Privacy by Design

理论架构与技术实战

讲师简介

专注于数据安全与隐私保护领域

演 讲 者： 胡恺健

江湖称号： 魔　风

从业经验： 现任广州诸子云常务理事、广东省等级保护专家、CSA云安全联盟大中华区研究专家、CSA隐私与个人信息法律组成员、DPOHUB会员。专注于全球金融科技的数据安全与隐私保护工作，在数字政府、金融科技、互联网电商的网络安全规划设计、信息安全治理与管理、数据安全、隐私保护、安全运营等领域具有丰富的实践经验。

安全认证： CISSP \ CISA \ CIPM \ CIPT \ CDPO \ CISP-DSG \ EXIN-DPO \ CDPSE \ C-CCSK \ ISO 27001 LA \ISO 27701 IA \ CCNA \ 网络规划设计师等安全与数据隐私认证

文章发布： 《唯品会信息安全培训体系》、《信息安全宣传动画制作的艺术》、《探索隐私保护数字化解决方案》、《企业云原生数据防泄漏（DLP）架构与运营实践指南》、《关于隐私治理在企业落地的思考》、《诸子项目-Privacy By Design最佳实践调研分析报告》

欢迎实名加微信交流

目录

Catalogue

- 1. 隐私保护的底层逻辑
- 2. Privacy by Design理论架构
- 3. Privacy by Design技术实战
- 4. Q&A

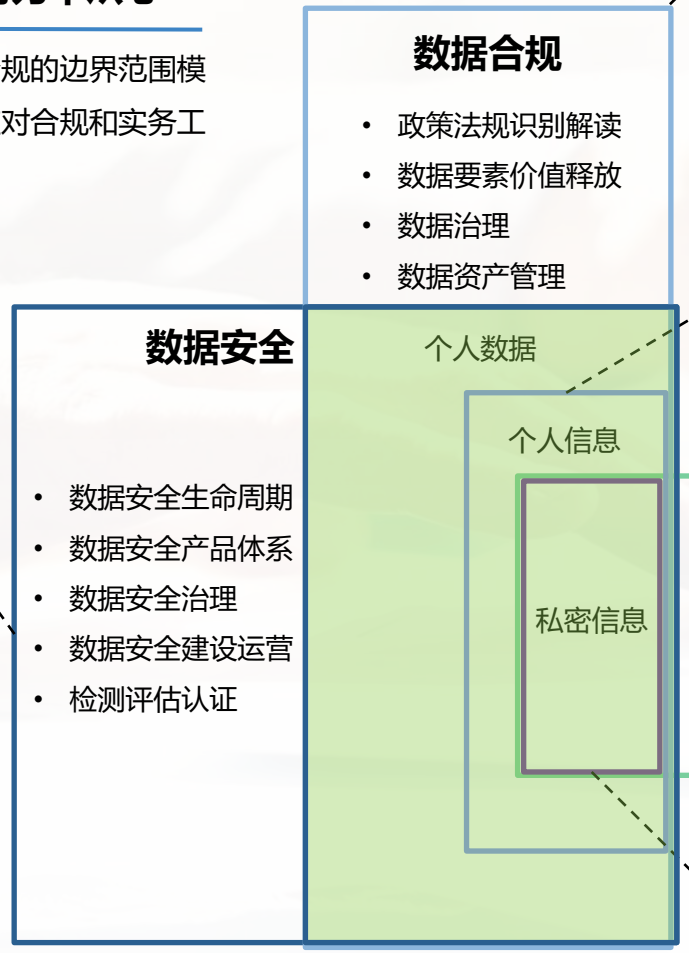
01 隐私保护的底层逻辑

我们在讨论隐私保护的时候，到底在研究什么问题？从隐私边界、定义和违规的角度来推演隐私保护底层逻辑！

隐私保护的边界与范围

痛点：隐私边界范围模糊，企业应对力不从心

隐私保护、个人信息保护、数据安全和数据合规的边界范围模糊，企业的组织、制度、技术、运营领域在应对合规和实务工作时力不从心。



- 中国数据基础制度和数据要素价值（产权、流通、交易、使用、分配、治理、安全）
- 数据资产管理（数据模型、标准、质量、主数据、元数据、数据安全、资产流通、价值评估、资产运营）
- 数据跨境合规评估与备案
- 个人信息安全影响评估
- 通用及行业的数据合规政策、法规和标准

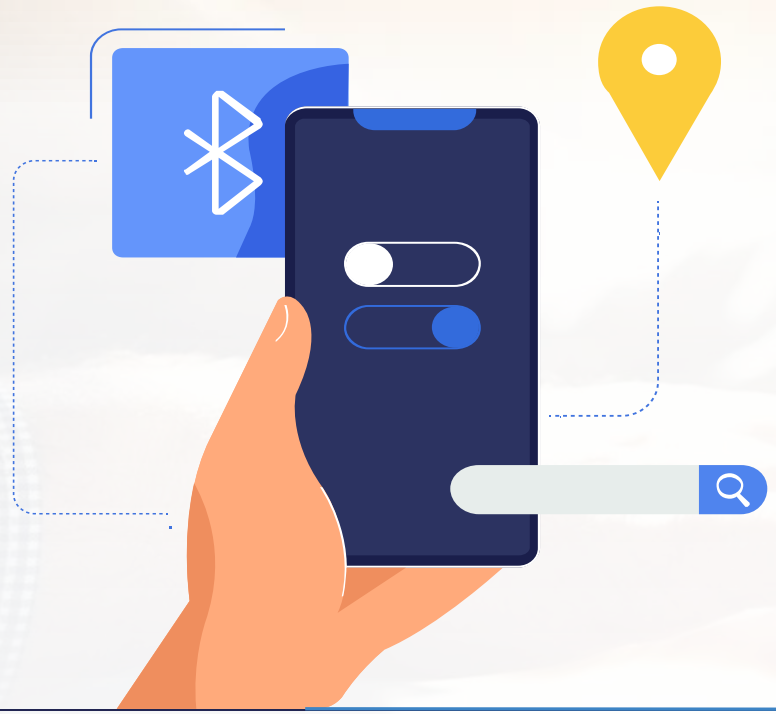
- 国内App个人信息保护执法检查范畴

- 中国民法典的隐私权保护范畴

- 数据安全能力成熟度评估DSMM
- 数据安全管理认证

- 私密信息的两个条件：“能够识别自然人”和“主体不愿为他人知晓”
- 主体的合理隐私期待
- 普通人的一般合理认知

隐私保护的多维定义



典型的隐私保护释义

中华人民共和国民法典

隐私是自然人的私人生活安宁和不愿为他人知晓的**私密空间**、**私密活动**、**私密信息**。

Alan Westin的隐私四种状态--合理隐私期望

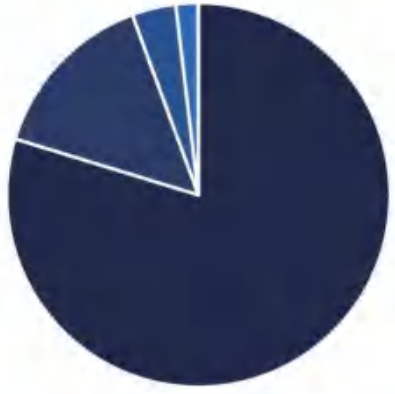
Alan Westin对于隐私表述为四种不同的状态：第一是“**独处（Solitude）**”，代表个体独立存在，脱离群体，不受他人观察的状态；第二是“**私密（Intimacy）**”，指个体是群体的一部分，与群体成员共同协商信任、信息共享和保密的规则；第三是“**匿名（Anonymity）**”，指当个体在公共场合时，他们仍然保持着没有身份识别和监视的自由；第四是“**保留（Reserve）**”，指当个体处于一个很大的群体中时，他们仍然保持着停止交流或脱离他人的能力，以创造一个心理障碍，防止不必要的入侵。

	Information Collection	*Information Processing*	*Information Dissemination*	*Invasion*
Subjective Harms	**Psychological** (Embarrassment, anxiety, suicide[8])			
	Behavioral (Changed behavior, reclusion)			
Objective Harms	**Lost Opportunity** (Employment, insurance, housing, education)			
	Economic Loss (Inconvenience, financial costs)			
	Lost Liberty[9] (Bodily injury, incarceration, death)			
	Social Detriment (Lost of trust, shunning, ostracism, banishment)			

Ryan Calo的隐私危害维度理论

Ryan Calo的隐私危害维度理论，将隐私危害分为**客观危害**与**主观危害**。隐私客观危害是指个人隐私受到侵犯且已知存在直接伤害的情况下，**可以测量和观察到的伤害**。隐私主观危害的存在无法观察或测量，但当个人主观认为或感知到已经被隐私危害，这种危害也会对个人造成心理上的**负担**、**阴影**和**恐慌**等精神压力，然后会采取与客观危害的处理步骤来保护自己。对于网络安全专家和隐私专家来说，挑战在于认识到 “对危害心理感知”和“经历过真实危害”同样都可能对个人隐私产生显著的负面影响。

隐私违规--GDPR Vs 中国 的执法区别



- 缺乏保障信息安全的技术和组织措施
- 数据处理的法律依据不足
- 违反数据处理基本原则
- 数据主体权利没有充分实现
- DPO任命违反法律要求
- 与监督机构的合作不足
- 未充分履行信息义务
- 未签署数据处理协议
- 未充分履行数据泄露通知义务

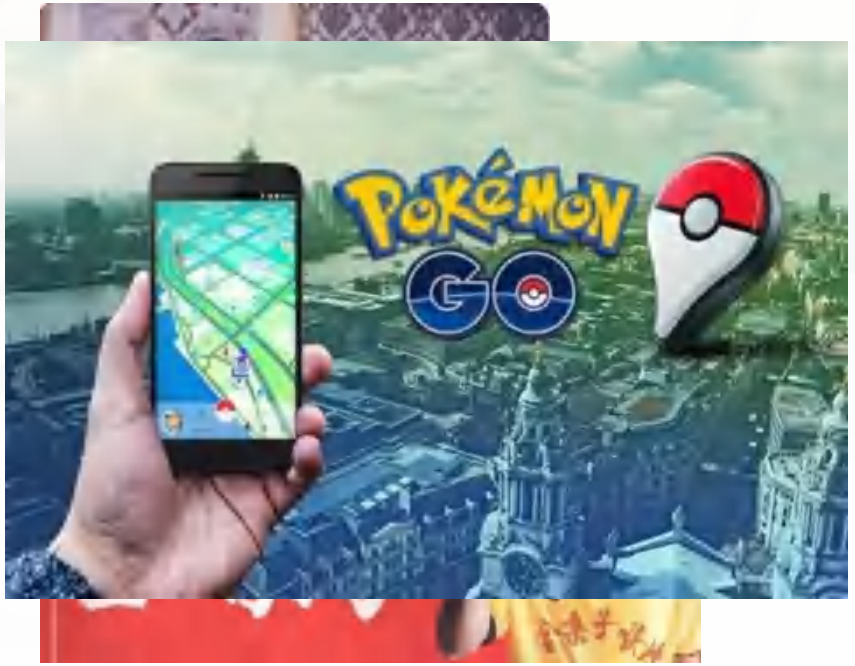
违反	罚款总额
缺乏保障信息安全的技术和组织措施	€332,567,289（49次）
数据处理的法律依据不足	€61,202,963（68次）
违反数据处理基本原则	€15,495,940（29次）
数据主体权利没有充分实现	€7,756,539（13次）
DPO任命违反法律要求	€60,000（2次）
与监督机构的合作不足	€59,911（10次）
未充分履行信息义务	€31,300（10次）
未签署数据处理协议	€9,380（1次）
未充分履行数据泄露通知义务	€7,400（1次）

*数据来源：《GDPR执法案例全景白皮书》

*数据来源：《个人信息安全年度报告（ 2022）》

隐私违规--信息生命周期各阶段的威胁与危害

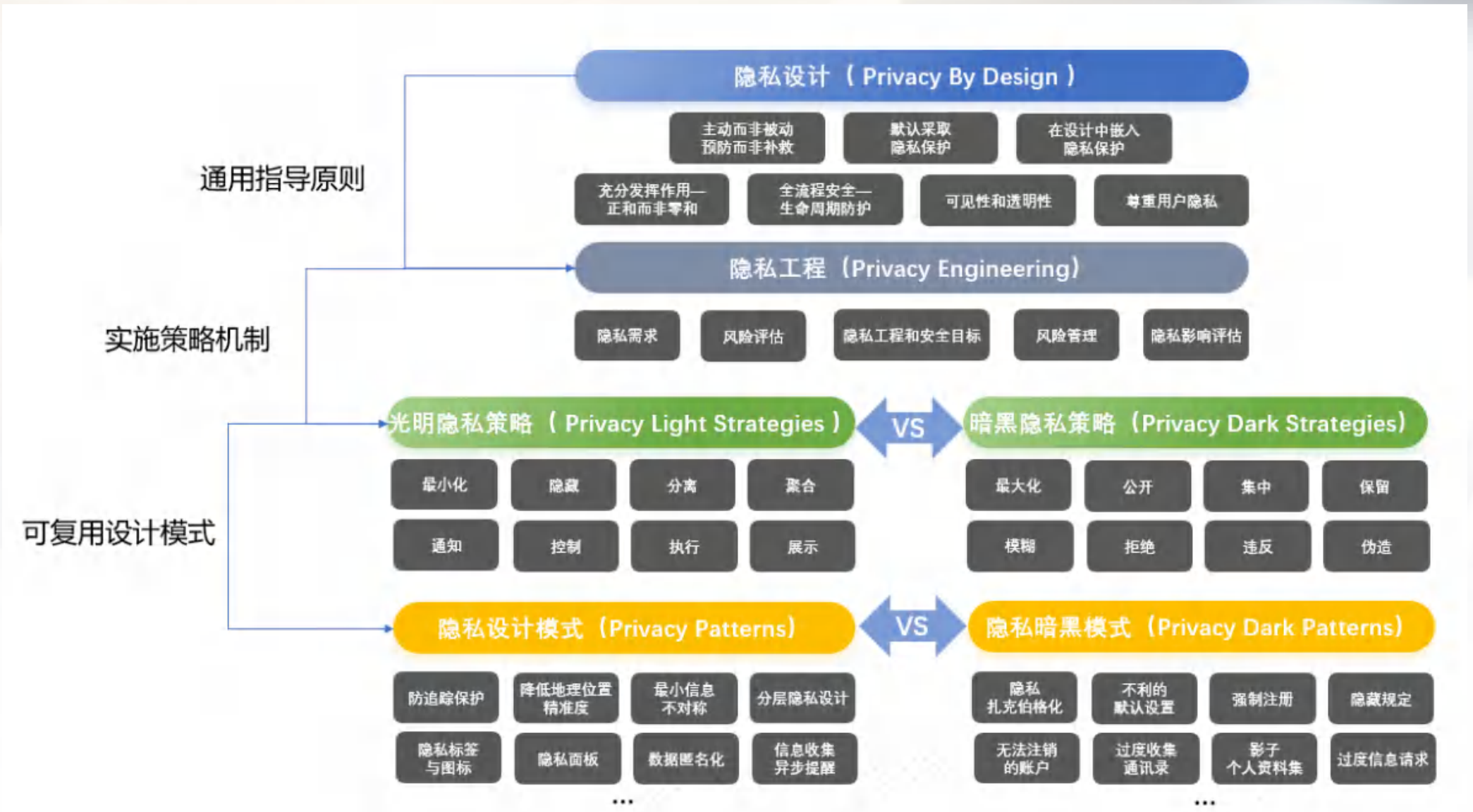
信息收集	信息处理	信息传播	隐私侵犯
监控（Surveillance）	信息聚合（Aggregation）	违反保密性 (Breach Of Confidentiality)	打扰（Intrusion）
审问（Interrogation）	不安全性（Insecurity）	披露（Disclosure）	决策干扰 (Decisioinal Interference)
	恶意识别（Identification）	暴露（Exposure）	
	二次使用（Secondary Use）	访问范围蔓延 (Increased Accessibility)	
	排除（Exclusion）	敲诈勒索（Blackmail）	
		挪用（Appropriation）	
		曲解（Distortion）	



