ICS
CCS

DB11

北　京　市　地　方　标　准

DB11/T ××××—××××

政务大数据安全技术框架

Technical framework of government big data security

（征求意见稿）

××××－××－××发布　　××××－××－××实施

北京市市场监督管理局　发布

目　　次

前　言

本文件按照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。

本文件由北京市经济和信息化局提出并归口。

本文件由北京市经济和信息化局组织实施。

本文件起草单位：北京市大数据中心、中电长城网际系统应用有限公司、北京信息安全测评中心、联通数字科技有限公司、北京云集至科技有限公司、北京启明星辰信息安全技术有限公司、数据堂（北京）科技股份有限公司、京信数据科技有限公司、北京天融信网络安全技术有限公司、北京数字认证股份有限公司、厦门市美亚柏科信息股份有限公司、中国长江三峡集团有限公司。

本文件主要起草人：

政务大数据安全技术框架

1 范围

本文件提出了政务大数据安全技术框架，规定了政务大数据域安全要求、政务大数据域间协同安全要求以及基础设施安全要求等。

本文件适用于指导政务部门以及参与政务大数据处理活动的相关组织开展政务大数据安全技术体系规划、建设与管理，也适用于指导网络安全主管部门对政务大数据安全保护的监督管理。

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本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 22239 信息安全技术 网络安全等级保护基本要求

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 35274 信息安全技术 大数据服务安全能力要求

GB/T 38664.2 信息技术 大数据 政务数据开放共享 第2部分：基本要求

GB/T 39477 信息安全技术 政务信息共享 数据安全技术要求

GB/T 39786 信息安全技术 信息系统密码应用基本要求

DB11/T 1918 政务数据分级与安全保护规范

3 术语和定义

GB/T 35295界定的以及下列术语和定义适用于本文件。

3.1

大数据 big data

具有体量巨大、来源多样、生成极快且多变等特征并且难以用传统数据体系结构有效处理的包含大量数据集的数据。

[来源：GB/T 35295—2017,2.1.1]

3.2

政务大数据 government big data

政务部门在履行职责过程中制作或获取的，以电子化形式记录、保存的大数据。

3.3

政务大数据域 government big data domain

在同一安全策略下，处理政务大数据的软件系统的集合。

注：数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。

3.4

政务大数据参与方 participant of government big data

参与政务大数据处理活动的主体。

3.5

政务大数据基础设施 infrastructure for government big data

为政务大数据处理活动提供算力、存储、网络、安全等服务的基础设施。

4 政务大数据安全技术框架的构成

4.1 总体架构

综合考虑政务大数据流动过程中的数据处理功能边界和安全责任边界，政务大数据安全包括：政务大数据域安全、域间协同安全和政务大数据基础设施安全。安全责任分别由不同的政务大数据参与方承担。政务大数据安全技术框架如图1所示。

