
# 数据安全标准与产业实践

刘贤刚　　中国电子技术标准化研究院信息安全研究中心主任

2018 ISC 互联网安全大会 中国·北京
Internet Security Conference 2018　Beijing·China
（原中国互联网安全大会）

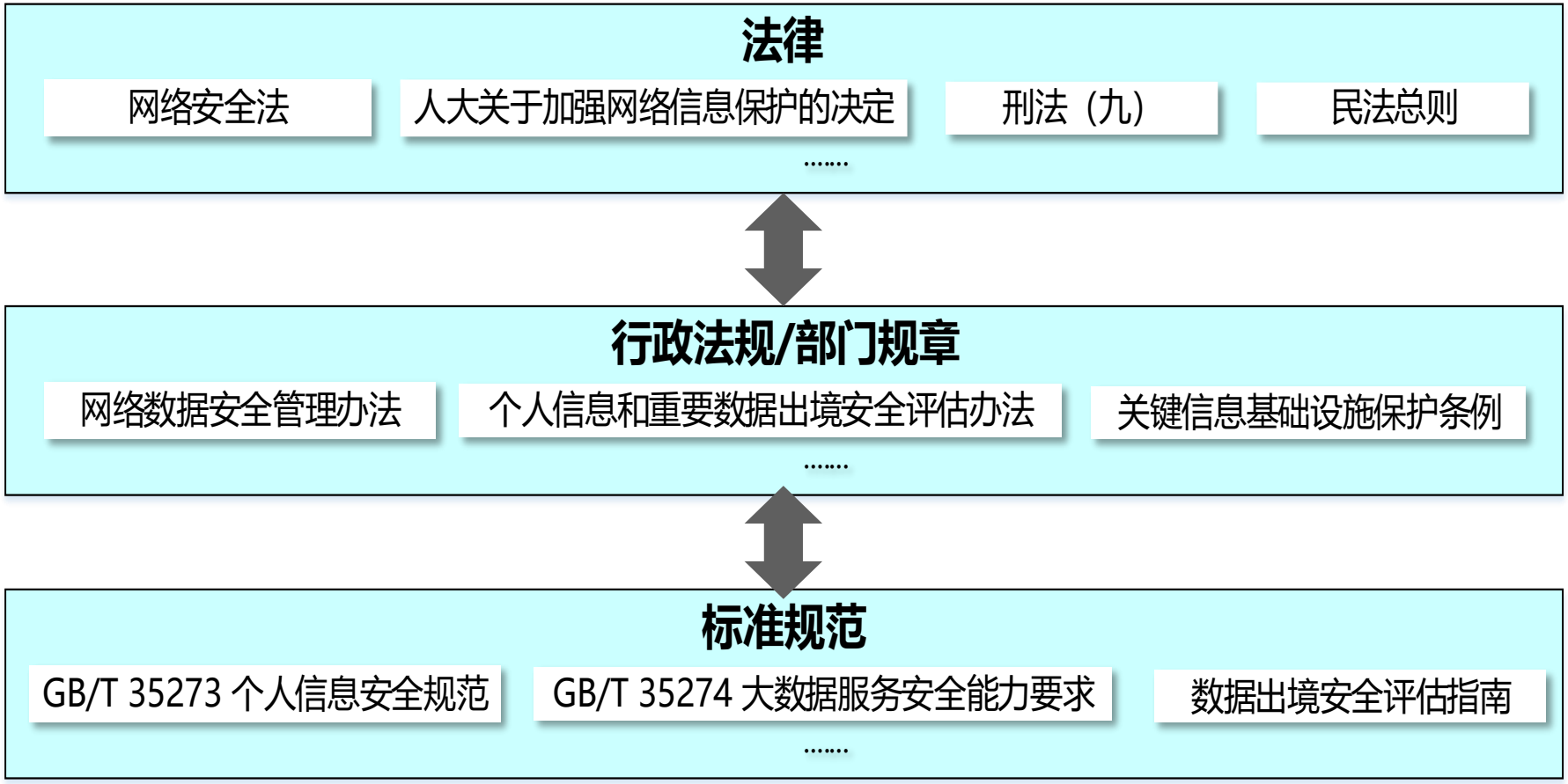
# 目 录

- 数据安全国家标准进展
- 个人信息保护标准与产业实践
- 数据安全能力标准与产业实践

# 数据安全国家标准进展

# 数据安全的政策和标准

- 习近平总书记在中央政治局第二次集体学习国家大数据战略会议上强调要**切实保障我国数据安全。**
- **《网络安全法》**：国家建立和完善**网络安全标准体系。**提及数据16处：数据安全、个人信息保护、数据跨境流动、国家层面的数据安全等。
- **数据安全国家标准是对国家法律法规和政策规章的细化支撑，也是大数据安全保障体系的重要组成部分。**

