ICS 35.020
L 72

DB3301

浙 江 省 杭 州 市 地 方 标 准

DB 3301/T 0322.3—2020

数据资源管理
第3部分：政务数据分类分级

2020－10－31 发布　　2020－11－30 实施

杭州市市场监督管理局　　发 布

目　　次

前　言

本部分按照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。

本次发布DB3301/T 0322《数据资源管理》分为4个部分，以后根据工作需要，再视情增补。

——第 1 部分：政务数据安全监管；

——第 2 部分：政务数据安全责任；

——第 3 部分：政务数据分类分级；

——第 4 部分：政务数据共享流程。

本部分为DB3301/T 0322的第3部分。

本部分由杭州市数据资源管理局提出并归口。

本部分起草单位：杭州市数据资源管理局、萧山区数据资源管理局、杭州安恒信息技术股份有限公司、阿里云计算有限公司、数字扁担（浙江）科技有限公司。

本部分主要起草人：夏鹏、任子骁、丁熙、齐同军、章建平、郭鹏飞、樊兴悦、周俊、张敏翀、孙茂阳、刘诚征、王梦婕。

数据资源管理 第3部分：政务数据分类分级

1 范围

本部分规定了数据资源管理过程中分类分级原则、数据分类方法、数据分级方法、关键问题等要求。

本部分适用于指导政务数据的分类分级工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 信息安全技术 术语

GB/T 35273-2020 信息安全技术 个人信息安全规范

DB3301T 0276 政务数据共享安全管理规范

3 术语和定义

GB/T 25069和DB3301/T 0276 界定的以及下列术语和定义适用于本文部分。

3.1

数据分类

将具有某种共同属性或特征的数据，根据应用场景、数据来源、共享属性、开放属性等属性或特征，按照一定的原则和方法进行归类。

3.2

数据分级

根据数据的敏感程度和数据遭篡改、破坏、泄露或非法利用后对受侵害客体的影响程度，按照一定的原则和方法进行定级。

4 分类分级原则

4.1 科学性

应按照数据多维度特征和逻辑关联进行科学系统化的分类，且分类规则相对稳定，不宜经常变更。

4.2 实用性

不应设置无意义的类目或级别，分类分级结果应符合普遍认知。

4.3 自主性

各部门在归集和共享数据前，应按照本指南自主完成数据分类分级工作，分类分级宜细化至字段级。

5 数据分类方法

5.1 根据应用场景分类

依据政府数字化转型工作中体现的应用场景，数据分类为：

——经济调节数据；

——市场监管数据；

——公共服务数据；

——社会管理数据；

——生态环境保护数据；

——府运行数据。

5.2 根据数据来源分类

依据数据来源，数据分类为，

——政府部门数据，根据来源部门进行细化；

——法人及其他组织数据；

——民个人数据。

5.3 根据共享属性分类

依照《政务信息资源目录编制指南（试行）（发改高技2017）》政务信息资源元数据共享属性，数据分类为：

——无条件共享数据；

——有条件共享数据；

——不予共享数据。

5.4 根据开放属性分类

依照《政务信息资源目录编制指南（试行）（发改高技2017）》政务信息资源元数据开放属性，数据分类为：

——无条件开放数据；

——有条件开放数据；

——不予开放数据。

6 数据分级方法

6.1 数据分级

根据数据的敏感程度数据和数据遭篡改、破坏、泄露或非法利用后对国家安全、社会秩序、公共利益和公民、法人、其它组织的合法权益（受侵害客体）的影响程度，按照表1和表2可分为1级、2级、3级、4级，并根据就高原则进行定级，报部门主要负责人审批同意。

表 1　依据敏感程度定级标准

数据级别	敏感程度	判断标准
1级	公开数据	依法公开和披露的数据。
2级	一般敏感数据	不宜公开的数据，但在公民、法人和其它组织授权下可在一定范围内共享的数据。
3级	高度敏感数据	不能公开的数据，但在公民、法人和其它组织授权下可在小范围内共享的数据。
4级	极度敏感数据	涉及公民、法人和其他组织核心利益的数据，不得公开、不宜共享。

表 2　依据影响程度定级标准

数据级别	影响程度	判断标准
1级	无	数据被破坏后，对国家安全、社会秩序、公共利益以及对公民、法人和其它组织的合法权益均无影响。
2级	轻微	数据被破坏后，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。
3级	中等	数据被破坏后，对公民、法人和其他组织的合法权益造成严重损害，或对社会秩序和公共利益造成损害，但不损害国家安全。
4级	严重	数据被破坏后，会对社会秩序和公共利益造成严重损害，或对国家安全造成损害。

