聚·变

第二届顺丰信息安全峰会分论坛

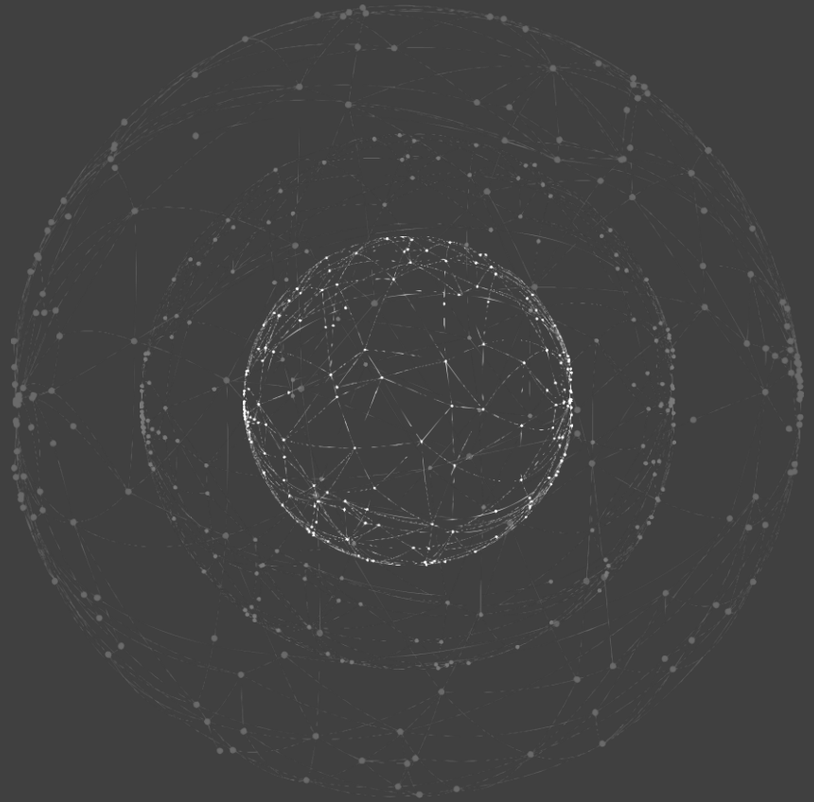
网络空间安全

个人信息保护标准实施对企业合规的影响

GB/T 35273 个人信息安全规范

中国电子技术标准标准化研究院

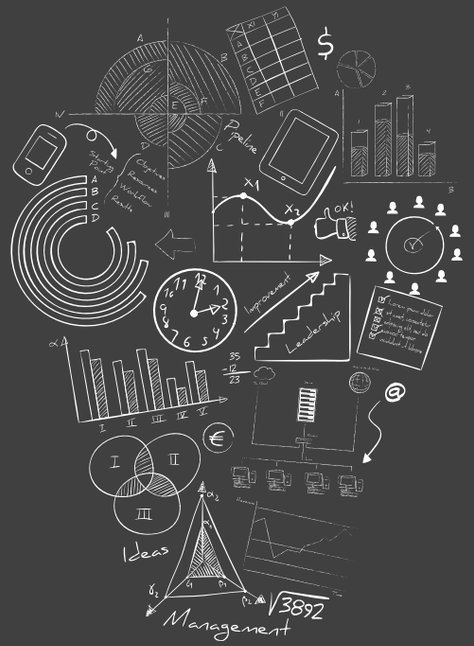
CESI 何延哲 2018.8



体会

Impression

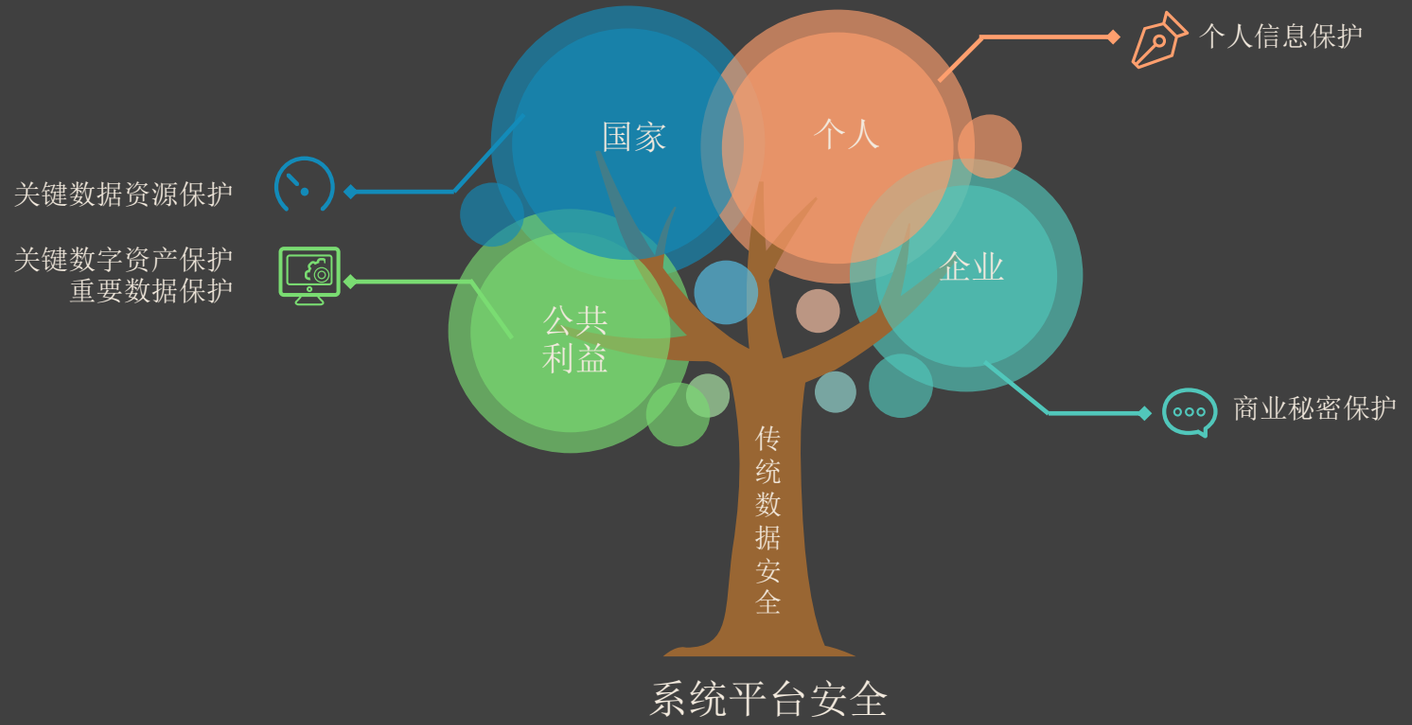
- 网络安全+
- 从IT到DT
- 数据安全时代



演变
Trend

- Before 2017
- 2017-2018
- 未来

范畴
Scope

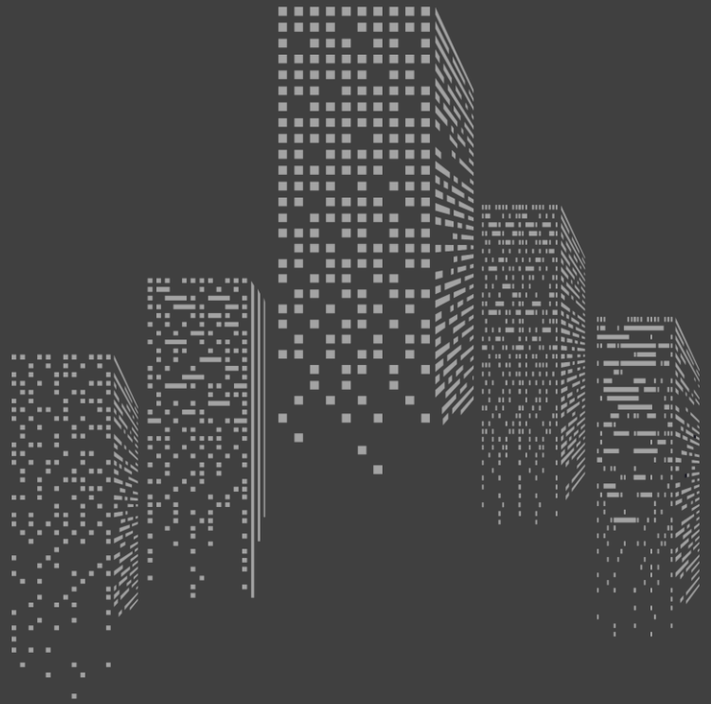