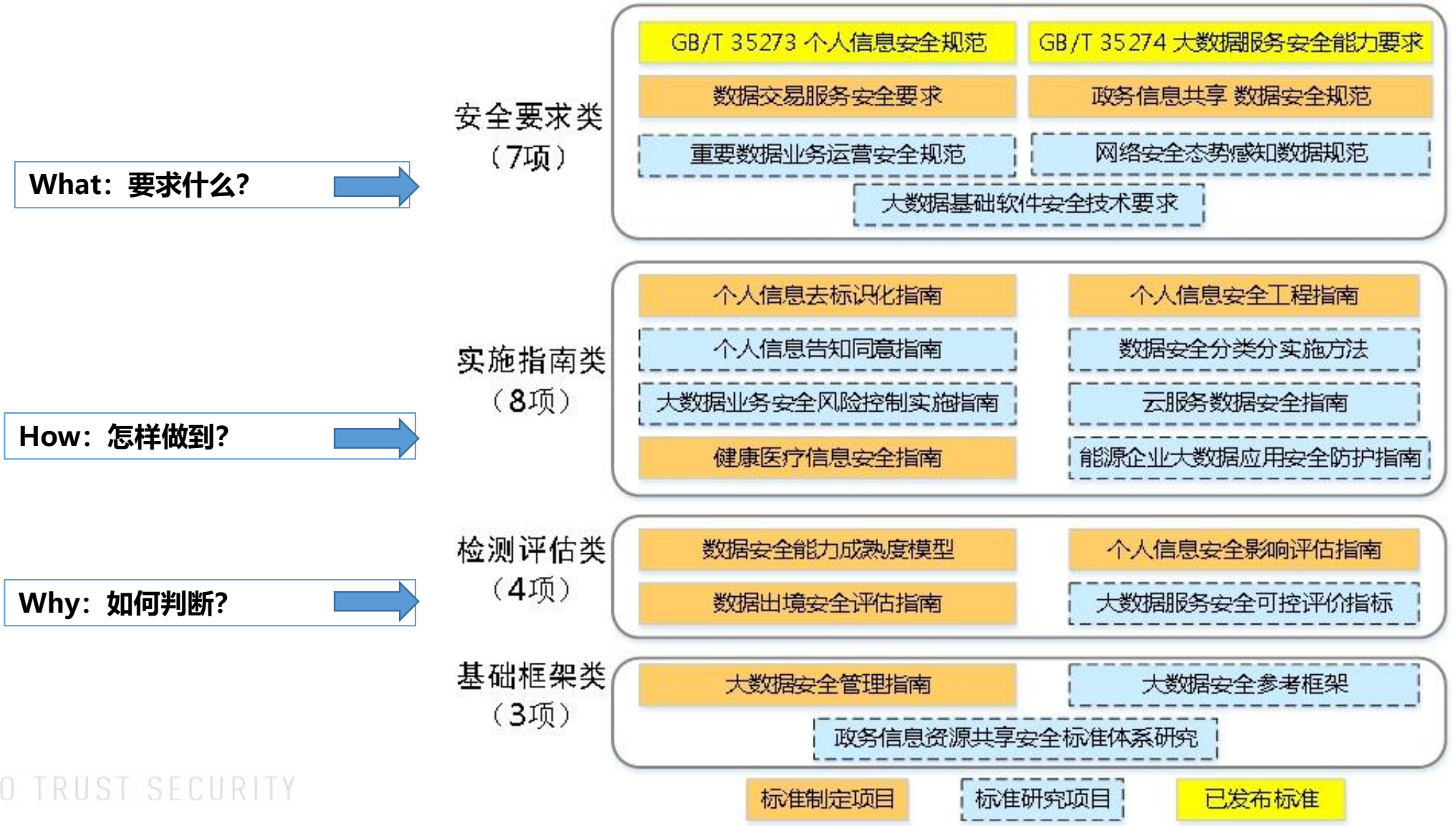


# 数据安全国家标准制定项目

| 序号 | 名称 | 状态 | 立项时间 |
|---|---|---|---|
| **1** | **信息安全技术 个人信息安全规范** | **GB/T 35273-2017** | **2016** |
| **2** | **信息安全技术 大数据服务安全能力要求** | **GB/T 35274-2017** | **2016** |
| 3 | 信息安全技术 大数据安全管理指南 | 报批稿 | 2016 |
| 4 | 信息安全技术 数据安全能力成熟度模型 | 报批稿 | 2017 |
| 5 | 信息安全技术 数据交易服务安全要求 | 报批稿 | 2017 |
| 6 | 信息安全技术 数据出境安全评估指南 | 征求意见稿 | 2017 |
| 7 | 信息安全技术 个人信息去标识化指南 | 报批稿 | 2017 |
| 8 | 信息安全技术 个人信息安全影响评估指南 | 征求意见稿 | 2017 |
| 9 | 信息安全技术 个人信息安全工程指南 | 草案 | 2018 |
| 10 | 信息安全技术 健康医疗信息安全指南 | 草案 | 2018 |
| 11 | 信息安全技术 政务信息共享 数据安全规范 | 草案 | 2018 |