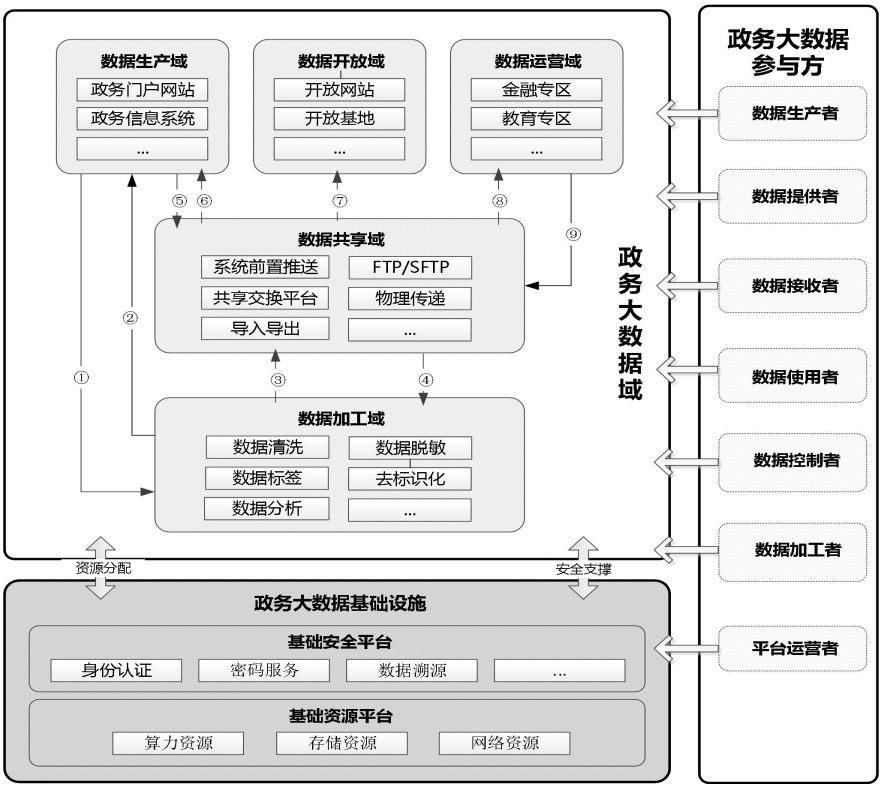


图1 政务大数据安全技术框架

4.2 政务大数据域

4.2.1 政务大数据域的类型

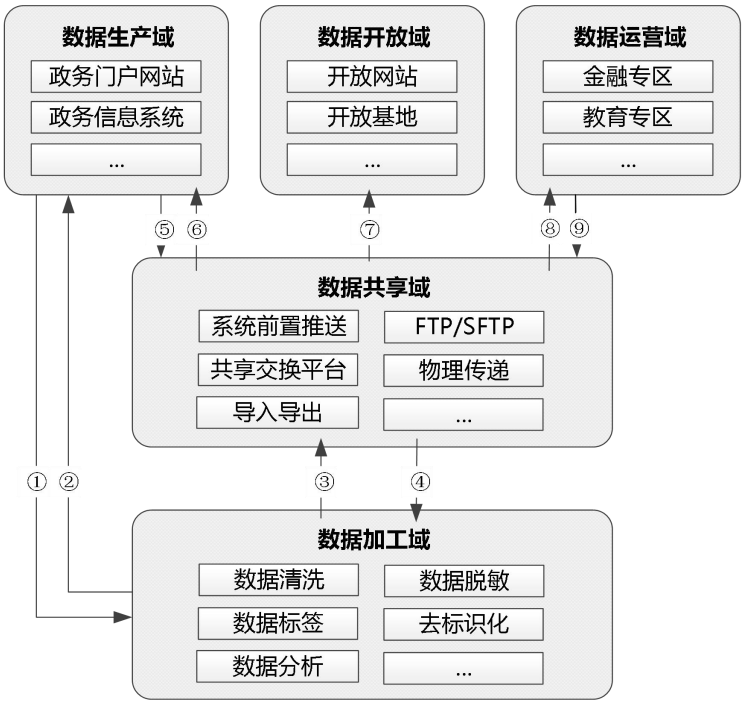
综合考虑政务大数据的流动环节和落地场景，政务大数据域包括：数据生产域、数据加工域、数据共享域、数据开放域、数据运营域五类，各数据域的主要功能如表1所示（数据域示例见附录A.1）。

表1 政务大数据域主要功能

名称	主要功能
数据生产域	对政务大数据进行收集、生产和使用的实体集合
数据加工域	对政务大数据进行加工以形成政务大数据资产的实体集合
数据共享域	面向政务部门提供或获取政务大数据的实体集合
数据开放域	面向社会提供政务大数据的实体集合
数据运营域	面向社会特定群体提供政务大数据，以开展数据运营服务的实体集合

4.2.2 政务大数据域间协同关系

政务大数据在各个政务大数据域之间流动的情况，如图2所示。



标引序号说明：

1—数据生产域收集、生产的数据，进入到数据加工域进行加工；

2—经数据加工域加工后的数据，进入到数据生产域进行使用；

3—经数据加工域加工后的数据，进入数据共享域进行共享；

4—数据共享域中的数据，进入数据加工域进行加工；

5—数据生产域收集、生产的数据，进入共享域进行共享；

6—数据共享域中的数据，进入数据生产域进行使用；

7—数据共享域中的数据，进入数据开放域面向社会进行开放；

8—数据共享域中的数据，进入数据运营域以开展数据运营；

9—数据运营域产生新数据，进入数据共享域以进行共享。

图2 政务大数据域间流动图

不同政务大数据域之间进行数据流动时，应要按照协议或者约定进行安全协作联动和互相配合，即域间安全协同。域间安全协同的目的是为了达成数据流动过程中的特定安全需求。主要的域间协同关系见表2。