国家
个人
公共
利益
企业
传统数据安全
关键数据资源保护
关键数字资产保护
重要数据保护
个人信息保护
商业秘密保护
系统平台安全

特征
Feature

一

- 因人而起
- 因时而变
- 因人而异

标准的定位



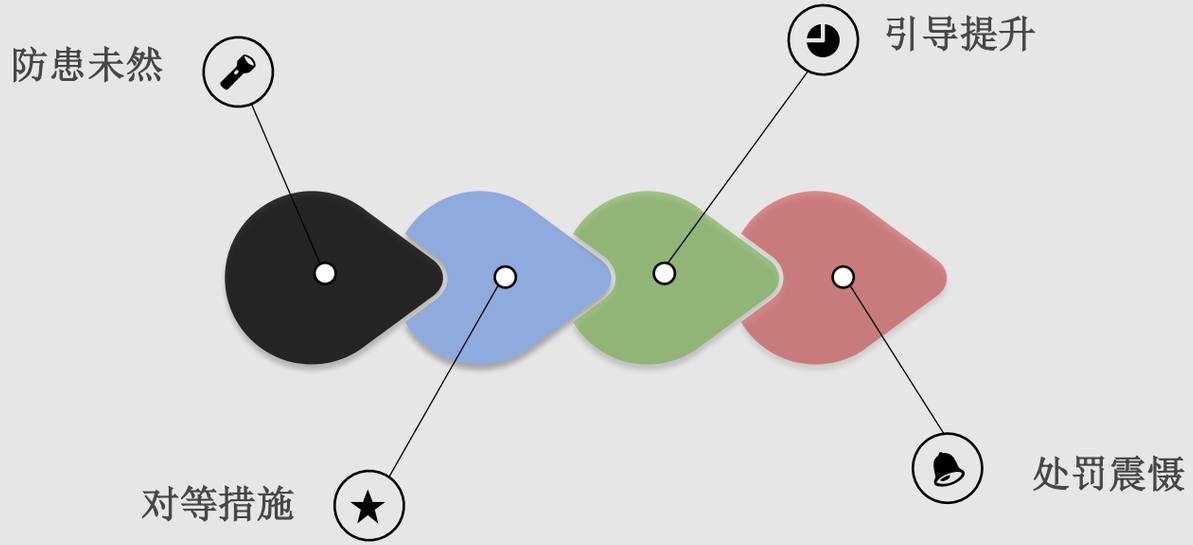
现实意义

Realism

- 为什么需要标准
- 需要什么样的标准
- 如何使用标准

Date | May 2018

#2-01 政策思路与监管导向



#2-01 政策思路与监管导向

- 《网络安全法》实施前，国家网信办在2017年5月31日就其实施的有关情况回答了记者提问。网信办表示，多个配套制度文件正在抓紧研究起草，国家标准化部门正抓紧组织制定《个人信息安全规范》等国家标准。
- 2017年08月25日，国家互联网信息办公室有关负责人就《互联网跟帖评论服务管理规定》答记者问。指明建立用户信息保护制度。《网络安全法》第四十条、四十一条、四十二条、四十三条、四十四条、四十五条对用户信息保护制度作了规定，国家标准化部门正抓紧组织制定《个人信息安全规范》，因此本《规定》仅对此作了原则性表述。
- 2018年01月10日，国家互联网信息办公室网络安全协调局约谈“支付宝年度账单事件”当事企业负责人。网络安全协调局负责人指出，支付宝、芝麻信用收集使用个人信息的方式，不符合刚刚发布的《个人信息安全规范》国家标准的精神，违背了其前不久签署的《个人信息保护倡议》的承诺。

#2-01 政策思路与监管导向

- 中央网信办等四部门指导信安标委秘书处组织开展隐私条款评审及签署“个人信息保护倡议书”

