



2018 (第三届)
数据安全与隐私保护大会

数据安全 刻不容缓

——数据安全与隐私保护合规评估培训

2018年9月

风险咨询高级经理 张楠驰



2018 (第三届) 数据安全与隐私保护大会

目录

1. 数据安全环境与背景	3
2. 个人隐私保护法规框架	9
3. 数据安全通用原则	19
4. 评估方法与实践	30



2018 (第三届) 数据安全与隐私保护大会

1 | 数据安全环境与背景

大数据正在成为打造企业竞争优势的重要资源

利用大数据推动企业的每个数字化环节，实现可持续发展

企业的各个层面

企业面临的挑战



网络安全问题加剧的催化剂

物联网
\$6260亿

预计2018年消费者移动支付市场收入将达6260亿美元
资料来源：高盛分析2016

传感器

移动
85%

到2020年，85%的业务关系的建立实现智能化
资料来源：高德纳2015

分析

3D打印
99%

在具有加入网络可能性的设备中，99%的设备目前处于未连接状态
资料来源：思科，Rob Soderbury 2017

社交

云计算
36%

36%的企业无法识别复杂的网络攻击
资料来源：安永全球信息安全调查

人工智能

网络
81%

81%的高管认为数据是决策的核心依据
资料来源：安永《打造分析型企业，提升价值创造能力》



企业数据安全问题日益突出

2018 (第三届) 数据安全与隐私保护大会



2个

每时每刻，全世界有2个企业
因为信息安全问题而倒闭
《中国财富》



27.9%

发生1万条数据泄露事件的可能性
《2018年Ponemon数据泄露损
失研究》



386万美元

平均数据泄露成本
《2018年Ponemon 数据泄露损
失研究》



148美元

每条数据泄露的平均成本
《2018年Ponemon 数据泄露损
失研究》



665,000美元

平均数据泄露恢复成本
《NetDeligence 2016 Cyber
Claim Study 》



915亿

总体对中国经济损失约915亿元
《中国网民权益保护调查报告
(2016) 》

2018 (第三届) 数据安全与隐私保护大会

我们身边充满威胁的数据安全环境

个人信息买卖已形成产业链

1800件 300亿条 40个行业
4200人 390内鬼 近100黑客

1月	10万户	北京顾某使用软件撞库盗号，并出售账号和程序
3月	20亿条	江苏淮安“K8社工库”被捣毁，查获大量公民信息
5月	1100万条	湖北宜昌非法获取并出售股民信息、银行理财信息
5月	未知	湖南怀化5名罪犯通过购买和撞库，后出售及刷单
6月	1200万条	四川广元35名罪犯，倒卖四川全省学生及家长信息
6月	1亿条	山东淄博打掉侵犯公民个人信息的犯罪源头2个
6月	500万条	江苏徐州摧毁一条黑客和快递公司内部员工黑产
6月	未知	山东威海5名银行员工非法出售账户余额及流水
6月	7万条	内蒙古赤峰一团伙利用“快递单号生成器”爬虫
8月	2200万条	福建泉州捣毁了买卖公民个人信息的“浮云网”

我国
7.72亿
网民

来源：
1：CNNIC发布的《第35次中国互联网发展状况统计报告》
2：中国互联网协会发布的《中国网民权益保护调查报告2015》
3：中国证券网报道
4：百度手机卫士监测数据
5：CNCERT，网络安全信息与动态周报
6：漏洞盒子统计

84%
网民个人身份信息被泄露

23万+
每年发生的网络诈骗案，最严重的为冒充银行

915亿
因诈骗、个人信息泄露等遭受的总体经济损失

1000元+
网民各类权益侵害造成的平均经济损失

60万+
网站和个人电脑给黑客控制

1亿+
伪基站

¥500+

个人金融账户

¥200+

个人信息账户

¥0.01+

客户交易信息

¥100K

1亿条Cookie

面洽

知识产权/战略/财务

数据来源：中国互联网协会《中国互联网发展报告2018》

客户数据泄漏已经成为影响公司业务运营的重大威胁

隐私保护大会



造成企业重大经济损失

2017年10月雅虎发布公告称，之前发现的安全漏洞造成至少30亿用户的信息被盗。大规模的网站信息遭窃的案件，使得雅虎股价跌幅超过6%。

企业受到合规性处罚



2017年11月Uber被爆出曾向黑客支付10万美元封口费以隐瞒影响了5,700万个账户的数据泄露事件。该事件引发各国政府关注，优步在英国甚至面临多项处罚措施。菲律宾全国隐私委员会要求其遵守《数据隐私法案》的正式泄漏通知程序。

导致用户声誉受损



知名婚外情网站shleyMadison.com遭到黑客攻击，近3700万用户数据和公司信息被盗。至少已经有两人因隐私曝光自杀。在此之前，这一事件还引发了多起诈骗和勒索。

引发企业管理层动荡

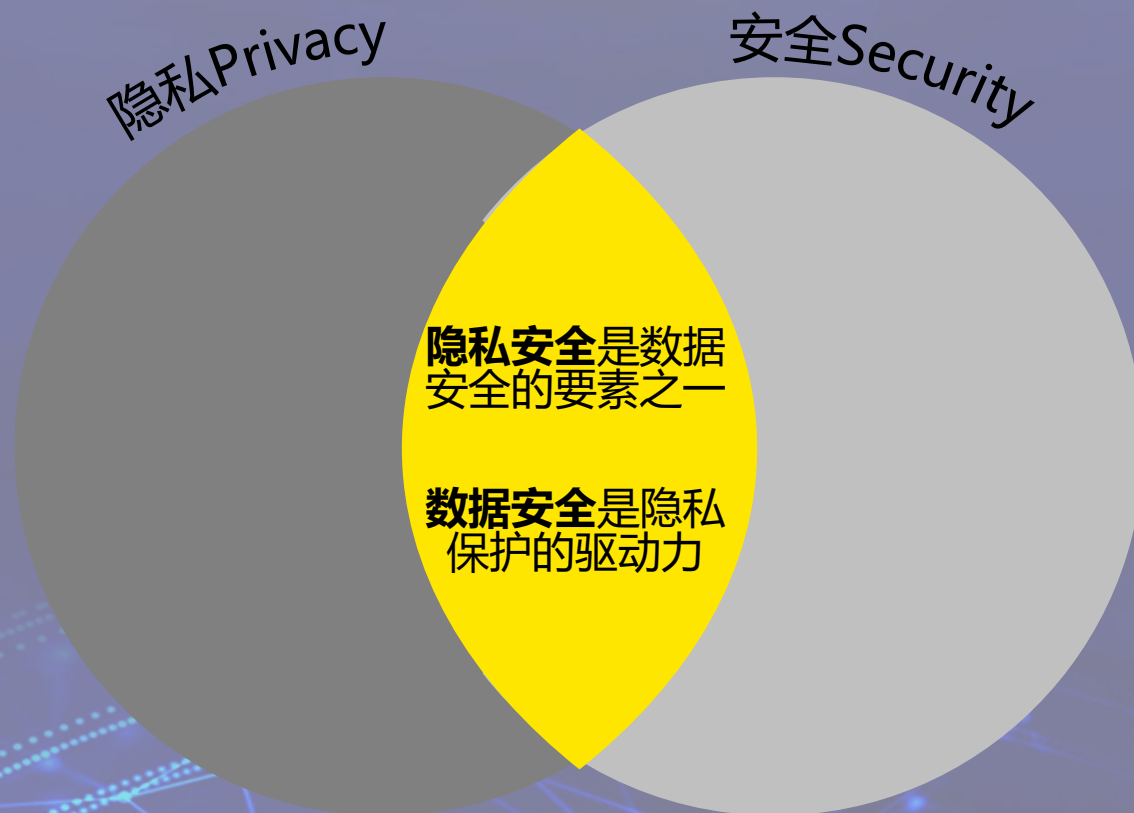
美国知名征信机构Equifax爆发的数据泄露事件导致1.43亿用户信息被泄露。最终公司CEO兼董事长Richard Smith引咎辞职。公司股价出现暴跌，跌幅一度超过37%，并有继续下跌的风险。



数据安全与隐私保护的关系

2018 (第三届)
数据安全与隐私保护大会

There can be no privacy without security. Security alone does not assure privacy.





