ICS 03.060
A 11

T/ZAIF

互 联 网 金 融 团 体 标 准

T/ZAIF 1002—2020

互联网金融组织数据分类分级指南

Reference guide for data classification and grading of organization in the Internet finance industry

2020－07－24 发布　　2020－09－01 实施

浙江互联网金融联合会　　发 布

目　　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由浙江互联网金融联合会提出并归口。

本标准起草单位：连连银通电子支付有限公司、浙江省标准化研究院、中国计量大学、浙江大学互联网金融研究院。

本标准起草人：童将、徐冬香、钱朝霞、胡珊珊、于娉、陈晓蓉、梁艳华、楼超艳、李巍霞、朱岩。

引　言

随着信息技术的快速发展，网络应用逐步普及，近年来信息技术与金融行业内应用程度进一步加深，行业机构都沉淀了大量数据。金融行业业务种类繁多，数据呈现出复杂性高、多样性强的特点。采用规范的数据分类、分级方法，有助于行业机构厘清数据资产、确定数据重要性或敏感度，并针对性地采取适当、合理的管理措施和安全防护措施，形成一套科学、规范的数据资产管理与保护机制，从而在保证数据安全的基础上促进数据开放共享。

数据分类是数据保护工作中的一个关键部分，是建立统一、准确、完善的数据架构，实现集中化、专业化、标准化数据管理的基础。行业机构按照统一的数据分类方法，依据自身业务特点对产生、采集、加工、使用或管理的数据进行分类，可以全面清晰地厘清数据资产，有利于数据的维护和扩充。

数据分级是以数据分类为基础，采用规范、明确的方法区分数据的重要性和敏感度差异，确定数据级别。数据分级有助于行业机构根据数据不同级别，确定数据在其生命周期的各个环节应采取的数据安全防护策略和管控措施，进而提高机构的数据管理和安全防护水平，确保数据的完整性、保密性和可用性。

本标准为数据分类分级工作提供指导，结合行业特点提出一种从业务到数据逐级划分的数据分类分级方法，同时提供数据分类分级管理的相关建议，供互联网金融行业相关机构参考。

互联网金融组织数据分类分级指南

1 范围

本标准规定了互联网金融行业内组织数据分类分级的术语和定义、数据范围、数据分类分级方法、数据分类要求和数据分级要求。

本标准适用于互联网金融行业内组织、行业、其他相关机构数据的分类分级。

本标准不适用于涉及国家秘密的数据。

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，仅所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 10113—2003 分类与编码通用术语

GB/T 22240—2008 信息安全技术 信息系统安全等级保护定级指南

GB/T 25069—2010 信息安全技术 术语

JR/T 0071—2012 金融行业信息系统信息安全等级保护实施指引

3 术语和定义

下列术语和定义适用于本文件。

3.1

数据 data

信息的可再解释的形式化表示，以适用于通信、解释或处理。

注：可以通过人工或自动手段处理数据。

[来源：GB/T 5271.1—2020，定义01.01.02]

3.2

保密性 confidentiality

信息不能被未授权的个人、实体或者过程利用或知悉的特性。

[来源：GB/T 29246—2012，术语和定义2.9]

3.3

可用性 availability

根据授权实体的要求可访问和使用的特性。

[来源：GB/T 29246—2012，术语和定义2.7]

3.4

完整性 integrity

保护资产的准确和完整的特性。
[来源：GB/T 29246—2012，术语和定义2.25]

3.5

网络数据 network data

通过网络收集、存储、传输、处理和产生的各种电子数据。

3.6

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自然人个人身份的各种信息,包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

4 数据范围

数据范围涵盖互联网金融行业内组织经营和管理活动中产生、采集、加工、使用或管理的网络数据或非网络数据（非经网络收集、存储、传输、处理和产生的各种电子或非电子数据），包括但不限于：

a) 组织通过开展业务或经其他渠道获取的用户个人信息，个人身份信息、财产信息、账户信息、信用信息、交易信息及其他反映特定个人某些情况的信息，其中关于个人信息采集安全指南见附录 A；
b) 业务管理相关信息，如：监管信息、统计信息、公告信息等。此处“监管信息”，特指组织收到的来自监管部门的信息或按照监管部门要求报送的信息；
c) 经营管理数据，如：客户管理信息、渠道管理信息、经营状况信息、人力管理信息、财务管理信息、技术管理信息等；
d) 其他数据完整性、保密性和可用性遭到破坏，可能严重危害国家安全、国计民生、公共利益的各类数据。