- 中央网信办通报约谈有关公司情况时引用

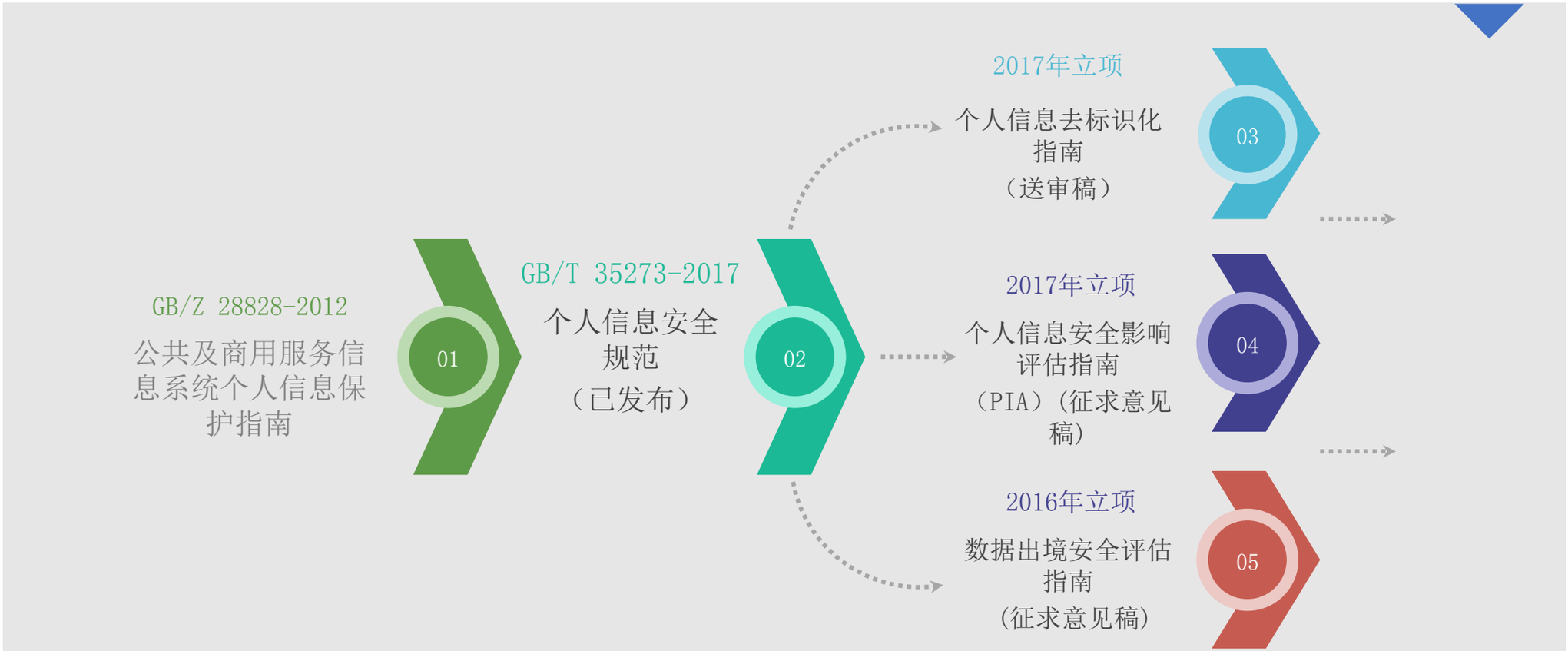
银监会《银行业金融机构数据治理指引》引用

我国政府在联合国网络犯罪有关会议中引用

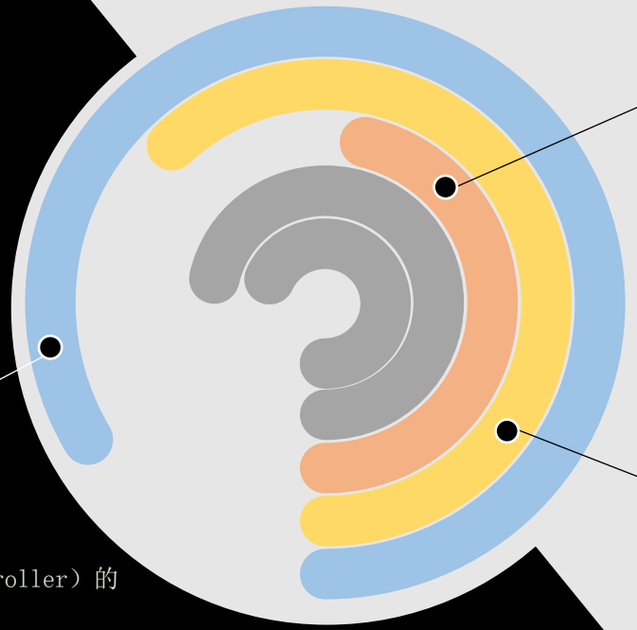
中消协制定个人信息保护相关评审方案时引用

……

#2-02 个人信息保护标准体系



#2-03 标准的适用性



Object

对象

本标准主要针对个人信息控制者（controller）的处理个人信息的过程提出安全要求。

Content

内容

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

Usage

用途

本标准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。

#2-04 标准制定思路

实效性Effective

标准要求是否会对个人信息安全现状改善有立竿见影的效果

全面性Comprehensive

标准要求是否能够涵盖所有的个人信息处理场景和控制点，是否能够与国际接轨

制约的可能Restrictive

标准要求是否和现状差异过大，是否适应当前的发展趋势

可操作性Operational

标准要求是否具有普遍指导意义，是否有拿来即用的效果

#2-05 标准的主要内容

一

权责一致原则

对其个人信息处理活动对个人信息主体合法权益造成的损害承担责任。

二

目的明确原则

具有合法、正当、必要、明确的个人信息处理目的。

三

选择同意原则

向个人信息主体明示个人信息处理目的、方式、范围、规则等，征求其授权同意。

四

最少够用原则

只处理满足用户授权同意的目的所需的最少信息类型和数量。

五

公开透明原则

以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则等。

六

确保安全原则

采取足够的管理措施和技术手段，保护个人信息的保密性、完整性、可用性。

七

主体参与原则