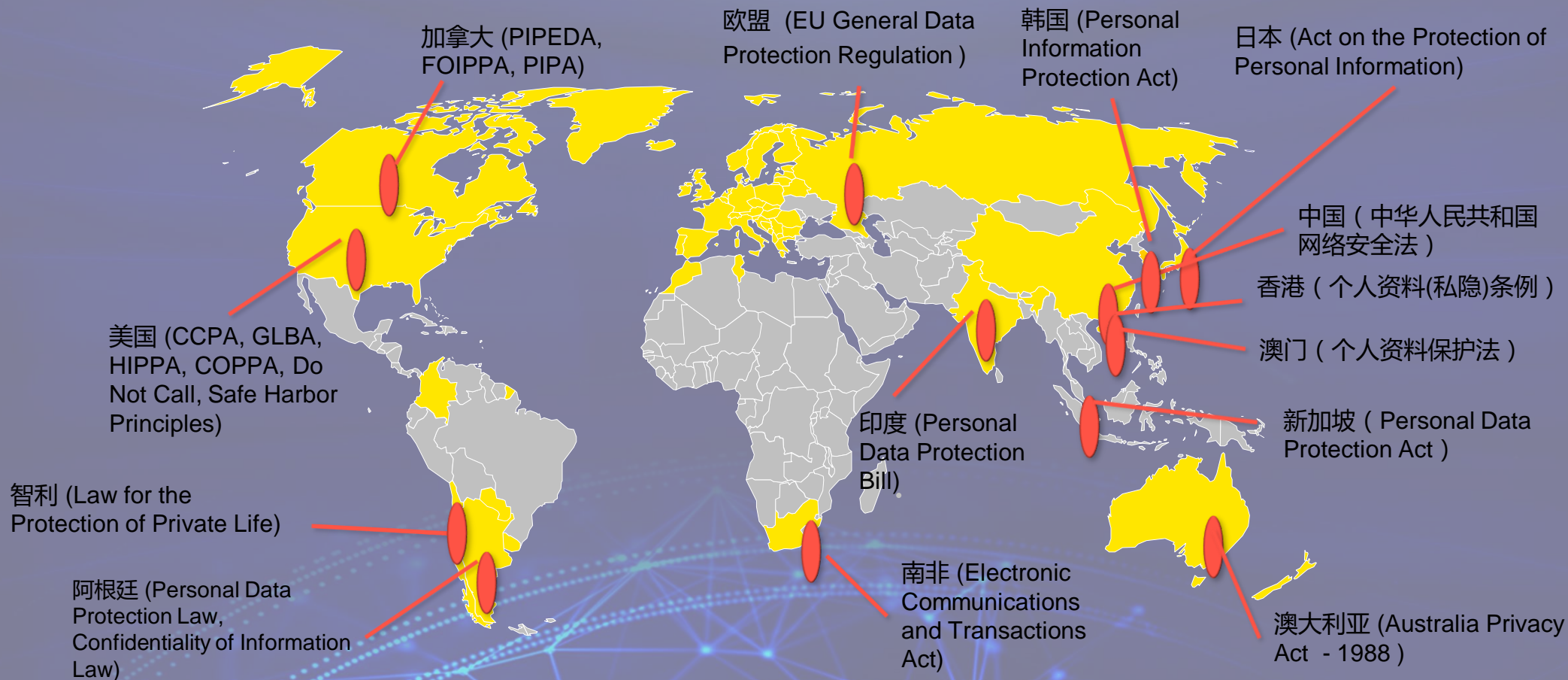
2018 (第三届) 数据安全与隐私保护大会

2 | 个人隐私保护法规框架

全球个人信息保护法律法规环境

2018 (第三届) 数据安全与隐私保护大会

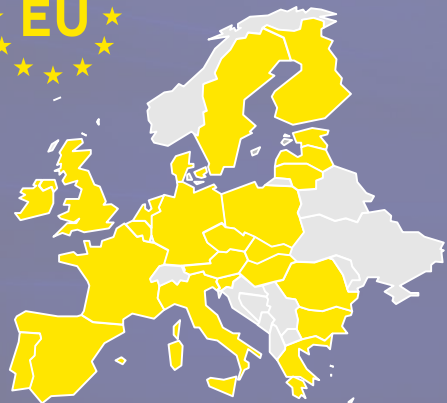
从全球来看，大多数国家和地区已经颁布和施行了隐私保护法规：



以上信息截止2018年7月

欧盟通用数据保护条例GDPR

- ▶ 《通用数据保护条例》 General Data Protection Regulation (GDPR)



《通用数据保护规范》
(GDPR) 是一项综合性的
数据保护法，将于2018年5
月25日生效。本法适用于控
制或处理欧盟居民数据的任
何组织，无论其地理位置。

4% 全球收入

财务影响: 除了潜在的处罚外，企业还面临着合规不确定性导致的内部不稳定带来的巨大成本。



业务影响: 企业收集和存储了大量数据，但对存储的数据了解甚少，不知道它们是什么，存储在哪里，下一步要做什么。

72 小时

响应时间: 事件响应的有效管理至关重要，企业必须确保其组织完全履行合规义务。

非欧盟企业的责任

GDPR可应用到欧盟以外的数据处理活动，如果数据处理的目的是：

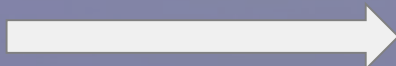
- ▶ 产品提供给在欧盟的个人信息权利人或在欧盟提供支持服务（例如：在线商店，IT服务提供商，外包合作伙伴，处理欧盟内的个人信息权利人数据的处理者）；或
- ▶ 监控欧盟居民个人信息权利人的互联网活动如数据画像（例如：监控购物行为）
- ▶ 作为“处理者”处理欧盟内个人信息权利人的个人数据

例如，中国香港的企业实体向欧盟公民和/或在欧盟的一个分支机构提供服务时，将会被要求遵守通用数据保护条例，以及当地特定的法律及数据保护法律。

欧盟通用数据保护条例GDPR GDPR的发展历程

1995年数据保护指令 (95/46 / EC)

- 国家法律的拼凑
- 欧盟各国的数据保护水平不同
- 执法选项非常有限
- 新技术的开发和数据传输的巨大增长



通用数据保护条例(GDPR)

- 欧盟的统一保护
- 增加欧盟公民对其个人数据的控制权
- 法律的确信性和执法选择的改善

时间线

2012

2013

2014

2015

2016

2017

2018

2012年1月欧洲委员会 (EC) 提议撰写 GDPR

2014年3月
欧盟议会通过
一份中间版本

2015年12月15日
GDPR条例正式被通过

2016年4月14日
欧盟议会正式批准发布GDPR

2018年5月25日
GDPR正式生效

欧盟通用数据保护条例GDPR

GDPR条例内容

GDPR类型和关注点

为了更好地理解条例，GDPR合规要求可以分为11个类型

10 个章节

99 款条例

414 个要求

99款GDPR条例

Article 3, 5, 26, 27, 24, 30, 36-39, 44-49, 51-52, 57, 59-60, 62, 64-78, 79, 83...