5 数据分类分级方法

5.1 总则

5.1.1 数据分类是按照 GB/T 10113—2003 中的线分类法为基础进行分类。

5.1.2 数据分级是按照 GB/T 22240—2008 中的定级方法为基础进行分级。

5.1.3 在数据分类基础上，对已分类数据按照数据泄露或损坏造成的影响及其在保密性、完整性和可用性三个方面所表现出的重要程度进行分级，形成统一的分类分级方法。

5.2 分类分级流程

5.2.1 总体说明

5.2.1.1 本标准提供的数据分类分级方法，分为三个阶段：

a) 第一阶段：业务细分，解决业务分类问题，同时确定数据的管理主体；
b) 第二阶段：数据归类，在明确数据管理主体和业务分类的基础上，重点解决数据分类问题；
c) 第三阶段：级别判定，在数据分类基础上，进行数据定级。

5.2.1.2 数据分类后，宜同时明确数据的具体“数据形态”，即所处的系统、存储的媒介、物理位置等。

5.2.2 业务细分阶段

业务细分阶段应考虑：

a) 目标：对业务条线细分后，得到一系列有较清晰界限的业务类，根据业务流程梳理所有涉及到的数据；
b) 过程说明：根据本机构实际情况，按照推荐的方法，梳理“业务条线”，细分“业务流程”。

5.2.3 数据归类阶段

数据归类阶段应考虑：

a) 目标：
   1) 定业务流程中涉及数据对应的“数据类”；
   2) 对“数据类”细分得到数据子类；
   3) 如有必要，对数据子类进行细分。
b) 方法：
   1) 依据第一阶段划分的每个业务流程中的数据，对数据进行归类；
   2) 按照数据性质、重要程度、管理需要、使用需要等要素，将“数据类”细分为不同的数据子类；
   3) 如有必要，按照细分方法，进一步细分为数据子类。
c) 过程：
   1） 先确定各个业务下的全部数据（各种数据表、数据项、数据文件等），称为“数据类”。这个过程用于确定某类业务下存在的数据。例如先确定“核心业务”业务下的各类数据表、数据项、数据文件等；
   2） 之后对 “数据类”按照“细分方法”细分后得到数据子类。通常一个“数据类”下，有多个不同的数据子类。例如，“核心业务”下的数据子类可能有“客户类”、“账户类”等；
   3） 数据类可根据需要，按照细分方法再细分，得到数据子类；
   4) 数据分类层级过少，不利于定级；过多，不利于管理。一般划分到适合本机构定级需要即可，宜不超过三个层级。

5.2.4 级别判定阶段

级别判定阶段应考虑：

a) 目标：对已完成分类的数据子类进行定级；
b) 方法：采用基于影响的判定方法。由影响对象、影响范围、影响程度三要素判定；
c) 过程：将已划分完，可定级的数据子类，按照“基于影响的判定方法”进行定级。

6 数据分类要求

6.1 数据分类原则

6.1.1　科学性原则：按照互联网金融行业数据的多维特征及其相互间客观存在的逻辑关联进行科学和系统化的分类。

6.1.2　稳定性原则：互联网金融行业数据的分类应选择分类对象的最稳定的本质特性作为数据分类的基础和依据。

6.1.3　实用性原则：互联网金融行业数据分类要确保每个类目下要有数据，不设没有意义的类目，数据类目划分要符合用户的普遍认识。

6.1.4　扩展性原则：数据分类方案在总体上应具有概括性和包容性，能够实现各种类型互联网金融行业数据的分类，以及满足将来可能出现的数据类型。

6.1.5　规范性原则：所使用的词语或短语应能确切表达数据类目的实际内容范围，内涵、外延清楚；在表达相同的概念时，保证用语一致性；在不影响数据类目涵义表达的情况下，保证用语简洁性；在行业已有统一数据用语的情况下，使用统一数据用语。

