ICS35.040
L80

中华人民共和国国家标准

GB/T XXXX-XXXX

信息安全技术
数据安全分类分级实施指南

Information security technology—

Implementation Guides of Data Security Classification

（草案）

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

本标准依据GB/T1.1—2009给出的规则进行起草。

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。

本标准主要起草单位：中国移动集团公司、中国电子技术标准化研究院、四川大学、公安部第三研究所、华为技术有限公司、国家互联网应急中心、深圳市腾讯计算机系统有限公司、中电长城网际系统应用有限公司、北京京东叁佰陆拾度电子商务有限公司、中国科学院计算机网络信息中心、北京天融信科技有限公司、中国科学院软件研究所、启明星辰信息技术集团股份有限公司、陕西省信息化工程研究院、广州天懋信息系统股份有限公司、中国软件与技术服务股份有限公司、深圳开源互联网安全技术有限公司、上海计算机软件技术开发中心、北京数字认证股份有限公司、北京微步在线科技有限公司、杭州华三通信技术有限公司、河南山谷网安科技股份有限公司、西北大学、西安未来国际信息股份有限公司、成都勤智数码科技股份有限公司、中电长城网际应用有限公司、中国软件与技术股份有限公司、北京元心科技有限公司、国家计算机网络应急技术处理协调中心、新华三技术有限公司、三六零科技股份有限公司、北京奇安信科技有限公司

本标准主要起草人：

引　　言

随着国家大数据发展战略的实施，“互联网+”行动的深入推进，大数据资源价值不断提升，电信、互联网、金融、政务、交通等各领域相关的大数据应用也在蓬勃发展。这些大数据应用涉及的数据量大、种类多，同时又包含有很多用户相关重要数据。

大数据应用在不断发展创新的同时，由于数据违规收集、数据开放与隐私保护相矛盾以及粗放式“一刀切”管理方式等给大数据应用的发展带来严峻的安全挑战。大数据资源的过度保护不利于大数据应用的健康发展，数据分类分级的安全管控方式能够避免“一刀切”带来的问题，实现大数据应用与个人权益的有效平衡。