Article 23-24, 26-27, 31, 37-39...

Article 23, 27, 35, 37, 39-41, 44-50, 51, 57...

Article 15-44...

Article 4, 12-23, 25, 26, 28-33, 36, 37, 44, 51-76

Article 26, 28-33, 36, 37, 44-49...

Article 33-36...

Article 39, 47, 70...

Article 1, 4-6, 8-10, 12-23, 51, 58, 83...

十一大类型

1.治理

2.风险管理

3.合规

4.政策

5.流程

6.产品

7.信息安全

8.供应商管理

9.事件管理

10.培训和意识

11.数据清单

欧盟通用数据保护条例GDPR GDPR框架概述

2018 (第三届)
数据安全与隐私保护大会

如果该组织在欧盟内的多个国家存在，将根据组织主要机构的位置指定首席执行官或“监督机构”DPA的间的争议将由欧洲数据保护委员会处理

主监管机关 (LDPA)

隐私声明中应明确告知数据主体个人信息收集的目的、方式、范围、数据主体权利、个人信息存储期限等GDPR要求告知的内容。

隐私声明

原则上禁止将欧盟公民的个人信息向欧盟以外的国家转移，仅在符合GDPR中规定的例外场景或为个人信息提供充分保护时方可进行跨境传输。

跨境传输

当使用cookie或类似追踪技术时，须以opt-in的方式获取数据主体同意且要为其提供撤销同意的渠道，另外数据主体应享有拒绝控制者对其进行自动化分析或人群画像的权利

缓存和画像

GDPR核心要求

数据主体权利

数据主体有权行使被访问权，纠正权，遗忘权，数据可携带权，限制处理权，反对权及自动化决策相关的权利。

告知和同意

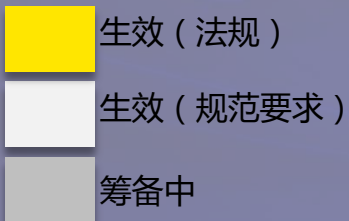
在收集和处理个人信息前应告知并获取数据主体同意。

隐私影响评估 (DPIA)

在进行数据处理之前，控制者应当对就个人数据保护所设想的处理操作方式的营销进行风险评估。

隐私保护设计 (PbD)

在产品/服务设计之初应考虑隐私数据保护需求



网络安全法

保守国家秘密法

刑法修正案 (七) (九)

个人信息保护法

侵权责任法

消费者权益保护法

反不正当竞争法

测绘法

人大常委会《关于加强网络信息保护的決定》

两高《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》

《电信和互联网用户个人信息保护规定》

《信息安全技术 公共及商用服务信息系统个人信息保护指南》

《信息安全技术 个人信息安全规范》

《关于金融机构进一步做好客户个人金融信息保护工作的通知》

《网络预约出租汽车经营服务管理暂行办法》

个人信息安全规范 发展历程

2018 (第三届) 数据安全与隐私保护大会

2009年2月

第七次 **《刑法》** 修正案中增加了侵犯公民个人信息的犯罪行为。

2009

2013年10月

个人信息被纳入 **《消费者权益保护法》** 的保护范围。

2013

2014

2016年11月

《网安法》 确立了个人信息保护、内容识别、方法和责任原则

2016

2017

2018

2019

2012年11月

MIIT 发布了第一个保护个人信息的国家标准

2014年6月

《网络侵权司法解释》 规定了披露个人信息的侵权责任

2017年12月

中国国家标准化管理委员会 发布了 **《信息安全技术——个人信息安全规范》**

个人信息安全规范 与网络安全法的映射关系

中国网络安全法

个人信息安全规范

1	第二十二条：网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意	5.3 收集个人信息时的授权同意 5.4 征得授权同意的例外 5.5 收集个人敏感信息时的明示同意 5.6 隐私政策的内容和发布
2	第四十条：网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。	规范中的所有章节
3	第四十一条：个人信息收集和使用规定	第5~8节：个人信息的收集、保存、使用、委托处理、共享、转让和公开披露
4	第四十二条：未经被收集者同意而共享信息的例外情况和发生个人信息安全事件时应立即采取补救措施。	第3节：匿名化和去标识化的定义 第7~8节：个人信息的使用、委托处理、共享、转让和公开披露 第9节：个人信息安全事件处置
5	第四十三条：个人信息主体有权删除和更正个人信息。	7.4~7.10：个人信息主体对信息的访问、更正、删除、撤回同意、注销账户、请求响应的权利。
6	第四十四条：任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。	5.1 收集个人信息的合法性要求