7　关键问题

7.1　数据分级注意事项

数据分级时，应满足如下要求：

——法律法规明确保护的数据，数据级别应定为 3 级以上；

——未明示公开要求的个人数据不得低于 2 级；

——没有任何安全级别标识的数据，默认为 2 级。

7.2　安全级别变更原则

安全级别变更原则包括：

——从原始数据中直接部分复制出来的新数据级别不应高于原有数据级别；

——从多个原始数据直接合并的新数据不应低于原有数据级别；

——对不同数据选取部分数据进行合并形成的新数据，应根据新数据的关键要素进行重新判定；

——数据内容不发生变化时，进行级别变更时需有明确的依据；

——安全级别变更时，应由本组织机构的主要领导人进行审批同意；
——汇聚数据的安全级别须经数据使用方和数据资源管理机构联合评估确认后进行判定。

7.3 级别变更场景

7.3.1 等级提升

发生以下场景时，应考虑提升数据级别：
——聚合多家业务部门数据；
——大量数据进行聚合；
——发生特定事件导致数据具有敏感性。

7.3.2 等级降低

发生以下场景时，可考虑降低数据级别：
——数据已被公开或披露；
——数据进行脱敏或删除关键字段；
——数据经过较长时间（需明确数据含义和时间点）；
——发生特定事件导致数据失去敏感性时。

附 录 A
（资料性附录）
数据共享、开放与安全级别

数据共享属性、数据开放属性与安全级别对照关系表如表A.1所示。

1级数据建议无条件共享，无条件开放；

2级以上数据，建议通过申请审批方式获得，对外有条件开放；

4级数据，原则上不予共享，禁止对外开放。未进行安全等级标识的数据不得进行共享开放。

表 A.1 数据共享、开放与安全级别对照关系

	对照关系			
安全级别	1 级	2 级	3 级	4 级
共享属性	无条件共享	有条件共享		不予共享
开放属性	无条件开放	有条件开放	不予开放	

附 录 B
（资料性附录）
数据分级特征与示例

数据分级特征与示例见表B.1。

表 B.1 数据分级特征与示例表

数据类型	数据级别			
	1 级	2 级	3 级	4 级
政府部门	数据特征： 可向社会公众提供和不受限制地使用。 示例： 机构职能、法律法规、发展规划、工作动态、人事任免、人员招录、财经信息、行政执法、公共服务、城市交通基础设施（如停车场位置）等政府依法公开的信息，包括主动公开信息和依申请公开信息。	数据特征： 不宜向公众公开的数据。 示例： 1.调查、讨论、处理过程中的政府信息:法律法规/发展规划/产业政策等草案、招投标/专项资金预审材料等信息。 2.不宜向公众公开的行政行为信息：专项检查、项目备案、行政确认、行政调解、非公开合同等信息。 3.行政机构内部运转管理信息:机关财务/党务等内部运转信息、机关纪委/巡视工作内部信息、工作方案、谈话记录、事故调查、内部审计报告、一般工作批示/指示、请示分析建议、内部工作文件和参考文献资料等信息。	数据特征： 1.法律法规和强制性标准定义的重要数据。 2.仅向特定职能部门、特殊岗位/层级政府职员披露的不涉密其它重要数据。 示例： 1.涉及国家安全的相关数据，如国防军工、人口健康、海洋环境等领域数据。 2.其它重要数据：组织人事信息、重大事项决策、纪检监察、调查取证、重要工作指示等信息。	数据特征： 保密法律法规、规范性文件明确定义/特殊岗位/涉密系统 示例： 国家秘密
法人和其他组织	数据特征： 企业主动披露的信息。 示例： 公司新闻、企业网站、招商规则、活动规则、层演讲、社会责任、产品信息、业绩说明、投资者互动、路演材料等企业主动披露信息。	数据特征： 法人和其他组织向政府披露的未被法律法规明确保护的数据。 2 级数据一般为法人和其他组织内控信息。 示例： 非公开报告、非公开合同、内部备忘录、项目建设方案、产品类目、生产计划、招投标文件等。	数据特征： 法律法规明确保护的企业数据。泄露会给企业带来直接经济损失或名誉损失的信息。 示例： 《中华人民共和国专利法》：发明专利。 《中央企业商业秘密保护暂行规定》：改制上市、并购重组、产权交易、财务信息、投融资决策、产购销策略、资源储备、客户信息、招投标事项等经营信息；设计、程序、产品配方、制作工艺、制作方法、技术诀窍等技术信息。	数据特征： 保密法律法规、规范性文件明确定义/特殊岗位/涉密系统 示例： 国家秘密