信息安全技术　数据安全分类分级实施指南

1　范围

本标准草案主要包括数据安全分类分级模型、数据分类方法、数据分级方法和数据安全分类分级管理流程等相关技术要求。

本标准草案适用于数据安全分类分级的技术指导依据。

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 25069—2010 信息安全技术　术语

GB/T AAAAA—AAAA 信息技术 大数据 术语

GB/T BBBBB—BBBB 信息技术 大数据参考框架

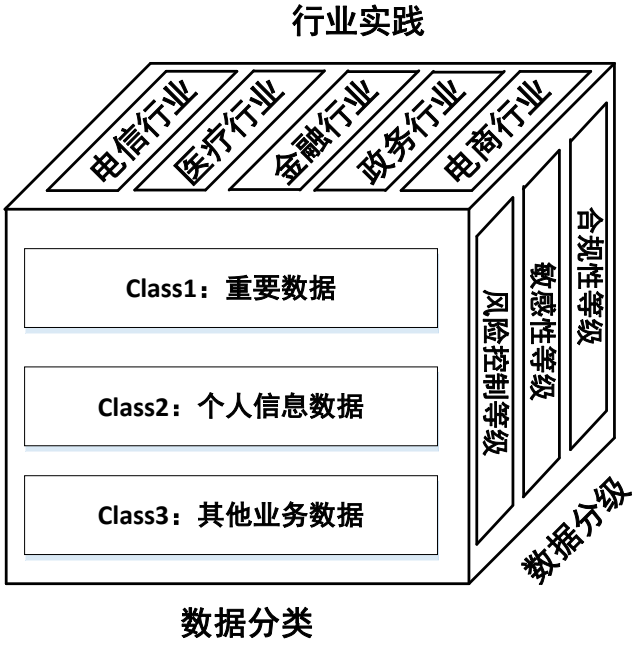
3　术语、定义和缩略语

3.1 术语和定义

3.2 缩略语

4　数据安全分类分级模型

为保护数据应用开展过程中所涉及的相关数据的安全，明确数据安全管控分类分级的方法，针对不同级别的数据，开展关键安全点梳理，并针对不同的安全点提出安全防护措施。



数据安全分类分级模型

数据分类分级模型可以划分为三个维度：1、数据分类；2、数据分级；3、行业实践。

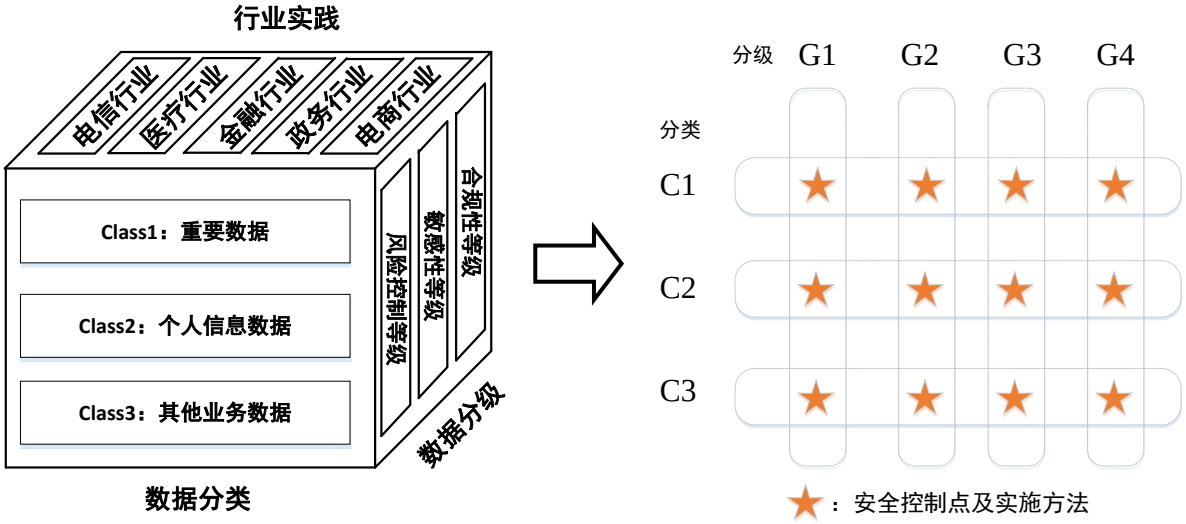
1. 在数据分类中对数据应用过程中涉及的数据进行分类，可按照数据的重要程度进行划分，如划分为重要数据、个人信息数据和其他业务数据；
   1) 重要数据：关键信息基础设施运营者在境内运营中收集、产生、控制的不涉及国家秘密，但与国家安全、经济发展、社会稳定，以及企业和公共利益密切相关的数据；
   2) 个人信息数据：以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等；
   3) 其他业务数据：企业或公共组织从事经营活动或例行社会管理功能、事务处理等一系列活动产生的可存储的数据，不包含重要数据和个人信息数据。
2. 数据分类之后可根据实际情况，在每个类别下可对数据进行分级，根据各级的安全管控需求，梳理安全控制点，然后提出分类分级的安全管控规则，常见的分级原则如下：
   1) 基于等级保护的数据分级：第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。第一级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护；第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。国家信息安全监管部门对该级信息系统安全等级保护工作进行指导；第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。国家信息安全监管部门对该级信息系统安全等级保护工作进行监督、检查；第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。国家信息安全监管部门对该级信息系统安全等级

保护工作进行强制监督、检查；第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。国家信息安全监管部门对该级信息系统安全等级保护工作进行专门监督、检查。

2) 基于风险防控的数据分级：A 级可接受风险、B 级一般不可接受风险、C 级严重不可接受风险；

3) 基于数据敏感性的数据分级：可划分为极敏感级、敏感级、较敏感级、低敏感级；

3. 各行业可以根据生产中实际的数据以及数据的特点，制定数据分类分级原则，并针对分类分级情况开展安全防控。



5 数据分类方法

5.1 重要数据

5.1.1 定义、范畴

重要数据是指关键信息基础设施运营者在境内运营中收集、产生、控制的不涉及国家秘密，但与国家安全、经济发展、社会稳定，以及企业和公共利益密切相关的数据，包括这些数据的原始数据和衍生数据，一旦未经授权披露、丢失、滥用、篡改或销毁将会造成以下后果：

1. 危害国家安全、国防利益、破坏国际关系；
2. 损害国家财产、公共利益和公民生命财产安全；
3. 影响国家预防和打击经济与军事间谍、政治渗透、有组织犯罪等，
4. 影响行政机关依法调查处理违法、渎职或涉嫌违法、渎职的行为；
5. 干扰政府部门依法开展监督、管理、检查、审计等行政活动，妨碍政府部门履行职责；
6. 危害国家关键基础设施、关键信息基础设施、政府信息系统安全；
7. 扰乱市场秩序，造成不公平竞争，破坏市场规律，影响产业发展；
8. 可推论出国家秘密事项；

9. 损害国家、企业、个人的其他利益和声誉，影响国家实力、形象或影响力；

10. 影响或危害经济、文化、科技、资源等其他国家安全事项。

5.1.2 安全控制点

1. 网络运营者在中华人民共和国境内运营中收集和产生的重要数据，应当在境内存储。
2. 网络运营者在中华人民共和国境内运营中收集和产生的重要数据，因业务需要，确需向境外提供的，应当按照《个人信息和重要数据出境安全评估办法》进行安全评估。
3. 重要数据出境时，应该重点评估一下内容：
   1) 数据出境的必要性；
   2) 涉及个人信息情况，包括个人信息的数量、范围、类型、敏感程度，以及个人信息主体是否同意其个人信息出境等；
   3) 涉及重要数据情况，包括重要数据的数量、范围、类型及其敏感程度等；
   4) 数据接收方的安全保护措施、能力和水平，以及所在国家和地区的网络安全环境等；
   5) 数据出境及再转移后被泄露、毁损、篡改、滥用等风险；
   6) 数据出境及出境数据汇聚可能对国家安全、社会公共利益、个人合法利益带来的风险；
   7) 其他需要评估的重要事项。

4. 出境重要数据存在以下情况之一的，网络运营者应报请行业主管或监管部门组织安全评估：
   1) 含有或累计含有 50 万人以上的个人信息；
   2) 数据量超过 1000GB；
   3) 包含核设施、化学生物、国防军工、人口健康等领域数据，大型工程活动、海洋环境以及敏感地理信息数据等；
   4) 包含关键信息基础设施的系统漏洞、安全防护等网络安全信息；
   5) 关键信息基础设施运营者向境外提供个人信息和重要数据；
   6) 其他可能影响国家安全和社会公共利益，行业主管或监管部门认为应该评估。
   7) 行业主管或监管部门不明确的，由国家网信部门组织评估。

5.2 个人信息数据

5.2.1 定义、范畴

一、个人信息的定义

目前，世界各国在立法中使用的与个人信息数据相关的有三个概念：个人数据、个人隐私与个人信息。与个人信息在概念上最为接近的是“个人数据”。其实，从个人数据较为统一的概念上理解，其与个人信息在基本内涵是相同的，区别在于表述的习惯不同，西方国家或者说国际立法上习惯称为个人数据（personal data），而国内一般习惯概括为个人信息（personal information）。可参考GB/T《信息安全技术 个人信息安全规范》。