个人信息安全规范 关键内容

2018 (第三届) 数据安全与隐私保护大会

关键定义

- ☐ 个人信息
- ☐ 个人敏感信息
- ☐ 明示同意
- ☐ 去标识化
- ☐

用户同意类型

- ☐ 授权同意
- ☐ 明示同意

个人信息处理生命周期

- ☐ 收集
- ☐ 保存
- ☐ 使用
- ☐ 共享
- ☐ 转让
- ☐ 公开披露

7大基本原则

1. 权责一致原则
2. 目的明确原则
3. 选择同意原则
4. 最少够用原则
5. 公开透明原则
6. 确保安全原则
7. 主体参与原则

安全管理

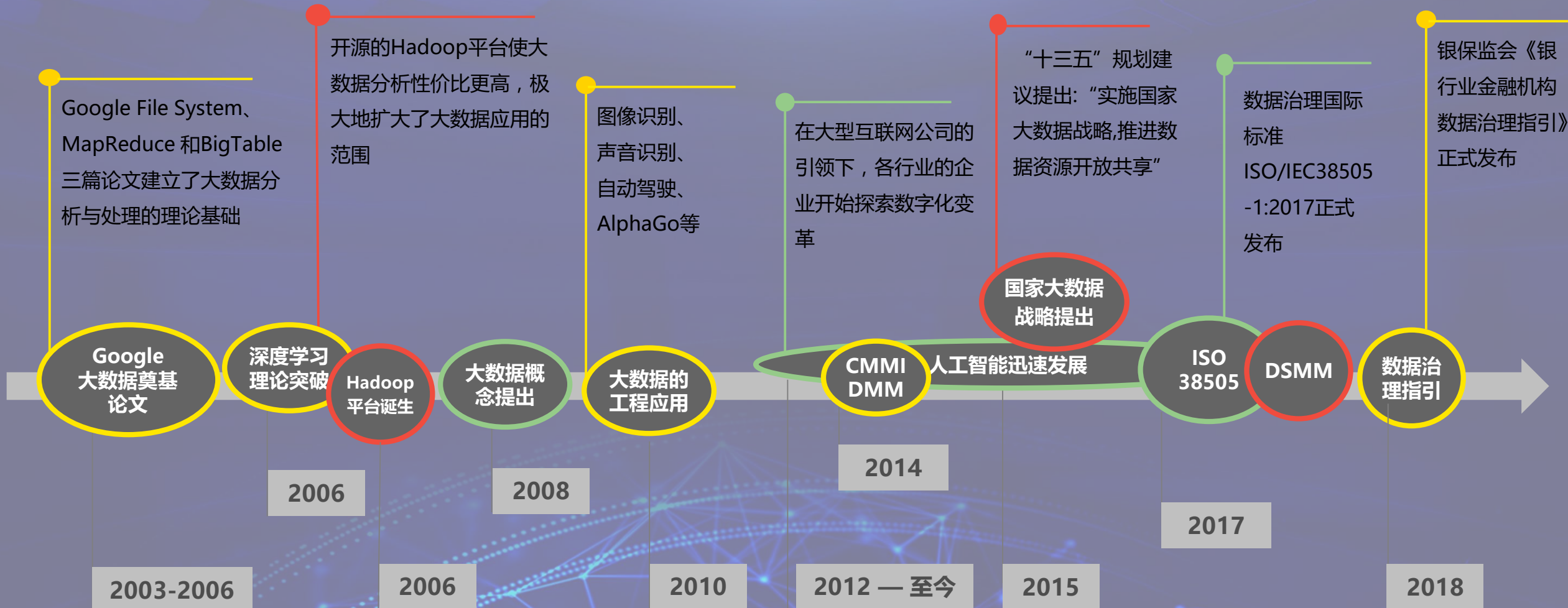
- ☐ 事件响应
- ☐ 组织
- ☐ 政策
- ☐



2018 (第三届) 数据安全与隐私保护大会

3 | 数据安全通用原则

响应大数据战略，护航数字化转型数据安全与隐私保护大会



数据安全通用原则

1. 从数据资产要素角度界定保护对象

商业秘密：根据《反不正当竞争法》，商业秘密是指不为公众所知悉，能为权利人带来经济利益、具有实用性并经权利人采取保密措施的技术信息和经营信息。

保密性 -
“经权利人采取保密措施”

“权利人有效控制着商业秘密、他人不经过不正当手段难以很快知悉该商业秘密。”

1 秘密性 - “不为公众所知悉”
公众：相对于行业内的“知情人”而言
一定范围内知情并不表示破坏了秘密性

四大要素

价值性 - 2
“能为权利人带来经济利益”

- ▶ 现实的价值和潜在的价值
- ▶ 积极信息和消极信息
- ▶ 持续使用和短暂使用
- ▶ 不具有竞争价值的信息不构成商业秘密

4
实用性 -
能够在生产经营中被实际利用
具体的、确实的、可以实施的

3

个人信息的管理范围和类型

个人信息

个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

GDPR中，个人数据是指任何指向一个已识别或可识别的数据主体的信息，该可识别的自然人能够被直接或间接地识别，



识别：从信息到个人，由信息本身的特殊性识别出特定自然人，个人信息应有助于识别出特定个人。



关联：从个人到信息，如已知特定自然人，则由该特定自然人在其活动中产生的信息（如个人位置信息、个人通话记录、个人浏览记录等）即为个人信息。

个人敏感信息

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

敏感的个人数据类似于以往数据保护指令中的定义，但仅在GDPR中提及了“遗传数据”和“生物特征数据”。

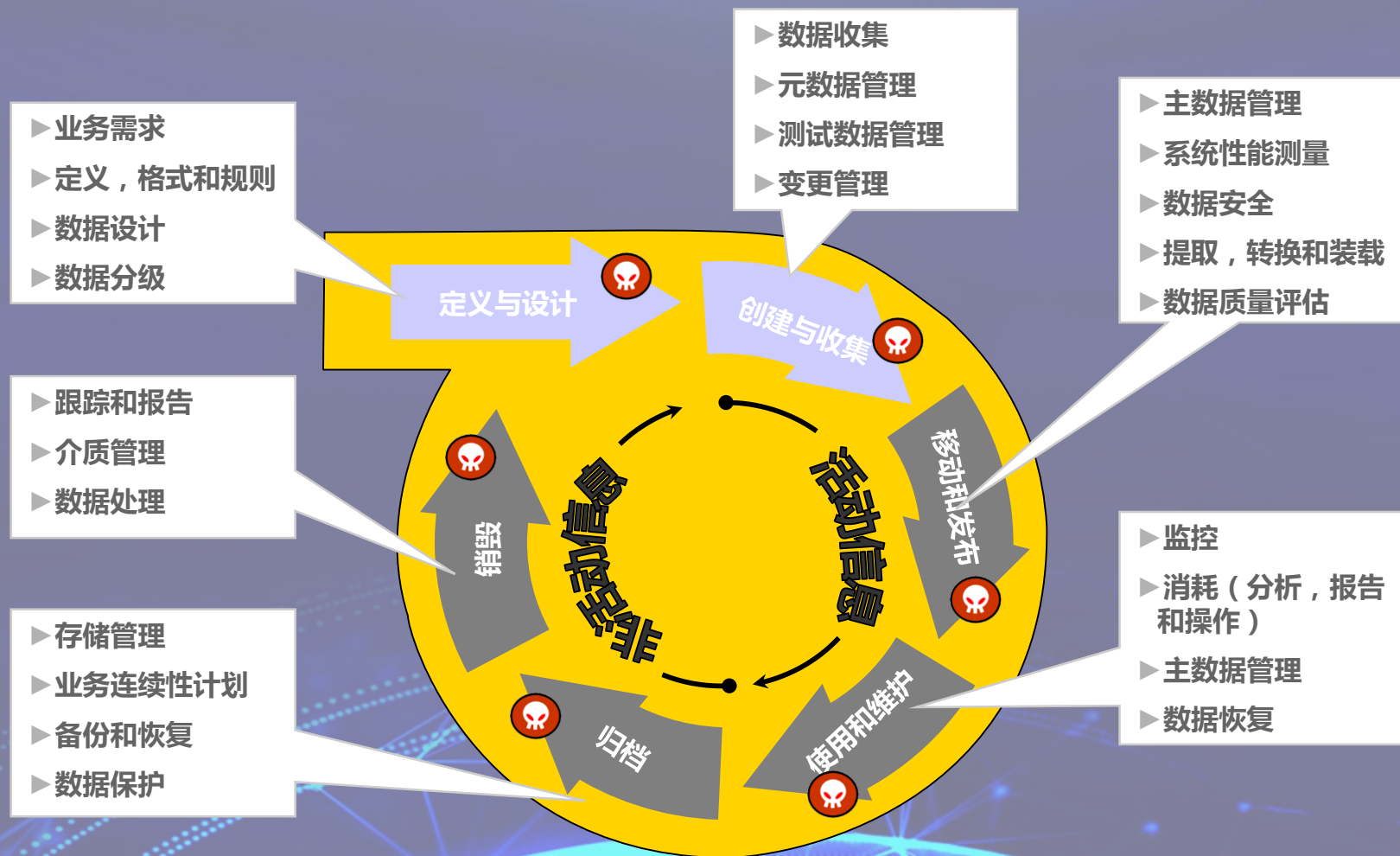
匿名化(Anonymous)数据：
与已识别或可识别的自然人无关的数据，不受GDPR的影响。

假名化(pseudonymization)数据：

特定方面与已识别或可识别的自然人分离的数据，该数据受GDPR的约束。

数据安全通用原则



2. 从数据生命周期着眼进行数据保护



在数据生命周期内, 数据及保证数据质量的需求是不断变化的

根据数据的生命周期对个人信息进行保护安全与隐私保护大会

在整个个人信息处理生命周期中包括收集、保存、使用、共享、转让、公开披露和其他活动。不同的个人信息敏感程度会产生不同等级的安全需求。

数据处理活动	 <u>个人信息</u>	 <u>个人敏感信息</u>
收集	收集个人信息时的授权 <u>同意</u>	收集个人敏感信息时的 <u>明示同意</u> 区分核心业务功能和附加功能
保存	保存时间最小化 去标识化处理	保存时间最小化 去标识化处理 采用加密等技术措施
使用	基于角色职责的访问控制	基于角色职责的访问控制 <u>根据业务流程的需求触发操作授权</u>
共享、转让	<u>告知</u> 共享、转让个人信息的目的、数据接收方的类型，并事先征得授权同意	告知涉及的个人敏感信息的类型、数据接收方的身份和数据安全能力，并事先征得 <u>明示同意</u>
公开披露	告知公开披露个人信息的目的、类型，并事先征得个人信息主体明示同意	告知公开披露个人敏感信息的目的、类型、 <u>涉及内容</u> ，并事先征得个人信息主体明示同意