			《纳税人涉税保密信息管理暂行办法》：纳税人技术信息、经营信息。	
公民个人		数据特征： 个人向政府披露的不属于3级的反映特定自然人活动情况的各种信息。2级数据一般仅向特定人群公开。 示例： 未公开的工作经历、家庭成员、婚姻状况、照片（用于识别目的）、教育程度、日程安排、电子邮箱等个人信息。	数据特征： 法律法规明确保护的个人隐私数据。泄露会给个人带来直接经济损失的信息。 示例： 《中华人民共和国网络安全法》、两高关于个人信息刑事案件适用法律的解释、《电信和互联网用户个人信息保护规定》等：姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、账号密码、财产状况、健康状况、行踪轨迹等。 《纳税人涉税保密信息管理暂行办法》：纳税人、主要投资人以及经营者不愿公开的个人事项。 其它个人敏感信息，参见GB/T 35273-2020。	数据特征： 保密法律法规、规范性文件明确定义/特殊岗位/涉密系统 示例： 国家秘密

附 录 C
（资料性附录）
数据分级保护基本要点

数据分级保护基本要点参见表C.1。

表 C.1 数据分级保护要点

	1 级	2 级	3 级	4 级
数据采集	1.应明确数据采集的目的、用途和范围，规范数据采集的流程和方法 2.应明确数据采集的渠道及外部数据源，要求外部数据提供方说明数据来源，并对信息来源的合法性进行确认 3.宜针对在线的数据采集过程执行有效的日志记录，实现对数据采集过程的可追溯	1.应明确数据采集的目的、用途和范围，规范数据采集的流程和方法 2.应明确数据采集的渠道及外部数据源，要求外部数据提供方说明数据来源，并对信息来源的合法性进行确认。 3.宜建立统一的数据采集流程，以保证组织机构数据采集流程实现的一致性，以及授权过程的有效记录。 4.宜采取必要的技术手段对采集的数据进行校验，以保证其完整性和一致性。 5.宜实施数据采集过程的数据防泄漏安全技术措施，防止数据在采集过程中的泄露，如数据加密、采集链路加密、敏感字段脱敏等。 6.宜针对在线的数据采集过程执行有效的日志记录，实现对数据采集过程的可追溯。 7.应对外部收集的数据和数据源进行识别和记录，即通过数据溯源的机制能够保证数据管理人员能够追踪其加工和计算的数据来源。	1.应明确数据采集的目的、用途和范围，规范数据采集的流程和方法 2.应明确数据采集的渠道及外部数据源，要求外部数据提供方说明数据来源，并对信息来源的合法性进行确认 3.应建立统一的数据采集流程，以保证组织机构数据采集流程实现的一致性，以及授权过程的有效记录 4.应采取必要的技术手段对采集的数据进行校验，以保证其完整性和一致性 5.应实施数据采集过程的数据防泄漏安全技术措施，防止数据在采集过程中的泄露，如数据加密、采集链路加密、敏感字段脱敏等。 6.应针对在线的数据采集过程执行有效的日志记录，实现对数据采集过程的可追溯 7.应对外部收集的数据和数据源进行识别和记录，即通过数据溯源的机制能够保证数据管理人员能够追踪其加工和计算的数据来源	1.应明确数据采集的目的、用途和范围，并经采集部门主管领导审核确认，并对授权过程进行有效记录。 2.仅允许通过经认证的存储介质或可信的传输通道采集数据，并采取技术措施保证其完整性和一致性。 3.应采取加密措施防止数据的在采集过程中的泄露。 4.应对采集过程进行有效的日志记录，实现对数据采集过程的可追溯。 5.应实施数据采集过程的数据防泄漏安全技术措施，防止数据在采集过程中的泄露，如数据加密、采集链路加密、敏感字段脱敏等。 6.应针对在线的数据采集过程执行有效的日志记录，实现对数据采集过程的可追溯 7.应对外部收集的数据和数据源进行识别和记录，即通过数据溯源的机制能够保证数据管理人员能够追踪其加工和计算的数据来源。
数据		1.宜建立安全的数据传输通道，例如VPN，专线等	1.应建立安全的数据传输通道，如VPN，专线等	1.应建立安全的数据传输通道，如VPN，专线等

