小的方式。

c) 处理个人信息应取得个人同意，该同意应由个人在充分知情的前提下自愿、明确作出。

d) 不应以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务，处理个人信息属于提供产品或者服务所必需的除外。

e) 不应提前向用户申请超出当前业务功能或者服务外的权限，不应利用频繁弹窗反复申请与当前服务场景无关的权限。

f) 处理个人信息的数量、频次、精度应控制在最小必要范围内，不应超范围处理个人信息。

g) 个人信息在App端侧的读取、写入、删除、修改等操作应为服务所必需，不应超出用户同意的操作范围。

h) 在非服务所必需或者无合理场景下，不应自启动或者关联启动其他App。

i) 对于不影响其他服务功能的独立服务功能模块，应向用户提供关闭或者退出该独立服务功能的选项，不应因用户采取关闭或者退出操作而拒绝提供其他服务。

j) 利用个人信息进行自动化决策，应保证决策的透明度和结果公平、公正，同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。

k) 使用第三方服务的，应制定管理规则，明示第三方服务提供者的名称、功能、个人信息处理规则等内容；应与第三方服务提供者签订个人信息处理协议，明确约定各自的权利和义务，并对第三方个人信息处理活动进行监督。

l) 按照本文件中规定的分级方法对其提供的服务进行分级，确定服务的用户个人信息保护级别后，服务提供方应按照对应级别所规定的要求，在处理个人信息过程中提供相应的保护机制，对用户个人信息处理工作流程进行规范化管理。服务处理的个人信息发生变化时，应对该服务重新分级。

7.3.2 第5级服务保护要求

第5级服务除遵循基本保护要求外，还应遵循以下保护要求。

a) 只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下方可处理个人信息。

b) 在处理用户个人信息前进行个人信息保护影响评估，向用户告知处理个人信息的必要性以及对个人权益的影响，并征得用户单独同意。

c) 实施严格的技术和管理措施，保护用户的知情权、选择权，保护用户个人信息的机密性、完整性，确保用户个人信息访问控制安全，建立严格的用户个人信息安全管理规范以及数据实时监控机制。

   1) 在信息的收集、存储、传输的过程中应使用高强度的加密措施，保障数据的机密性和完整性。

   2) 对信息采取严格的访问控制措施，应定义严格的用户个人信息各生命周期（包括信息收集、存储、使用、加工、传输、提供、公开、删除等各个环节）安全管理规范。

   3) 设置内部的数据审批流程及制度，并对用户个人信息的使用进行实时监控及预警。

d) 第5级服务中涉及的其他级别的分级要素，其保护要求按相应级别服务的保护要求执行。

7.3.3 第4级服务保护要求

第4级服务除遵循基本保护要求外，还应遵循以下保护要求。

a) 在具有特定的目的和充分的必要性，并采取必要保护措施的情形下处理个人信息。

b) 在处理用户个人信息前进行个人信息保护影响评估，向用户告知处理个人信息的必要性以及对个人权益的影响。

c) 实施必要的技术和管理措施，保护用户的知情权、选择权，保护用户个人信息的机密性、完整性，确保用户个人信息访问控制安全，建立用户个人信息安全管理规范以及数据准实时监控机制。

   1) 在信息的收集、存储、传输的过程中应采取必要的加密措施，保障数据的机密性和完整性。

   2) 对信息采取严格的访问控制措施，应定义严格的用户个人信息各生命周期（包括信息收集、存储、使用、加工、传输、提供、公开、删除等各个环节）安全管理规范。

   3) 设置内部的数据审批流程及制度，并对用户个人信息的使用进行准实时监控及预警。

d) 第4级服务中涉及的其他级别的分级要素，其保护要求按相应级别服务的保护要求执行。

7.3.4 第3级服务保护要求

第3级服务除遵循基本保护要求外，还应遵循以下保护要求。

a) 实施基本的技术和管理措施，保护用户的知情权、选择权，确保用户个人信息访问控制安全，建立用户个人信息安全管理规范。对信息采取必要的访问控制措施，定义用户个人信息各生命周期（包括信息收集、存储、使用、加工、传输、提供、公开、删除等各个环节）安全管理规范。

b) 第3级服务中涉及的其他级别的分级要素，其保护要求按相应级别服务的保护要求执行。

7.3.5 第2级服务保护要求

第2级服务除遵循基本保护要求外，还应遵循以下保护要求。

a) 实施基本的技术和管理措施，保护用户知情权、选择权，确保用户个人信息访问控制安全。

b) 第2级服务中涉及的其他级别的分级要素，其保护要求按相应级别服务的保护要求执行。

7.3.6 第1级服务保护要求

第1级服务除遵循基本保护要求外，还应实施基本的技术和管理措施，确保用户个人信息访问控制安全。

参 考 文 献

[1] 中华人民共和国个人信息保护法(2021年8月20日第十三届全国人民代表大会常务委员会第三十次会议通过)