02 Privacy by Design理论架构

重新构建PbD的框架，形成有层次逻辑的理论架构

Privacy by Design理论架构介绍



再谈Privacy by Design历史和7项基本原则

- **历史**：加拿大安大略省的Ann Cavoukian教授，她在20世纪90年代首先提出了Privacy by Design的7项基本原则，这些隐私设计原则是隐私保护系统设计的一个重要里程碑；
- **应用**：PbD的7项基本原则也在GDPR的Article 25 作为数据保护的重要指导原则明确列出，作为全球最严格的数据合规法律中的重要条款；
- **缺点**：PbD的7项基本原则的缺点是太过抽象，难以落地。

隐私工程--连接理论与实践的桥梁

隐私工程

NISTIR 8062的定义是： “隐私工程是指系统工程的一门专业学科，专注于在系统处理PII时避免给个人带来不可接受的隐私侵犯后果。”

隐私原则

抽象的概念

Privacy by Design提供了抽象的理论原则，用于指导系统工程建设过程中隐私保护的考虑要素。

翻译

系统要求

可实现的隐私需求

将隐私保护的需求整合到**软件开发生命周期**以及**组织和技术管理流程**的工程实践，是**以结果为导向的过程。**同时，为了使整个隐私工程的结果可信，与隐私期望相同，并应提供充分的系统实现证据支持。

隐私工程--三个目标

确保隐私实现结果与预期一致的北极星

与安全工程的CIA，保密性、完整性和可用性三目标类似，隐私工程也有自己的目标。根据NISTIR 8062《联邦系统中的隐私工程和风险管理》，目标是**可预测性**、**可管理性**和**不可关联性**。

可预测性（或透明性）

可预测性的目的是让所有利益相关者对一个系统进行可靠的假设，特别是其数据和对该数据的处理。充分详细告知用户处理方式建立信任，提供充足证据满足审计和可问责性，持续改进，降低风险的正向循环。

可管理性（可干预性）

提供对个人信息的细粒度控制，确保个人信息主体、控制者、处理者等相关方能够适当干预信息系统的个人信息处理过程。反过来说，如果没有隐私的可管理性，我们就不能确信数据控制者已经做好了个人信息识别、数据准确性、数据变更、数据删除和数据权利响应等管理活动。

不可关联性

采取措施对个人信息去标识或匿名化处理，减少个人信息链接到个人信息主体引起的安全风险。

多角度剖析隐私工程活动内容--NISTIR 8062

隐私需求

- 关注合规要求、业务实际隐私需求，定义系统保护能力，并且提供隐私需求已被满足的证据

风险模型

- 如果以传统的风险评估理论去评估隐私领域的风险，可能会抓不住重点。例如安全中的威胁和脆弱性，在隐私领域不好表达。**需要扩充隐私类的风险类型。**

隐私影响评估

- 对拟研发和已存在系统、技术活项目中存在的现实或潜在的对个人隐私的影响进行评估。包括数据泄露途径、隐私权利影响（限制自主决定权、差别性待遇、名誉受损、精神压力、财产受损），并推荐实践方法减缓隐私侵犯。

隐私工程与安全目标

- 追求信息安全与隐私的相互融合和支持（ISO 27001+27701）。
- 落实隐私工程的三个目标，通过匹配系统能力要求，确保系统满足隐私工程目标和安全CIA目标，最终达成安全与隐私目标，并解决相应风险。

风险管理框架

- 重在选择控制和技术，一般可参照SP 800-37信息系统和组织的风险管理框架进行实施

多角度剖析隐私工程活动内容--NISTIR 8062

隐私需求

- 关注合规要求、业务实际隐私需求，定义系统保护能力，并且提供隐私需求已被满足的证据

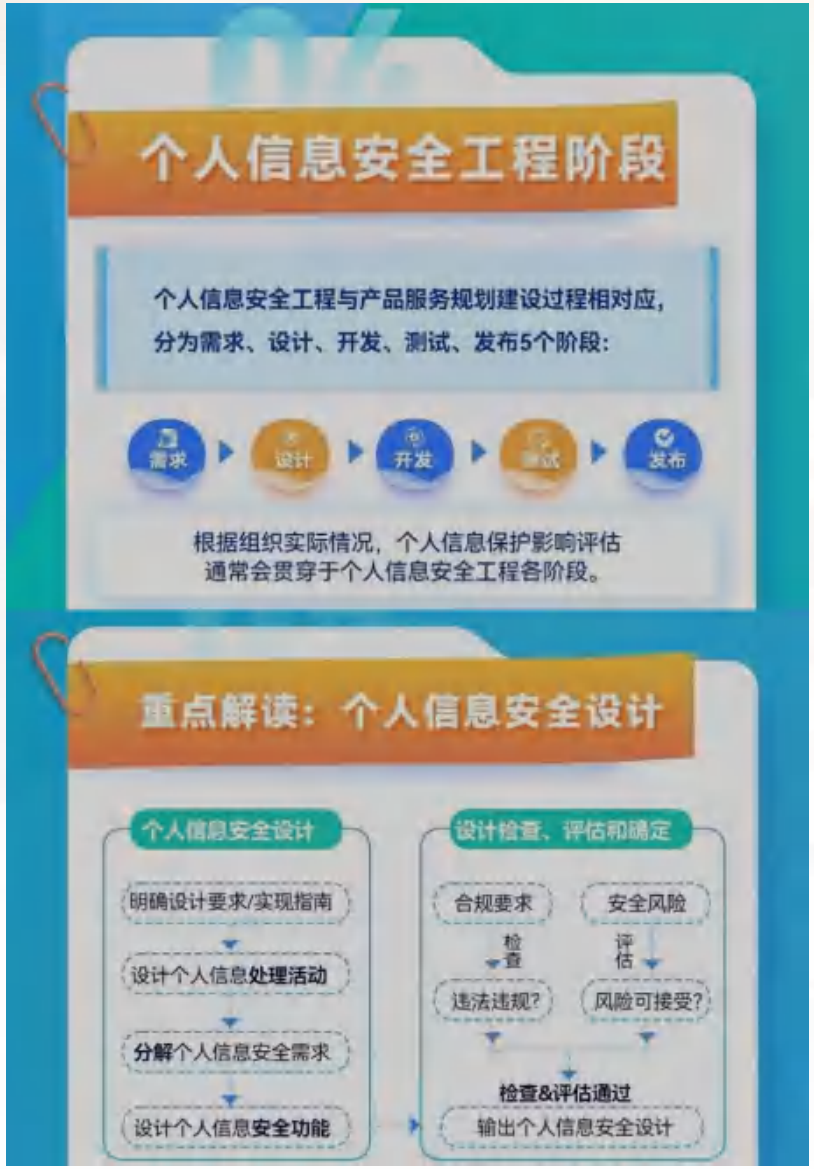
隐私影响评估

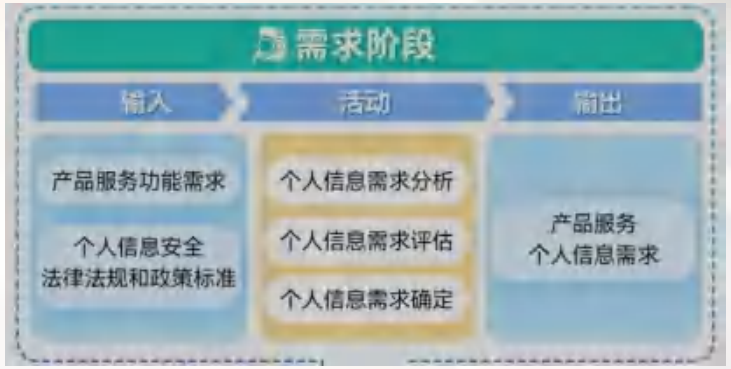
- 对拟研发和已存在系统、技术活项目中存在的现实或潜在的对个人隐私的影响进行评估。包括数据泄露途径、隐私权利影响（限制自主决定权、差别性待遇、名誉受损、精神压力、财产受损），并推荐实践方法减缓隐私侵犯。

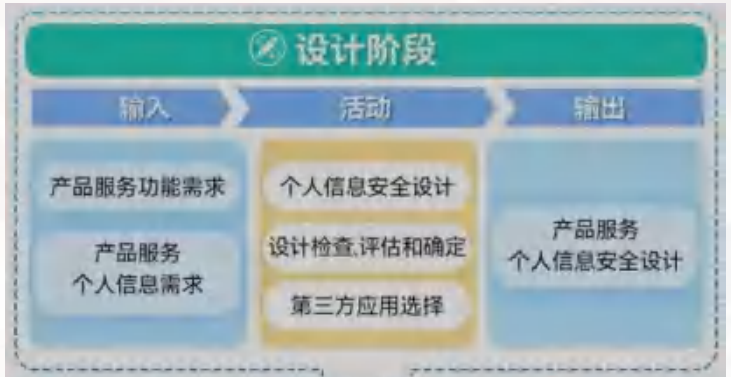
风险管理框架

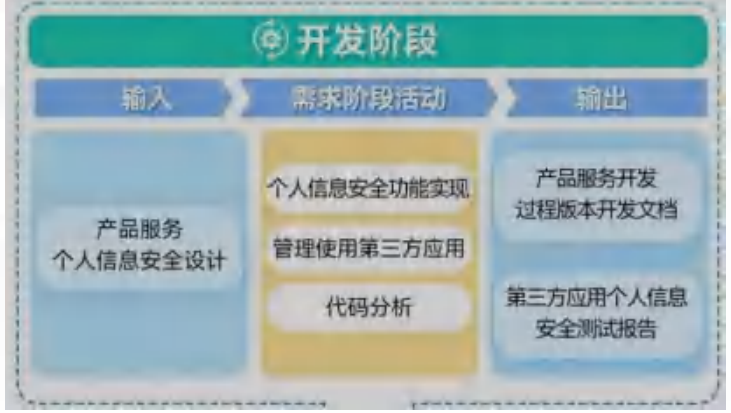
- 重在选择控制和技术，一般可参照SP 800-37信息系统和组织的风险管理框架进行实施