向个人信息主体提供能够访问、更正、删除其个人信息，以及撤回同意、注销账户等方法。

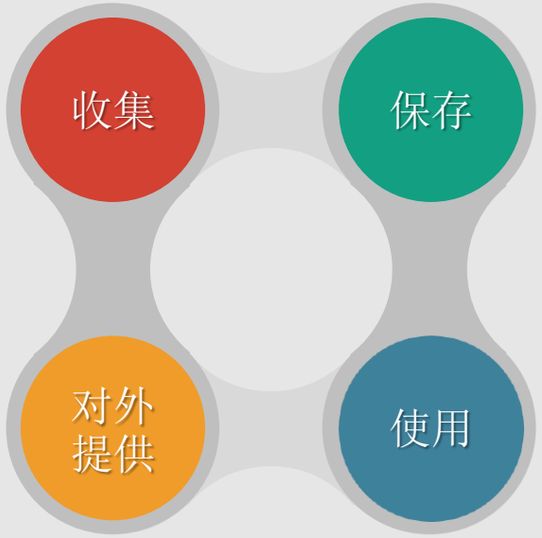
#2-05 标准的主要内容

Collection of PI

- 合法性要求和最小化要求
- 授权同意和例外
- 敏感信息明示同意
- 隐私政策的内容和发布

External providing of PI

- 委托处理要求
- 共享、转让要求
- 收购、兼并、重组要求
- 公开披露要求
- 共同的个人信息控制者要求
- 跨境传输要求



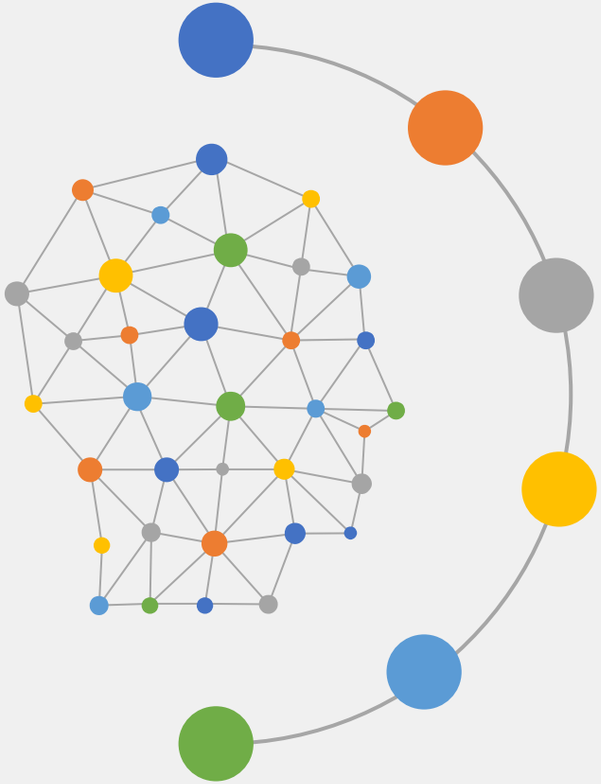
Retention of PI

- 保存时间最小化
- 去标识化处理
- 敏感信息传输和存储
- 个人信息控制者停止运营

Use of PI

- 访问控制措施
- 使用和展示限制
- 访问、更正、删除、撤回同意、注销账户、获取副本等机制
- 响应个人信息主体的请求和申诉管理

#04 标准的主要内容



安全事件处置

建立安全事件应急处置和报告机制
安全事件发生时应及时向个人信息主体告知

明确责任部门与人员

应任命个人信息保护负责人和个人信息保护工作机构
应建立、维护和更新组织所持有的个人信息清单

开展个人信息安全影响评估

定期（至少每年一次）开展个人信息安全影响评估
评估个人信息处理活动对个人信息主体合法权益的影响

数据安全能力

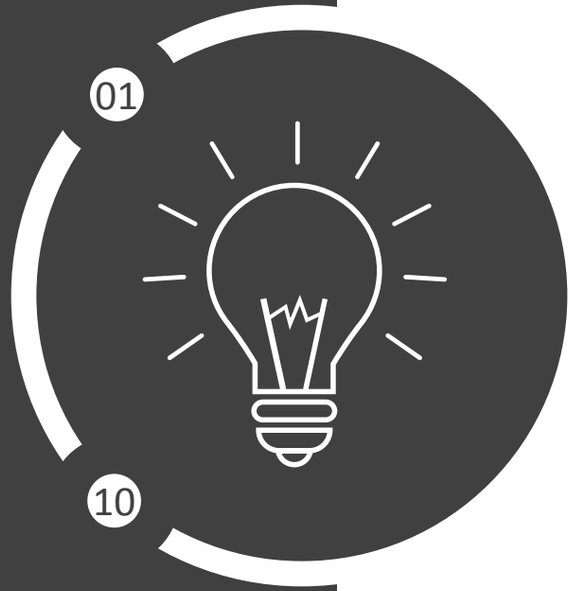
个人信息控制者应根据有关国家标准的要求，建立适当的数据安全能力，落实必要的管理和技术措施，防止个人信息的泄漏、损毁、丢失。

人员管理与培训

与从事个人信息处理岗位上的相关人员签署保密协议
对个人信息处理岗位上的相关人员开展个人信息安全专业化培训和考核

安全审计

应对隐私政策和相关规程，以及安全措施的有效性进行审计
应及时处理审计过程中发现的个人信息违规使用、滥用等情况


01
10


《个人信息安全规范》
实施参考框架
对内建立体系
能力
提升域
不同产品线
拓展
⑦ 提升数据
安全能力
⑧ 去标识化
