

《信息安全技术 网络数据分类分级要求》（征求意见稿）要点解读

作者：段志超 | 蔡克蒙 | 胡敏喆¹

2022年9月14日，全国信息安全标准化技术委员会秘书处（“信安标委”）发布了《信息安全技术 网络数据分类分级要求》（征求意见稿）（“《分类分级要求》”）。《分类分级要求》进一步细化和落实了《数据安全法》第21条的数据分类分级要求，阐明了数据分类分级的基本原则、数据分类分级框架和方法以及数据分类分级实施流程，并以附录形式详细介绍了数据分级要素识别常见考虑因素、影响对象考虑因素、影响程度参考示例等数据分类分级时所需关注的参考要点以及基于数据描述对象的行业领域数据分类参考示例、衍生数据定级参考、动态更新情形参考、一般数据分级参考、个人信息分类示例等常见的数据分类分级示例，为各行业、各领域、各地方、各部门和数据处理者开展数据分类分级工作提供了指导和帮助。本文旨在简析《分类分级要求》提出的分类分级框架及思路，并提示需关注的重点事项。

一、数据分类分级的意义

数据分类分级是数据安全保护最重要的基础性工作。数据处理者对数据进行分类和分级可更清晰地梳理数据资产，针对不同类型、不同级别的数据制定和采取不同的安全保护措施，从而实现数据安全保护与数据流通利用的平衡。

数据分类工作旨在对数据资产盘点梳理并进行标准化、专业化管理，将常见、稳定的属性或特征作为数据分类的依据，从而便于依照类别建立完善有序的数据架构，以实现高效准确的数据管理与使用。

数据分级工作则强调基于数据在经济社会发展中的重要程度，以及一旦遭到泄露、篡改、破坏或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，通过定量与定性相结合，根据数据分级要素开展数据影响分析，从而为数据划分不同级别。数据处理者应针对不同级别的数据，制定对应的安全策略、确定适当的对外开放程度并在全生命周期采取不同的安全保护措施。

近年来，我国先后在多部法律法规政策文件中强调数据分类分级相关工作的重要性。

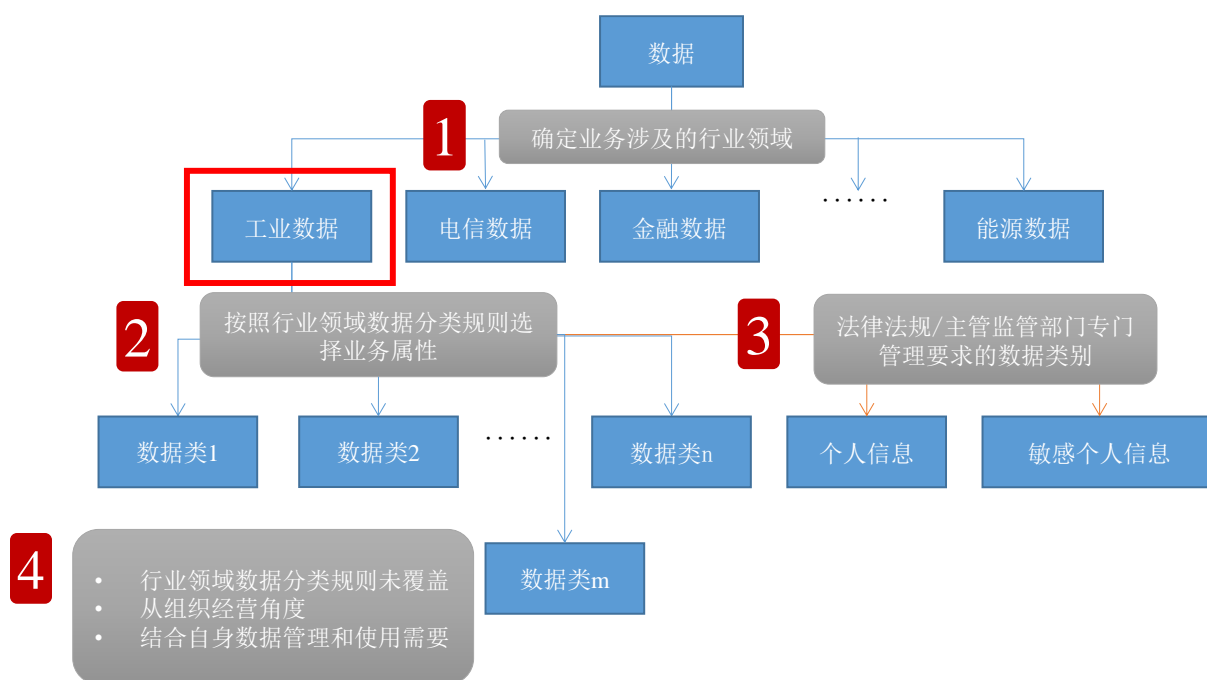
- 2020年4月9日，中共中央、国务院发布的《关于构建更加完善的要素市场化配置体制机制的意见》提出“要推动完善适用于大数据环境下的数据分类分级安全保护制度，加强政务数据、企业商业和个人数据的保护”；