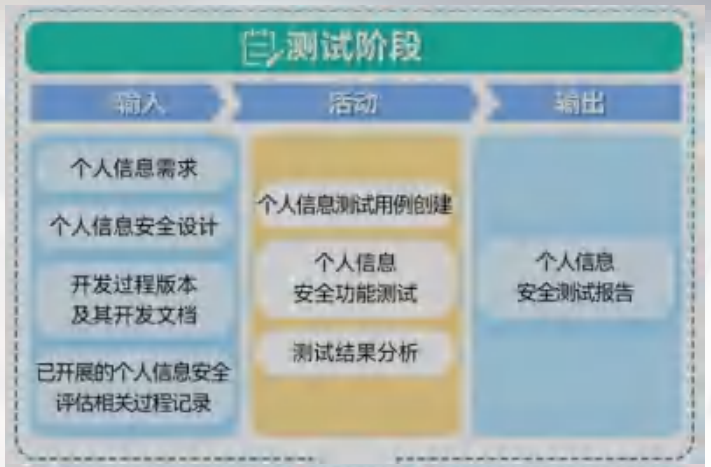
多角度剖析隐私工程活动内容--个人信息安全工程指南（隐私嵌入SDL）

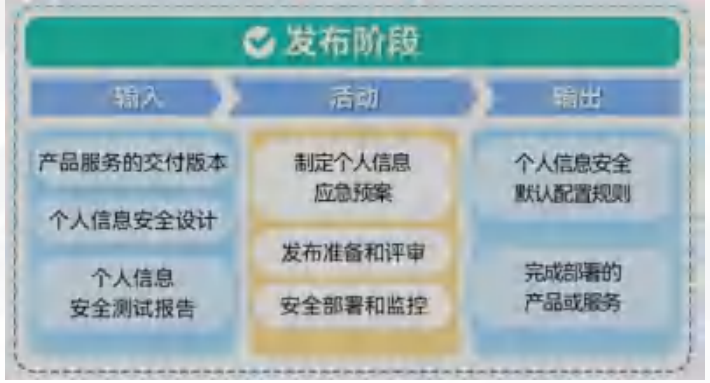






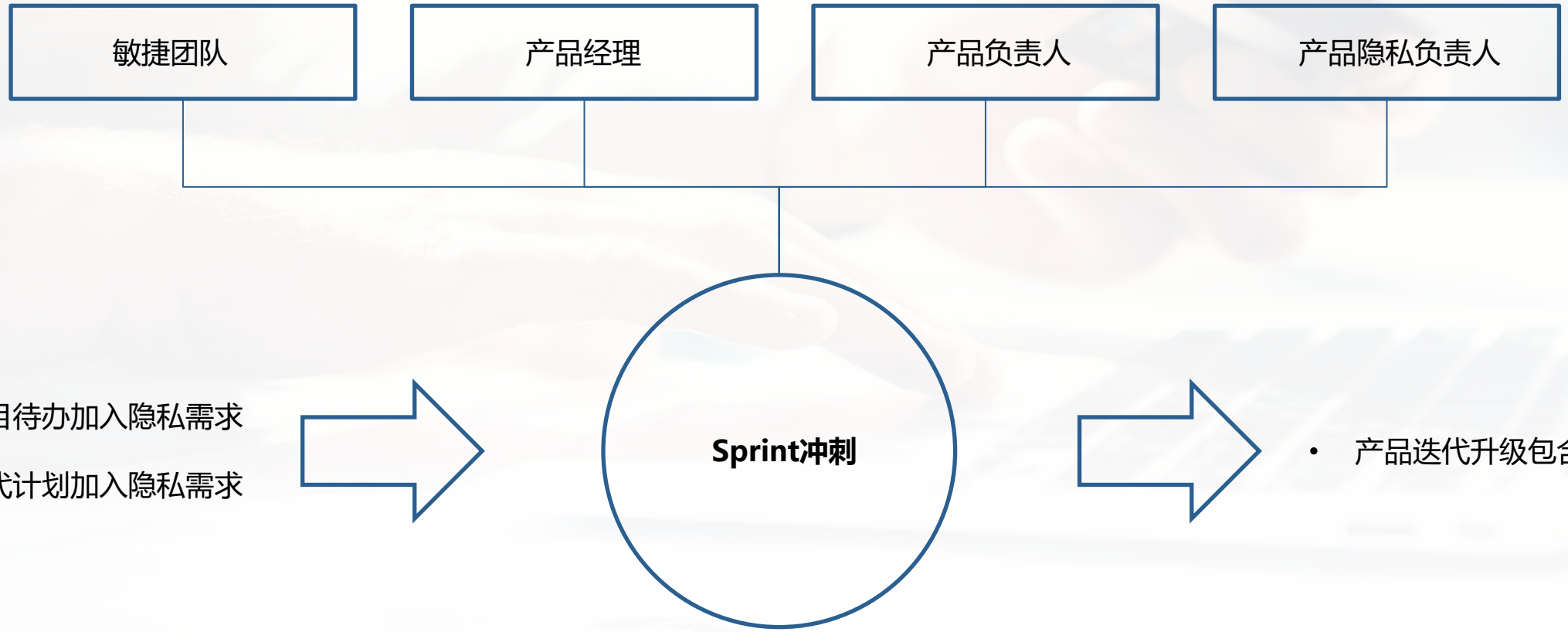






*数据来源：一图读懂 | 国家标准 GB/T 41817-2022《信息安全技术 个人信息安全工程指南》

多角度剖析隐私工程活动内容--嵌入敏捷开发与DevSecOps



- 项目待办加入隐私需求
- 迭代计划加入隐私需求

- 产品迭代升级包含隐私结果

多角度剖析隐私工程活动内容--嵌入敏捷开发与DevSecOps

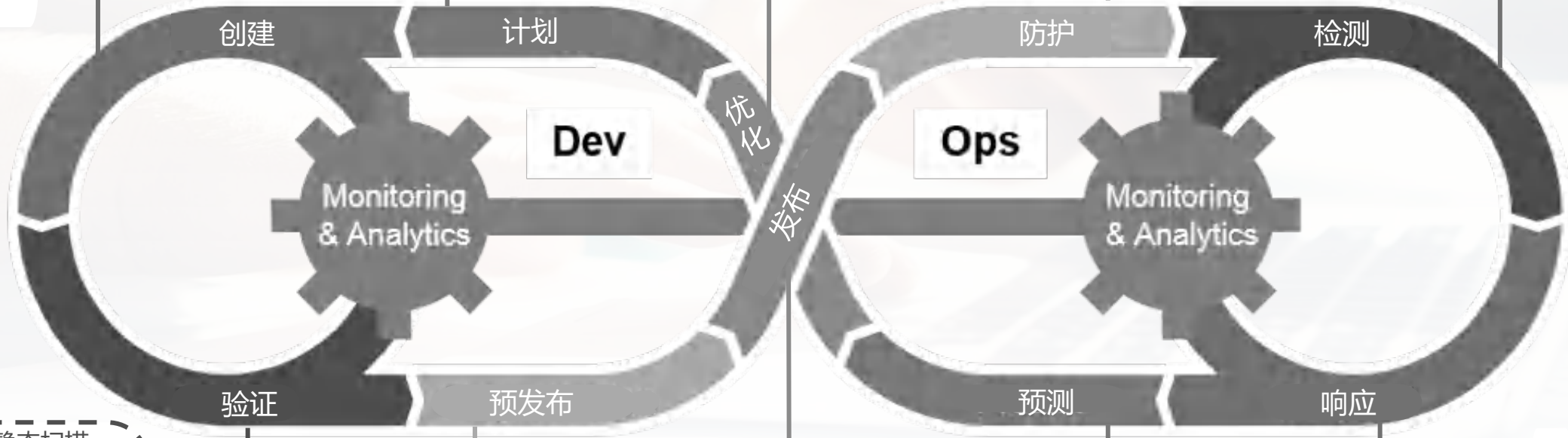
- 安全编码规范
- 产品隐私规范
- IDE安全插件
- 源代码安全检测
- 开源组件安全检测

- 安全与隐私培训
- 安全隐私需求集成
- 安全与隐私评审
- 隐私影响评估（PIA）
- 轻量级威胁建模
- 安全开发红线
- 安全与隐私设计方案

- 定期会议
- 架构优化
- 流程优化
- 准确度优化

- NGFW
- WAF
- IPS
- 数据加密
- 数据脱敏
- 访问控制

- 漏洞扫描（主机/应用）
- 资产威胁管理
- 漏洞管理
- 补丁管理
- 数据异常行为检测
- SDK异常调研监控
- API接口敏感数据外传检测



- 源代码静态扫描
- 开源组件安全扫描
- 镜像安全扫描
- 隐私合规测试
- APP合规扫描
- 黑盒安全测试
- 交互安全测试
- 渗透测试

- 主机漏洞扫描
- 安全基线核查
- 环境安全部署验证
- 应用隐私配置标准
- 隐私管理平台配置

- 剩余风险处置
- 漏洞修复
- 代码签名
- APP加壳加固
- 部署安全指南

- 威胁情报
- 态势感知
- 预警监测

- 安全事件响应处置
- 安全事件分析溯源
- 安全监管联动
- 个人数据泄露响应

隐私模式--可反复使用的隐私组件、代码和设计经验

设计模式在隐私领域的演进

Privacy Design Patterns

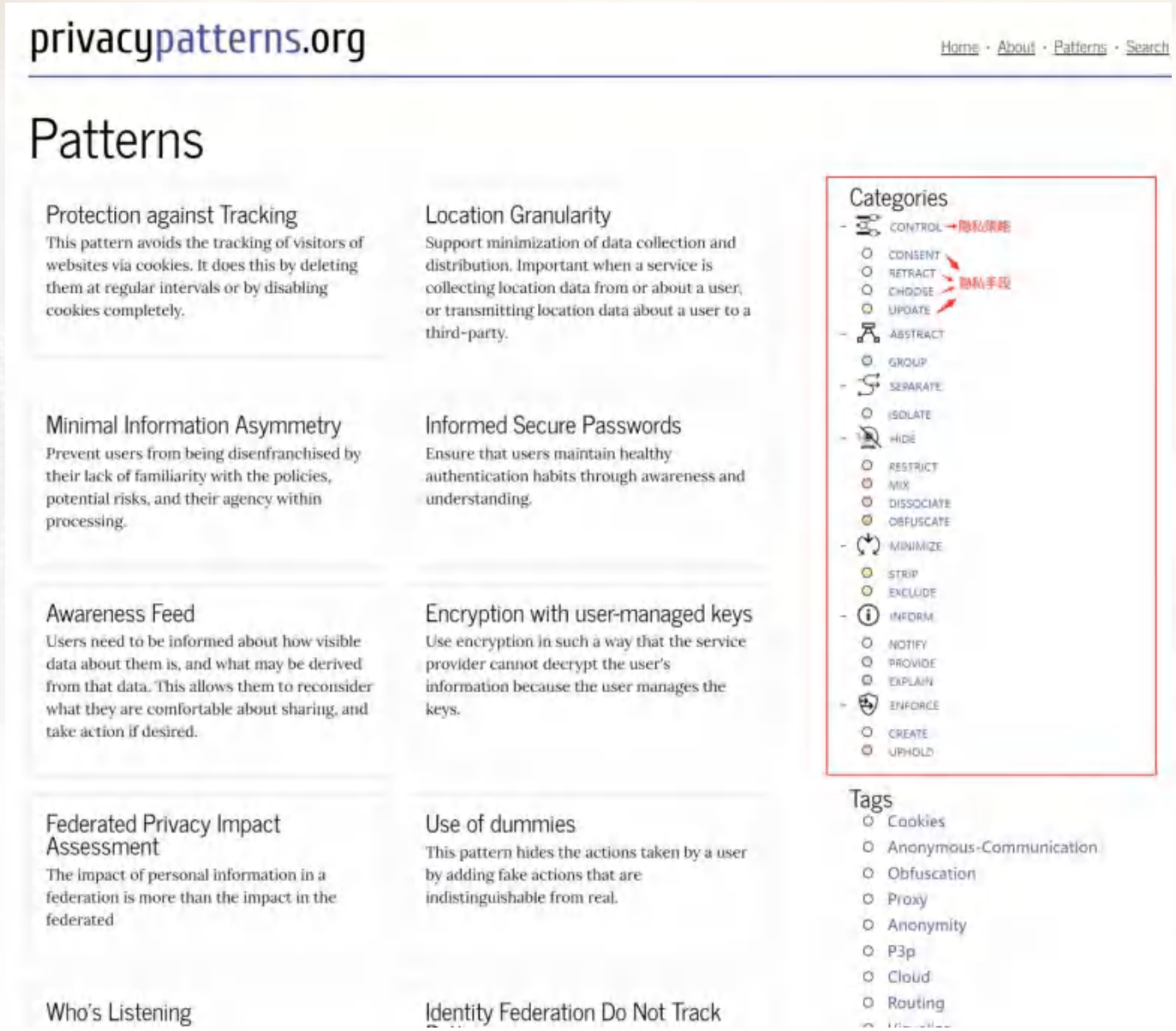
设计模式的由来

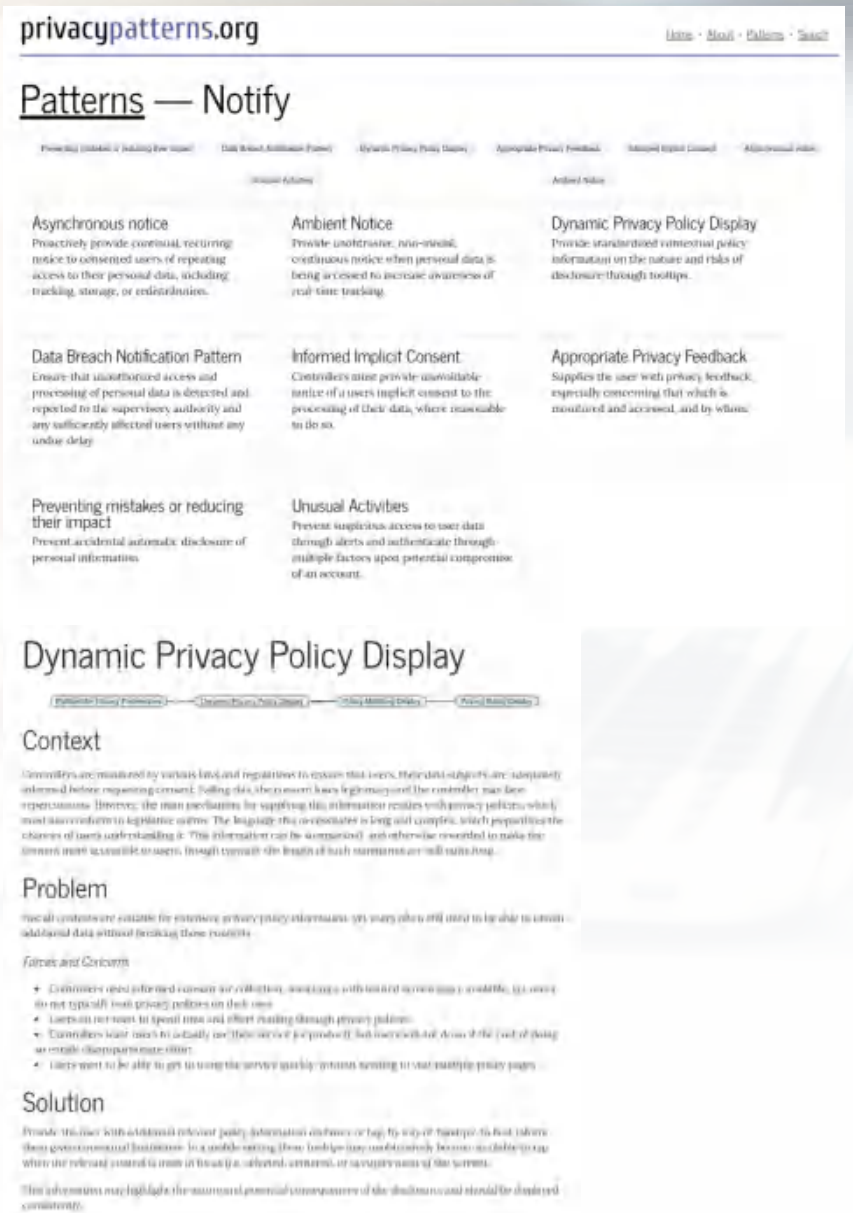
在产品设计和软件开发，我们经常都会提及设计模式（Design Pattern），随着《设计模式：可重用面向对象软件的元素（Design patterns: elements of reusable object-oriented software）》这篇论文的发布，这个概念在1994年的时候已经被广泛接受。设计模式（Design Pattern）是一套被反复使用、多数人知晓的、经过分类编目的、代码设计经验的总结。使用设计模式是为了可重用代码、让代码更容易被他人理解、保证代码可靠性、程序的重用性。