6.2　数据分类方法

按照数据资源所涉及的知识范畴，将数据按照主题进行分类，采取大类、中类和小类三级分类法。同时从保护数据完整性的需求考虑，当同一主题的数据处于不同的数据形态时，其完整性保护的策略和方法是不同的，因此数据形态是数据分类的补充分类维度。互联网金融行业业务数据项和延伸数据线基本分类如表1和表2所示。

表 1　业务数据项基本分类

业务类型	数据类型	数据子类型
核心业务数据	客户类	客户基本信息，包括生日、性别、职业、职位、民族、姓名、地址、户口、工作单位、财务情况、婚姻情况等； 客户身份信息，包括身份证、护照、社保卡、居住证及其他法定证件影印件及号码等与自然人法定身份紧密相关的数据； 生物识别信息，包括但不限于基因、指纹、声纹、掌纹、耳廓、虹膜、面部特征等； 实名认证信息，包括视频认证信息、身份图片认证信息、财产图片认证信息等； 客户财产信息，如银行卡号、鉴别信息、存款信息、房产信息、资金流水等； 客户信用信息，如征信信息；
	账户类	账号信息、开户信息、冻结金额、额度、结算账号、结算金额、支付信息、余额、利率、期数、本金等
	交易类	交易日期、交易金额、交易种类、交易渠道、交易来源、交易日志信息、订单日志等
	产品类	支付密码、查询密码、介质号码（卡号）、产品代码、产品核心、产品状态等
	客户合约类	合约名称、合约签约机构、合约状态、签约渠道、费率、合约有效期、合约详情等
	渠道类	渠道名称、渠道类型、渠道寿命、折旧率、渠道故障信息等
	技术类	开发代码、测试用例、配置管理、测试方案等
	公共类	公共条件信息，如基准费率，财务类信息、资源信息等
	员工类	员工信息，如薪资、联系方式、教育信息、档案等
	业务管理类	监管信息、统计信息、公告信息等
	.....	

表 1 （续）

业务类型	数据类型	数据子类型
指标数据	规模类	总资产、各类贷款信息、投资信息、负债信息、存款信息、业务交易量、人员机构、所有者权益等
	效益类	营业收入、利息收入、利息支出、营业支出、中间业务收入等
	风险类	
	市场类	
	客户类	
	.....	
报表文件	月报、季报、年报	
	未公开报表	
综合管理类数据		
非核心业务数据		
电子报文		
影像数据		

表 2　延伸数据项基本分类

数据类型	数据子类型		数据类型	数据子类型
系统类	系统架构图		应用类	软件设计文档
	软硬件配置参数			数据结构
	数据库结构			数据字典
	系统密钥			软件测试文档
	系统管理员用户名与口令			程序源码
	运行维护手册			应用配置参数
	监控指标			应用管理员用户与口令
	.....			安装手册
网络类	网络拓扑结构图			运行维护手册
	网络配置参数			.....
	防火墙策略		运行类	操作手册
	路由策略			运行作业脚本
	网络协议、密钥、IP 地址与端口号			运行工管理员用户名与口令
	网络管理员用户名与口令			.....
	运行维护手册		环境类	机房电力、空调配置与参
	监控指标			运行维护手册
	.....			.....