**现有22项数据安全标准项目，已发布2项大数据安全国家标准，在研9项国家标准**

# 数据安全国家标准制定和研究项目

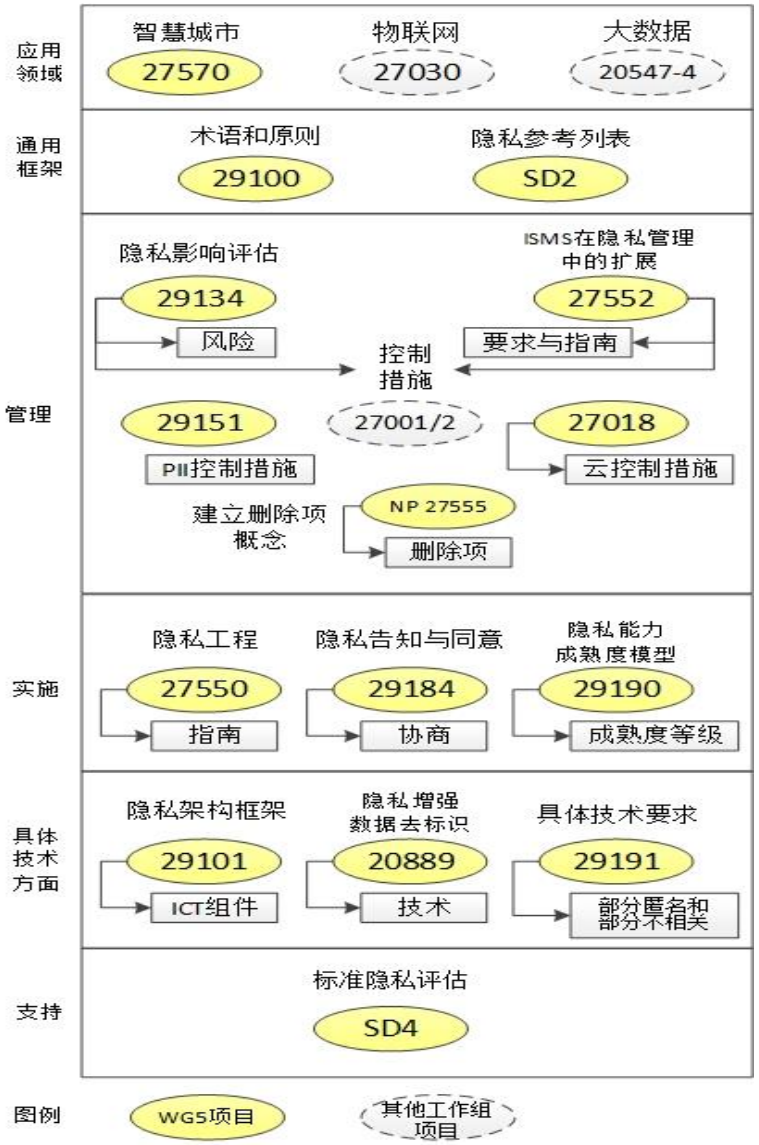


# SC27的数据安全标准

| 序号 | 标准名称 | 标准状态 | 编辑 |
| --- | --- | --- | --- |
| **1** | **ISO/IEC 20547-4《信息技术 大数据参考架构 第4部分：安全与隐私保护》** | **第四版工作组草案** | **中国、德国** |
| 2 | ISO/IEC 19086-4《云计算 服务水平协议（SLA）框架第4 部分：安全与隐私保护》 | FDIS最终国际标准草案 | 美国 |
| 3 | ISO/IEC 27040:2015 《信息技术 安全技术 存储安全》 | 已出版 | |
| 4 | ISO/IEC 27030《信息技术 安全技术 物联网的安全和隐私指南》 | 第一版工作组草案 | 日本、美国 |
| **5** | **ISO/IEC 27045《大数据安全与隐私 过程》** | **NP新标准立项** | **中国、加拿大** |
| **6** | **《大数据安全与隐私 实现指南》** | **SP标准研究项目** | **中国、加拿大** |
| **7** | **《数据安全》** | **SC层面研究组** | **中国、美国** |

# SC27的隐私保护标准

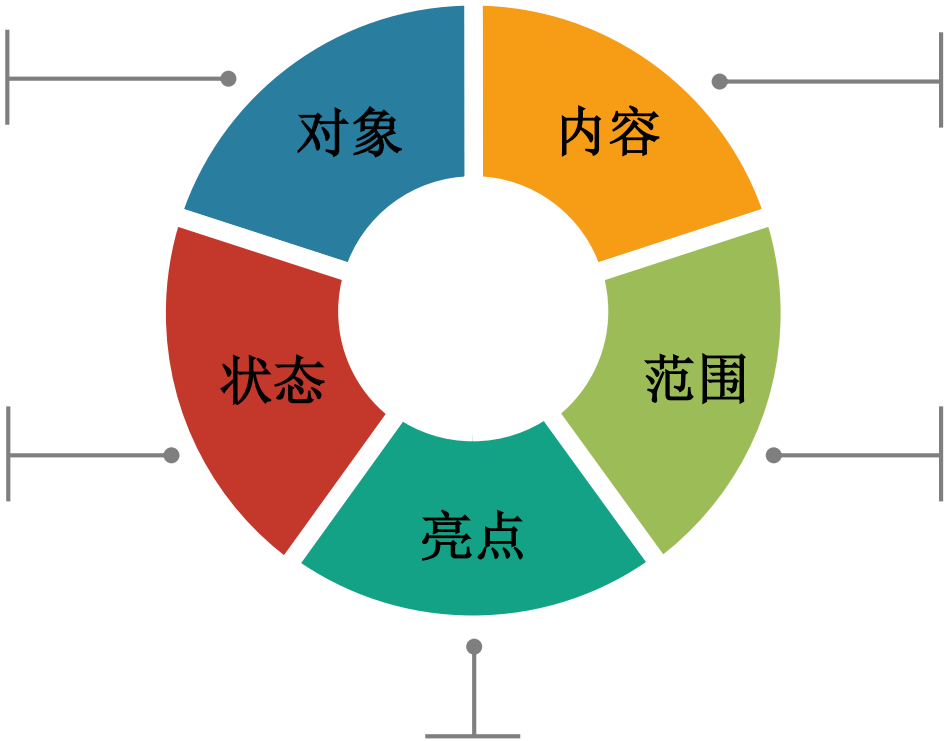
## SC27隐私保护标准体系



# 个人信息安全规范

涉及个人信息处理活动的各类组织

GB/T 25273-2017




本标准规范了开展收集、保存、使用、共享、转让、公开披露等个人信息处理活动应遵循的原则和安全要求。

适用于规范各类组织个人信息处理活动，也适用于主管监管部门、第三方评估机构等组织对个人信息处理活动进行监督、管理和评估。

个人信息保护七大原则

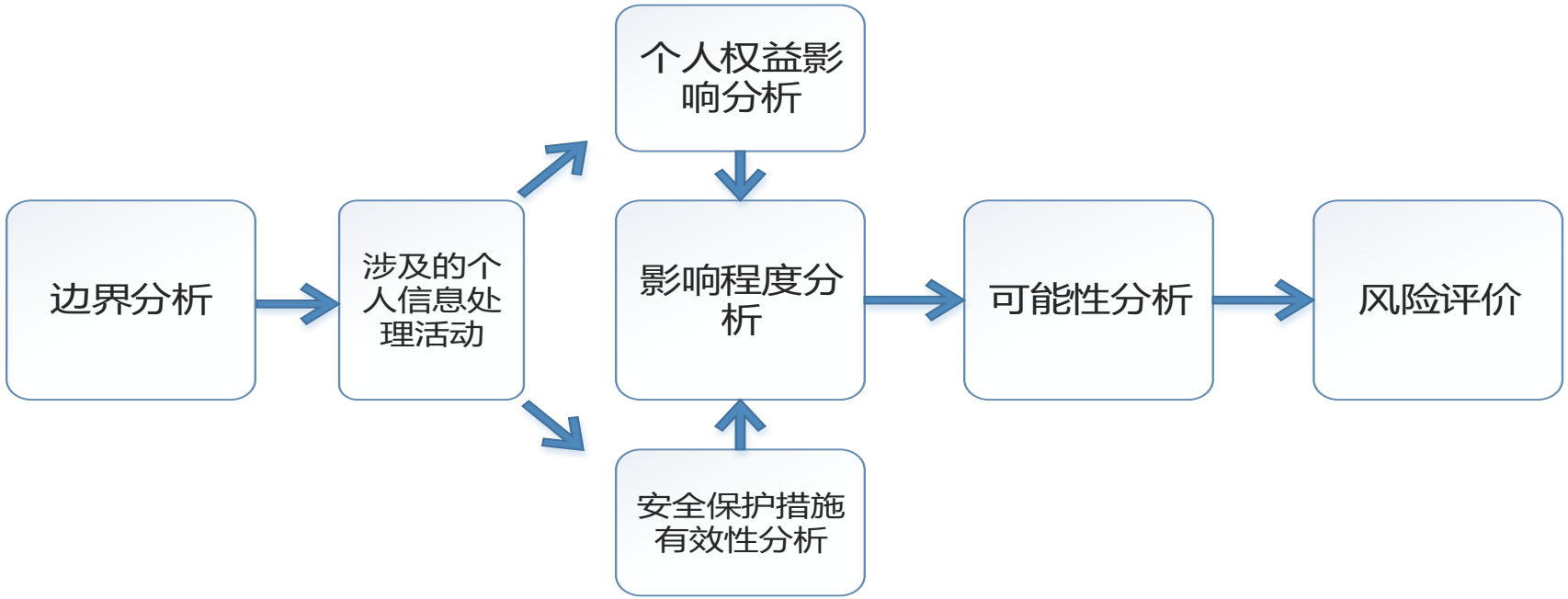
权责一致原则、目的明确原则、选择同意原则、最少够用原则、公开透明原则、确保安全原则、主体参与原则