技术应用
⑨ 个人信息
安全工程
④ 建立
信息清单
⑤ 实施
影响评估
⑥ 发布
隐私政策
⑩ 合规能力展
示 (如倡议书)
③
规范授权 主体权利 合同协议 培训审计
标准 差距 分析 改进
职责
划分
② 工作
计划
①
责任
主体
高层
支持
责任域
关键工作域
对外接受监督
平台
生态内拓展

04

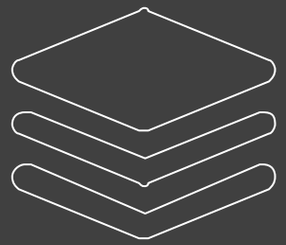
10

建立信息清单


主动提供
源头：个人信息主体主动填写的信息
自动采集
源头：个人信息主体的设备和软件（手机、PC、浏览器、APP等）
间接获取
源头：第三方已有个人信息、公开渠道的个人信息等
加工处理
源头：已有个人信息+个人信息主体的行为

建立信息清单

04



10

Delegated processing

个人信息控制者作出委托行为，不得超出已征得个人信息主体授权同意的范围。

特定对象+控制权未转移

委托处理

Sharing

个人信息控制者向其他控制者提供个人信息，且双方分别对个人信息拥有独立控制权的过程。

特定对象+同时拥有控制权

共享

Transfer of control

将个人信息控制权由一个控制者向另一个控制者转移的过程。

特定对象+控制权转移

转让

Public disclosure

向社会或不特定人群发布信息的行为。

非特定对象

公开披露

#05 标准实施指引-个人信息安全影响评估（PIA）

- 影响个人自主决定权
- 名誉受损或精神压力

- 引发差别性待遇
- 个人财产受损

#05 标准实施指引-个人信息安全影响评估（PIA）

#风险评价

- 四方面风险
- 严重与高风险不可接受

风险等级		可能性级别			
		低	中	高	很高
影响级别	严重	中	高	严重	严重
	高	中	中	高	严重
	中	低	中	中	高
	低	低	低	中	中

#06 标准实施指引-发布隐私政策

简介

为落实《网络安全法》要求，提升网络运营者个人信息保护水平，**中央网信办、工业和信息化部、公安部、国家标准委**指导开展**个人信息保护提升行动之隐私条款专项工作**。