表2 政务大数据域间协同关系

	数据生产域	数据加工域	数据共享域	数据开放域	数据运营域
数据生产域	/	●	●	/	/
数据加工域	●	/	●	/	/
数据共享域	●	●	/	●	●
数据开放域	/	/	●	/	/
数据运营域	/	/	●	/	/
注：“●”代表存在着域间协同关系，“/”代表不存在域间协同关系。					

4.3 政务大数据基础设施

政务大数据基础设施包括基础资源平台和基础安全平台等。基础资源平台为政务大数据处理活动提供统一的算力、存储和网络等基础资源服务；基础安全平台为政务大数据处理活动提供统一的身份认证、密码服务、数据监测溯源等基础安全保障，如图3所示。

图3 政务大数据基础设施图

4.4 政务大数据参与方

根据参与方在政务大数据流动过程中的角色类型，政务大数据域和基础设施的参与方可分为数据控制者、数据生产者、数据加工者、数据使用者、数据提供者、数据接收者和平台运营者七类。一个组织或个人可以承担多个角色，一个角色可以对应多个组织或个人。

政务大数据参与方的定义见表3，政务大数据域和基础设施的参与方见表4，参与方的示例见附录A.2。

表3 参与方角色定义

角色	定义
数据控制者	有权决定数据处理目的、方式，对数据进行管控的组织、个人
数据生产者	收集、生产数据的组织、个人
数据加工者	清洗、加工数据的组织、个人
数据使用者	使用、消费数据的最终用户
数据提供者	向政务大数据域提供数据的组织、个人
数据接收者	从政务大数据域接收数据的组织、个人
平台运营者	政务大数据基础设施的所有者、管理者和服务提供者

表4 政务大数据域和基础设施的参与方

		数据控制者	数据生产者	数据加工者	数据使用者	数据提供者	数据接收者	平台运营者
政务大数据域	数据生产域	●	●	/	●	●	●	/
	数据加工域	●	◐	●	/	●	●	/
	数据共享域	●	◐	/	/	●	●	/
	数据开放域	●	/	/	●	/	●	/
	数据运营域	●	/	/	●	●	●	/
政务大数据基础设施	基础资源平台	/	/	/	/	/	/	●
	基础安全平台	/	/	/	/	/	/	●
注：“●”代表存在参与关系，“◐”有存在参与关系的可能性，“/”代表不存在参与关系。								

5 政务大数据域安全要求

5.1 通用要求

政务大数据域的参与方应满足如下要求：

a）应按照GB/T 22239、GB/T 35273、GB/T 35274、GB/T 38664.2、GB/T 39477、GB/T 39786等要求对政务大数据进行保护；