数据安全通用原则

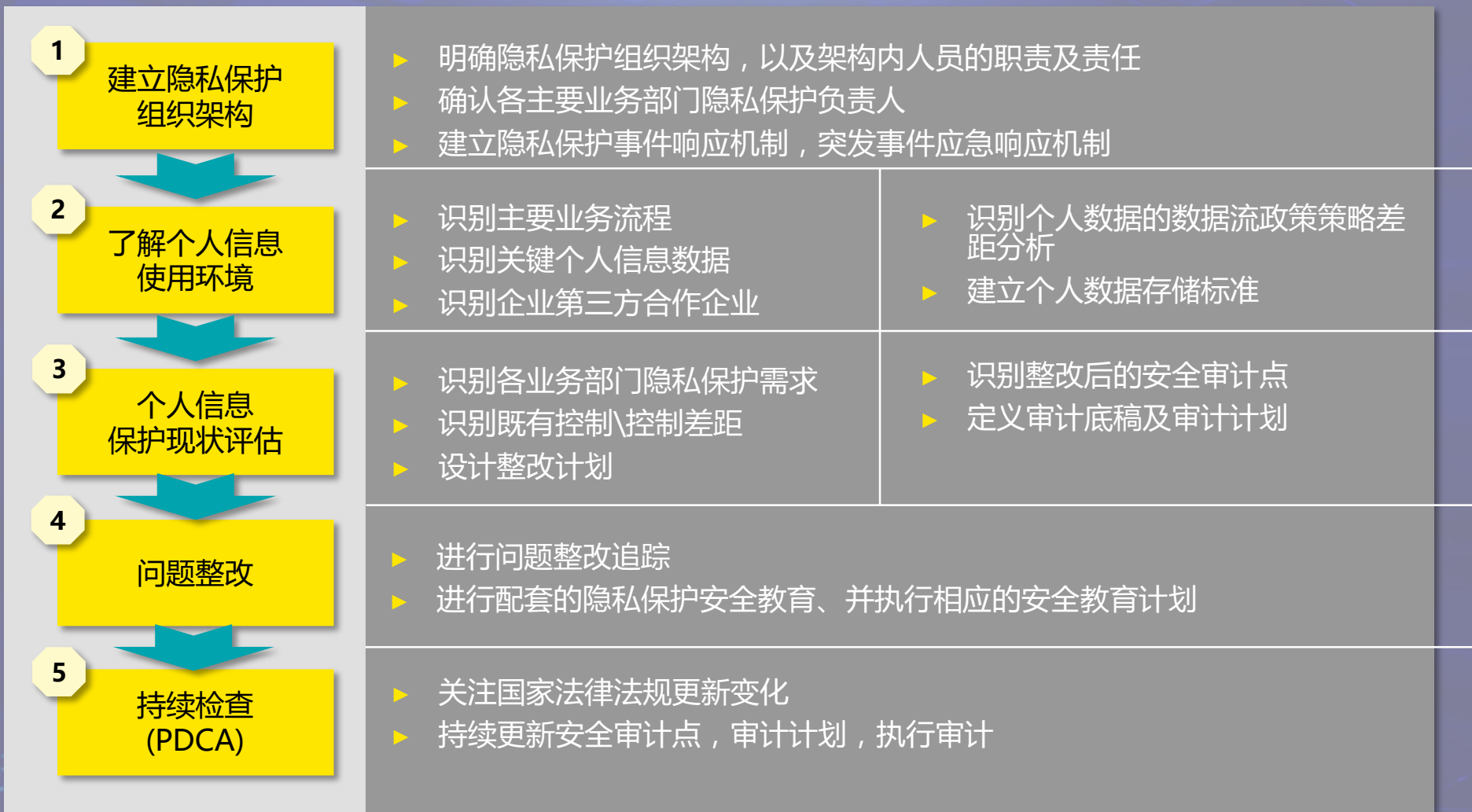
3. 建立自上而下的数据保护体系

我们从“公司治理层面”，“流程与数据层面”，“IT支持层面”三个不同的角度评估数据保护控制，以确保建立自上而下的全面数据保护体系。

公司治理层面	数据治理	风险评估					
	制度与流程	意识培训					
	数据分类与分级	技术管理					
	合规性	安全事件管理					
流程与数据层面	数据产生	业务场景分析	关键数据识别	数据流转识别	安全策略设计	快速见效建议	
	数据获取						
	数据传输						
	数据使用						
	数据存储						
	数据销毁						
IT支持层面	应用运行支持	安全需求调研	安全控制识别	系统分类分级	系统基线要求	系统基线配置	系统基线检查
	主机运行支持						
	网络运行支持						
	数据库运行支持						
	物理设备运行支持						

- ▶ 为使数据安全防护方案有效，应建立“自顶而下”的方法，以全盘地解决数据泄漏问题
- ▶ 应建立治理机制，定义角色及其职责，以有效地管理和维护此方案
- ▶ 应根据全面的数据安全风险评估所发现的差距，加强所有支持性IT流程
- ▶ 应采用涵盖全部三个领域（人员、流程、技术）的技术解决方案，以有效的监控、防止、和响应所有潜在的数据泄漏