7　数据分级要求

7.1　数据分级原则

7.1.1　依从性原则：数据级别划分应满足相关法律、法规及监管要求。

7.1.2　可执行性原则：宜避免对数据进行过于复杂的分级规划，保证数据分级使用和执行的可行性。

7.1.3　时效性原则：数据的分级具有一定的有效期。数据的级别可能因时间变化按照一些预定的安全策略发生改变。

7.1.4　自主性原则：机构可根据自身的数据管理需要，例如战略需要、业务需要、对风险的接受程度等，按照数据分类原则进行分类之后，按照数据分级方法自主确定数据层级，并为数据定级，但不宜将高敏感度数据定为低敏感度级别。

7.1.5　合理性原则：数据级别宜具有合理性，不能将所有数据集中划分一两个级别中，而另外一些没有数据。级别划定过低可能导致数据不能得到有效保护；级别划定过高可能导致不必要的业务开支。

7.1.6　客观性原则：数据的分级规则是客观并可以被校验的，即通过数据自身的属性和分级规则就可以判定其分级，已经分级的数据是可以复核和检查的。

7.1.7　流程差别化原则：应采取不同的安全策略和管理流程，差别对待不同安全等级的数据资产。

7.2　数据分级方法

7.2.1　数据定级影响要素如下：

a)　影响对象，划分为：行业、机构、客户；
b)　影响范围，划分为：多个行业、行业内多机构、本机构；
c)　影响程度，一般指数据安全属性（完整性、保密性、可用性）遭到破坏后带来的影响大小，划分为：严重、中等、轻微、无。

7.2.2　影响对象应考虑：

a)　影响对象为行业的情形：一般指数据的安全属性（完整性、保密性、可用性）遭到破坏后，可能对本行业及其他行业中一个或多个行业的经济活动秩序、生产经营秩序等造成影响；
b)　影响对象为机构的情形：一般指数据的安全属性（完整性、保密性、可用性）遭到破坏后，可能对行业内一家或多家机构的经济活动秩序、生产经营秩序等造成影响；
c)　影响对象为客户的情形：一般指数据的安全属性（完整性、保密性、可用性）遭到破坏后，可能对公民、法人、组织的社会权益、经济利益等造成影响。

7.2.3　影响程度宜综合考虑数据类型特征。例如：涉及个人信息的数据安全属性（保密性）遭到破坏产生的影响程度通常要高于已公开披露信息；交易、结算类型的数据安全属性遭到破坏产生的影响程度通常要高于非实时的行情信息类数据等。影响程度分类如表 3 所示。

表 3　影响程度分类

影响程度	参考说明
严重	可能导致全部业务无法开展，造成重大经济损失 可能引发公众广泛诉讼或集体诉讼，甚至引发群体性事件 可能导致监管部门严重处罚（包括取消经营资格、长期暂停相关业务等）的情况
中等	可能导致部分业务无法开展，造成较大经济损失 可能引发一定数量用户对本机构诉讼 可能导致监管部门较严重处罚（包括一段时间内暂停经营资格或业务等）的情况
轻微	可能导致个别业务无法开展，造成轻微经济损失 可能导致监管部门轻微处罚（包括罚款、公开批评等）的情况 可能对本机构声誉造成一定程度损害
无	不造成任何影响

7.2.4 数据等级标识

数据定级一般使用等级描述标识进行描述。本标准中的数据等级分为四级，描述标识分为数据级别标识和数据重要程度标识两类，相互一一对应：

a) 数据级别标识，从高到低划分为：4、3、2、1；

b) 数据重要程度标识，与数据级别标识相对应，从高到低划分为：极高、高、中、低；

c) 数据特征，数据级别从高到低，一般具有如表 4 所述数据特征。

表 4 数据特征

数据级别标识	数据重要程度标识	数据特征
4	极高	数据的安全属性（完整性、保密性、可用性）遭到破坏后数据损失后，影响范围大（跨行业或跨机构），影响程度一般是“严重”； 数据主要用于行业内大型或特大型机构中的重要业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用
3	高	数据的安全属性（完整性、保密性、可用性）遭到破坏后数据损失后，影响范围中等（一般局限在本机构），影响程度一般是“严重”； 数据用于重要业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用
2	中	数据的安全属性（完整性、保密性、可用性）遭到破坏后数据损失后，影响范围较小（一般局限在本机构），影响程度一般是“中等”或“轻微” 数据用于一般业务使用，一般针对受限对象公开；一般指内部管理且不宜广泛公开的数据
1	低	数据的安全属性（完整性、保密性、可用性）遭到破坏后数据损失后，影响范围较小（一般局限在本机构），影响程度一般是“轻微”或“无” 数据一般可被公开或可被公众获知、使用