隐私设计模式诞生

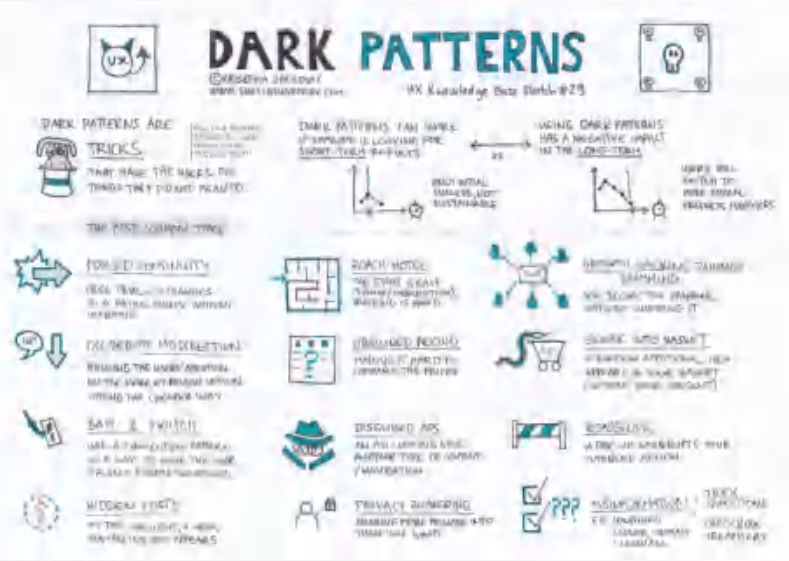
是隐私设计策略的具体可复用的设计实现方式，相关的隐私设计模式可以常见于各种Web和App产品里面，以及组织的隐私保护流程当中。

隐私模式--可反复使用的隐私组件、代码和设计经验





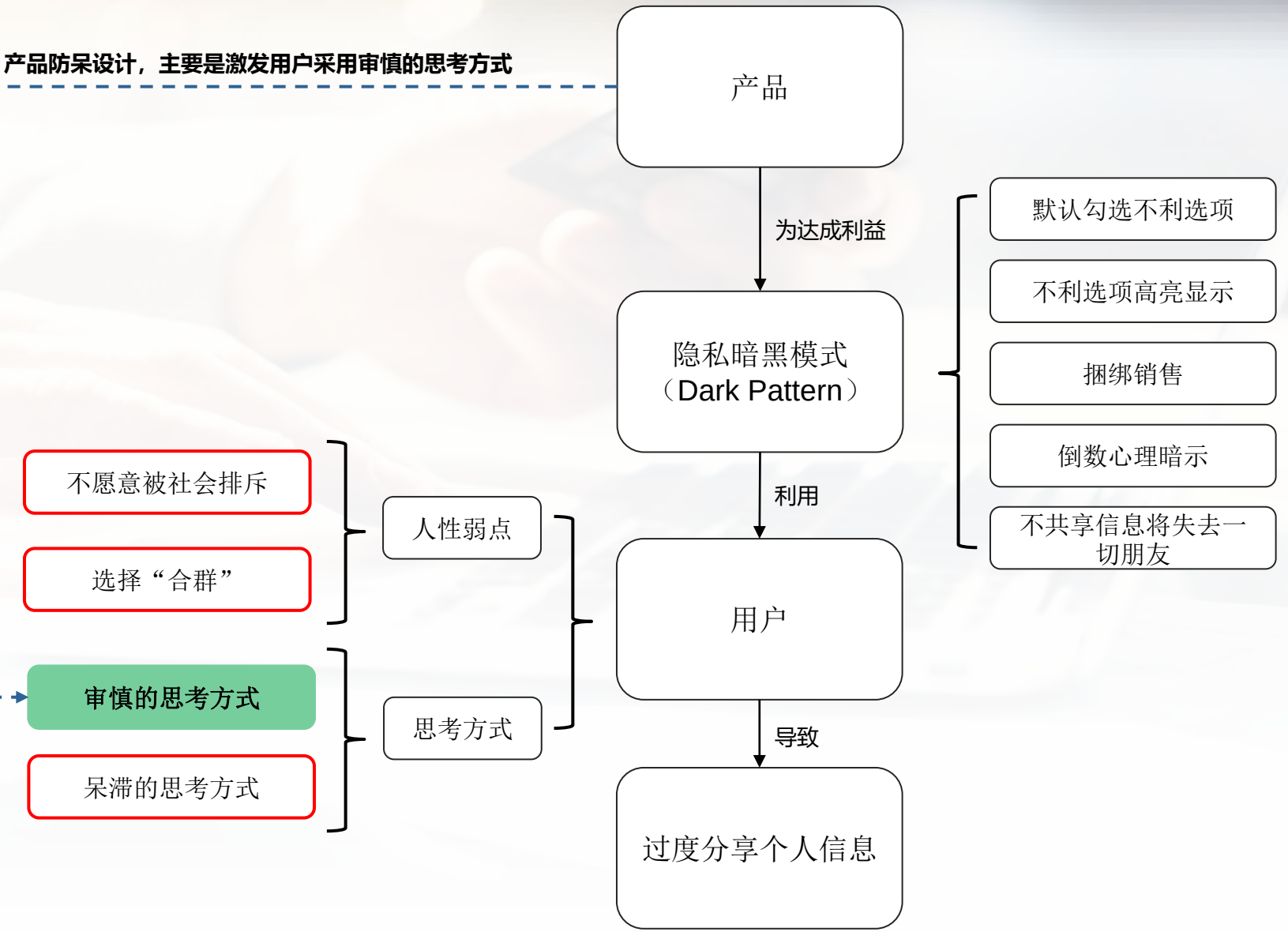
隐私暗黑模式（Dark Patterns）--隐私界的“PUA”



暗黑模式定义

当产品和软件开发的设计模式在隐私方面形成一种通过**欺骗**、**诱导**、**胁迫**、**劝说**和**PUA**（Pick-up Artist）的方式使个人放弃自己隐私信息的时候，我们将这种产品界面和解决方案统称为隐私的“暗黑模式（Dark Patterns）”。

产品防呆设计，主要是激发用户采用审慎的思考方式



隐私暗黑模式--经典案例

暗黑模式
Dark Patterns

在2016年，由Benjamin Erb等5位作者编写的《来自黑暗面的故事：隐私暗黑策略和隐私暗黑模式（Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns）》就提出了最原始的8种暗黑模式的常见表现形式。

隐私扎克伯格化
(Privacy Zuckering)

因早期Facebook故意设置过于复杂、细粒度和难以理解的隐私选项，使用户提供更多个人数据，因此得名。

无法注销的账户
(Immortal Accounts)

无法顺利地在应用中找到注销账户的按钮，或者注销账户的条件十分复杂、繁琐和苛刻。达成条件后，甚至也无法完全注销。

不利的默认设置
(Bad Defaults)

在应用软件注册账号时，系统自动帮你选择了不利的默认设置，使你默认就会分享更多的个人数据和隐私。

过度收集通讯录
(Address Book Leeching)

获取手机的通讯录访问权限后，不断读取该用户的联系人信息，并向他们发起推销活动。

强制注册
(Forced Registrations)

强制注册描述了一种情况，即一个人被迫注册一个帐户以使用服务的部分功能，尽管从技术上讲，注册对于使用该服务是不必要的。

影子个人资料集
(Shadow Profiles)

在用户无感知的情况下，使用用户数据与补充数据，创建非用户或用户的隐藏档案。可用于链接可能有共同特征的用户，如都有一个共同的心理治疗师。

隐藏规定
(Hidden Stipulations)

提供内容冗长的、包含法律网络安全专业术语的、晦涩难懂、不符合通用语言习惯、字体格式杂乱的隐私政策，从而让用户不思考选择同意。

过度信息请求
(Information Milking)

通过导入邮件或手机通讯录，以获取更多的联系方式，从而邀请更多人注册或购买商品，或发送推销广告。

隐私暗黑模式--隐私“防呆设计”的定义与实践

核心目的： 防止用户不经意的误操作导致隐私侵害。

实现隐私防呆设计的方法：

1.要依靠监管机构的强制执法，避免隐私暗黑模式的出现；

2.企业自身通过Privacy by Design的整套方法论，按照隐私工程方法，落实隐私策略，形成可复用的隐私模式，确保企业全面贯彻。

信息准确传递

让用户明确完成某隐私选择的后果。UI界面提供准确的隐私选项名称、数据控制者联系方式和监管机构信息。

隐私政策概述

在隐私政策的开始/顶部，提供可折叠的目录，包含隐私政策的不同段落，做到清晰指引和快速跳转。

提供名词定义

使用通俗的语言解释数据保护的专有技术名词。可以采用文本或悬停显示悬浮框的方式。

突出重点

让数据保护相关的元素或行为在界面中具有视觉冲击力。例如收集人脸数据时，应重点突出**处理目的**和**可替代选项**。

跨设备一致性

隐私设置应该具备跨设备的一致性，同一账号在Web和App的版本中应该保持一致。

数据保护引导

创建账户后，应在用户引到指南中提供数据保护信息的设置引导，以便用户顺利找到隐私偏好设置。

隐私面板

可以提供隐私面板来告知用户自己的个人数据被使用的综合情况，通常可以使用数字指标、图表等直观方式展示。

隐私通知

提高用户对与数据处理有关的方面、变化或风险的认识（例如数据泄露）。通知可以通过多种方式实施，如通过收件箱信息、弹出窗口、网页顶部的固定横幅等。

二次确认

在用户选择重要的隐私选项时，应提供二次确认按钮。例如将个人数据进行公开发布时。

挽回错误

在用户不小心选择了错误的隐私设置，或给予同意后又后悔了，这时应该提供撤回同意和修改设置的明显选项。

使用图标和符号

通过图标、符号和颜色来直观表达将要实施的数据处理活动或表达隐私设置。例如一个锁，一个盾牌或者一个红色禁止符号。

使用例子

除了强制性信息清楚准确地说明处理的目的外，还可以使用例子来说明特定的数据处理，使其对用户来说更加具体。

03 Privacy by Design技术实战

对核心内容进行重点介绍

Privacy by Design 最佳实践调研分析报告简介

一份来自对隐私设计的热爱与梦想而构筑的报告书

项目专家组：8位行业安全与隐私专家

项目简介：由**安在诸子云组织发起。**本报告从**产品设计的初心出发**，帮助读者了解隐私保护的**广义定义**、**深层客观需求**和**用户主观期待**，从而实施产品隐私设计，使读者可以更从容地面对监管不断频繁出台的细则要求，甚至超越合规，以隐私价值实现为目标来建立隐私设计框架。本报告重点对隐私设计（PbD）**顶层指导原则**和**框架**进行分解，并与隐私设计实际落地场景进行**衔接**。旨在通过对隐私威胁、违规场景进行解释，通过**整合与构建隐私设计概念的层级关系图**，在PbD七原则、隐私工程、隐私策略和隐私模式方面进行**正反面对比**，剖析良好隐私设计原则和策略原理，通过落地步骤和实施路径引导隐私设计在企业中的落地方法，最后将知名产品在重点领域的隐私设计最佳实践向读者进行展示，为隐私设计落地提供体系化和更接地气的调研分析结论。

文章特色：

（1）深度剖析，图文并茂：本报告篇幅183页，配图103张，编制历时7个月。

（2）理念引进，技术先驱：大量调研全球文献资料，引入先进的隐私理念和实践。

（3）注重实践，受众广泛：强调理念与实践的融合与映射，提供能落地的工具和建议。

1.PbD技术实战--数据清单（DI）与数据处理活动记录（RoPA）

1.PbD技术实战--数据清单（DI）与数据处理活动记录（RoPA）

识别要求

数据清单

- 结构化个人数据
  - 数据主体填写提交（Web表单提交）
  - 自动化数据采集（数据埋点、权限采集）
  - 第三方渠道采集（API采集、库表交换）
  - 离线录入（Excel、CSV）
- 非结构化个人数据
  - 数据主体主动提交（照片、附件等）
  - 自动化数据采集（录音、视频）
  - 第三方渠道采集（Office文档、PDF）