建立个人信息保护体系



数据安全通用原则

4. 趋同的保护原则



最小权限原则

只授予处理者能够实现处理目的的**最小权限**和**最少信息**，达到处理目的后，应及时在限定时间内删除相关信息



安全保障原则

采取适当的并与数据资产重要性相适应的**管理措施和技术手段**，确保数据安全，防止未经授权的检索、披露及丢失、泄露、损毁和篡改。



质量一致原则

保证处理过程中的数据资产**保密、完整、可用**，并确保数据质量，检验数据处于**有效和更新**状态。



可审计性原则

明确各项数据处理活动的责任，采取相应的措施落实**监控、记录和审计**，并对数据处理过程进行记录以便于追溯。



目的明确原则

处理个人信息具有**特定、明确、合理的目的**，不扩大使用范围，不在个人信息主体不知情的情况下改变处理个人信息的目的。



个人同意原则

处理个人信息需要征得个人信息主体的同意。



公开告知原则

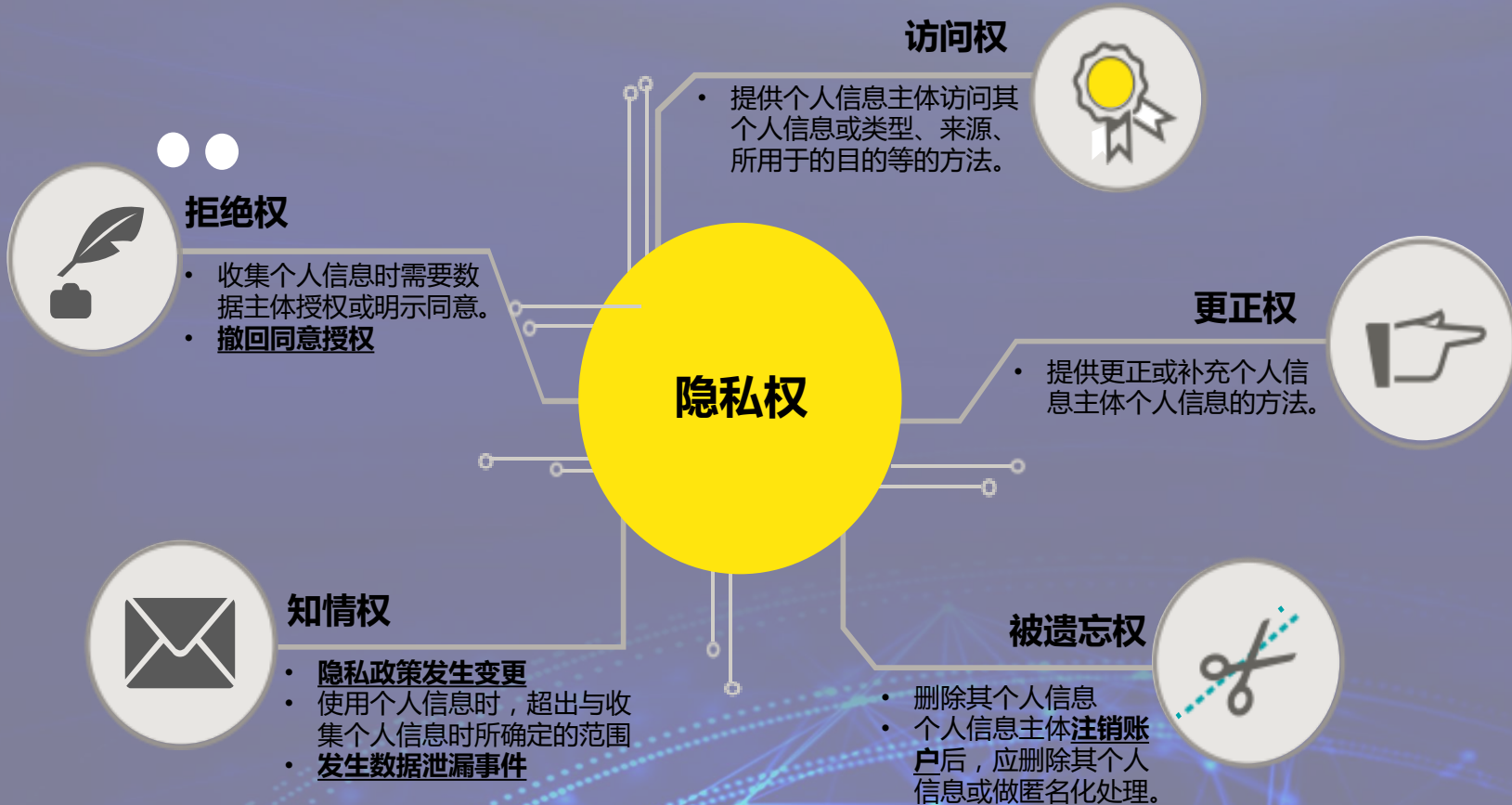
对个人信息主体要**尽到告知、说明和警示的义务**。以明确、易懂和适宜的方式如实向个人信息主体告知处理个人信息的目的、个人信息的收集和使用范围、个人信息保护措施等信息。



诚信履行原则

按照收集时的承诺，或基于法定事由处理个人信息，在达到既定目的后不再继续处理个人信息。

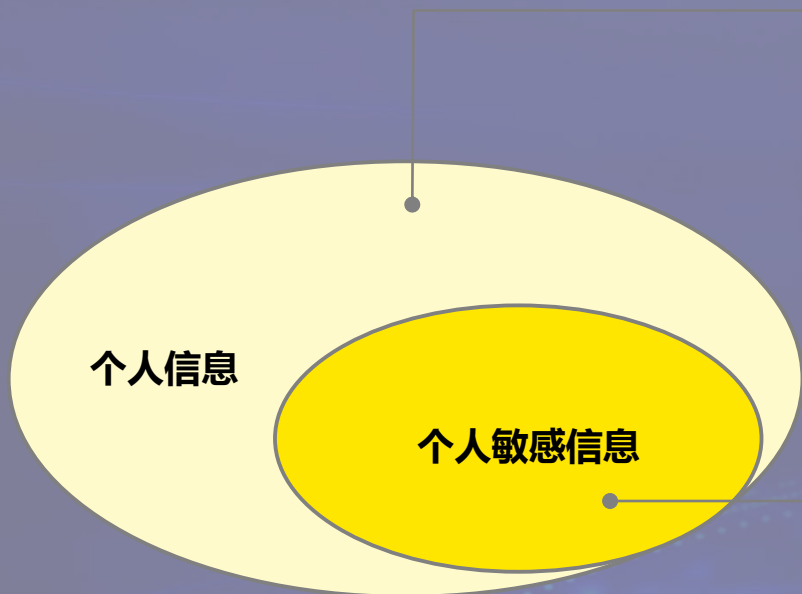
隐私保护的附加原则： 1. 数据主体的隐私权利



GDPR的数据主体权利

1. 访问权 (第12/15条)
2. 纠正权 (第12/16/19条)
3. 可移植权 (第20条)
4. 删除权 (被遗忘权) (第17条)
5. 数据加工限制 (第18条)
6. 反对加工处理的权利 (第22条)
7. 知情权 (第12/13/14条)

隐私保护的附加原则： 2. 明示同意是个人信息保护的基线



收集个人信息时的授权同意

- 应向个人信息主体**明确告知**所提供产品或服务不同业务功能分别收集的个人信息类型，
- 收集、使用个人信息的规则

间接获取个人信息时：

- 要求个人信息提供方说明个人信息来源，并对其个人信息来源的合法性进行确认
- 应了解个人信息提供方已获得的个人信息处理的授权同意范围
- 如开展业务需进行的个人信息处理活动超出该授权同意范围，应在获取个人信息后的合理期限内或处理个人信息前，**征得个人信息主体的明示同意**。

收集个人敏感信息时的**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

区分核心和附加业务功能

- **核心业务功能：** **明确告知**拒绝提供或拒绝同意将带来的影响。
- **附加功能：**应向个人信息主体**逐一**说明个人敏感信息为完成何种附加功能所必需，并允许个人信息主体逐项选择是否提供或同意自动采集个人敏感信息。当个人信息主体拒绝时，可不提供相应的附加功能，但**不应以此为理由停止提供核心业务功能**，并应保障相应的服务质量。