7.2.5 数据定级规则

数据定级规则可参见表5。

表 5 数据定级规则

影响对象	影响范围	影响程度	数据一般特征	数据重要程度标识	数据级别标识
行业	多个行业	严重	数据主要用于行业内大型或特大型机构中的重要业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用	极高	4
机构	行业内多机构	严重		极高	4
客户	行业内多机构	严重		极高	3
机构	本机构	严重	数据用于重要业务使用，针对特定人员公开，且仅为必须知悉的对象访问或使用	高	3
客户	本机构	严重		高	3
影响对象	影响范围	影响程度	数据一般特征	数据重要程度标识	数据级别标识
机构	本机构	中等、轻微	数据用于一般业务使用，针对受限对象公开；一般指内部管理、办公类且不宜广泛公开的数据	中	2

表5 （续）

影响对象	影响范围	影响程度	数据一般特征	数据重要程度标识	数据级别标识
客户	本机构	中等	公开的数据	中	2
机构	本机构	无	数据可被公开或可被公众获知、使用	低	1
客户	本机构	轻微		低	1

A A

附 录 A
（规范性附录）
个人信息采集安全指南

A.1 明确责任部门与人员

A.1.1 法定代表人或主要领导人对个人信息采集安全负全面领导责任，包括为个人信息采集安全工作提供人力、财力、物力保障。

A.1.2 个人信息采集安全执行负责人、责任部门或工作人员其职责包括但不限于：

——对组织内个人信息采集安全负总责；

——负责开展组织内个人信息采集安全风险评估；

——制定、签发和实施个人信息采集的安全策略和规程；

——主动接受监督，与相关部门签署责任书，对接有关部门开展个人信息采集安全方面的工作。

A.1.3 遵守个人信息采集安全有关的法律法规、政策、行业标准等。

A.1.4 与从事个人信息采集岗位上的相关人员签署保密协议，必要时应开展背景审查。

A.1.5 明确内部涉及个人信息采集的安全职责，以及发生安全事件的处罚机制。

A.1.6 定期（至少每年一次）或在个人信息采集安全策略发生重大变化时，开展个人信息采集安全培训和考核，确保相关人员熟练掌握个人信息采集安全策略和规程。

A.2 明确个人信息采集安全措施

A.2.1 制定个人信息采集安全相关的策略和规程，包括但不限于：

——个人信息采集合规；

——采集方式；

——采集目的；

——个人信息采集传输；

——采集存储等相关规程。

A.2.2 定期（至少每年一次）审查和更新策略和规程相关文件，并评估策略和规程的实施效果。

A.2.3 明确建立、维护和更新采集的个人信息清单，清单内容包括但不限于：

——采集的个人信息类别和数量；

——与个人信息的采集相关的所有信息系统。

A.2.4 对可访问个人信息的内部授权人员，确保责任分离和最小授权，使其仅具备完成职责所需权限，并对权限管理建立追责制度。

A.2.5 对个人信息的采集活动设定相应的权限、审批和管理流程，括但不限于：

——监测并记录个人信息采集活动；

——对个人信息采集活动应进行内部审批或备案。

A.2.6 在采集个人信息的过程中，防止个人信息被窃取、篡改或劫持。

A.2.7 在信息系统设计阶段，做好个人信息安全规划，宜采用以下机制：

——系统默认关闭对个人信息的采集功能，采集该类信息时，应在用户使用系统过程中设置明确告知的功能，征得用户同意；

——系统提供个人选择的功能，供个人信息主体选择何种个人信息可被采集，并提供撤回同意的方

法；

——系统提供删除已采集个人信息的机制，实现个人信息主体注销账户后删除个人信息，法律法规另有规定的除外；

——系统对个人信息采集行为进行自动化审计；

——系统对个人信息的采集提供加密机制。

A.3 明确个人信息采集基本要求

A.3.1 个人信息采集的需求需确保目的合法、正当，能清晰、准确地予以描述，可对目的合法性进行验证，考虑因素包括但不限于：