b）应根据DB11/T 1918对政务大数据进行分级安全保护；

c）宜根据GB/T 37988对自身数据安全保护能力进行评定。

5.2 数据生产域

5.2.1 数据控制者安全技术要求

数据控制者应采取相应措施以满足以下安全技术要求：

a）应获得数据提供者的授权，并在授权范围内合法处理数据；

b）应制定数据生产规程，明确政务信息资源分类分级、目录编制、存储、备份、归档等相关要求；

c）应对数据生产者数据生产行为进行授权；

d）应具备对政务数据生产过程的追溯和安全审计能力，定期对数据生产者的数据生产行为进行评估和审计；

e）应在发现可能违反法律、行政法规或者侵犯他人等合法权益时，立即停止数据生产行为并采取相应的补救措施。

5.2.2 数据生产者安全技术要求

数据生产者应采取相应措施以满足以下安全技术要求：

a）应遵守政务数据生产规程，在控制者授权范围内进行数据生产，确保政务数据生产过程的合法性、正当性，确保数据的真实性和有效性；

b）应对生产数据进行分类分级并标识；

c）应建立生产数据的数据资源目录，明确数据的使用范围和条件；

d）应根据生产数据的重要性、量级、使用频率、敏感性等因素进行分域分级存储；

e）应对生产数据进行定期备份，并适时进行归档；

f）应在收集个人信息过程中采用身份鉴别等安全机制，保障数据的真实性；

g）应采取必要的安全管控措施，确保数据收集过程中，个人信息和重要数据不被泄露，确保采集数据的完整性和一致性；

h）应记录数据生产过程。

5.2.3 数据提供者安全技术要求

数据提供者应采取相应措施以满足以下安全技术要求：

a）应保证所提供数据的合法性、真实性和有效性；

b）应向数据控制者进行授权，明确所提供数据的使用范围和条件。

5.2.4 数据使用者安全技术要求

数据使用者应采取相应措施以满足以下安全技术要求：

a）应在授权范围内合法使用数据；

b）应在数据使用过程中，采取相应的安全措施，避免重要数据和个人信息的泄露、篡改和滥用。

5.3 数据加工域

5.3.1 数据控制者安全技术要求

数据控制者应采取相应措施以满足以下安全技术要求：

a）应获得数据提供者的授权，并在授权范围内处理数据；

b）应制定数据加工规程，明确政务信息资源分类分级、目录编制、清洗、脱敏、标识、存储、备份、归档等相关要求；

c）应对数据加工者进行授权，明确授权目的和范围；

d）应设置严格的数据访问控制规则，限制数据加工终端的外部接入IP数量和地址，保证数据加工操作仅限制在合法授权范围内，并采取技术措施禁止未经授权的操作行为；

e）应具备对政务数据加工过程的追溯和安全审计能力，对数据加工过程进行监督，并定期对数据加工者的数据加工行为进行评估和审计；

f）应在发现可能违反法律、行政法规或者侵犯他人等合法权益时，立即停止数据加工行为并采取相应的补救措施。

5.3.2 数据加工者安全技术要求

数据加工者应采取相应措施以满足以下安全技术要求：

a）应获得数据控制者的授权，并在授权范围内合法加工数据；

b）采取技术手段和管理措施，确保在数据清洗操作中对所获取或清洗生成的数据进行保护，包括但不限于衍生数据以及操作日志等；

c）应利用数据脱敏的技术工具或服务组件，支持如泛化、抑制、干扰等数据脱敏技术，宜具备对非结构化数据进行脱敏处理的能力，以及对脱敏处理效果的验证能力；

d）应采用技术手段对数据进行标识，宜配置自动发现和标识重要数据和个人信息的技术工具或服务组件；

e）应对数据进行分类分级并标识；

f）应建立数据资源目录，明确数据的使用范围和条件；

g）应根据数据的重要性、量级、使用频率、敏感性等因素进行分域分级存储；

h）应对数据进行定期备份，并适时进行归档；

i）未经许可不得留存委托加工的数据；

j）不得非法向他人转让委托加工的数据；

k）应留存数据加工日志，并在数据加工报告中记录安全事件的处置情况。

5.4 数据共享域

5.4.1 数据控制者安全技术要求

数据控制者应采取相应措施以满足以下安全技术要求：

a）应获得数据提供者的授权，并在授权范围内合法共享数据；

b）应对数据接收者进行授权，明确授权目的和范围；

c）应建立数据共享规范，保证数据共享安全策略的有效性；

d）应建立数据共享目录，明确数据共享的范围和条件；

e）应针对不同的共享场景，制定不同的数据安全策略，包括但不限于：共享条件、权限控制、静态脱敏、动态脱敏、加解密、水印、审计、隐私计算等；

f）应审核共享数据的应用场景，确保共享数据使用没有超出提供者的授权范围；

g）应具备对政务数据共享过程的追溯和安全审计能力，定期对数据共享行为进行评估和审计；

