

ICS 33.030

M 21

YD

中华人民共和国通信行业标准

YD/T 2782-2014

电信和互联网服务 用户个人信息保护 分级指南

Telecom and internet service—
User personal information protection—Classification and guideline

2014-12-24 发布

2014-12-24 实施

中华人民共和国工业和信息化部 发布

目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 缩略语	1
4 用户个人信息保护分级概述	1
5 用户个人信息保护分级方法	1
5.1 分级对象	1
5.2 级别划分	1
5.3 分级方法	2

前 言

本标准是“电信和互联网服务 用户个人信息保护”系列标准之一。该系列标准的名称及结构预计如下：

- 电信和互联网服务 用户个人信息保护 定义及分类；
- 电信和互联网服务 用户个人信息保护 分级指南；
- 电信和互联网服务 用户个人信息保护技术要求 移动应用商店；
- 电信和互联网服务 用户个人信息保护技术要求 即时通信服务；
- 电信和互联网服务 用户个人信息保护技术要求 电子商务服务。

随着服务管理要求的逐步细化，将不断补充和完善电信和互联网服务用户个人信息保护的相关标准。

本标准按照GB/T1.1-2009给出的规则起草。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：工业和信息化部电信研究院、阿里巴巴（中国）有限公司、深圳腾讯计算机系统有限公司、北京奇虎科技有限公司、中国联合网络通信集团有限公司、中国移动通信集团公司、中国电信集团公司、新浪网技术（中国）有限公司、北京搜狐互联网信息服务有限公司、北京中创信测信息技术有限公司、北京卓易讯畅科技有限公司、苏宁云商集团、浙江维尔科技有限公司。

本标准主要起草人：李 成、汤立波、葛雨明、韩 涵、张雪丽、崔媛媛、陈小江、蔡晓丹、张元胄、史 琳、傅 彤、范 勇、马 铮、刘利军、胡莉琼、王兰芳、许章毅、周 晶、杨澄宇、周惠雯、王春阳、陆 捷。

电信和互联网服务 用户个人信息保护 分级指南

1 范围

本标准规定了电信和互联网服务用户个人信息保护的分级对象和分级方法。

本标准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保护。

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。

YD/T 2781-2014 电信和互联网服务 用户个人信息保护 定义及分类

3 缩略语

下列缩略语适用于本文件。

IMEI	International Mobile Equipment Identity	移动设备国际身份码
IMSI	International Mobile Subscriber Identification Number	国际移动用户识别码
MAC	Media Access Control	介质访问控制
SIM	Subscriber Identity Module	用户身份识别模块

4 用户个人信息保护分级概述

用户个人信息保护分级的对象是电信和互联网服务。

用户个人信息保护分级的目标是根据服务所收集和使用的用户个人信息，对电信和互联网服务进行用户个人信息保护级别划分。电信和互联网服务提供方应按照本标准中规定的分级方法对其提供的服务进行分级。

本系列标准对不同类型和级别的电信和互联网服务提出不同的用户个人信息保护要求，遵循同级别的不同类型服务应当承担同等程度的用户个人信息保护要求的原则。电信和互联网服务提供方应按照相应级别的管理要求及技术要求对其提供服务过程中涉及的用户个人信息的收集、存储、转移、使用和销毁等工作流程进行规范化管理。

5 用户个人信息保护分级方法

5.1 分级对象

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。

5.2 级别划分

电信和互联网服务用户个人信息保护级别划分的原则：根据电信和互联网服务所收集、存储、转移和使用的用户个人信息确定服务的用户个人信息保护级别。

本标准按照YD/T 2781-2014《电信和互联网服务 用户个人信息保护 定义及分类》中定义的用户个人信息分类，确定电信和互联网服务的用户个人信息保护级别。

本标准将电信和互联网服务的用户个人信息保护级别由低到高划分为1-5级，服务所收集、存储、转移和使用的用户个人信息敏感性越高，该服务的用户个人信息保护级别就越高。

按照用户个人信息保护分级方法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收集和使用个人信息过程中提供相应的保护机制。由于服务内容发生变化而导致收集、存储、转移和使用过程中涉及的用户个人信息发生变化时，应对该服务重新分级。