数字化工具

数据发现与扫描工具

- 通过自定义个人数据规则，正则表达式、数据特征、关键字匹配等技术，对数据库进行扫描，发现数据。
- 数据分类分级标签

数据防泄漏DLP

- 通过对终端、服务器、存储对象内的文档进行指纹识别、关键字匹配、深度内容识别，从而发现并管理非结构化的数据。

配套管理活动

数据分类分级服务

重点完成个人数据部分

1.PbD技术实战--数据清单（DI）与数据处理活动记录（RoPA）

识别要求

实体清单

- 客户（数据主体）
- 本企业（控制者）
- 供应商（处理者）
- 合作伙伴（处理者）
- 子公司（处理者）
- 控股公司（处理者）

数字化工具

数据映射管理工具

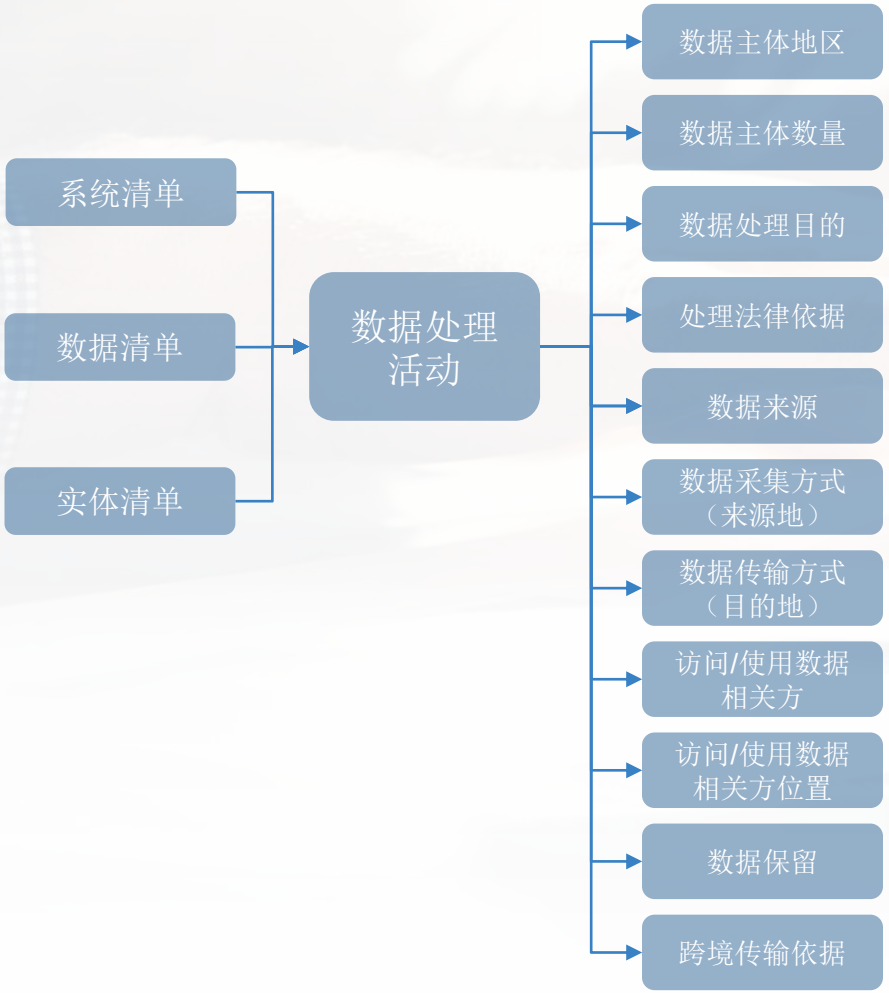
配套管理活动

实体梳理服务

- 联合业务、产品、开发、采购、法务团队，公司涉及数据处理的相关方进行识别和整理。

1.PbD技术实战--数据清单（DI）与数据处理活动记录（RoPA）

识别要求



数字化工具

数据映射管理工具

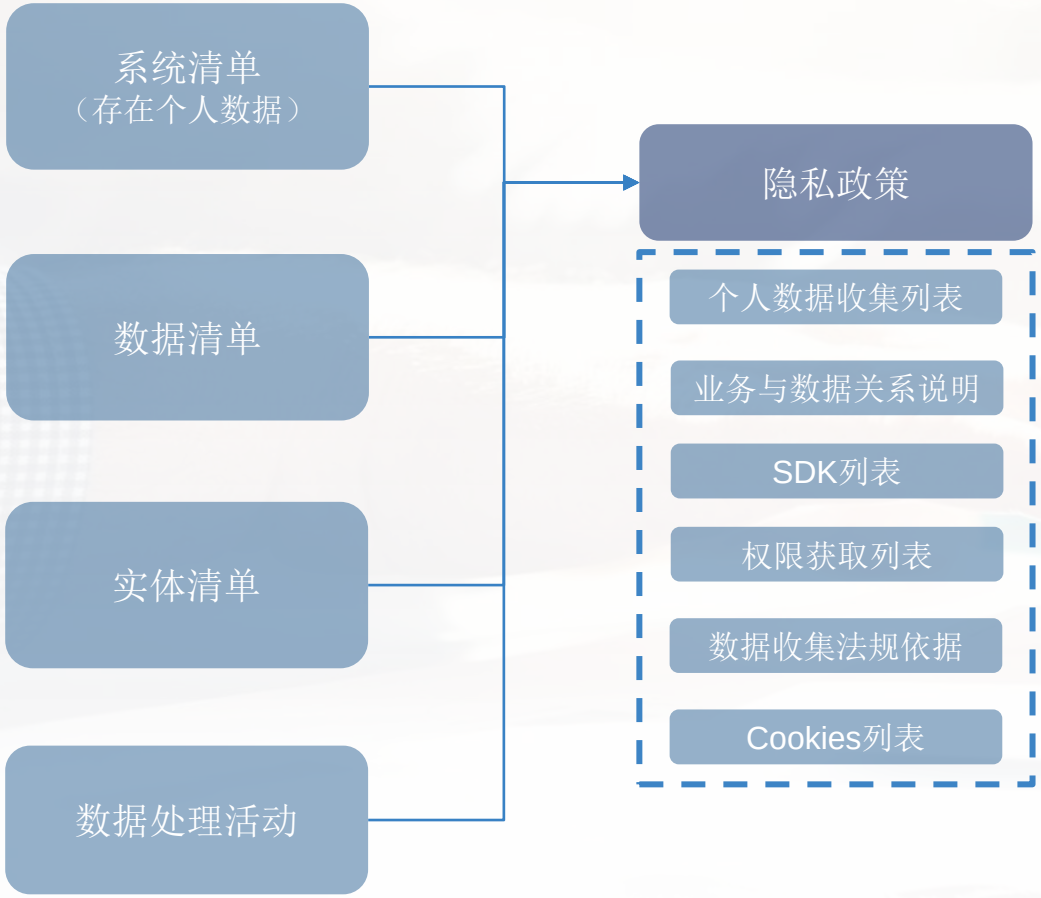
- 通过数据映射管理工具录入数据处理活动。
- 数据映射管理工具可根据系统清单、数据清单、实体清单和数据处理活动要素，自动绘制数据映射关系。

配套管理活动

数据处理活动梳理

- 联合业务、产品、开发团队，对应用系统个人数据处理活动进行业务功能模块的分解。
- 每个业务功能模块记录一个数据处理活动。

1.PbD技术实战--数据清单（DI）与数据处理活动记录（RoPA）



支付宝APP - 涉及收集用户信息的第三方SDK列表

APPENDIX A: Cookie Table

We may update this Cookie Policy from time to time to reflect, for example, changes to the cookies we use or for other operational, legal or regulatory reasons. If we do, you will be notified when you first visit our website after the change. You can also revisit this page if you wish to keep yourself informed.

Internal Cookies and Technologies

The following are first-party cookies used on properties including coinbase.com and other domains operated by Coinbase.

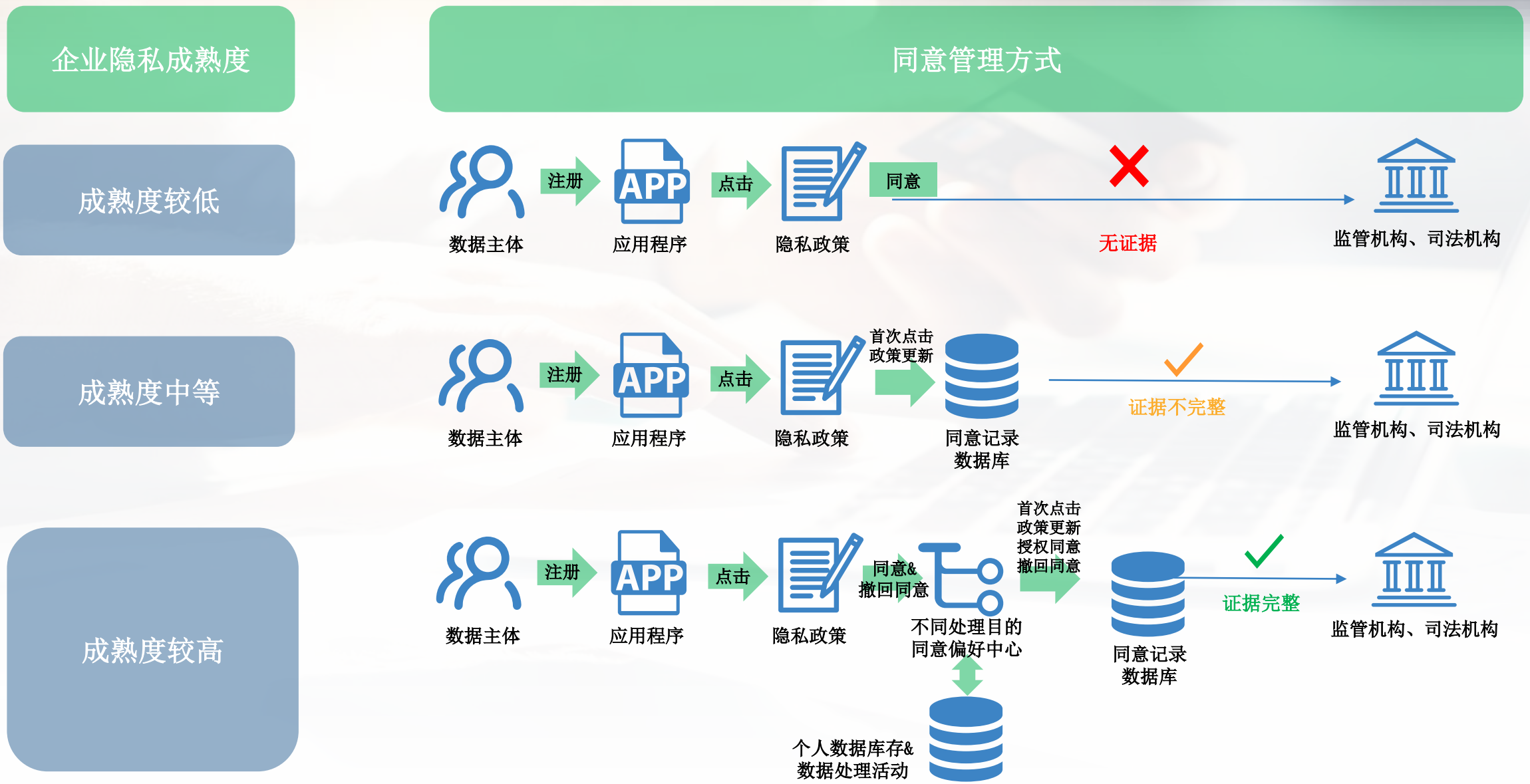
Name	Purpose	Retention
amplitude_device_id	Testing purposes	10 years
ba	Security and fraud monitoring	2 days
ob-rfm	Support website performance	10 seconds
__cfduid	Security Purposes	30 days
cf_ob_info	Security Purposes	1 minutes
cf_use_ob	Security Purposes	1 year
_coinbase_lax	Security Purposes	Session
_coinbase_session	Security Purposes	30 days
_coinbase_strict	Security Purposes	Session
__cf_bm	Bot management	30 minutes
cf-country	Sets region-based default cookie settings	Session
coinbase_device_id	Device identification and testing	10 years
coinbase_locale	Sets default locale/language	Session
df	Security and fraud monitoring	10 years

(12) android.permission.WRITE SYSTEM（读写系统设置权限）：允许应用读写系统设置项

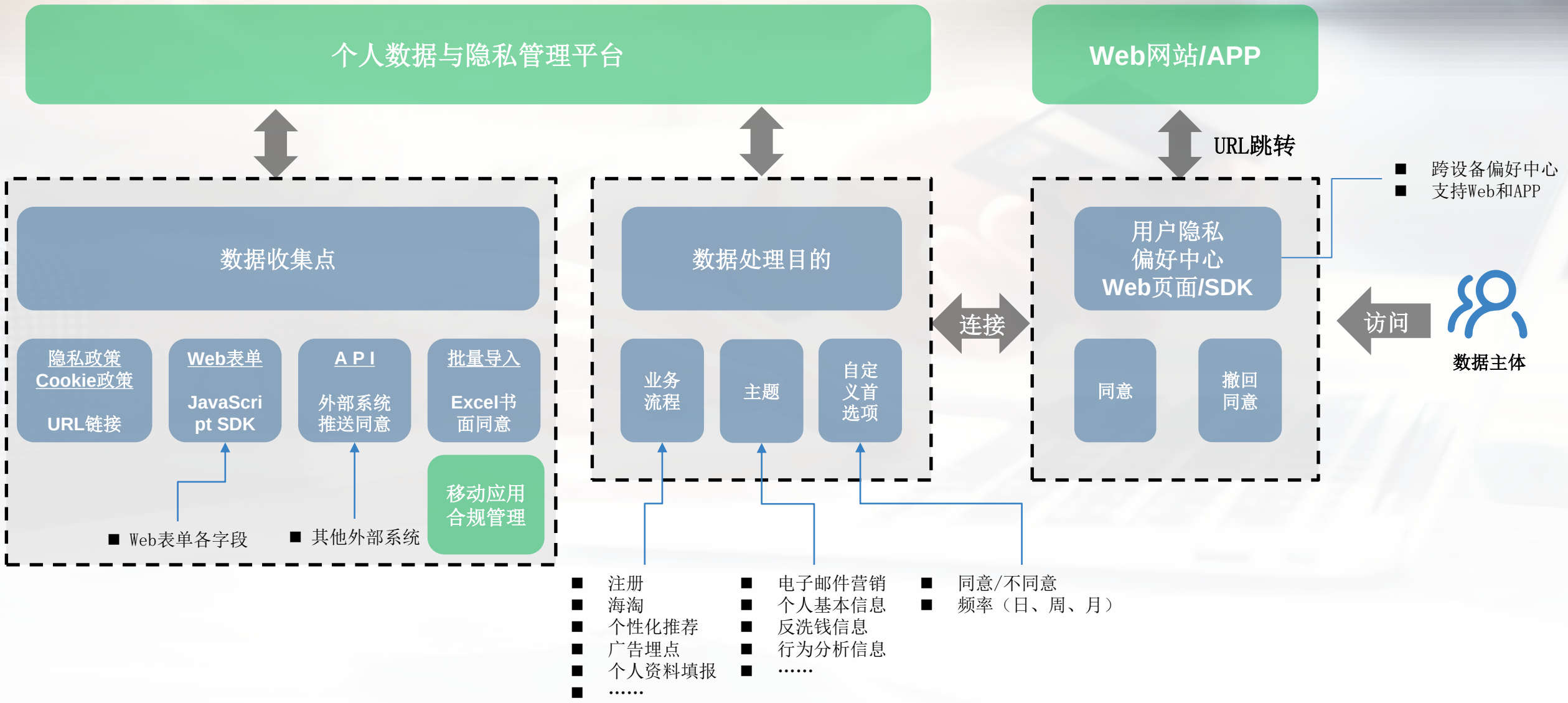
(13) android.permission.GET_TASKS（获取任务信息权限）：允许应用获取当前或最近运行的应用