传输		2.宜对数据进行加密传输 3.加密算法应符合国家密码管理的相关规定	2.应对传输通道两端进行主体身份鉴别和认证 3.应对数据进行加密传输 4.加密算法应符合国家密码管理的相关规定	2.应对传输通道两端进行主体身份鉴别和认证 3.应对数据进行加密传输 4.加密算法应符合国家密码管理的相关规定
数据存储	1.宜对存储系统的账号权限进行管理； 2.宜建立数据备份机制，定期进行数据的备份。	1.宜对存储系统的账号权限进行统一管理； 2.宜对存储系统的访问进行鉴权和日志记录； 3.应建立数据备份机制，定期进行数据的备份。	1.应对存储系统的账号权限进行统一管理； 2.应对存储系统的访问进行鉴权和日志记录； 3.非可信或离线环境应进行加密存储； 4.应建立数据备份机制，定期进行数据的备份； 5.应建立异地备份措施，数据异地备份。	1 应对存储系统的账号权限进行统一管理； 2.应对存储系统的访问进行鉴权和日志记录； 3.应进行加密存储； 4.应建立数据备份机制，定期进行数据的备份； 5.应建立异地备份措施，数据异地备份。
数据处理	1.应建立数据分析结果的输出和使用的安全审查、合规风险评估和数据使用授权流程。	1.宜建立访问控制矩阵，明确可访问用户和可访问内容。 2.应对用户进行身份鉴别。 3.应建立数据分析结果的输出和使用的安全审查、合规风险评估和数据使用授权流程。 4.数据的使用和分析过程应进行日志记录，并定期审计。 5.应使用数据资源管理部门确认过的邮件系统、即时通讯、个人设备、传真打印机来处理数据。	1.应建立访问控制矩阵，明确可访问用户和可访问内容。 2.应采用口令、密码、生物识别等两种或两种以上组合的鉴别技术对用户进行身份鉴别。 3.数据分析前应进行脱敏，并对脱敏过程进行日志记录和监控。 4.应建立数据分析结果的输出和使用的安全审查、合规风险评估和数据使用授权流程。 5.数据的使用和分析过程应进行日志记录，并定期审计。 6.应使用数据资源管理部门确认过的邮件系统、即时通讯、个人设备、传真打印机来处理数据，并全程监控进行必要的阻断。	1.应建立访问控制矩阵，明确可访问用户和可访问内容。 2.应采用口令、密码、生物识别等两种或两种以上组合的鉴别技术对用户进行身份鉴别。 3.数据分析前应进行脱敏，并对脱敏过程进行日志记录和监控。 4.应建立数据分析结果的输出和使用的安全审查、合规风险评估和数据使用授权流程。 5.数据的使用和分析过程应进行日志记录，并定期审计。 6.应使用数据资源管理部门确认过的邮件系统、即时通讯、个人设备、传真打印机来处理数据，并全程监控进行必要的阻断。
数据共享	1.宜建立数据共享目录，明确数据的共享范围和使用属性；	1.应建立数据共享目录，明确数据的共享范围和使用属性； 2.对共享数据的使用申请进行严格审批和授权。	1.应建立数据共享目录，明确数据的共享范围和使用属性 2.对共享数据的使用申请进行严格审批和授权。	1.一般情况不允许共享。 2.若需共享应采取一事一议制，经相关责任人审批授权后，进行脱密降级后共享。

		3.建立数据共享的唯一通道，定义数据共享接口，并对数据共享过程进行日志记录和审计。	3.建立数据共享的唯一通道，定义数据共享接口，并对数据共享过程进行实时监控，日志记录和审计。 4.数据共享前应进行脱敏处理。	
数据销毁	1.对数据销毁过程进行记录。	1.建立数据销毁的审批机制，设置销毁相关监督角色，监督操作过程，并对审批和销毁过程进行记录控制； 2.确保以不可逆方式销毁数据及其副本内容。	1.建立数据销毁的审批机制，设置销毁相关监督角色，监督操作过程，并对审批和销毁过程进行记录控制； 2.使用国家权威机构认证的机构或设备对存储介质进行物理销毁，或联系其执行销毁工作。	1.建立数据销毁的审批机制，设置销毁相关监督角色，监督操作过程，并对审批和销毁过程进行记录控制； 2.使用国家权威机构认证的机构或设备对存储介质进行物理销毁，或联系其执行销毁工作。

参 考 文 献

[1] GB/T 21063.4-2017 政务信息资源目录体系 第四部分：政务信息 资源分类
[2] GB/T 38667-2020 信息技术 大数据 数据分类指南