# 个人信息去标识化指南

- 为个人信息去标识化工作的开展建立整体的原则，并指导、规范个人信息去标识化工作的方法和过程，提升组织机构的合规能力。
- 本标准一方面可以为个人信息处理相关方提供去标识化的指导，另一方面则为第三方机构测评提供依据。
- 本标准旨在在实现数据可用性和个人信息安全平衡的前提下，促进数据的共享开放。

# 个人信息安全影响评估指南

- 本标准规定了个人信息安全影响评估的基本概念、框架、方法和流程。
- 本标准适用于各类组织自行开展个人信息安全影响评估工作。同时为国家主管部门、第三方测评机构等开展个人信息安全监管、检查、评估等工作提供的指导和依据。



# 个人信息保护标准

个人信息去标识化指南（报批稿）

**关键技术支撑标准**

个人信息安全规范（GB/T 35273）

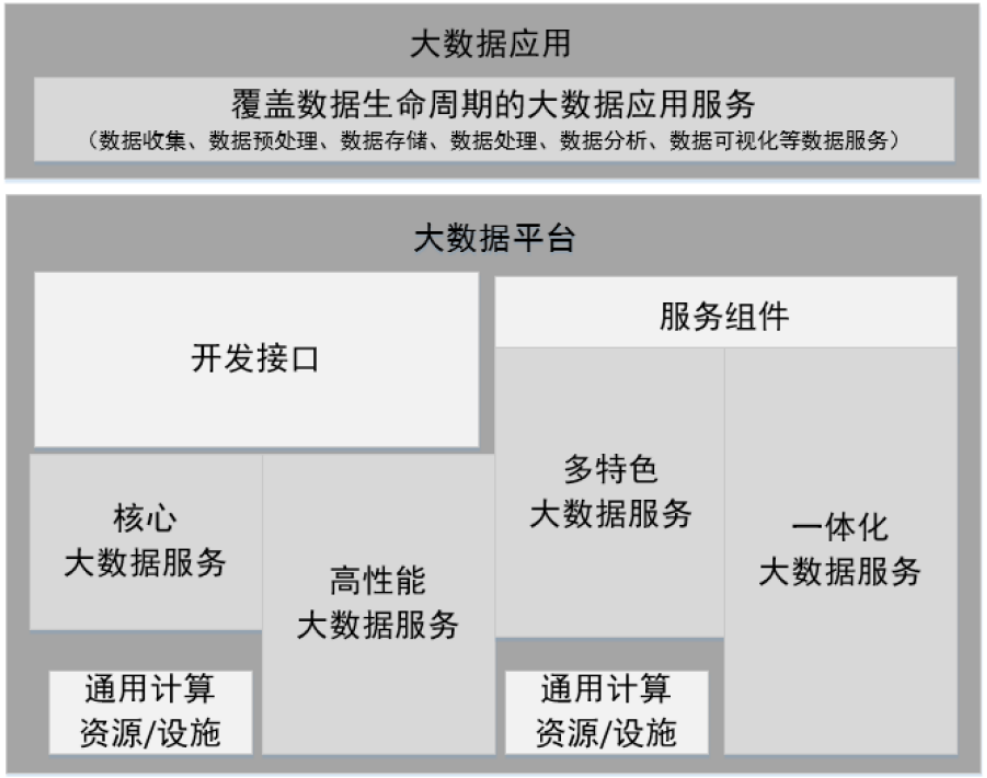
**基础标准**

个人信息安全影响评估（草案）

**效果验证标准**

# 大数据服务安全能力要求（GB/T 35274-2017）

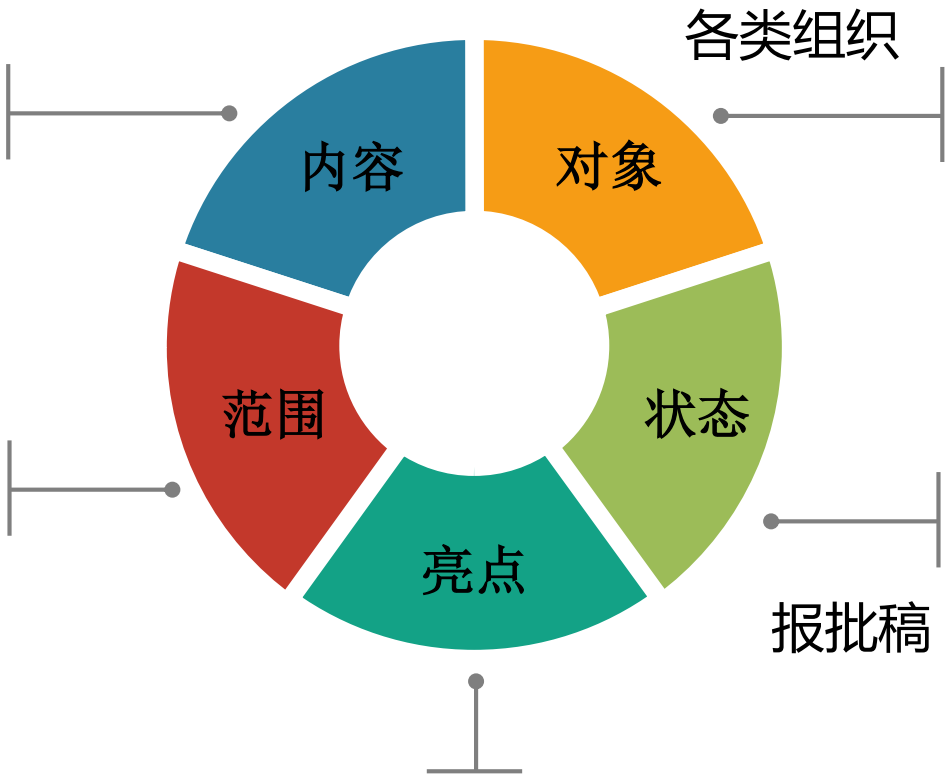
- **标准化对象：**大数据服务提供者（组织）
- **标准主要内容：**本标准规定了大数据服务提供者应具有的组织相关基础安全能力和数据生命周期相关的数据服务安全能力。
- **标准适用范围：**可为政府部门、企事业单位等组织机构的大数据服务安全能力建设提供参考，也适用于第三方机构对大数据服务提供者的大数据服务安全能力进行审查和评估