最高人民法院、最高人民检察院首次就打击侵犯个人信息犯罪出台的司法解释与《中华人民共和国网络安全法》中所称个人信息，均指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。

二、个人信息的分类

根据不同的标准，个人信息可以划分为不同的类别：

以能否直接识别本人为标准，个人信息可以分为直接个人信息和间接个人信息。直接个人信息，是指可以单独识别本人的个人信息，如身份证号码、基因等；间接个人信息，是指不能单独识别本人，但和其他信息结合可以识别本人的个人信息。

以个人信息是否涉及个人隐私为标准，个人信息可以分为敏感个人信息和琐细个人信息(trivial data)。敏感个人信息，是涉及个人隐私的信息。根据英国1998年《资料保护条例》的规定，敏感个人信息是“由资料客体的种族或道德起源，政治观点，宗教信仰或与此类似的其他信仰，工会所属关系，生理或心理状况，性生活代理或宣称的代理关系，或与此有关的诉讼等诸如此类的信息组成的个人资料”。琐细个人信息是指不涉及个人隐私的信息。根据瑞典《资料法》的规定，琐细信息是指“很明显的没有导致被记录者的隐私权受到不当侵害的资料”。这点同我国《信息安全技术 公共及商用服务信息系统 个人信息保护指南》中对于个人信息的划分基本一致，即分为个人敏感信息和个人一般信息。

以个人信息的处理技术为标准，可以将个人信息划分为电脑处理个人信息与非电脑处理个人信息。

以个人信息是否公开为标准，可以分为公开个人信息和隐秘个人信息。公开个人信息，是指通过特定、合法的途径可以了解和掌握的个人信息。隐秘个人信息和公开个人信息对应，是指不公开的个人信息。这种分类的法律意义在于，公开个人信息无论是否属于敏感个人信息，都已经丧失了隐私利益，不能取得敏感个人信息的特殊保护。

以个人信息的内容为标准，个人信息还可以分为属人的个人信息和属事的个人信息。属人的个人信息反映的是个人信息本人的自然属性和自然关系，它主要包括本人的生物信息。属事的个人信息反映的是本人的社会属性和社会关系，它反映出信息主体在社会中所处的地位和扮演的角色。

个人信息还可以分为纳税信息、福利信息、医疗信息、刑事信息、人事信息和户籍信息等，不同信息的具体保护方式亦不相同。

5.2.2 安全控制点

信息泄漏。信息泄露依然是目前个人信息安全常见的风险。因一些掌握个人信息的公司对信息管理不严，加之恶意程序、各类钓鱼和欺诈事件频发，导致大量个人信息遭到泄露。人为倒卖信息、手机泄露、PC电脑感染、网站漏洞是个人信息泄露的四大途径。

信息发布。一些机构如人口统计、医疗、卫生等出于研究需要，经常要发布相关个人信息数据，尽管数据中已经隐匿了个人的标识信息，如姓名、身份证号等属性，但是，一些机构和个人仍然可以通过

对发布的数据和其他渠道获得的数据时行链接处理，进行链式攻击，推演出隐私数据，从而造成隐私泄露。

信息共享。许多在线服务要求人们共享私人信息，但是，共享数据后会有什么结果，数据会怎样被连接起来，具有较大的不确定性，如何确保数据正常使用情况下数据隐私不被泄漏，让用户对共享后的数据仍能进行细粒度控制，这都是个人信息安全必需着力控制的环节。

信息访问控制。由于大数据应用范围广泛，它通常要为来自不同组织或部门、不同身份与目的的用户所访问，实施访问控制是基本需求。然而，在大数据的场景下，有大量的用户需要实施权限管理，且用户具体的权限要求未知。面对未知的大量数据和用户，预先设置角色十分困难。信息访问控制成为当前个人信息安全方面重要的研究课题。

信息计算存储。从基础技术角度来看，大数据依托的基础技术是NoSQL（非关系型数据库），NoSQL缺乏数据安全机制，且允许不断对数据记录添加属性，其安全性要重新评估，另外，云计算的出现使用户不再对数据和环境拥有完全控制权，个人对存放在云中的数据不能像从前那样具有完全的管理权，变得非常不可控。云环境中用户数据安全与隐私保护更加困难。

信息可信保障。网络的数据并非都可信，过去往往认为“有图有真相”，事实上图片可以移花接木、时空错乱，或者照片是对的，可是文字解释是捏造的。信息不可信主要体现在伪造数据和数据失真两个方面。或伪造数据制造假象，或数据在传播中逐步失真，无法做到通过信息安全技术手段鉴别所有数据来源的真实性。

5.3 业务数据

5.3.1 定义、范畴

业务数据是企业或公共组织从事经营活动或例行社会管理功能、事务处理等一系列活动产生的可存储的数据。业务数据既包括从事业务经营活动或社会管理活动、事务处理等过程中的产生的决策数据、运营数据、结果数据和统计汇总分析数据，也包括承载业务运行的各种软硬件资源的基础资源数据、运行管理数据和统计分析数据。

5.3.2 安全控制点

企业或公共组织应该从以下几点进行业务数据安全管理和控制：

1. 建立信息安全管理机构或小组，由单位主要领导负责。落实使用单位安全管理主体责任，明确安全管理目标和计划并组织实施和量化考核。

2. 强化安全意识，建立安全检查实施细则和开展全员安全教育培训。

3. 结合行业特点，建立行业的数据安全技术标准、数据安全应急处置方案，容灾备份方案。

4. 信息系统建设在设计、施工和验收使用时，需有配套的保证数据安全加密校验机制，严格执行等保要求和等保测评。

5. 利用 IT 技术手段，对业务数据系统相关的软硬件设施进行严密的监控管理。实时监控网络设备、应用和数据库服务器、操作系统、数据库服务、应用系统、存储系统的异常情况并及时进行整改。