¹ 实习生甘雨丰对本文的写作亦有贡献。

- 《网络安全法》第 21 条规定，“网络运营者应当采取数据分类、重要数据备份和加密等措施”。
- 《数据安全法》正式提出了数据分级分类制度，并在分级分类基础上要求对核心数据和重要数据做出重点保护。其中，第 21 条规定，“国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。”全国人大常委会法制工作委员会也在立法说明文件中将数据分类分级制度列为数据安全制度之首。
- 《个人信息保护法》第 51 条同样将个人信息分类管理规定为个人信息处理者需采取的基本安全保护措施²。
- 《网络数据安全管理条例（征求意见稿）》（“**数安条例**”）第 5 条规定“国家建立数据分类分级保护制度。按照数据对国家安全、公共利益或者个人、组织合法权益的影响和重要程度，将数据分为一般数据、重要数据、核心数据，不同级别的数据采取不同的保护措施。国家对个人信息和重要数据进行重点保护，对核心数据实行严格保护。”

二、细化数据分类框架及方法

在信安标委 2021 年 12 月发布的《网络安全标准实践指南 网络数据分类分级指引》（“**分类分级指引**”）的基础上，《分类分级要求》对数据分类方法做出了更明确和具体的要求。数据处理者开展数据分类的相关流程和要点如下：



² 《个人信息保护法》第五十一条“个人信息处理者应当根据个人信息处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失：…（二）对个人信息实行分类管理…”

（一）按照行业领域进行分类

《分类分级要求》明确数据分类应先按照业务所属行业领域将数据分为不同行业领域数据，例如：工业数据、电信数据、金融数据等。对于数据处理者而言，其应当首先明确自身业务涉及的行业领域。

（二）根据业务属性做进一步分类

在按照行业领域进行分类的基础上，各行业各领域主管（监管）部门将根据本行业本领域业务属性，例如：业务领域、责任部门、描述对象、上下游环节、数据主题、数据用途、数据处理、数据来源等，对行业领域数据进行细化分类。数据处理者应当按照所属行业领域的数据分类规则，灵活选择业务属性对该业务运营过程中收集和产生的数据进行分类。附件 A 给出了基于数据描述对象的行业领域数据分类参考示例，将行业领域数据分为用户数据、业务数据、经营管理数据以及系统运行和安全数据。