h）应在发现可能违反法律、行政法规或者侵犯他人等合法权益时，立即停止数据共享行为并采取相应的补救措施；

i）应建立在数据共享完成后对数据共享通道缓存的数据进行安全删除的相关机制。

5.5 数据开放域

5.5.1 数据控制者安全技术要求

数据控制者应采取相应措施以满足以下安全技术要求：

a）应获得数据提供者的授权，并在授权范围内合法开放数据；

b）应对数据使用者进行授权，明确授权目的和范围；

c）应建立数据开放规范，保证数据开放安全策略的有效性；

d）应建立数据开放目录，明确数据开放的范围和条件；

e）应制定数据开放计划；

f）提供开放数据的访问接口及格式规范，确保使用者能高效的获取开放数据；

g）宜具备对待开放数据进行重要数据及个人信息的检查能力，确保涉及重要数据、个人信息等数据不向社会开放；

h）在涉及使用者数量巨大、数据开放对社会影响大时，宜定期发布社会责任报告，包括数据保护措施、发生的安全事件及应对处理情况等内容；

i）应具备对政务数据开放过程的追溯和安全审计能力，定期对数据开放行为进行评估和审计；

j）应在发现可能违反法律、行政法规或者侵犯他人等合法权益时，立即停止数据开放行为并采取相应的补救措施。

5.5.2 数据使用者安全技术要求

数据使用者应采取相应措施以满足以下安全技术要求：

a）应在授权范围内合法使用数据；

b）应保证开放数据使用环境和使用过程的安全性，以防数据的泄露和滥用。

5.6 数据运营域

5.6.1 数据控制者安全技术要求

数据控制者应采取相应措施以满足以下安全技术要求：

a）应获得数据提供者的授权，并在授权范围内合法运营数据；

b）应对数据使用者进行授权，明确授权目的和范围；

c）应建立数据运营规范，保证数据运营安全策略的有效性；

d）应审核运营数据的应用场景，确保运营数据使用没有超出提供者的授权范围；

e）涉及数据交易活动的，应提供证明数据交易合法性的授权文件；

f）涉及个人数据的，应得到个人数据主体的明示同意，以保证数据主体的合法权益；

g）不得非法向他人转让共享获得的数据；

h）在数据运营过程中，应明确数据泄漏防护策略，采取关键字、正则表达式、黑白名单、数据指纹等技术措施，及时发现和阻止敏感数据的泄漏；

i）宜支持基于区块链和数字水印技术实现对数据运营服务过程的溯源；

j）应具备对政务数据运营过程的追溯和安全审计能力，定期对数据运营行为进行评估和审计；

k）应在发现可能违反法律、行政法规或者侵犯他人等合法权益时，立即停止数据运营行为并采取相应的补救措施。

5.6.2 数据使用者安全技术要求

数据使用者应采取相应措施以满足以下安全技术要求：

a）应在授权范围内合法使用数据；

b）应保证开放数据使用环境和使用过程的安全性，以防数据的泄露和滥用。

6 政务大数据域间协同安全要求

6.1 通用要求

政务大数据域间协同通用安全要求包括：

a）数据提供者应对数据接收者进行授权，明确数据权责是否全部或部分转移给接收方；

b）数据提供者应确保数据来源的合法性；

c）数据接收者应确保数据安全保护级别不低于数据提供者，避免数据从高安全等级流向低安全等级；

d）数据接收者应根据数据提供者的授权，保护数据相关方合法权益；

e）应建立相应的安全控制措施，如冗余链路、数据传输加密等，保证数据传输过程中数据的安全性和完整性；

f）应采取数字签名等技术措施，保证数据提供者和数据接收者的真实性。

6.2 数据生产域与数据加工域间协同安全

6.2.1 数据生产域安全技术要求

数据生产域应满足以下安全技术要求：

a）应明确数据加工限制和约束条件，确保数据加工不能损害相关权利人的合法权益；

b）应明确数据加工需求，形成数据加工需求说明书；

c）应按照最小化原则提供用于加工的数据；

d）应采取相应的措施，控制数据加工者对数据的访问。

6.2.2 数据加工域安全技术要求

数据加工域应满足以下安全技术要求：

a）接受加工委托时应提供其安全保障能力的证明材料；

b）应验证接收数据的完整性及是否与数据加工需求相一致；

c）应将加工过程中发现异常数据及时告知对方，涉及敏感数据的在告知时应进行加密传输。

6.3 数据加工域与数据共享域间协同安全

6.3.1 数据加工域安全技术要求

数据加工域应满足以下安全技术要求：

a）接受加工委托时应提供其安全保障能力的证明材料；

b）应全面准确理解数据加工安全需求；

c）应验证接收数据的完整性及是否与数据加工需求相一致；

d）应将加工过程中发现异常数据及时告知对方，涉及敏感数据的在告知时应进行加密传输。