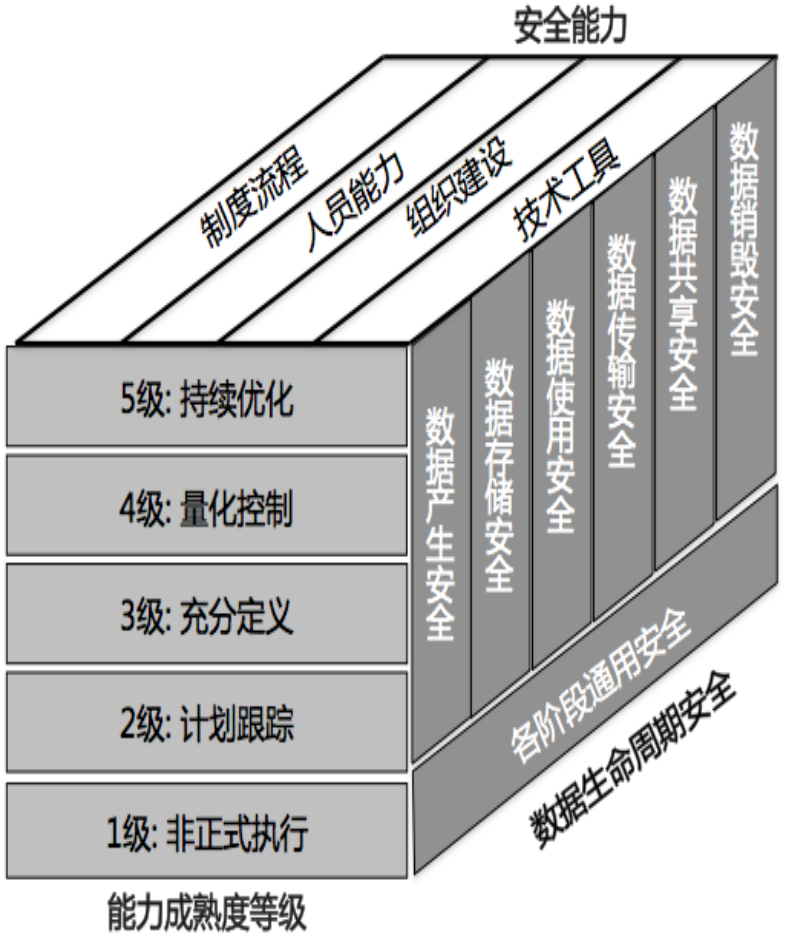


# 数据安全能力成熟度模型

定义了**数据安全能力成熟度模型**，基于组织的数据生命周期，从**组织建设、人员能力、制度流程**以及**技术工具**四个能力维度，针对组织在大数据环境下的电子化数据的数据安全过程域，构建规范性的大数据安全能力成熟度评估方法。