评审对象

专项工作由**全国信息安全标准化技术委员会秘书处**负责具体组织工作。

首批选取用户数量大、与民众生活密切相关、社会关注度高的十款互联网产品和服务，分别为：

社交类：微信、新浪微博

电商类：淘宝网、京东商城

支付类：支付宝

地图类：高德地图、百度地图

出行类：滴滴出行、携程旅行网、航旅纵横。

#06 标准实施指引-发布隐私政策

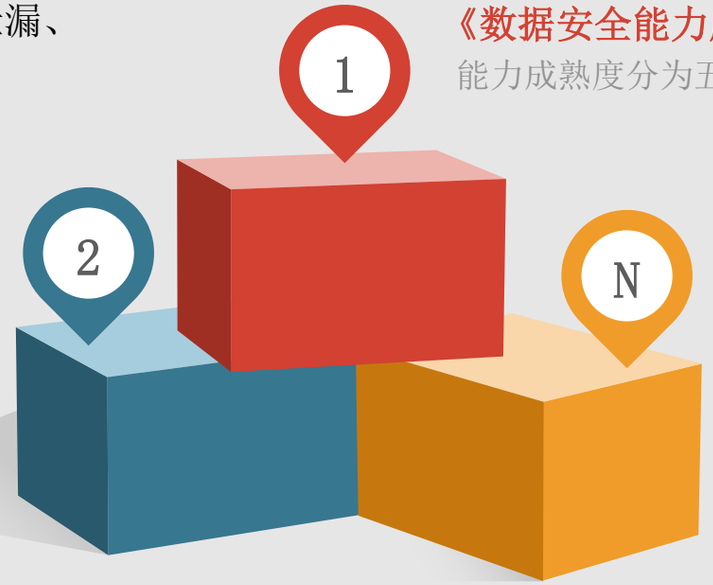
附录D 隐私政策模板

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……。 最近更新日期：XXXX年XX月。 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： 电子邮件： 电　　话： 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： 1. 我们如何收集和使用您的个人信息 2. 我们如何使用 Cookie 和同类技术 3. 我们如何共享、转让、公开披露您的个人信息 4. 我们如何保护您的个人信息 5. 您的权利 6. 我们如何处理儿童的个人信息 7. 您的个人信息如何在全球范围转移 8. 本政策如何更新 9. 如何联系我们 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。

#07 标准实施指引-提升数据安全能力

个人信息控制者应根据有关国家标准的要求，建立适当的数据安全能力，落实必要的管理和技术措施，防止个人信息的泄漏、损毁、丢失。



《数据安全能力成熟度模型》

能力成熟度分为五级，尚未发布

GB/T 35274-2017 《信息安全技术 大数据服务安全能力要求》

针对服务过程

系统、平台类安全标准

等级保护系列

云服务安全

27000系列

……

#08 标准实施指引-去标识化等技术应用

De-identification

通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别个人信息主体的过程。

注：去标识化建立在个体基础之上，保留了个体颗粒度，采用假名、加密、哈希函数等技术手段替代对个人信息的标识。

Delete

在实现日常业务功能所涉及的系统中去除个人信息的行为，使其保持不可被检索、访问的状态。

Anonymization

通过对个人信息的技术处理，使得个人信息主体无法被识别，且处理后的信息不能被复原的过程。

注：个人信息经匿名化处理后所得的信息不属于个人信息。

Disposal/Erasure

在物理环境和介质中彻底删除数据，且无法复原。

#09 标准实施指引-个人信息安全工程（PbD）

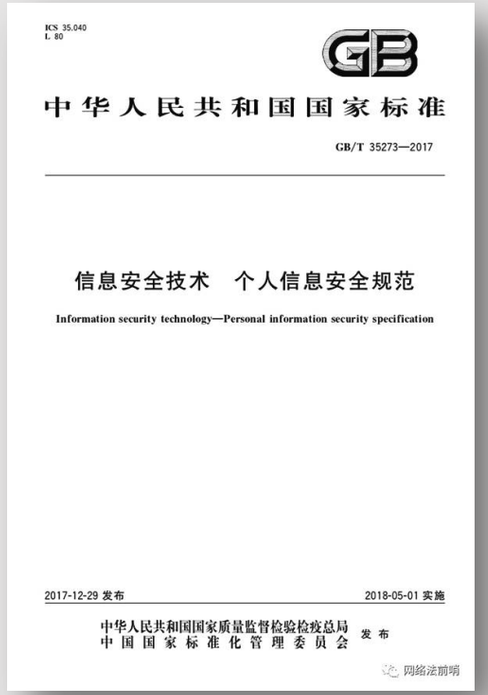
#10 标准落地-开发相关认证

一审两证

- 获得信息安全管理体系认证证书和个人信息安全管理体系认证证书；
- 认证依据：GB/T35273-2017《信息安全技术个人信息安全规范》和GB/T22080-2016《信息技术 安全技术 信息安全管理体系要求》。