5.3 分级方法

5.3.1 第5级服务的分级方法及基本保护要求

第5级服务分级要素包括（以下分级要素依据YD/T 2781-2014《电信和互联网服务 用户个人信息保护 定义及分类》的规定）：

——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；

——A1-3（生理标识）：包括但不限于指纹、声纹、虹膜、脸谱等；

——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。

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涉及第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级服务基本保护要求：第5级分级要素应实施严格的技术和管理措施，保护用户的知情权和选择权，保护用户个人信息的机密性和完整性，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。例如，在收集、转移和使用用户个人信息时应征得用户同意，在信息的存储以及收集和转移的传输过程应使用高强度的加密措施，保障数据的机密性和完整性，应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、生成、存储、使用、传输和销毁等各个环节）安全管理规范，应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。

第5级服务中涉及到的其他级别的分级要素，其保护要求见相应级别服务的保护要求。

5.3.2 第4级服务的分级方法及基本保护要求

第4级服务分级要素包括（以下分级要素依据YD/T 2781-2014《电信和互联网服务 用户个人信息保护 定义及分类》的规定）：

——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、宗教信仰、民族、国籍等；

——B1-2（联系人信息）：包括但不限于通信录、好友列表、群组列表等用户资料数据；

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

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涉及第5级服务分级要素，但涉及第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级服务基本保护要求：针对第4级分级要素应实施必要的技术和管理措施，保护用户的知情权和选择权，保护用户个人信息的机密性和完整性，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。例如，在收集和转移用户个人信息时应征得用户同意，在信息的收集和转移的传输过程应采取必要的加密措施，保障数据的机密性和完整性，应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、生成、存储、使用、传输和销毁等

各个环节)安全管理规范,应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。

第4级服务中涉及到的其他级别的分级要素,其保护要求见相应级别服务的保护要求。

5.3.3 第3级服务的分级方法及基本保护要求

第3级服务分级要素包括(以下分级要素依据YD/T 2781-2014《电信和互联网服务 用户个人信息保护 定义及分类》的规定):

——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;

——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以及即时通信内容、互联网传输的涉及个人信息的数据文件、邮件内容等;

——B1-3(用户私有资料数据):包括但不限于用户云存储、终端、SD卡等存储的用户文字、多媒体等资料数据信息;

——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、设置权限博客内容等;

——C1-2(服务记录和日志):包括但不限于服务详单,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Cookie内容、服务访问记录、网址、业务日志和网购记录等;

——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地址和SIM卡IMSI信息等。

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涉及第4级、第5级服务分级要素,但涉及第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级服务基本保护要求:针对第3级分级要素应实施基本的技术和管理措施,保护用户的知情权和选择权,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。例如,在收集和转移用户个人信息时应征得用户同意,应对信息采取必要的访问控制措施,应定义用户个人信息各生命周期(包括信息收集、生成、存储、使用、传输和销毁等各个环节)安全管理规范。

第3级服务中涉及到的其他级别的分级要素,其保护要求见相应级别服务的保护要求。

5.3.4 第2级服务的分级方法及基本保护要求

第2级服务分级要素仅含 C1-3(消费信息及账单):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、代收费用和余额等(该分级要素依据YD/T 2781-2014《电信和互联网服务 用户个人信息保护 定义及分类》的规定)。

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涉及第3级、第4级、第5级服务分级要素,但涉及第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级服务基本保护要求:针对第2级分级要素应实施基本的技术和管理措施,保护用户知情权和选择权,确保用户个人信息访问控制安全。例如,在转移用户个人信息时应征得用户的同意,应对信息采取必要的访问控制措施。

第2级服务中涉及到的其他级别的分级要素，其保护要求见相应级别服务的保护要求。

5.3.5 第1级服务的分级方法及基本保护要求

第1级服务分级要素仅含C1-1（业务订购关系）：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（该分级要素依据YD/T 2781-2014《电信和互联网服务 用户个人信息保护 定义及分类》的规定）。

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涉及第2级、第3级、第4级、第5级服务分级要素，但涉及第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级服务基本保护要求：针对第1级分级要素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。例如，应对用户个人信息采取必要的访问控制措施。

中华人民共和国
通信行业标准
电信和互联网服务 用户个人信息保护
定义及分类

YD/T 2782-2014

*

人民邮电出版社出版发行
北京市丰台区成寿寺路 11 号邮电出版大厦
邮政编码: 100164
宝隆元(北京)印刷技术有限公司印刷
版权所有 不得翻印

*

开本: 880 × 1230 1/16 2015 年 1 月第 1 版
印张: 0.75 2015 年 1 月北京第 1 次印刷
字数: 11 千字

15115 • 613

定价: 10 元

本书如有印装质量问题, 请与本社联系 电话: (010)81055492