（三）应对法律法规或主管监管部门有专门管理要求的数据进行识别和分类

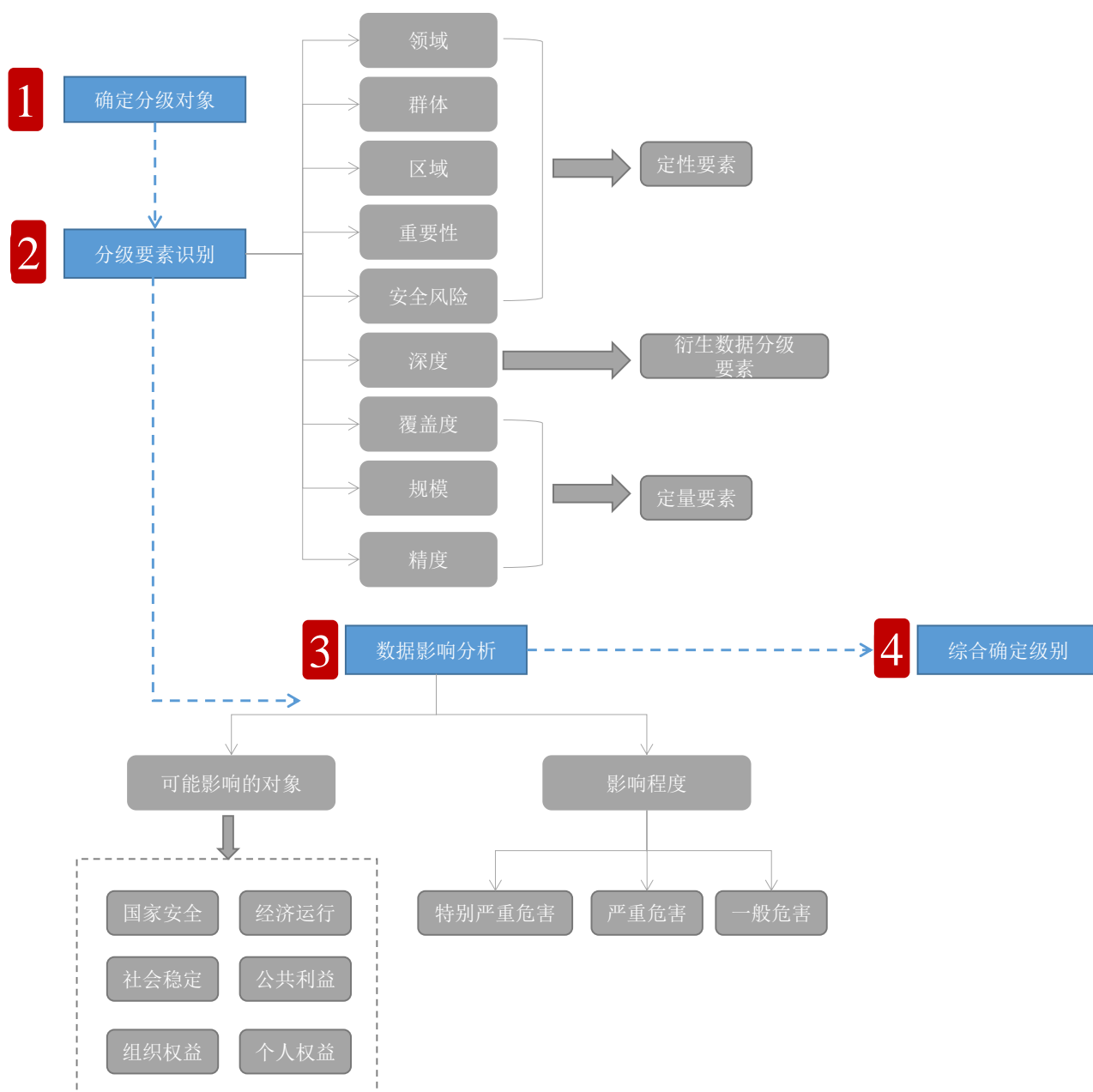
《分类分级要求》同时要求，数据处理者应当对法律法规或主管监管部门有专门管理要求的数据进行识别和分类，例如个人信息、敏感个人信息、测绘成果。这一做法有助于数据处理者落实法律法规的合规义务，例如：告知同意、单独同意、加密保护、境内存储、开展个人信息保护影响评估或数据出境评估等。