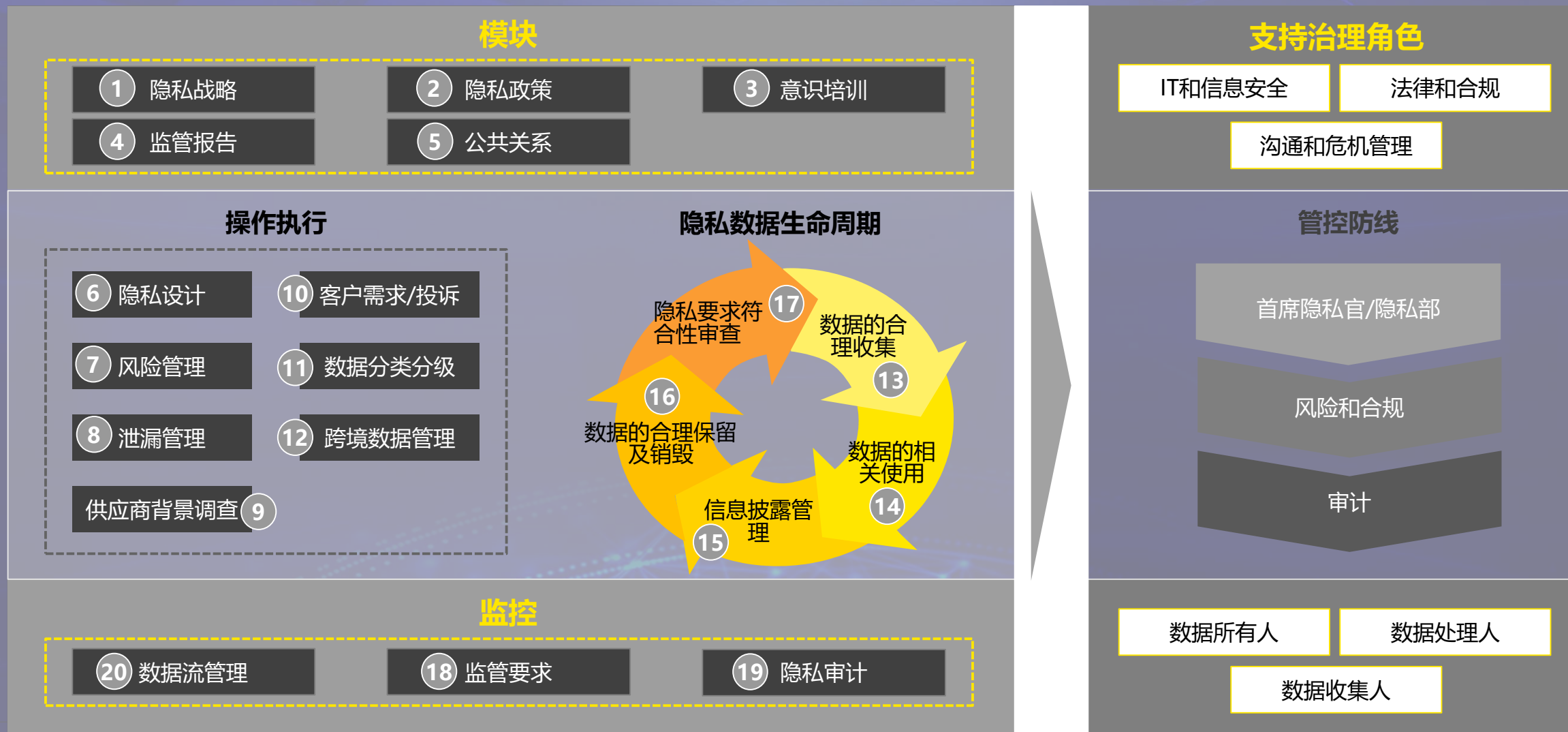


2018 (第三届) 数据安全与隐私保护大会

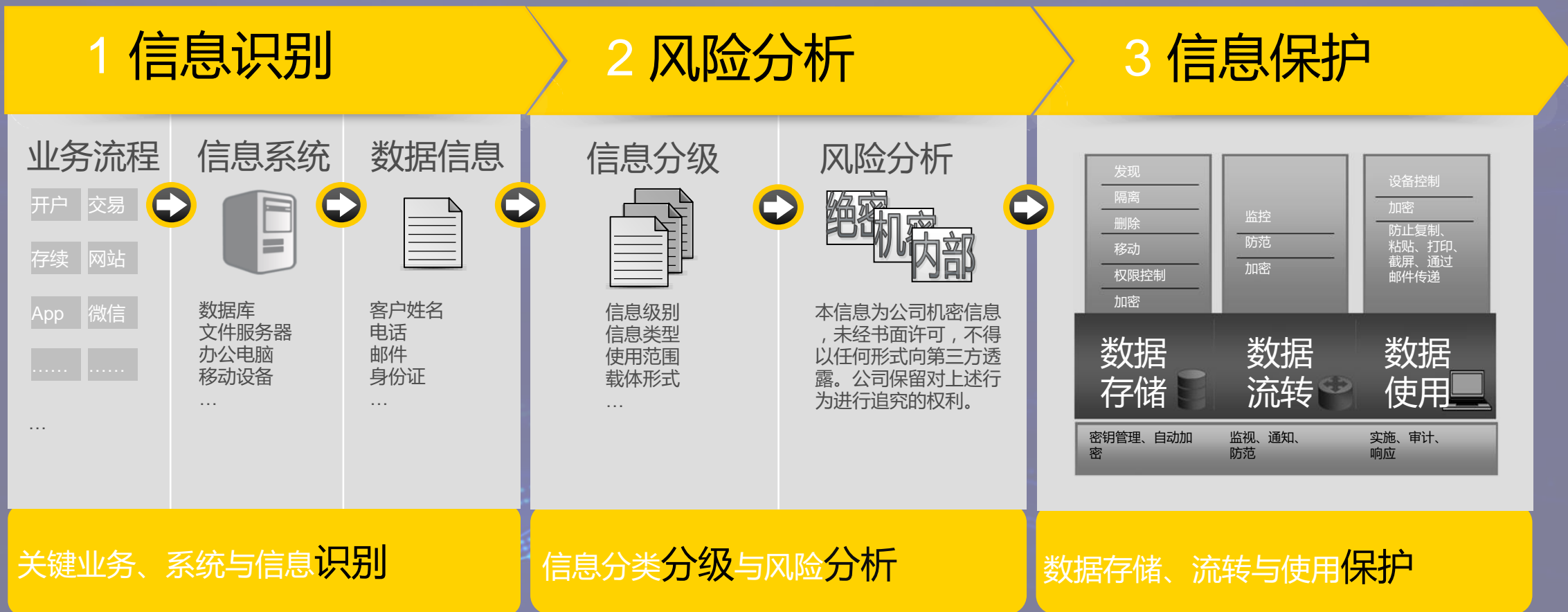
4 | 评估方法与实践

安永数据隐私管理模型

2018 (第三届) 数据安全与隐私保护大会



我们遵循“数据识别——风险分析——数据保护”的思路，对企业的各类关键业务流程中的数据进行保护。



隐私保护领域风险分析之 隐私影响评估的必要性

根据<ISO/IEC 29134: 2017 信息安全技术-隐私影响评估指南>及<英国信息专员办公室PIA执行守则>中的定义：

隐私影响评估 (Privacy Impact Assessment, 简称 PIA) 是一个协助企业去**识别和减少**项目中存在**隐私风险**的过程。对以下活动需要进行隐私影响评估：

1. 系统性及大规模的自动化数据分析时
2. 处理大规模敏感数据时
3. 大规模地监控公共无障碍区域时

根据欧盟WP248 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk"