6. 委托数据安全管理专业机构或企业进行数据安全维护服务，要严格审查其资质、信誉和同行业服务水平，签到正式服务合同和保密协议。

7. 积极开展数据安全风险评估工作，定期对数据相关软硬件设施和配套资源进行安全评估，及时发现问题，及时整改。

8. 对数据操作人员、查询人员、使用人员和运维服务人员签订保密协议，实行严格的保密管理制度，对关键岗位采用“双人在岗制”。

9. 结合数据安全技术如密码技术、访问控制和鉴权、环境安全、设备安全、防火墙、VPN、入侵检测/入侵防御、安全网关、容灾与数据备份等，进行多层次、全方位安全防护和加固。

6 数据分级方法

6.1 重要数据分级方法

应遵守国家和行业数据出境分级分类有关法律法规要求，分析重要数据对于国家经济安全、社会安全、政治安全等影响程度，明确重要数据归属级别、类别，并完善与之相匹配的数据出境管理机制。

对于禁止出境的重要数据，应严格禁止数据出境；对于限制出境的重要数据，应积极配合中央、地方网信办和相关行业主管部门开展的安全评估，通过安全评估后进行出境；对于允许出境的重要数据，应加强数据出境过程中的安全管理。

注：关于重要数据的分类与范围可参考《重要数据判定指南》。

6.2 个人信息分级方法

《信息安全技术 公共及商用服务信息系统 个人信息保护指南》将个人信息划分为个人敏感信息和个人一般信息。

个人敏感信息是指一旦遭到泄露或修改，会对标识的个人信息主体造成不良影响的个人信息。各行业个人敏感信息的具体内容根据接受服务的个人信息主体意愿和各自业务特点确定。例如个人敏感信息可以包括身份证号码、手机号码、种族、政治观点、宗教信仰、基因、指纹等。

个人一般信息是指除个人敏感信息以外的个人信息。

6.3 业务数据分级方法

业务数据分级应按照行业性的规范和标准，依据业务数据业务特征、安全要求、数据关联性、数据范围、信息公开要求等业务数据属性或特征，进行分级划分。划分原则应遵循以下要求：

1. 科学性：选择数据中最核心的本质属性或特征，作为分类的基础和依据，确保建立一个面向业务主题的分级体系。

2. 系统性:选定数据整体的属性或特征进行系统化抽象，形成一个科学合理的分级体系。

3. 可扩展性:分级应满足业务数据的不断发展和变化的需要。

4. 兼容性:分级应兼容国际、国家和行业相关标准及要求。

5. 行业性:分级应考虑业务数据的行业特点和要求，满足管理上和应用上的实际情况。

6. 安全性：分级应考虑数据的安全性要求，满足数据安全管理的要求。

总之，业务数据分级是数据管理的最基础性工作，同时又是一项系统性工程。因此，在业务数据分级的过程中，一定要以单位的具体需求为基础，以实用为出发点，采取正确的工作思路，多样化的手段对业务数据进行科学化、系统化的级次划分。

业务数据分级也可以依据业务数据风险控制等级进行分级分类，具体方法是采用是非判断法和威胁风险系数法。

是非判断法：依据专业技术人员的技术知识和行业经验对潜在威胁进行是非分级判断。

威胁风险系数法：依据威胁发生的可能性和威胁产生影响程度进行威胁指数计算，再依据威胁等级划分标准进行划分等级，具体算法：威胁指数 D=威胁发生的可能性 L*威胁影响程度 C。参数数值对应级别如下图：

威胁指数 D	A 级可接受风险（1—13）	B 级一般不可接受风险（14—18）		C 级严重不可接受风险（19—25）	
发生可能性 L	极低（1）	低（2）	中等（3）	高（4）	很高（5）
影响程度 C	几乎无（1）	轻微性（2）	一般性（3）	严重性（4）	非常严重（5）

附录 A 各行业数据分类分级实践

A.1 政务数据分类实践

为了科学、有效地对政府数据进行组织管理，该分类方法从政府数据本身的自然属性出发，结合政府数据所特有的行业属性特征，以及政府数据开放和共享需求，制定政府数据分类方法。

本标准采用多维度和线分类法相结合方法，首先在主题、行业和服务三个维度对贵州省政府数据进行分类，然后对于每个维度采用线分类法将其分为大类、中类和小类三级。

A.1.1 政务数据分类

1）主题分类

按照政府数据资源所涉及的知识范畴，将贵州省政府数据按照主题进行分类，采取大类、中类和小类三级分类法。

按主题将政府数据分为以下基础大类：经济、政治、军事、文化、资源、能源、生物、交通、旅游、环境、工业、农业、商业、教育、科技、质量、食品、医疗、就业、人力资源、社会民生、公共安全、信息技术。对于每一个大类主题，按线分类法划分中类。对于每个中类，按照线分类法划分小类。基础大类主题之外的其他主题可以作为扩展主题，依照主题分类方法进行分类。主题分类方法可参考《政务信息资源目录体系 第4部分：政务信息资源分类》。

2）行业分类

按行业将贵州省政府数据分为以下大类：农林牧渔业、采矿业、制造业、电力燃气及水的生产和供应业、建筑业、交通运输、仓储和邮政业、信息传输计算机服务和软件业、批发零售业、住宿和餐饮业、

金融业、房地产业、租赁和商务服务业、科学研究、技术服务和地质勘查业、水利、环境和公共设施管理业、教育、卫生、社会保障和社会福利业、文化、体育和娱乐业、公共管理和社会组织、国际组织。