（四）可结合自身数据管理需要进行增补分类

考虑到数据分类在实践中落地的复杂性，《分类分级要求》同时提出如果存在行业领域数据分类规则未覆盖的数据类型，数据处理者可从组织经营角度，结合自身数据管理和使用要求对数据进行分类，这为数据处理者结合自身管理需求对数据进行创新分类留下了一定的灵活空间。

三、细化数据分级框架及方法

根据《数据安全法》的要求，《分类分级要求》将数据从高到低分为核心数据、重要数据、一般数据三个级别，并明确数据分级框架的核心考虑因素为：数据在经济社会发展中的重要程度，以及一旦遭到泄露、篡改、破坏或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度。数据分级的具体流程及要点如下：



（一）列举数据分级要素

在《分类分级指引》的基础上，《分类分级要求》进一步明确了影响数据分级的要素，并在附录 B 中详细说明了数据领域、群体、区域、精度、规模、深度、覆盖度、重要性、安全风险等九个关键要素的定义及示例，增强了分级工作的可落地性。在前述要素中，领域、群体、区域、重要性、安全风险属于定性要素，精度、规模、覆盖度属于定量要素，深度则通常作为衍生数据的分级要素。

（二）扩充影响对象考量范围

《分类分级指引》规定的的数据分级考量影响对象主要包括国家安全、公共利益、个人合法权益以及组织合法权益，而《分类分级要求》则在此基础上增加了经济运行、社会稳定两类影响对象，并通过附录 C 对影响对象常见考虑因素进行了细化列举。数据处理者可依据附录 C 中列举的因素判断其处理的数据是否对某类对象产生影响。

（三）细化影响程度的判断基准

《分类分级要求》明确，对不同影响对象进行影响程度判断时，应当采取不同的基准：如果影响对象是组织或个人权益，则以本单位或本人的总体利益作为判断影响程度的基准；如果影响对象是国家安全、经济运行、社会稳定或公共利益，则以国家、社会或行业领域的整体利益作为判断影响程度的基准。附录 D 针对每一类影响对象均细化了特别严重危害、严重危害以及一般危害三个层次的影响程度的具体说明和示例。

（四）确定数据分级参考规则

《分类分级要求》通过矩阵图的方式明确了数据分级与影响对象、影响程度的关联关系，将数据按照级别从高到低分为核心数据、重要数据、一般数据三类。数据处理者在完成影响对象的识别和影响程度的评估后即可根据下表中的矩阵确定数据级别。

影响对象	影响程度		
	特别严重危害	严重危害	一般危害
国家安全	核心数据	核心数据	重要数据
经济运行	核心数据	重要数据	重要数据
社会稳定	核心数据	重要数据	一般数据
公共利益	核心数据	重要数据	一般数据
组织权益、个人权益	一般数据	一般数据	一般数据

（五）明确综合确定数据级别的规则

《分类分级要求》在给出上述分级规则的基础上还给出了综合确定数据级别的流程和规则，例如：

- 可以按照重要数据、核心数据、一般数据的顺序确定数据级别，在参考重要数据识别相关标准识别出重要数据后，再根据是否可能直接影响政治安全、国家安全重点领域、国民经济命脉、重要民生、重大公共利益确定相关数据是否为核心数据。如不属于重要数据或者核心数据，则相关数据可确定为一般数据。
- 对于数据集的级别，数据处理者可在数据项级别的基础上，按照就高从严的原则，将数据集包含数据项的最高级别作为数据集默认级别，但同时需考虑数据规模等数据要素的变化调高数据级别。
- 对于衍生数据的级别，数据处理者可按照就高从严原则，在原始数据级别的基础上进行分级，同时综合考虑加工后的数据深度等分级要素对国家安全、经济运行、社会稳定、公共利益、组织权益、个人权益的影响，对数据级别进行调整。附录 E 确立的衍生数据分级调整标准包括：降低脱敏数据级别、标签数据级别以及降低标识化程度的融合数据级别，提升涉及大规模群体特征或者行动轨迹的统计数据级别，提升关联、分析、挖掘大量多维数据的融合数据级别。