(14) android.permission.CHANGE_WIFI_STATE（改变WiFi状态权限）：允许应用改变WiFi状态

2.PbD技术实战--同意管理设计



2.PbD技术实战--同意管理设计

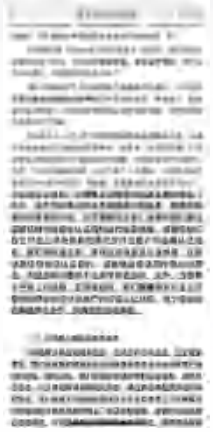


3.PbD技术实战--隐私通知分层设计

隐私通知分层设计

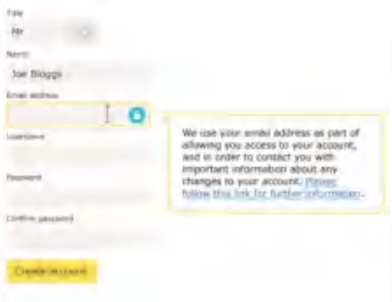
隐私设计领域，采用分层的隐私通知来达到更好的隐私透明度传达，比干巴巴的隐私政策文本更能触达用户的关切。隐私通知与用户界面进行深度融合，符合Privacy by Design的正和非零和原则，是一种产品功能与隐私设计的和谐双赢局面。

01 静态文本



02 增强告知

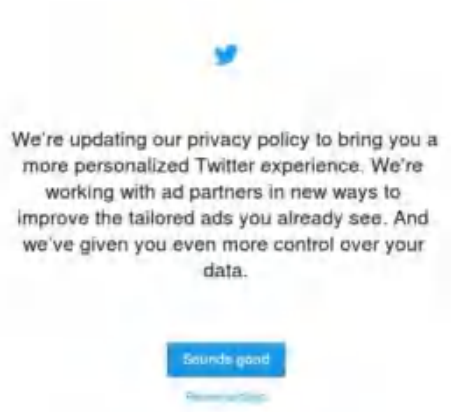
03 即时提示



04 单独同意

05 隐私图标与符号

06 隐私政策更新



3.PbD技术实战--隐私通知分层设计（单独同意）

图1 生物识别数据采集单独同意

图2 韩国网站的单独同意示例

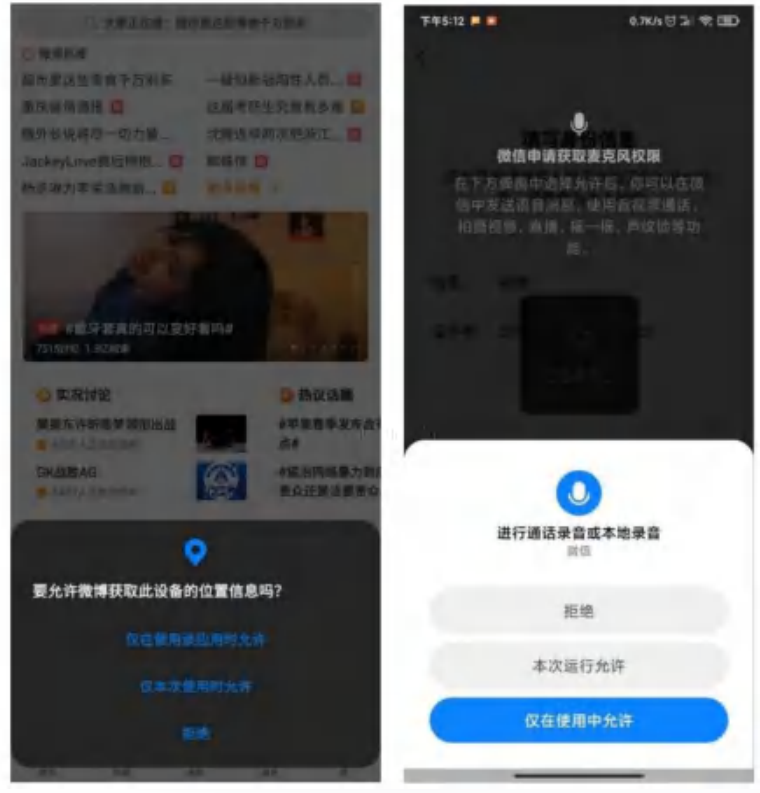
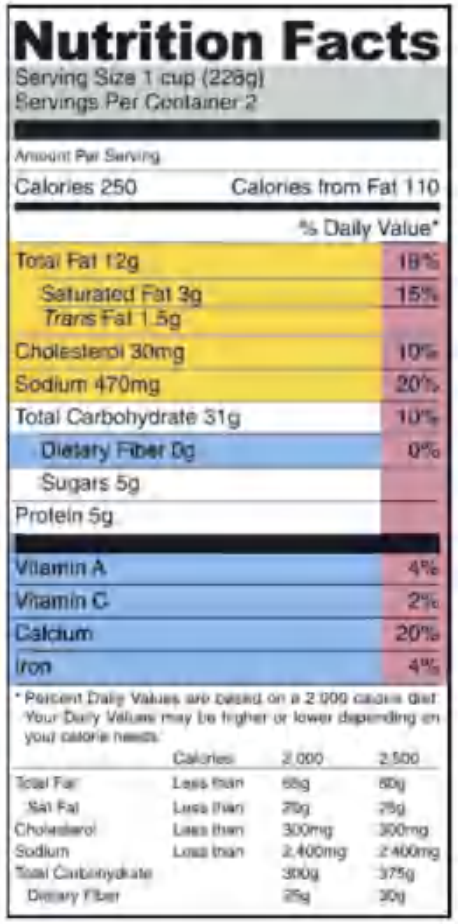


图3 App单独授权

3.PbD技术实战--隐私通知分层设计（图标与符号）



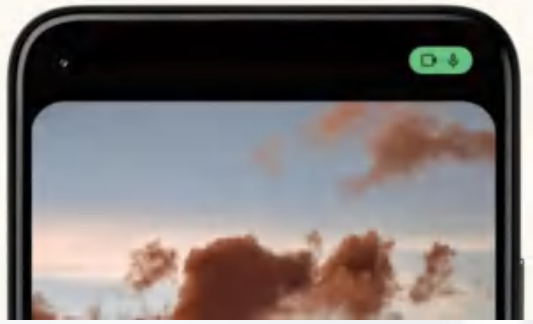


图1 营养表在隐私领域的应用

图2 照相机的快门声音

图3 录像功能的指示灯

3.PbD技术实战--隐私通知分层设计（元宇宙隐私保护新趋势）

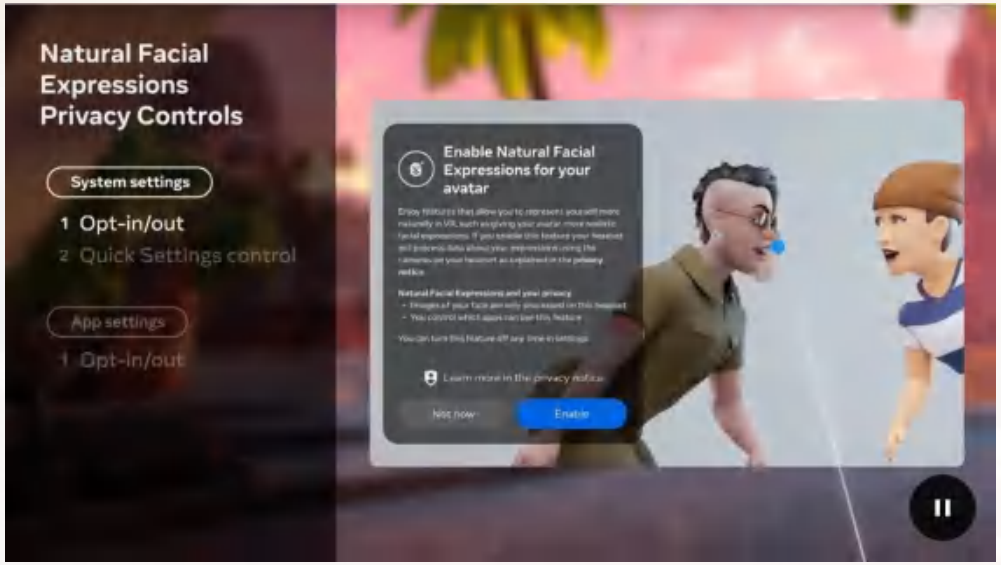


图1 Meta Privacy Notice

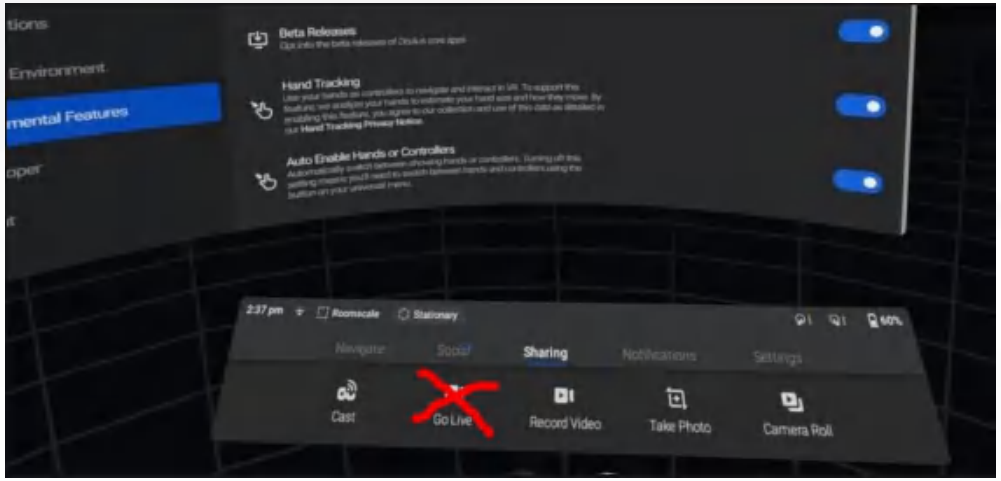


图2 Oculus Quest 数据共享控制界面

1.XR（AR、VR、MR等）技术中收集的数据类型

传感器信息：包括脸部摄像头、眼球运动捕捉、瞳孔跟踪、瞳孔大小、虹膜扫描、心率监测、温度监测、手势监测。

音频信息：头戴式设备的麦克风，用于社交沟通和互动。

空间和位置信息：摄像头、陀螺仪、深度传感器，6DoF追踪数据。

用户交互信息：应用程序登录、购买、支付。

2.隐私风险

隐私风险从数字世界向物理世界转移：多种多样的生物识别数据、敏感个人数据的收集，甚至是私密空间、私密活动的意外收集，都将突破数据最小化采集的限制等隐私原则。同时，数据采集的隐私通知和获取同意将更加困难。