对于每一个大类行业，按线分类法划分中类。对于每个中类，按照线分类法划分小类。行业分类方法见附表2。

3）服务分类

政府数据按服务分类基于以下依据：

1） 要对构建服务型政府形态具有技术指导作用；

2） 体现经济调节、市场监管、社会管理、公共服务等政府职能；

3） 有利于实现政府内部跨部门、跨行业、跨地区信息共享目标；

4） 以面分类法为主，与线分类法结合。

对于每一个大类服务，按线分类法划分中类。对于每个中类，按照线分类法划分小类。服务分类方法

A.1.2 政府数据分级

政府数据分级应充分考虑政府数据对国家安全、社会稳定和公民安全的重要程度，以及数据是否涉及国家秘密、是否涉及用户隐私等敏感信息直接相关。应该考虑不同敏感级别的政府数据在遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益（受侵害客体）的危害程度来确定政府数据的级别。

政府数据的分级由数据的敏感程度划分。政府数据的分级方法如表1所示。

表1 政府数据分级

	政府数据敏感程度		
	非敏感数据	**涉及用户隐私数据**	**涉及国家秘密数据**
等级划分	公开数据	内部数据	涉密数据

政府数据的分级结果将对政府数据的开放和共享提出不同要求。政府数据的分级结果将确定该类型政府数据是否适合开放和共享、数据开放和共享的范围，以及在对该级别政府数据进行开放和共享前是否需要脱密和脱敏（包括逻辑数据运算等处理方式）处理等。

表 2 不同政府数据等级管控要求

数据类型	数据等级管控要求
公开数据	政府部门无条件共享；可以完全开放。
内部数据	政府部门无条件共享；按国家法律法规决定是否开放，原则上不违反国家法律法规的条件下，予以开放或脱敏开放。
涉密数据	按国家法律法规处理，决定是否共享，可根据要求选择政府部门条件共享或不予共享；原则上不允许开放，对于部分需要开放的数据，需要进行脱密处理，且控制数据分析类型。

A.2 电信数据分类实践

A.2.1 电信数据分类

为便于对数据进行统一管理及推广应用，将电信企业各系统或平台涉及的用户数据整合纳入以下三大类。

表 1 数据分类表

类别	子类及范围
（A类）用户身份相关数据	**（A1）用户身份和标识信息：**（A1-1）自然人身份标识、（A1-2）网络身份标识、（A1-3）用户基本资料、（A1-4）实体身份证明、（A1-5）用户私密资料 **（A2）用户网络身份鉴权信息：**（A2-1）密码及关联信息
（B类）用户服务内容数据	**（B1）服务内容和资料数据：**（B1-1）服务内容数据、（B1-2）联系人信息
（C类）用户服务衍生数据	**（C1）用户服务使用数据：**（C1-1）业务订购关系、（C1-2）服务记录和日志、（C1-3）消费信息和账单、（C1-4）位置数据、（C1-5）违规记录数据 **（C2）设备信息：**（C2-1）设备标识、（C2-2）设备资料

a)用户身份相关数据（A 类）

用户身份相关数据包括用户身份标识信息和用户网络身份鉴权信息。

表 2 A 类数据详细内容

子类	范围	对应数据
A1.用户身份和标识信息	A1-1：自然人身份标识	客户姓名、证件类型及号码、驾照编号、银行账户、客户实体编号、集团客户编号、集团客户名称等
	A1-2：网络身份标识	联系电话、邮箱地址、网络客户编号、即时通信账号、网络社交用户账号等
	A1-3：用户基本资料	客户职业、工作单位、年龄、性别、籍贯、兴趣爱好等；集团客户所在省市、所在行业等
	A1-4：实体身份证明	身份证、护照、驾照、营业执照等证件影印件；指纹、声纹、虹膜等
	A1-5：用户私密资料	揭示个人种族、家属信息、居住地址、宗教信仰、个人健康、私人生活等用户私密信息 《征信业管理条例》等法律、行政法规规定禁止公开的用户其他信息
A2：用户网络身份鉴权信息	A2-1：用户密码及关联信息	用户网络身份密码及关联信息，如：手机客服密码，以及与密码关联的密码保护答案等

b)用户服务内容数据（B 类）

用户服务内容数据包括用户服务内容数据和联系人信息。

表 3 B 类数据详细内容

子类	范围	对应数据
B1：服务内容和资料数据	B1-1：服务内容数据	**电信网服务内容数据：**短信、彩信、话音等通信内容 **移动互联网服务内容信息：**包括：即时通信内容、群内发布内容、数据文件、邮件内容、用户上网

		访问内容等；用户云存储、SDN、IDC 等存储或缓存的非公开的私有文字、多媒体等资料数据信息
	B1-2：联系人信息	用户通讯录、好友列表、群组列表等用户资料数据

c)用户服务衍生数据（C 类）

用户服务衍生数据主要包括用户服务使用数据和设备信息。

表 4 C 类数据详细内容

子类	范围	对应数据
C1:用户服务使用数据	C1-1：业务订购关系	**基本业务订购关系**：品牌、套餐定制等情况 **增值业务订购关系**：邮箱、通讯录等增值业务的注册、修改、注销
	C1-2：服务记录和日志	**服务详单及信令**：包括语音、短信、彩信和数据详单等 **移动互联网服务记录**：包括 Cookie 内容、上网日志等
	C1-3：消费信息和账单	**消费信息**：停开机、入网时间、在网时间、积分、预存款、信用等级等 **账单**：每月出账的固定费用、通信费用等
	C1-4：位置数据	精确位置信息(如小区代码、基站号、基站经纬度坐标等) 大致位置信息(如地区代码等)
	C1-5：违规记录数据	用户违规记录，包括垃圾短信、骚扰电话等黑名单、灰名单等 业务违规记录，包括端口滥用、违规渠道、不良网站域名等记录、黑名单、灰名单等
C2：设备信息	C2-1：终端设备标识	唯一设备识别码 IMEI、设备 MAC 地址等
	C2-2：终端设备资料	终端型号、品牌、厂商等