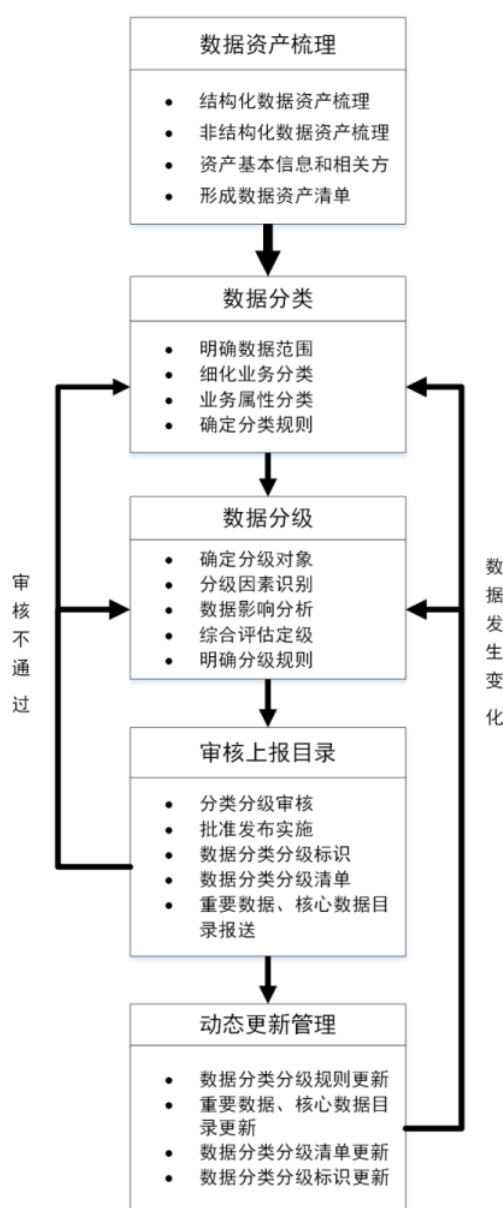
需要说明的是，数据分类分级工作并非一劳永逸，数据处理者需要结合业务变化动态更新数据的分类分级情况。为此，附录 F 列举了常见的需要对数据分类分级进行动态更新的情形，例如：数据内容未发生变化，但数据时效性、数据规模、数据应用场景、数据加工处理方式等发生显著变化；多个原始数据直接合并，导致原有的安全级别不再适用合并后的数据；发生数据安全事件，导致数据敏感性发生变化；因国家或行业主管部门要求，导致原定的数据级别不再适用等。

（六）提出行业分级规则

《分类分级要求》同时考虑到了各行业领域的特殊性，指出各行业各领域可以在遵循数据分级框架的基础上，结合行业领域数据分级要素识别、数据影响分析和综合确定级别等实践经验，制定本行业本领域数据分级规则。各行业各领域应当重点考虑明确本行业本领域重要数据目录或识别细则、核心数据目录建议以及一般数据范围等。

四、数据分类分级工作的实施流程

《分类分级要求》第 8 点给出了数据分类分级的实施流程建议，主要步骤包括：（1）数据资产梳理；（2）数据分类；（3）数据分级；（4）审核上报目录；（5）动态更新管理。具体实施流程请见下图：



五、结语

《分类分级要求》重点旨在明确网络数据分类分级的框架、方法以及实施流程，为行业领域主管（监管）

部门制定数据重要数据目录，各地方、各部门以及数据处理者开展数据分类分级工作提供了具体指引。企业作为数据处理者应参照《分级分类要求》积极开展数据资产梳理工作，明确企业分类分级数据范围，并持续关注各行业各领域关于数据分类分级的目录或识别指南动态，在行业领域标准规范框架下有序开展数据分类分级工作。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

段志超

电话： +86 10 8516 4123

Email: kevin.duan@hankunlaw.com

蔡克蒙

电话： +86 10 8516 4289

Email: kemeng.cai@hankunlaw.com