适用于组织机构评估自身的数据安全能力，也适用于第三方机构对组织机构的数据安全能力进行评估。

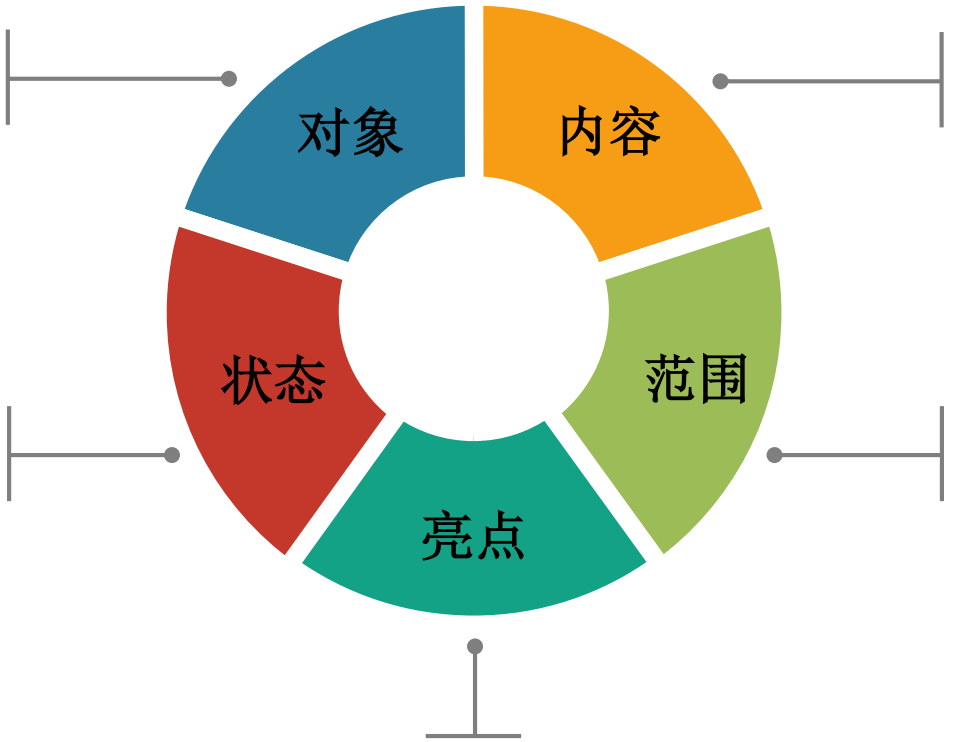



国际标准研究项目同步推进

# 数据交易服务安全要求

通过数据交易服务机构进行的数据交易服务




规定了通过数据交易服务机构进行的数据交易服务所涉及的交易参与方、交易对象和交易过程的安全要求

报批稿

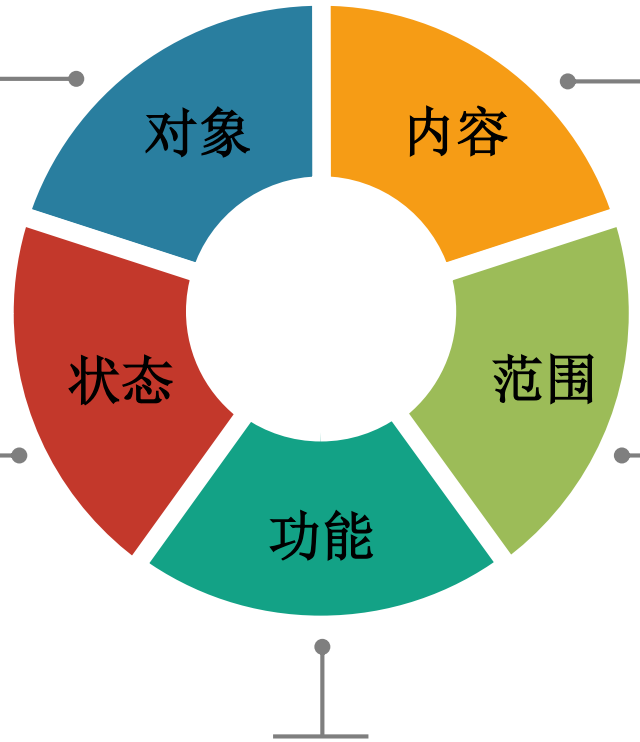
适用于提供数据交易服务的组织进行安全自评估，也适用于第三方机构对数据交易服务组织进行安全测评。

保障了交易参与方安全、交易对象安全、交易过程安全

# 数据处境安全评估指南

个人信息和重要数据出境安全评估

征求意见稿




提出了个人信息和重要数据出境的安全评估原则、流程、要点和方法。

适用于网络运营者、网络安全服务机构等开展个人信息和重要数据出境安全评估。

可为网络运营者进行数据出境安全管理制度和能力建设提供参考。

# 个人信息保护产业实践

# 网络运营者产品和服务普遍问题

隐私条款笼统不清，对收集、使用个人信息的目的、方式、范围、保存期限和地点等没有明确说明。

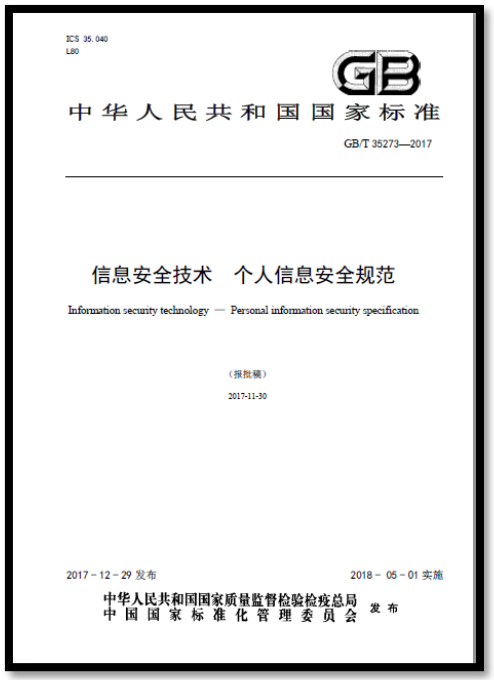

不主动向用户展示隐私条款，或展示的内容晦涩冗长。

大量收集与所提供服务无直接关联的个人信息，超越与用户的约定，擅自扩大范围收集、使用个人信息，私自共享、转让个人信息。

征求用户授权同意时，仅通过默认勾选、“一揽子”打包授权等形式，未给用户足够的选择权。

没有为用户提供访问、更正、删除其个人信息的途径，不给用户提供撤回授权、关闭权限、注销账户的方式。

# 标准试点




**开展GB/T 35273-2017《信息安全技术 个人信息安全规范》标准试点示范**

**Carry out the pilot demonstration of GB/T 35273-2017 Information Security Technology - Personal Information Security Specification**


**在中央网信办、工业和信息化部、公安部、国家标准委等4部门指导下，TC260开展了10款产品和服务的隐私条款评审。**

**Implement the review of privacy policies on 10 kinds of products and services under the guidance of Cyberspace Administration of China, the Ministry of Industry and Information Technology, the Ministry of Public Security and SAC.**

# 试点效果

- 10款产品和服务在隐私政策方面均有不同程度的提升。
- 10款产品和服务在隐私政策中，均明示其收集、使用个人信息的规则，并征求用户的明确授权。
- 其中，8款产品和服务做到了向用户主动提示、并提供更多选择权。
- 其中，5款产品和服务在满足以上功能的基础上，还提供了更便利的在线“一站式”撤回和关闭授权，在线访问、更正、删除其个人信息，在线注销账户等功能。

# 个人信息保护倡议


## 签署倡议

参评的**十家互联网企业**，主动发起了**个人信息保护倡议**，表示将：

- 尊重用户知情权和控制权
- 遵守用户授权
- 保障用户信息安全
- 保障产品和服务的安全可信
- 联合抵制黑色产业链
- 倡导行业自律
- 接受社会监督

# 个人信息保护合规实践

发布隐私政策是个人信息控制者遵循公开透明原则的重要体现，是保证**个人信息主体知情权**的重要手段，还是约束自身行为和配合监督管理的重要机制。**隐私政策应清晰、准确、完整地描述个人信息控制者的个人信息处理行为。**

| 隐私政策模版 | 编写要求 |
| --- | --- |
| 本政策仅适用于XXXX的XXXX产品或服务，包括……。<br>最近更新日期：XXXX年XX月。<br>如果您有任何疑问、意见或建议，请通过以下联系方式与我们联系：<br>电子邮件：<br>电　　话：<br>传　　真： | 该部分为适用范围。包含隐私政策所适用的产品或服务范围、所适用的用户类型、生效及更新时间等。 |
| 本政策将帮助您了解以下内容：<br>1. 我们如何收集和使用您的个人信息<br>2. 我们如何使用 Cookie 和同类技术<br>3. 我们如何共享、转让、公开披露您的个人信息<br>4. 我们如何保护您的个人信息<br>5. 您的权利<br>6. 我们如何处理儿童的个人信息<br>7. 您的个人信息如何在全球范围转移<br>8. 本政策如何更新<br>9. 如何联系我们<br>XXXX深知个人信息对您的重要性，并会尽全力保护您的个人信息安全可靠。我们致力于维持您对我们的信任，请在使用我们的产品（或服务）前，仔细阅读并了解本《隐私政策》。 | 该部分为隐私政策的重点说明，是隐私政策的一个要点摘录。目的是使个人信息主体快速了解隐私政策的主要组成部分、个人信息控制者所做声明的核心要旨。 |