A.2.2 电信数据分级

根据数据的敏感程度不同以及企业的实践经验，将电信企业所涉及的用户数据由低到高划分为1～5级。

表5 数据分级表

类别	子类及范围
第5级	（A1-4）实体身份证明、（A1-5）用户私密资料、（A2-1）用户密码及关联信息
第4级	（A1-1）自然人身份标识、（B1-2）联系人信息、（C1-4）位置数据

第3级	（A1-2）网络身份标识、（A1-3）用户基本资料、（B1-1）服务内容数据、（C1-2）服务记录和日志、（C2-1）终端设备标识、（C2-2）终端设备资料
第2级	（C1-3）消费信息和账单、
第1级	（C1-1）业务订购关系、（C1-5）违规记录数据

A.3 能源数据分类实践

能源大数据理念是将电力、石油、燃气等能源领域数据及人口、地理、气象等其他领域数据进行综合采集、处理、分析与应用的相关技术与思想。能源大数据不仅是大数据技术在能源领域的深入应用，也是能源生产、消费及相关技术革命与大数据理念的深度融合，将加速推进能源产业发展及商业新模式。

以国家电网为例，现有的数据分类大致如下：

电力数据主要来源于电力生产和电能使用的发电、输电、变电、配电、用电和调度各个环节，可大致分为三类：一是电网运行和设备检测或监测数据；二是电力企业营销数据，如交易电价、售电价、用电客户等方面数据；三是电力企业管理数据。

若以安全分区进行划分，数据主要分为两大类，包括生产控制数据和管理信息数据。安全分区是电力监控系统安全防护体系的结构基础，数据以安全分区为依据进行分类。发电企业、电网企业内部基于计算机和网络技术的业务系统，原则上划分为生产控制大区和管理信息大区。生产控制大区可以分为控制区（又称安全区 I）和非控制区（又称安全区Ⅱ）。在满足安全防护总体原则的前提下，可以根据业务系统实际情况，简化安全区的设置，但是应当避免形成不同安全区的纵向交叉联接。

（1）生产控制数据

生产控制大区的安全区划分为控制区和非控制区。如下：

1）控制区（安全区Ⅰ）：

控制区中的业务系统或其功能模块（或子系统）的典型特征为：是电力生产的重要环节，直接实现对电力一次系统的实时监控，纵向使用电力调度数据网络或专用通道，是安全防护的重点与核心。

控制区的数据来源于传统典型业务系统包括电力数据采集和监控系统（SCADA）、能量管理系统(EMS)、广域相量测量系统(PMS)、配网自动化系统（DAS）、变电站自动化系统、发电厂自动监控系统等，其主要使用者为调度员和运行操作人员，数据传输实时性为毫秒级或秒级，其数据通信使用电力调度数据网的实时子网或专用通道进行传输。该区内还包括有采用专用通道的控制系统，如：继电保护、安全自动控制系统、低频（或低压）自动减负荷系统、负荷管理系统等，这类系统对数据传输的实时性要求为毫秒级或秒级，其中负荷管理系统为分钟级。

2）非控制区（安全区Ⅱ）：

非控制区中的业务系统或其功能模块的典型特征为：是电力生产的必要环节，在线运行但不具备控制功能，使用电力调度数据网络，与控制区中的业务系统或其功能模块联系紧密。

非控制区的数据来源于传统典型业务系统包括调度员培训模拟系统、水库调度自动化系统、故障录波信息管理系统、电能量计量系统（TMR）、实时和次日电力市场运营系统等，其主要使用者分别为电

力调度员、水电调度员、继电保护人员及电力市场交易员等。在厂站端还包括电能量远方终端、故障录波装置及发电厂的报价系统等。非控制区的数据采集频度是分钟级或小时级，其数据通信使用电力调度数据网的非实时子网。

（2）管理信息数据

管理信息大区是指生产控制大区以外的电力企业管理业务系统的集合。管理信息数据来源于管理信息大区的传统典型业务系统如调度生产管理系统（DMIS）、行政电话网管系统、电力企业数据网等的数据。

实际操作中，根据数据的分类原则对跨专业数据共享、数据跨境等采取不同的防范措施，来提高系统整体安全防护能力，保证电力监控系统、个人敏感数据等重要数据的安全。

A.4 征信数据分类实践

与个人信息在概念上最为接近的是“个人数据”。如前所述，个人数据概念使用的较多的主要是欧盟成员国以及其他受 1995 年欧盟《个人数据保护指令》影响而立法的其他大多数国家。在普通法国家（英国作为欧盟成员国除外），如美国、澳大利亚、新西兰、加拿大等，以及受美国影响较大的亚太经济合作组织（APEC），则大多使用隐私法概念。在日本、韩国、俄罗斯等国，则使用“个人信息法”概念。所以，从个人数据较为统一的概念上理解，个人信息与个人数据两个概念的基本内涵是相同的，区别在于表述的不同，在国内一般习惯将其概括为个人信息（personal information），而西方国家或者说国际立法上则更习惯于称其为个人数据（personal data）。

个人信息保护的主要目的和逻辑前提是隐私权的保护问题。在最初的阶段，隐私权一直被作为侵权行为法上的权利，意味着与个人私生活有关的信息不受公开以及属于私事的领域不受干涉的自由，是一种要求他人放任自己独处而不受打扰的权利。而随着人类社会的不断发展，个人的私生活越来越暴露于各种强势团体、尤其是公权力面前，隐私权又逐步由私法上的权利演变为公民的宪法权利。