认证过程

- 体系建设：自行或委托专业机构
- 技术验证：中国电子技术标准化研究院、中国赛迪集团、国家信息中心
- 现场评审：中国网络安全审查技术与认证中心评审



ICS 35.040
L 80

GB

中华人民共和国国家标准

GB/T 35273—2017

信息安全技术 个人信息安全规范

Information security technology—Personal information security specification

2017-12-29 发布　　2018-05-01 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

网络法前哨

#10 标准落地-个人信息安全工程师培训

提供个人信息安全人员培训、数据安全能力成熟度人员培训，围绕个人信息保护、数据安全能力建设的法律法规、国家标准、隐私条款、实践指南等方面进行培训。

国内首家权威的个人信息保护课程

个人信息安全保护工程师
首次培训人员40人；已有数据安全能力成熟度评估认证人员10余人

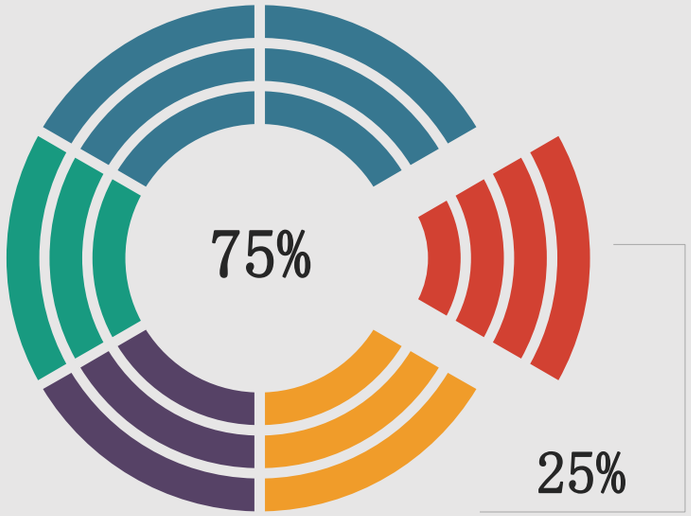
培训班人员分布

可持续合规

Continuous Compliance

Date | May 2018

#01 讨论-合规的价值



提升能力

提升保护能力，规避安全风险也是对业务最好的保护

增加余地

有效规避法律法规描述不清晰具体，操作余地不足的缺点

适应性强

新技术新应用对法律法规适用性不足可能会制约发展

合规义务

完成最基本的评估工作规避法律责任

#02 讨论-合规的方向

可知 01

可控 02

可示 03

可溯 04

可迭 05

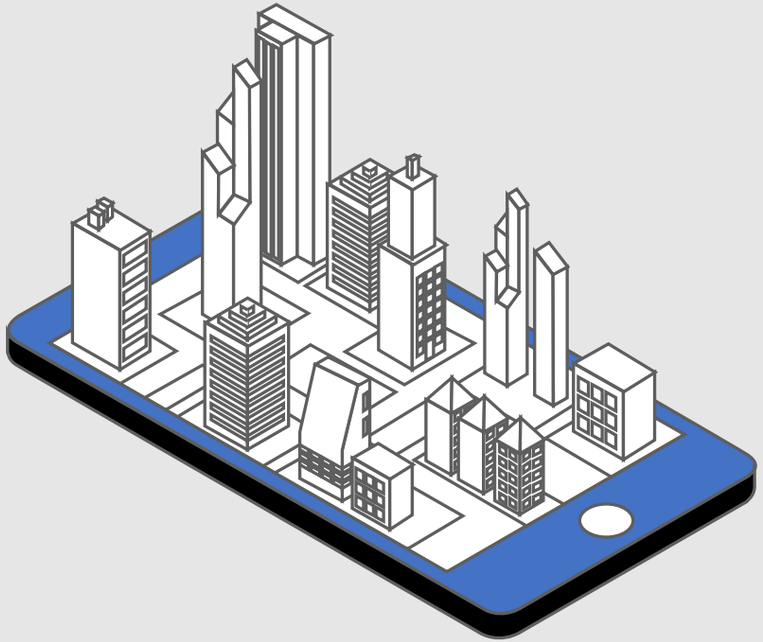
可预 06

#03 讨论-合规的建议

#01 循序渐进

#02 知己知彼

#03 与时偕行



THANK YOU