# 个人信息保护合规实践

**5.3　收集个人信息时的授权同意**

a)收集个人信息前，应向个人信息主体明确告知所提供产品或服务的**不同业务功能分别收集的个人信息类型**，以及收集、使用个人信息的规则（例如收集和使用个人信息的目的、收集方式和频率、存放地域、存储期限、自身的数据安全能力、对外共享、转让、公开披露的有关情况等），并获得个人信息主体的授权同意；

**5.5　收集个人敏感信息时的明示同意**

a)收集个人敏感信息时，应取得个人信息主体的明示同意。应确保个人信息主体的明示同意是其在**完全知情的基础上自愿给出的、具体的、清晰明确的愿望表示**；

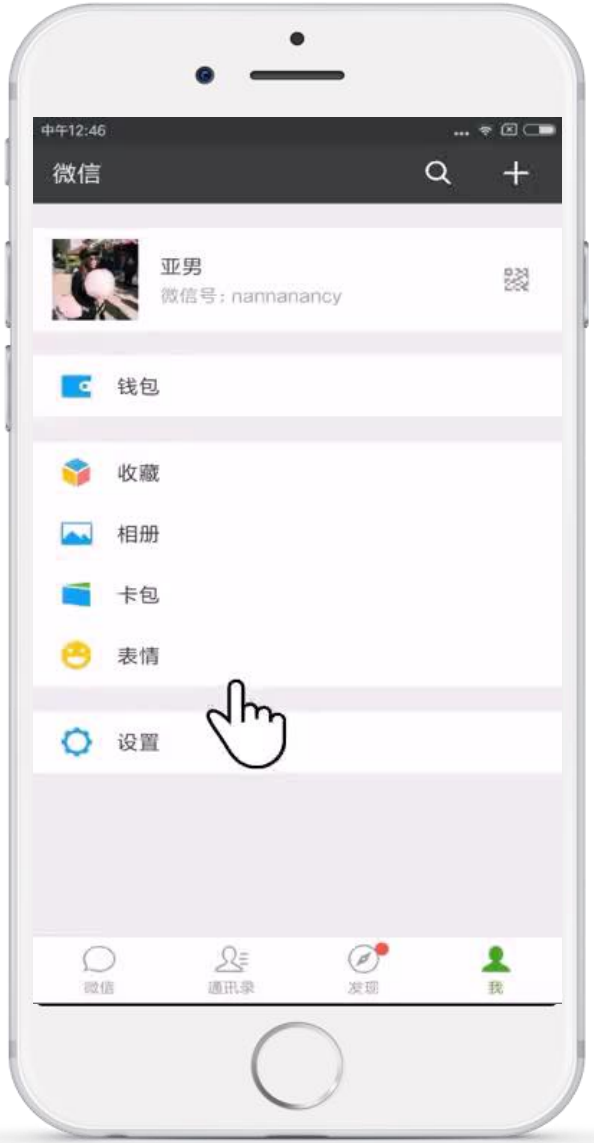
# 个人信息保护合规实践

### 7.8　个人信息主体注销账户

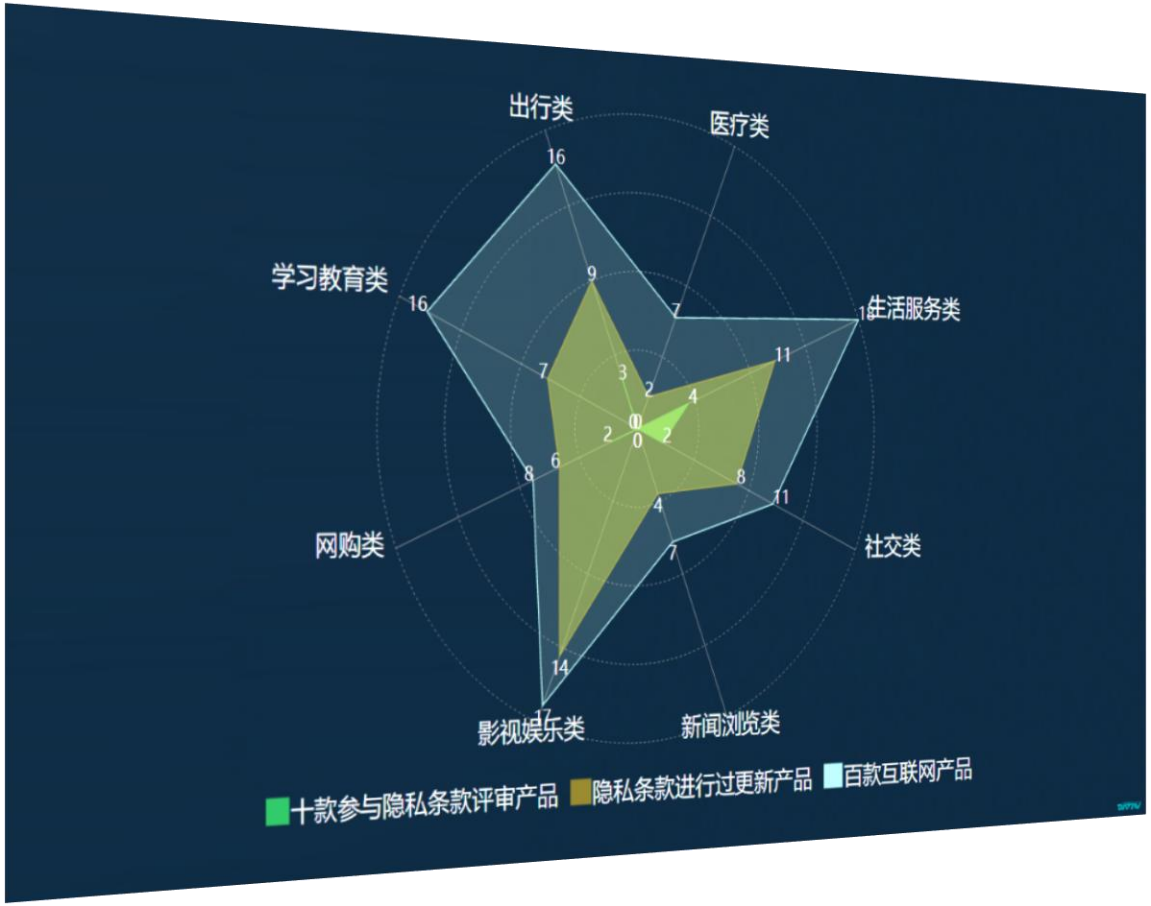
对个人信息控制者的要求包括：

a）通过注册账户提供服务的个人信息控制者，应向个人信息主体**提供注销账户的方法，且该方法应简便易操作**；

b）个人信息主体注销账户后，应删除其个人信息或做匿名化处理。



# 评审后期影响




## 评审对象

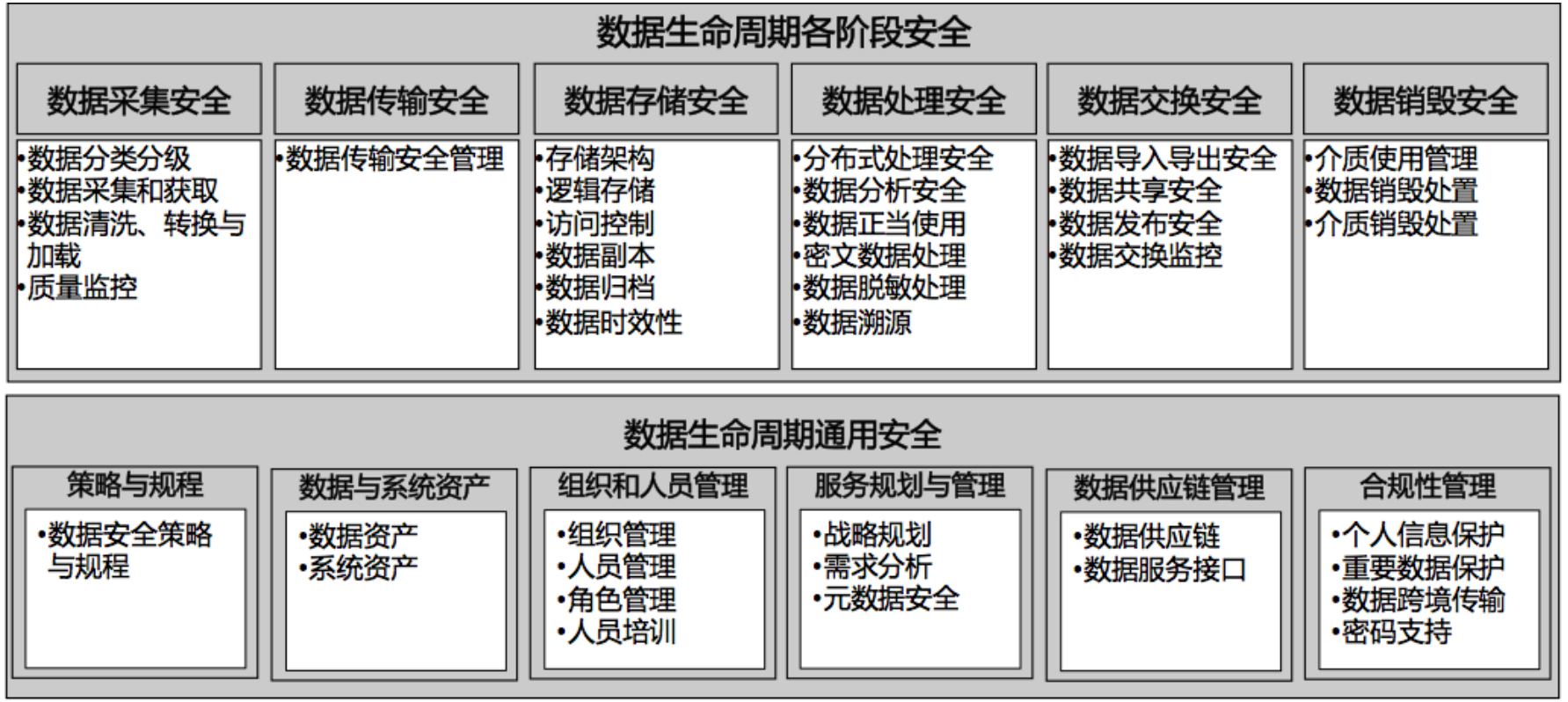