6.3.2 数据共享域安全技术要求

数据共享域应满足以下安全技术要求：

a）应明确数据提供方的加工需求；

b）应及时准确、完整的接收需要加工的数据，并提供给数据加工者；

c）应及时将数据加工者发现的异常数据反馈给数据提供者。

6.4 数据生产域与数据共享域间协同安全

6.4.1 数据生产域安全技术要求

数据生产域应满足以下安全技术要求：

a）应明确用于共享的数据的共享方式、范围、时效、授权条件及限制条件；

b）使用共享数据时，应严格按共享规则使用，并对共享数据进行有效保护；

c）应将使用过程中发现异常数据及时告知数据提供者，涉及敏感数据的在告知时应进行加密传输。

6.4.2 数据共享域安全技术要求

数据共享域应满足以下安全技术要求：

a）应严格按照数据提供者的授权进行数据共享；

b）提供数据时，应根据共享数据的安全等级确定安全共享方式。

6.5 数据开放域与数据共享域间协同安全

6.5.1 数据开放域安全技术要求

数据开放域应满足以下安全技术要求：

a）应严格按照数据提供者的授权，遵照数据开放目录和开放计划进行数据开放；

b）应及时发现不得开放的重要数据和个人信息，并告知数据提供者。

6.5.2 数据共享域安全技术要求

数据共享域应满足以下安全技术要求：

a）应严格按照数据提供者的授权，遵照数据开放目录和开放计划，向数据开放域提供数据；

b）应确保提供开放的数据不包含个人信息或重要数据。

6.6 数据运营域与数据共享域间协同安全

6.6.1 数据运营域安全技术要求

数据运营域应满足以下安全技术要求：

a）应提供其安全保障能力证明材料并获得数据运营授权；

b）未经提供者许可，不得留存共享获得的数据；

c）应在数据运营过程中，及时发现不在授权范围内的重要数据和个人信息，并通知数据提供者；

d）应定期向共享域报告数据安全运营情况，并提供相应的数据安全运营分析报告。

6.6.2 数据共享域安全技术要求

数据共享域应满足以下安全技术要求：

a）应评估运营域数据运营环境与限制和约束条件，确保运营域的数据运营活动不能损害相关权利人的合法权益；

b）应审核运营域的数据运营场景和行为，确保的运营域的数据运营服务没有超出数据运营授权范围；

c）提供运营数据时，应保证数据运营获得了授权并具备相应能力；

d）应对数据运营过程进行安全监督、检查和定期审计，并及时处理存在的运营安全问题。

7 政务大数据基础设施安全技术要求

平台运营者应采取相应措施以满足以下安全技术要求：

a）应按照GB/T 39786、GB/T 22239、GB/T 35273等要求对政务大数据基础设施进行安全保护；

b）宜按照GB/T 37988的要求对自身数据安全保护能力进行评定；

c）应通过技术和管理手段确保政务大数据基础设施安全，并完善统一身份认证、统一授权管理、数据密码保护、数据监测溯源等安全服务能力，以满足各政务大数据域的安全需求；

d）应自行或者委托网络安全服务机构对关键信息基础设施每年至少进行一次网络安全检测和风险评估，对发现的安全问题及时整改，并按照保护工作部门要求报送情况；

e）应完善网络安全应急预案，定期开展应急演练，在发生重大安全事件或者发现重大安全威胁时，应按照有关规定向相关机构报告，并及时进行应急处置。

附 录 A
（资料性）
域内系统及参与方示例

根据大数据应用场景的不同，各政务大数据域中所包含的实体及参与方各不相同，表A.1、表A.2分别给出了各域的实体示例和各参与方示例。

表 A.1 数据域实体示例

域类型	系统、平台或组件
数据生产域	政务部门门户网站、政务信息系统等
数据加工域	数据清洗、数据加工平台等
数据共享域	共享交换平台、目录链系统等
数据开放域	政务信息查询网站、DATA网站等
数据运营域	金融专区、竞赛专区等

表 A.2 政务大数据参与方示例

参与方	示例
数据生产者	政务部门
数据控制者	政务部门、北京市大数据中心、数据专区运营商
数据加工者	信息技术服务外包机构
数据使用者	个人、企业、政务部门
数据提供者	个人、企业、政务部门
数据接收者	个人、企业、政务部门
平台运营者	北京市大数据中心

参 考 文 献

[1]GB/T 35295 信息技术 大数据术语
[2]GB/T 37988 信息安全技术 数据安全能力成熟度模型
[3]促进大数据发展行动纲要 国发〔2015〕50号
[4]政务信息资源共享管理暂行办法 国发〔2016〕51号
[5]北京市政务信息资源管理办法（试行） 京政发〔2017〕37号
[6]北京市大数据行动计划工作方案 京政办发〔2018〕31号