3.隐私控制

（1）基于位置的隐私通知，提示用户在医院等敏感地点减少或停止录音、录像；

（2）在设备中嵌入编辑技术，默认会模糊或掩盖部分镜头；

（3）更多采用图标、符号、声音、指示灯、口头告知等隐私通知方式。

4.PbD技术实战--数据主体权利DSAR（架构）

数据主体访问请求

数据主体权利申请
Web表单自定义

数据主体身份认证

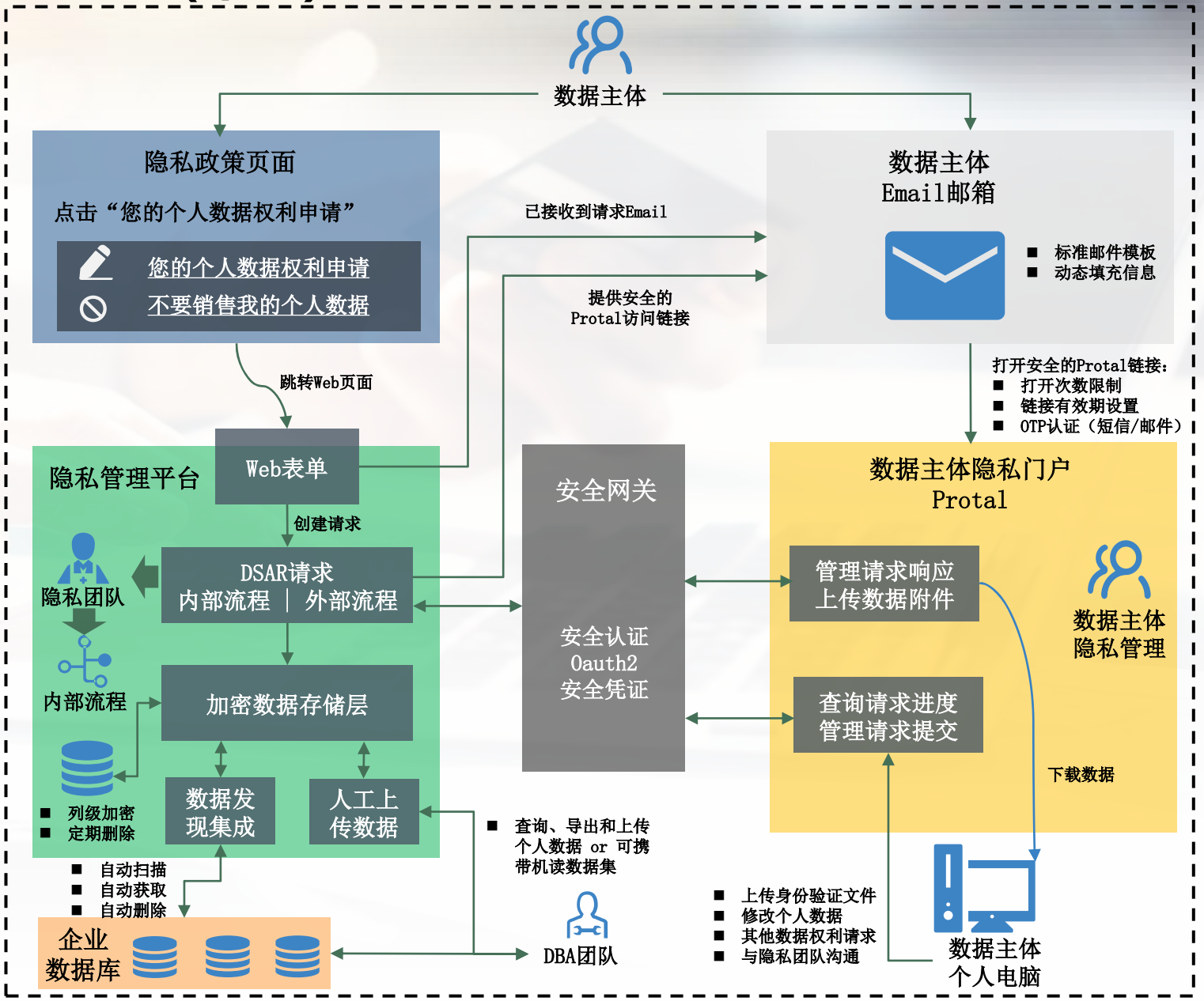
建立企业内部
请求响应工作流

响应邮件/响应话术
标准模板

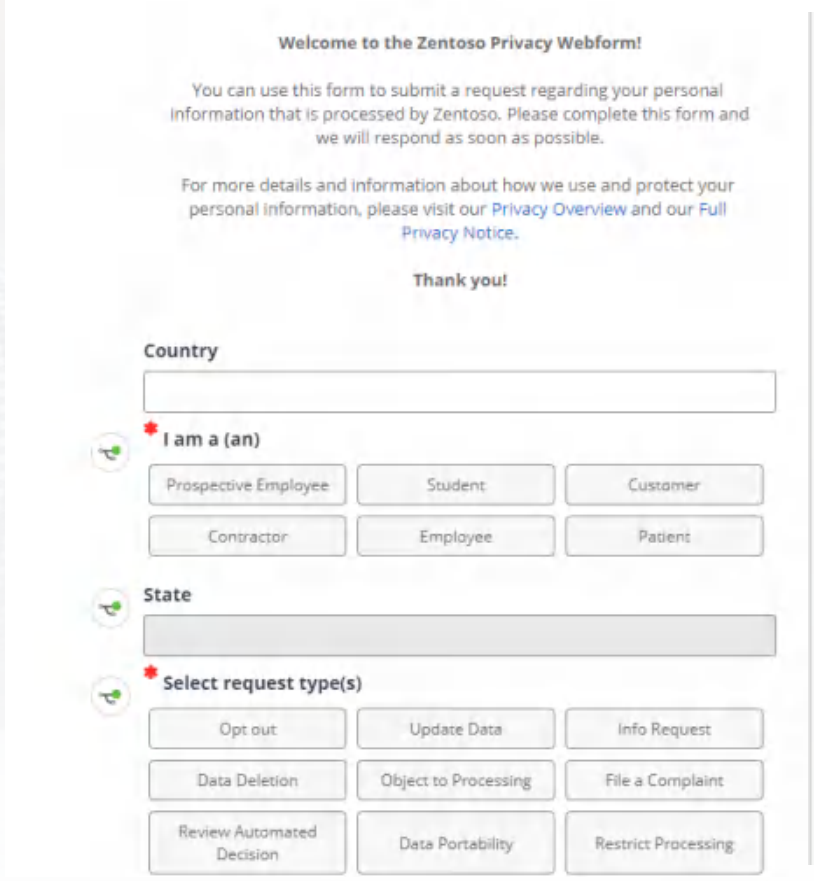
响应时间
及时提醒

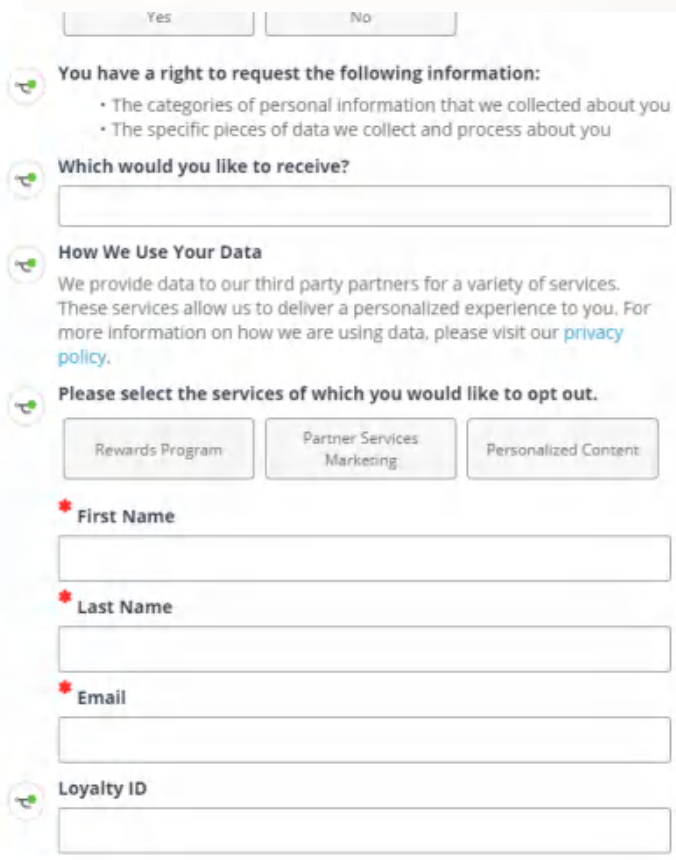
根据地理位置
识别数据主体
拥有的权利

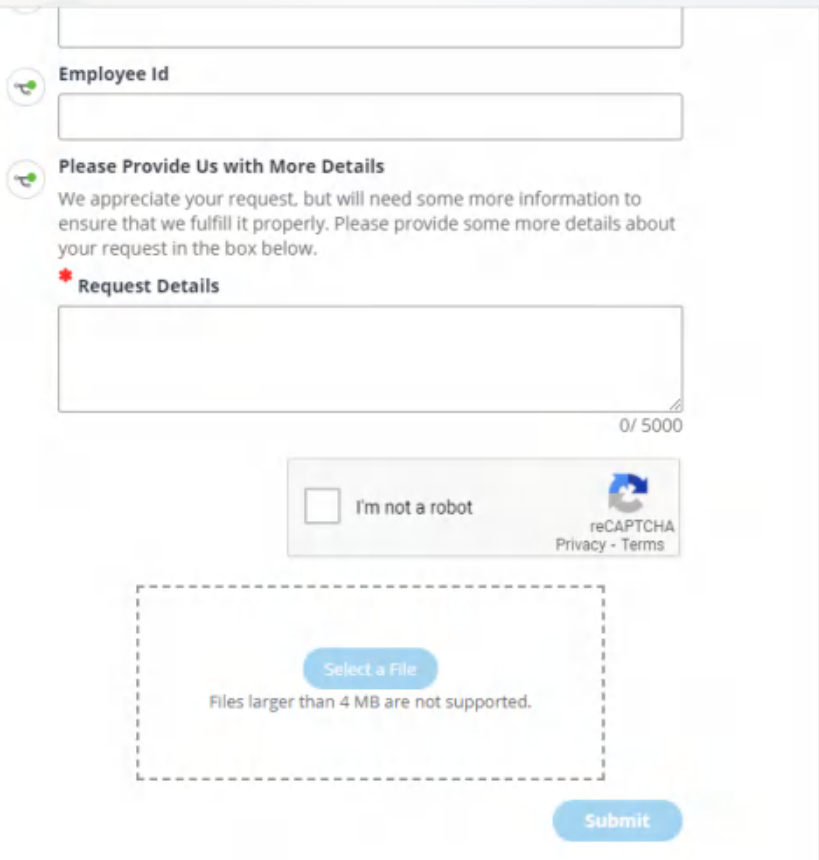
独立为数据主体提供
数据安全保障的隐私门户站点
（Protal页面）



4.PbD技术实战--数据主体权利DSAR（Web表单）







4.PbD技术实战--数据主体权利DSAR（处理流程）

数据主体访问请求响应流程管理

用户子任务

数据主体

客服

- 了解原因
- 客户挽留

业务

- 业务影响评估
- 业务流程审批

法务

- 法律法规符合性审批

隐私

- 隐私流程合规审批
- 数据保留审批

DBA

- 实施具体数据操作
- 查询、导出、上传个人数据

系统子任务

数据发现系统集成

数据映射更新

数据库操作（增删查改）

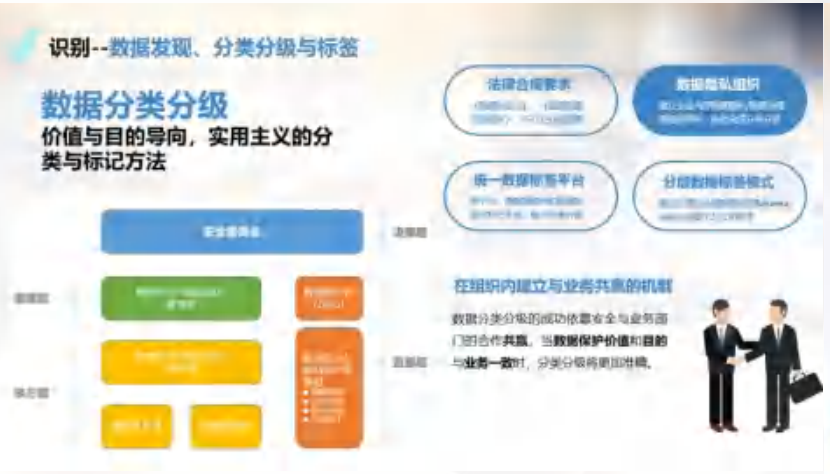
同意记录更新

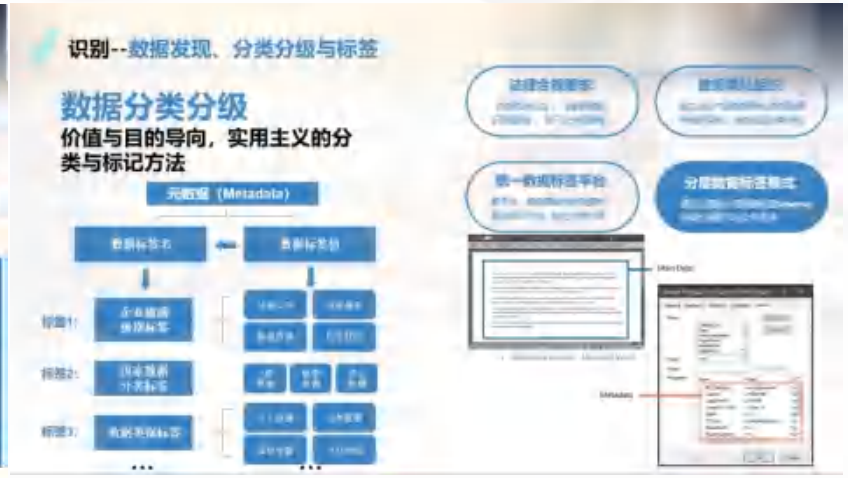
- 各类云端系统集成
- 自动化数据主体访问请求响应

*上述流程为举例，根据企业实际情况调整

5.PbD技术实战--数据发现、分类分级与标签

推荐以价值与目的为导向，实用主义的数据分类与标记方法。通过**识别法律合规要求**、**建立数据隐私组织**、**建设统一数据标签平台**、**构建分层数据标签模式**等**四个**步骤，实现**企业数据资产运营管理。**





5.PbD技术实战--数据发现、分类分级与标签（标签示例）

目前Google和Microsoft等国际巨头已经将不少非结构化的文档标签嵌入到日常的Office系统当中，可以在控制台完成标记、过滤和控制。

图1 Google Drive的数据标签

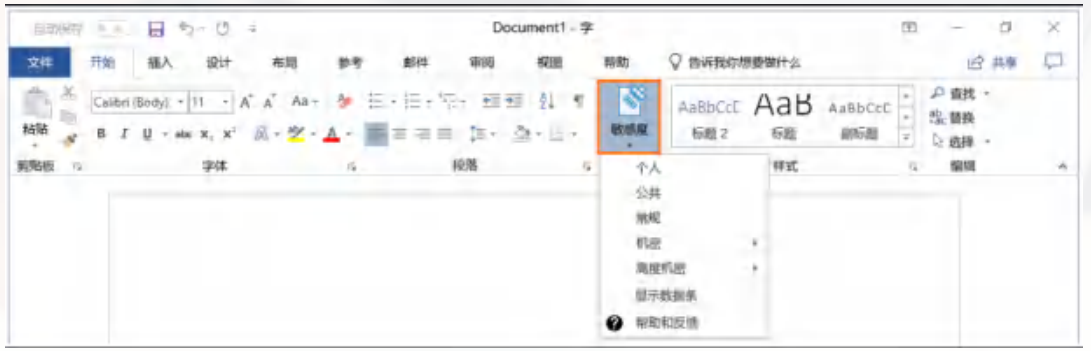


图2 Microsoft的MIP标签

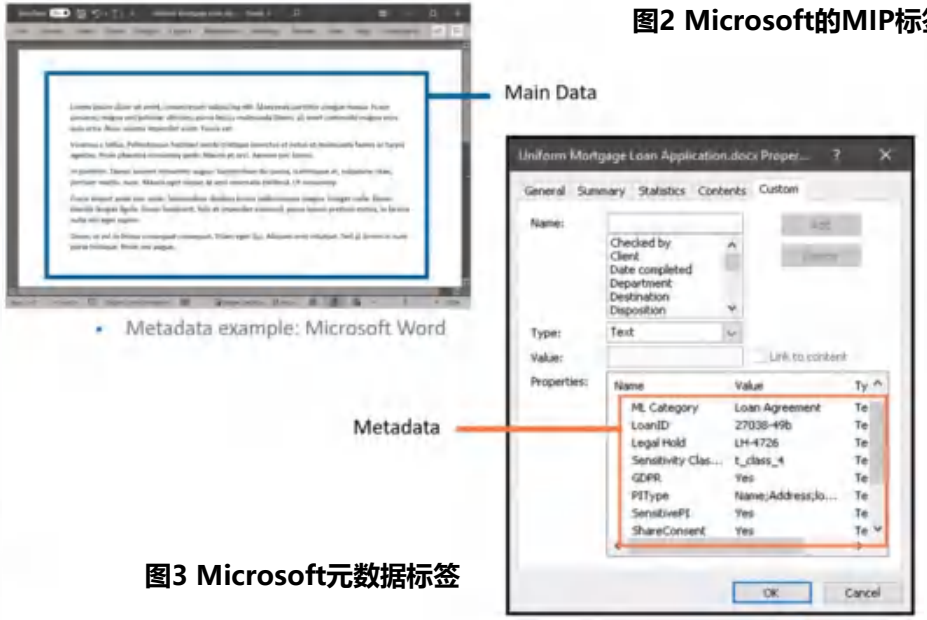


图3 Microsoft元数据标签

6.PbD技术实战--数据保留与存储期限

数据保留关键流程

数据保留合规要求的关键在于**梳理**与**数据时间戳标记**

Step 1

识别与梳理业务开展范围内，各司法管辖区的关键个人数据的**数据保留合规矩阵**。

Step 2

数据库设计或整改：**单独划分PII信息数据库表**，其他业务数据表采用**外键链接**方式，并且对数据记录增加**时间戳标记**。定期轮询时间戳，执行归档、删除任务。