后期对APP进行跟进，抽查的百款互联网产品中，社交类、影视娱乐类、网购类、生活服务类的互联网产品隐私条款更新比例大，专项工作对APP隐私条款有一定的促进效果。

# 数据安全能力标准产业实践

# 数据安全过程域

过程域划分

**根据数据生命周期的不同，将数据安全分为24个数据生命周期各阶段安全的过程域和16个数据生命周期通用安全**



# 数据安全能力成熟度模型推广应用

- 标准试点的重点行业领域

制造业　软件行业　金融行业

文娱行业　零售行业　物流行业

电力行业　服务行业　互联网+新型企业

- 标准地方试点---贵州、四川、宁夏
- 通过数据安全成熟度模型标准试点，提升组织安全能力，促进数据安全有序流动

中国南方电网 CHINA SOUTHERN POWER GRID 广州供电局有限公司　广发证券 GF SECURITIES　首旅如家　百世 BEST LOGISTICS　伊利

龍圖信息 DRAGON DREAM　极课大数据 FCLASSROOM　拾羽　SAKURA 樱花卫厨　。。。

# 谢 谢！

2018 ISC 互联网安全大会 中国 · 北京

Internet Security Conference 2018 Beijing · China

（原中国互联网安全大会）

中国电子技术标准化研究院