20 世纪 60 年代后，信息的大量收集、储存和利用成为可能，隐私权受到侵害的可能性越来越大。因此，传统意义上具有消极、被动等特点的隐私权概念已很难适应社会发展的需要。于是，又出现了所谓“个人信息控制权”的理论，即“所谓隐私权，乃是指个人自由地决定在何时、用何种方式、以何种程度向他人传递与自己有关的信息的权利主张”。这样，现代意义的隐私权在具有消极、静态、阻碍他人获取与个人有关的信息等特性的同时，更具有了与该信息有关的支配权的特点。

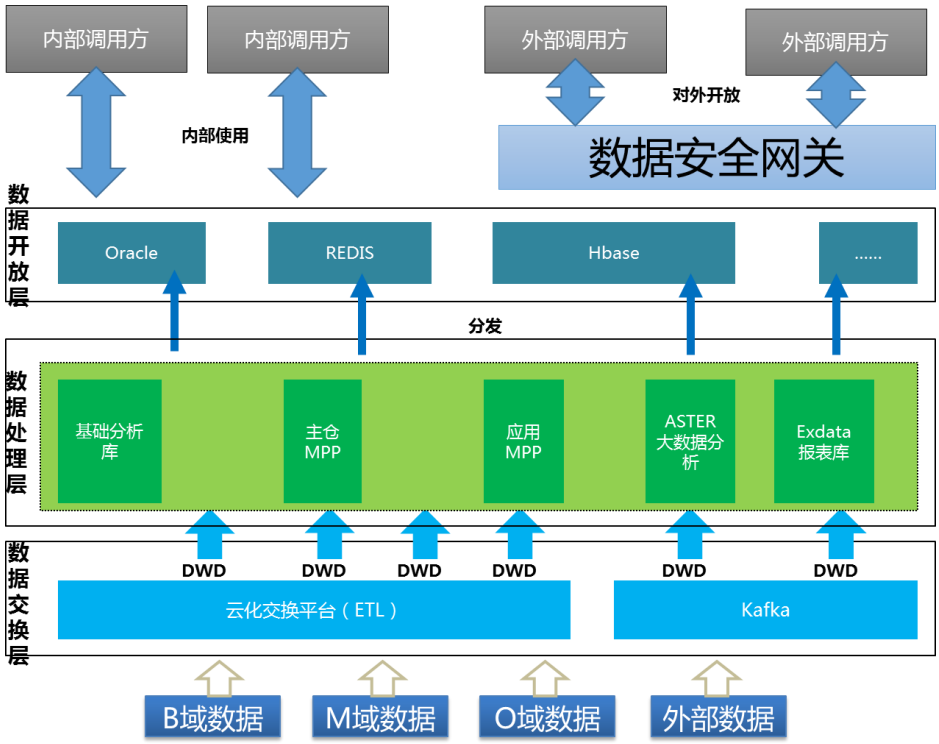
现代隐私权所保障的已不限于传统意义上尚不为人所知、不愿或者不便为人所知的私事（即一般而言的隐私），而是扩展到了所谓的个人信息，即识别出或者可以识别出个人的所有信息，这些信息可以以任何形式存在于任何媒介之上。个人信息不加保护必然带来以下问题：1．通过对各种个人信息的结合将可以描绘出本人的整体形象，进而导致他人知悉本人不愿为人所知的个人私事；2．本人有可能会因他人持有自己的各种个人信息而受到控制和支配；3．有关本人的各种决定难免会基于错误的个人信息做出。

个人信息主要包括：（1）个人数据：如姓名、性别、年龄、身高、体重、个人身世、血型、指纹、出生日期与地点、种族、身份证号、家庭地址、工作单位、学历、生活经历与习惯、健康状况等。（2）私人信息：如个人存款账号及密码、工资单及账号、股东卡账号及证券交易密码、信用卡号及密码、社会保险号码、私人财务清单、电话费清单、个人债务、购物习惯及偏好、消费者的信用和财产状况等（3）个人领域：公民的电话号码、手机号码、传呼号码、QQ 号码、通信地址、E-mail 地址及个人计算机内存储的信息等。（4）个人网络活动踪迹。如 IP 地址、浏览踪迹、活动内容，均属个人信息的隐私。

根据来源的不同，又可分为以下几类：一是来自于人，人们在互联网活动以及使用移动互联网过程中所产生的各类数据，包括文字、图片、视频等信息。二是来自于机，各类计算机信息系统产生的数据，以文件、数据库、多媒体等形式存在，也包括审计、日志等自动生成的信息。三是来自于物。各类数字设备所采集的数据，如摄像头产生的数字信号、医疗物联网中产生的人各项特征值、天文望远镜所产生的大量数据。

附录 B 数据安全分类分级管理流程

大数据平台数据流转如下图所示：



1. 数据采集：数据通过交换层的 ETL，kafka 等工具，从各个外部系统进行采集；
2. 数据存储：外部系统的数据通过采集，存储到大数据平台；
3. 分析处理：在数据处理层对于采集来的原始数据，进行计算分析，加工生成新的数据；
4. 数据分发：通过数据交换工具，将数据从数据处理层分发到内部系统，供应用使用
5. 数据使用：将数据提供给内部应用使用；
6. 对外开放：将内部的数据，通过安全网关提供给外部系统使用；

在这 6 个过程中，数据安全分类分级管理实施方法：

1. 数据采集环节：在已知数据类型时，可以在采集配置时增加标识数据类型和敏感级别，在数据录入 DACP 时自动追加标识。

2. 数据存储环节：通过租户隔离，控制不同租户间的数据互访；将所有存储的数据进行扫描检测，纳入 DACP 数据字典管理，并对 DACP 存储的数据通过自动和人工检测审核的方式，确定数据类型和敏感级别；