——遵循法律法规和公序良俗；

——履行合同义务所必需；

——不侵害个人信息主体的利益；

——维护公共利益所必需。

A.3.2 根据已确定的目的，确定所需采集的个人信息最小元素集，以及存放地域、存储期限、采集频率等处理规则。

A.3.3 确保在采集前，通过个人信息主体易于访问、获得方式，以清楚明白易懂的语言，向个人信息主体告知相关信息，告知内容包括但不限于：

——个人信息控制者的基本情况，包括注册名称、注册地址、常用办公地点和联系方式、个人信息安全专员的联系方式（如适用）等；

——采集个人信息的目的和依据，以及目的与所收集的个人信息的对应关系；

——采集个人信息的范围、存放地域等；

——提供个人信息后可能存在的安全风险，及不提供个人信息可能产生的影响；

——采取的个人信息安全保护措施；

——个人信息主体的权利和实现机制，如选择和撤回同意的方法、访问方法、更正方法、删除方法、注销账户的方法、获取个人信息副本的方法、约束信息系统自动决策的方法等；

——处理个人信息主体询问和投诉的内部渠道和机制，以及外部争议解决机构及联络方式。

A.3.4 除法律法规另有规定外，应确保在取得个人信息主体授权同意后，才采集个人信息，包括：

——事先明确个人信息主体的同意范围，不应强制要求个人信息主体同意超范围采集个人信息的要求；

——采集个人敏感信息时，确保个人信息主体的同意是在完全知情的基础上自愿给出的，如个人信息主体主动声明（电子或纸质形式）或主动点击“同意”选项，不得以默许同意方式获取用户同意；

——采集个人信息主体的身份证、护照、驾照等法定证件信息时，应专门提醒个人信息主体此次采集活动涉及其法定证件信息，并说明采集目的；

——在采集未成年人个人信息前应取得其监护人或法定代理人的明示同意。

A.3.5 实际采集的个人信息范围超出个人信息最小元素集时，不得因个人信息主体不同意而拒绝向其提供服务或降低服务质量。

A.3.6 采集动态性的个人信息时，应保持合理的频率，避免超出服务目的所必需并确保在采集前获得用户明示同意授权。

A.3.7 如个人信息主体对采集行为有疑义或反对，应停止采集活动。

A.4 个人信息采集安全审计

A.4.1　应对个人信息采集安全相关的策略和规程的及时性，合理合规性以及其落实情况进行审计，形成审计记录。

A.4.2　审计记录应能对个人信息采集安全事件的处置、应急响应和事后调查提供支撑。

A.4.3　审计记录留存应符合相关法律法规的要求。

A.4.4　审计过程中发现的所有个人信息采集违规情况，应及时通知到个人信息采集安全相关人员，并确保落实整改方案。

A.4.5　可使用自动化机制对采集个人信息的入口进行追踪。常见的收集个人信息的入口如网页、软件客户端、移动应用软件等。

参 考 文 献

[1] GB/T 32921—2016 信息安全技术 信息技术产品供应方行为安全准则
[2]《全国人大常委会关于维护互联网安全的决定》
[3]《全国人大常委会关于加强网络信息保护的决定》
[4]工业和信息化部令第24号《电信和互联网用户个人信息安全规定》
[5]GB/T 271.1—2000 息技术 词汇 第1部分：基本术语
[6]GB/T 9246—2012 信息技术 安全技术 信息安全管理体系 概述和词汇
[7]JR/T 071—2012 金融行业信息系统信息安全等级保护实施指引
[8]SDS/T 121—2004 数据分类与编码的基本原则与方法
[9]银行数据资产安全分级标准与安全管理体系建设方法，赵鹏，马泽君，乐嘉伟
[10]科学数据分类规范与分类词表，中国科学院数据应用环境建设与服务项目组，2009年9月征求意见稿
[11]ISO/IEC 27001-2013 信息技术 安全技术 信息安全管理体系要求
[12]ISO/IEC 27002-2013 信息技术 安全技术 信息安全管理实用规则