具有高风险的数据处理场景

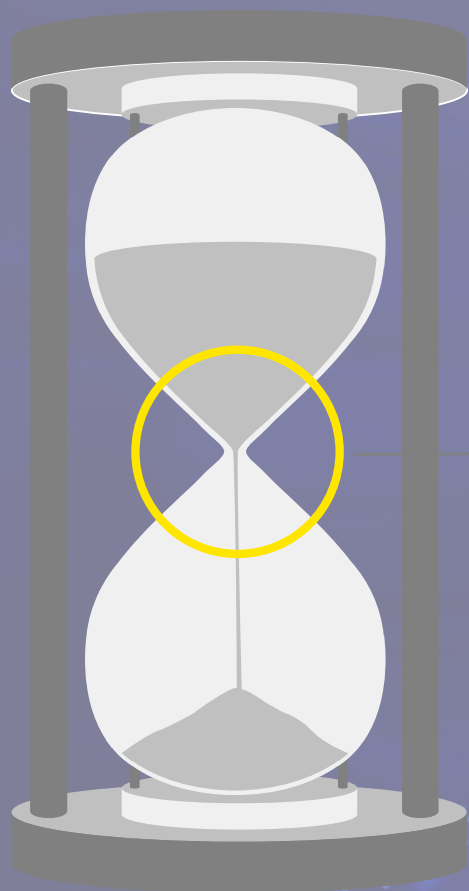
- 一、数据评估或评价(包含数据分析及预测)
- 二、支持自动化决策或具有相关影响的活动
- 三、系统监测
- 四、敏感数据处理
- 五、大规模的数据处理
- 六、经比对或合并的数据组
- 七、与弱势群体相关的隐私数据应用
- 八、企业导入创新应用解决方案
- 九、数据跨境
- 十、避免数据当事人执行其权力或服务及合约

隐私影响评估适用于广泛的项目类型



隐私保护领域风险分析之 隐私影响评估框架

2018 (第三届)
数据安全与隐私保护大会



- ✓ 影响个人自主决定权
- ✓ 引发差别待遇
- ✓ 个人财产受损
- ✓ 名誉受损或精神压力

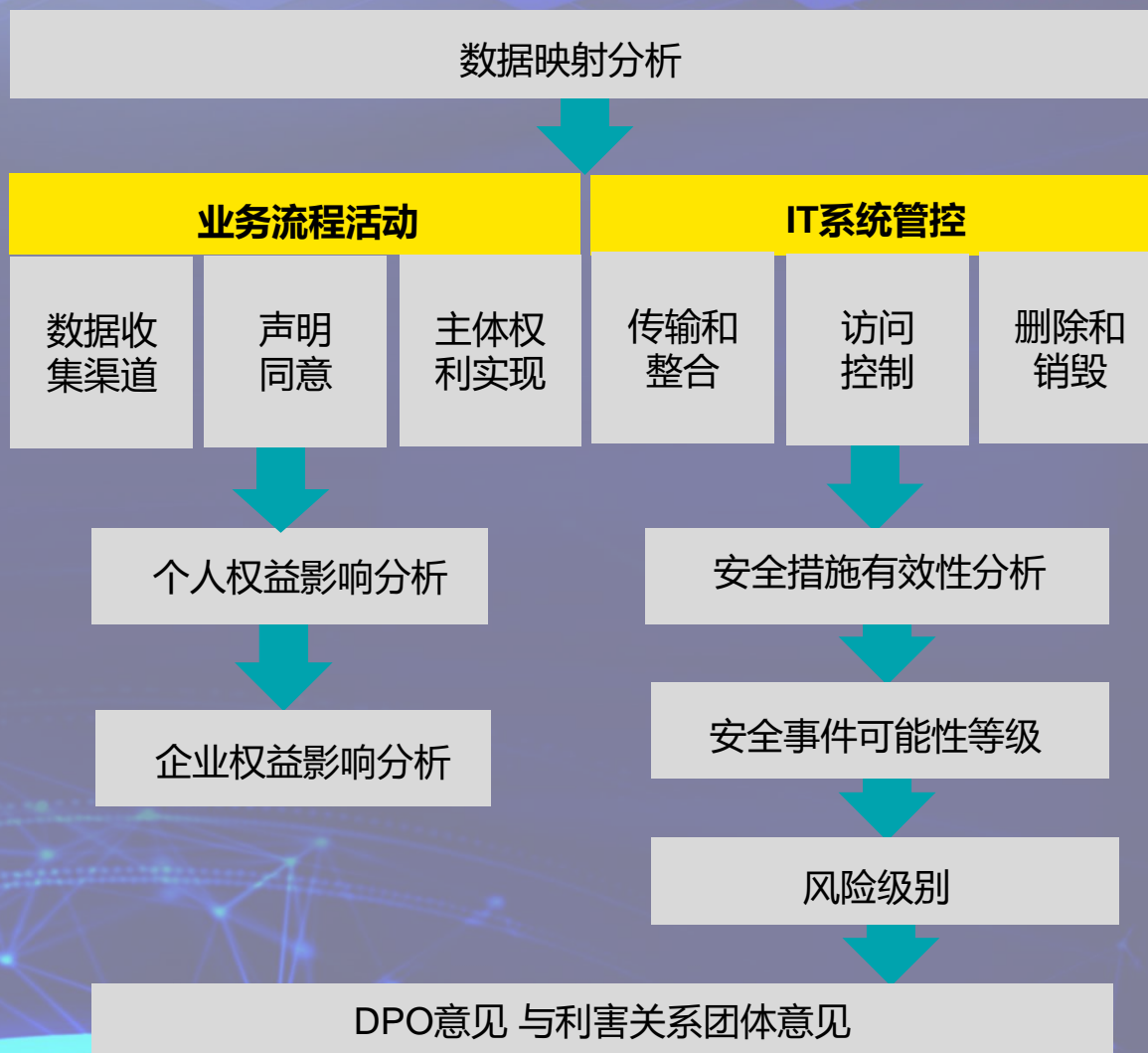
个人的关心



企业的保护诉求



- ✓ 违规成本
- ✓ 直接的业务损失
- ✓ 名誉损失
- ✓ 企业管理效能层面的损失



数据安全保护成熟度模型

管理域	初步的	发展中	已经成形	高级的	领先的	
数据治理	企业高层未被告知数据保护的风险。对于数据保护，没有管理层级别的监管措施。	●	●	●	●	存在着业务部门与IT部门共同承担责任的且成体系的数据保护规划，数据保护规划与企业战略目标相结合。
风险评估	对于评估来自数据的风险，没有正规的流程存在。	●	●	●	●	已经了解不同数据类型和终端相关联的风险。安全控制根据风险进行了优化。进行持续的数据泄漏风险评估。
合规性	对于数据保护的合规性需求仍然未知。	●	●	●	●	有一个适用的法律法规清单。对数据泄漏发生时需要的责任和惩罚已经知晓，并且有相应的应对计划。
制度与流程	关于数据保护的策略不存在或者不一致。	●	●	●	●	业务部门参与到制定/实施数据保护制度的过程中。数据保护制度公开且可以被相关部门访问到，会根据经常变化的业务需求作相应调整。
意识培训	数据保护没有在新员工培训中提到。员工与合作伙伴没有意识到他们的职责。	●	●	●	●	针对性的宣传涵盖了所有的用户（包括雇员，承包商，临时员工及顾问）。培训的完成情况会被追踪及监测。
数据分类与分级	数据级别与分类未定义	●	●	●	●	进行定期的评审以保证每个数据类型都有相应合适的控制措施。
安全事件管理	没有数据泄漏的定义或如何响应安全事件的文档。	●	●	●	●	数据泄漏被作为安全事件响应计划体系的一部分来处理。该计划包含了检测、告知、纠正和经验总结。
技术管理	没有用于监控或者检测数据丢失的技术方案存在。	●	●	●	●	技术解决方案已被部署，或者利用现有方案用于数据发现和策略执行。

风险 价值
成本

- ▶ 专注于相关的风险
- ▶ 与业务目标相对应
- ▶ 最小化的业务影响

风险 价值
成本

- ▶ 更低的成本
- ▶ 更高的效率
- ▶ 更低复杂度

改进的
数据保护

风险 价值
成本

- ▶ 更广的风险覆盖
- ▶ 改进的合作配合
- ▶ 积极主动的方法



2018（第三届） 数据安全与隐私保护大会

谢谢！