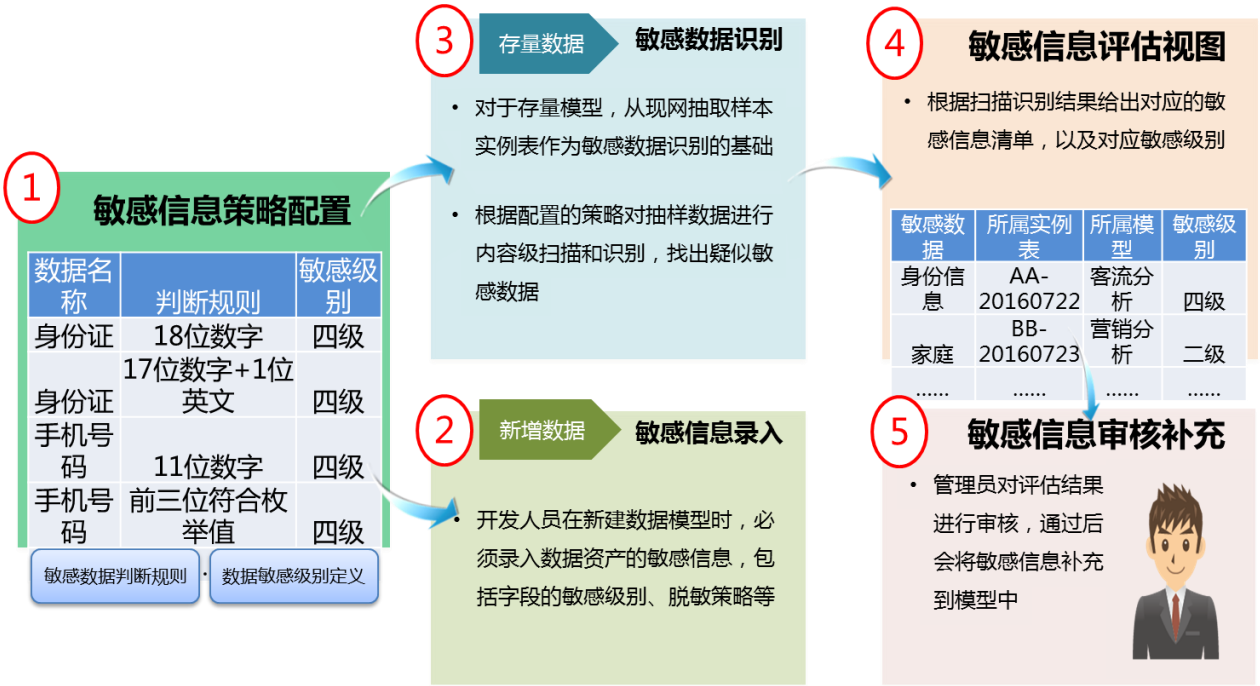
3. 分析处理环节：通过租户隔离，控制不同租户间的数据互访；对于通过基础数据新生成的数据模型，也纳入 DACP 数据字典管理，并对 DACP 存储的数据通过自动和人工检测审核的方式，确定数据类型和敏感级别；

4. 数据使用环节：对内部应用，通过账号权限、金库管理、数据脱敏进行分类分级管控。

5. 数据分发环节：将数据分发到内部系统时，通过业务评审，确认可以分发的数据类型与级别，对数据进行相应的分类分级管控；

6. 对外开放环节，通过业务评审，确认可以开放的数据类型和级别、需要采取的数据安全管控措施，引入可信的第三方安全算法，对数据进行加密，提高数据破解难度，减少数据在外网流通被破解的风险。主要通过数据安全网关进行防护。

数据分类分级处理：



对于数据的分类分级，通过元数据进行管理。采用两种方式进行

1. 新建元数据时，需要注明数据的分类分级；

2. 定时扫描机制，对于存量数据进行智能化扫描，得出数据的分类分级；后续将扫描结果由管理员做相应的确认，并更新到元数据相关信息中。

业务数据分类：

A 用户身份相关:用户身份相关数据包括用户身份标识信息和用户网络身份鉴权信息。

B 用户服务内容数据: 用户服务内容数据包括用户服务内容数据和联系人信息。

C 用户服务衍生数据: 用户服务验证数据主要包括用户服务使用数据和设备信息。

D 企业运营管理数据: 企业运营管理数据包括企业管理数据、业务运营数据、网络及 IT 系统运维数据和合作伙伴数据。

敏感数据分级：

数据分级应依据以下原则：

a) 各级界限明确原则：数据分级是按照数据敏感程度进行划分；

b) 就高不就低原则：如果同一批数据中各属性或字段的分级不同，需要按照定级最高的属性或字段的级别一并实施安全管控，即 “就高不就低”

数据的敏感级别分为字段级与内容级：

1. 字段级：具体表中的某个字段定义敏感级别。例如某个表中的身份证号，银行卡号等字段，属于敏感信息，定义为一级敏感信息。

2. 内容级：具体表中符合某种条件的数据定义敏感级别。例如用户表中，符合用户类别为党政军的属于一级敏感信息。

类别	定位	管控措施
第 4 级	极敏感级	实施严格的技术和管理措施，保护数据的机密性和完整性，确保数据访问控制安全，建立严格的数据安全管理规范以及数据实时监控机制。第 4 级数据严禁对外输出
第 3 级	敏感级	实施较严格的技术和管理措施，保护数据的机密性和完整性，确保数据访问控制安全，建立数据安全管理规范以及数据准实时监控机制。第 3 级数据在满足相关条件的前提下，可以对外开放
第 2 级	较敏感级	实施必要的技术和管理措施，确保数据生命周期安全，建立数据安全管理规范。第 2 级数据在满足相关条件的前提下，可以对外开放
第 1 级	低敏感级	实施基本的技术和管理措施，确保数据生命周期安全。第 1 级数据可以直接对外开放，但需要考虑对外开放的数据量及类别，避免由于类别较 多或者数据量过大，导致能够用于关联分析。