Step 3

非结构化数据保留：对OSS、S3等存储系统的文件产生时间进行过滤，定期通过**存储桶API**进行数据归档和删除处理。

Step 4

数据备份的处理：除了生产环境的数据外，对于**定期数据备份**也需要对其进行定期的时间戳扫描和处置。

Step 5

数据冻结计划：当引起法律诉讼时，应该对数据保留的自动化机制可以**实施人工干预**，避免司法传唤时证据缺失。

Step 6

建立数据保留政策与细则：在组织内进行**培训宣贯**。定期组织数据保留政策与细则落实情况的安全检查，确保措施执行到位。

7.PbD技术实战--数据库分散存储和隔离处理设计

- 敏感用户信息单独存储，原则上不得在非用户中心留存用户信息。如需使用用。户信息，应通过**接口调用，缓存计算，禁止落盘。降低数据向内部员工的披露程度。**
- 所有表格通过**UID**进行外链连接。
- 所有表格记录**生成时间戳**，作为后续统计数据保留与销毁的**“计时器”**。

UID	姓名	电话	邮箱	生成时间戳	注销时间戳
6adindindkdj	Steven Xiong	150XXXXXXXX	xxx@123.com	20220101162323	20221212171234
39dik3kd98dd	Alice Wei	189XXXXXXXX	alice@125.com	20220101160346	
375j6mf83m	Bob Li	135XXXXXXXX	bobli@666.com	20220101163586	

用户中心数据表

分散存储
Distribute

UID	交易流水号	交易金额	余额	生成时间戳
6adindindkdj	00000001	200000.00	250.00	202201041645341234
39dik3kd98dd	00000002	13000.00	3000.00	202201051603239837
375j6mf83m	00000003	5000.00	4567.50	202201061623233921

交易记录表

UID	活动编号	活动时间	奖励方式	生成时间戳
6adindindkdj	HD000001	2022.08.12	红包	2022021323 45341234
39dik3kd98dd	HD000002	2022.08.12	优惠券	2022030822 032393432
375j6mf83m	HD000003	2022.08.12	满减	2022090817 23232367

运营活动记录表

隔离处理
Isolate

业务活动　**地理位置**　**用户群体**　**SaaS多租户**

8.PbD技术实战--隐私措施嵌入供应链安全

Step 1

立项评审

建立关键的立项评审机制，将隐私评审作为重要流程卡点。

Step 2

供应商尽职调查

将隐私尽调项加入传统的信息安全尽调环节，对供应商“**起底**”。

Step 3

产品服务采购

参加重要采购活动的招投标答辩会议，发起现场审查和质疑。

Step 4

合同签订

建立DPA模板，将DPA签署纳入合同流程作为关键卡点。

Step 5

供应商绩效评价

定期对供应商隐私保护尽职情况进行多维度的评价。

Step 6

合同结束

确保合同结束时的数据保留、数据删除和销毁义务的充分有效性。

9.PbD技术实战--个人信息收集行为自动检测和拦截SDK

01

问题：App故意规避合规技术检测

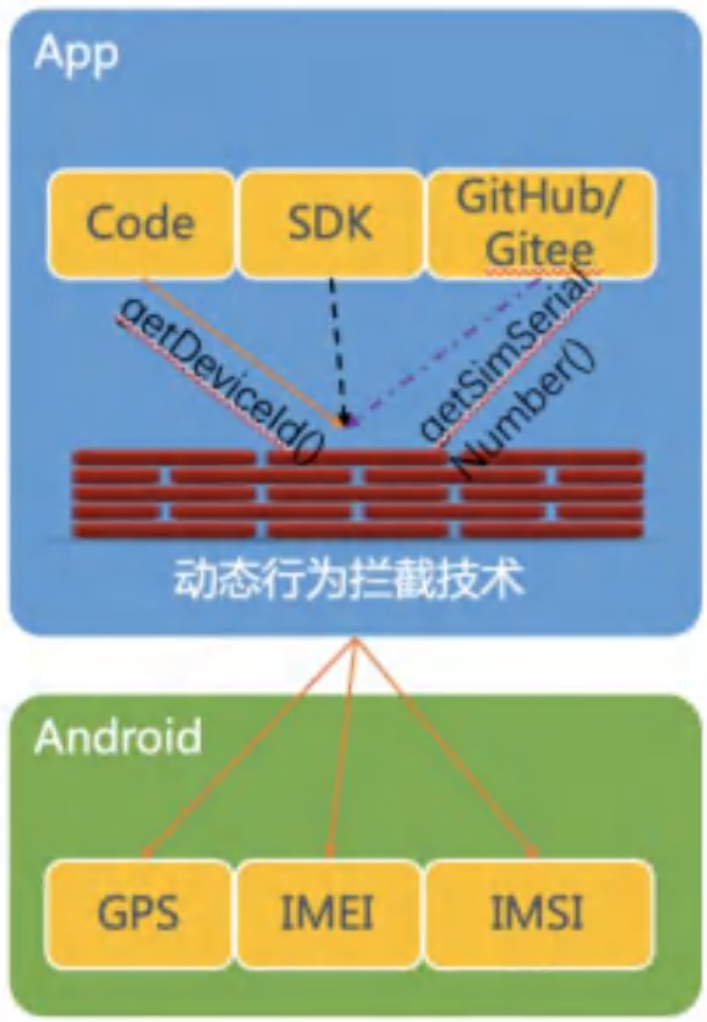
在一般的App隐私合规检测过程中，会存在部分SDK故意推迟收集个人信息时间，降低采集频率的方式来规避检测规则。例如，在登录界面停留20秒以上才开始收集信息，但检测规则可能在输入账号密码的过程只需要10秒，存在检测错位的情况，也就留下了个人信息收集的漏洞。

02

解决方案：自动化动态行为拦截技术

想杜绝个人信息收集行为违规，我们应该依赖自动化的检测和拦截手段，对第三方SDK收集个人信息的行为进行合规审计和动态行为拦截，而不是仅仅定期对App进行隐私合规扫描，从而满足国家对SDK的数据合规安全要求。

从技术层面进行分析，一个App包含自研代码、第三方SDK和开源代码，其中第三方SDK和源代码的运行权限与App自研代码相同，宿主App无法对闭源的SDK行为进行掌控。我们可以通过运行时**Hook技术来实现App内的“防火墙”**，从而使所有的第三方SDK的个人信息采集行为都被这个“防火墙”进行动态检测和拦截，从根源上解决第三方SDK的隐蔽收集行为。通过**Gradle Plugin + Transform + ASM来Hook并替换隐私方法调用**，管控App和第三方SDK的隐私行为，彻底解决隐私不合规问题。



10.PbD技术实战--隐私偏好中心与信任中心

1) Google 数据隐私安全设置

图 68 Google 数据隐私安全设置

图 69 Google 数据隐私安全设置（隐私设置、历史记录）

图 74 Apple 的隐私信任中心-1

图 75 Apple 的隐私信任中心-2

图 76 Apple 的隐私信任中心-2

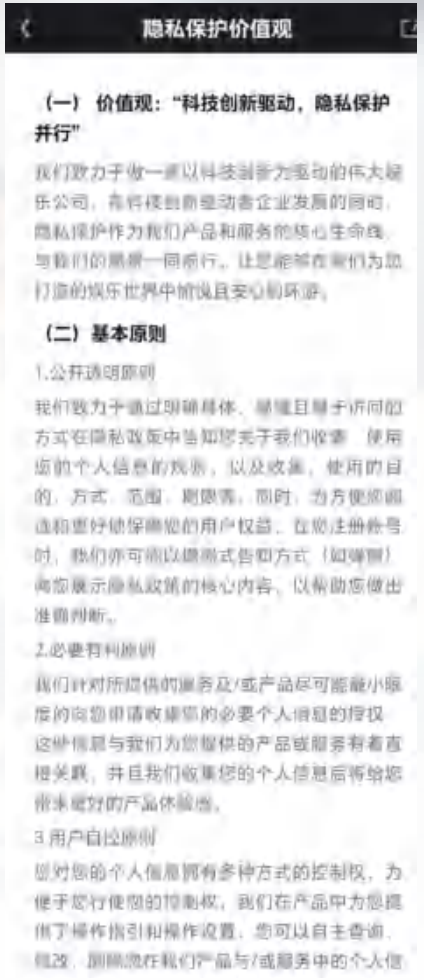
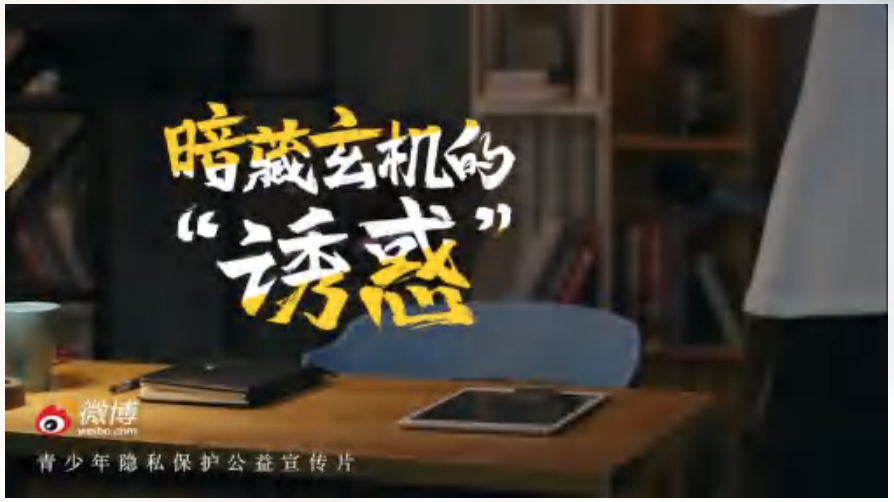


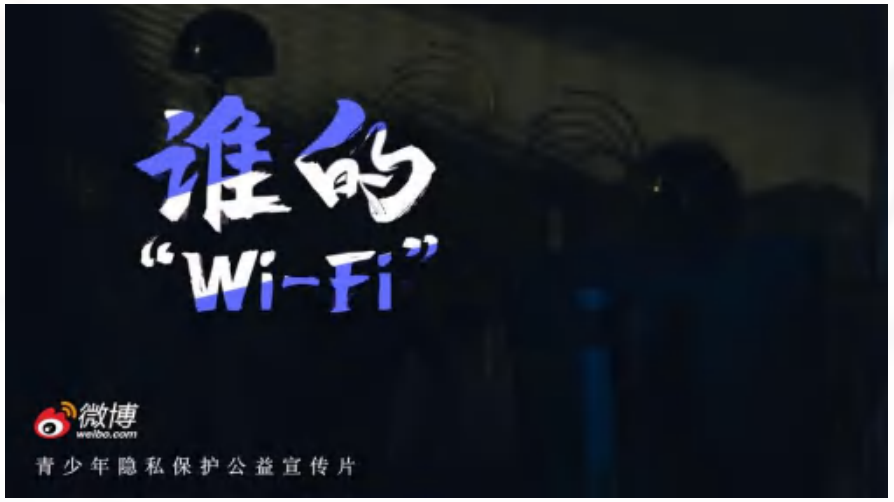
图1 Google的隐私偏好中心

图2 Apple的隐私信任中心

图3 爱奇艺的隐私中心

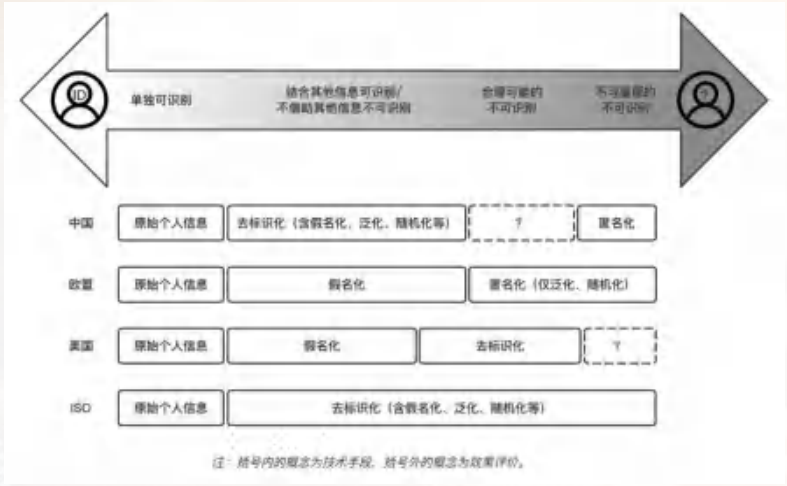
10.PbD技术实战--隐私偏好中心与信任中心

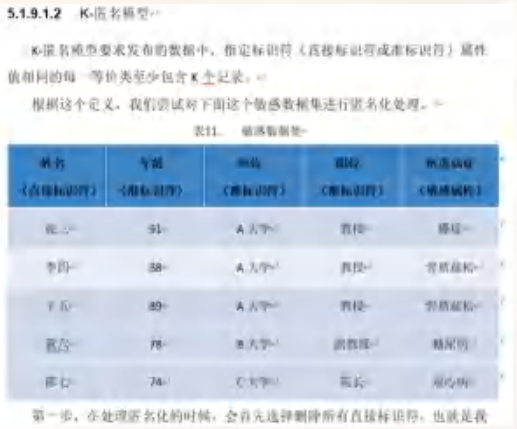




新浪微博的青少年隐私保护公益宣传片

11.PbD技术实战--匿名化的理论与工具




5.1.9.1.2 K-匿名模型

K-匿名模型要求发布的数据中，指定标识符（直接标识符或准标识符）属性值相同的每一等价类至少包含 K 个记录。

根据这个定义，我们尝试对下面这个敏感数据集进行匿名化处理。

表11. 敏感数据集

姓名（直接标识符）	年龄（准标识符）	地址（准标识符）	职位（准标识符）	疾病或症状（敏感属性）
张三	91	A 大学	教授	感冒
李四	58	A 大学	教授	骨质疏松
王五	89	A 大学	教授	骨质疏松
赵六	78	B 大学	副教授	糖尿病
孙七	74	C 大学	院长	冠心病

第一步，在处理匿名化的时候，会首先选择删除所有直接标识符，也就是我

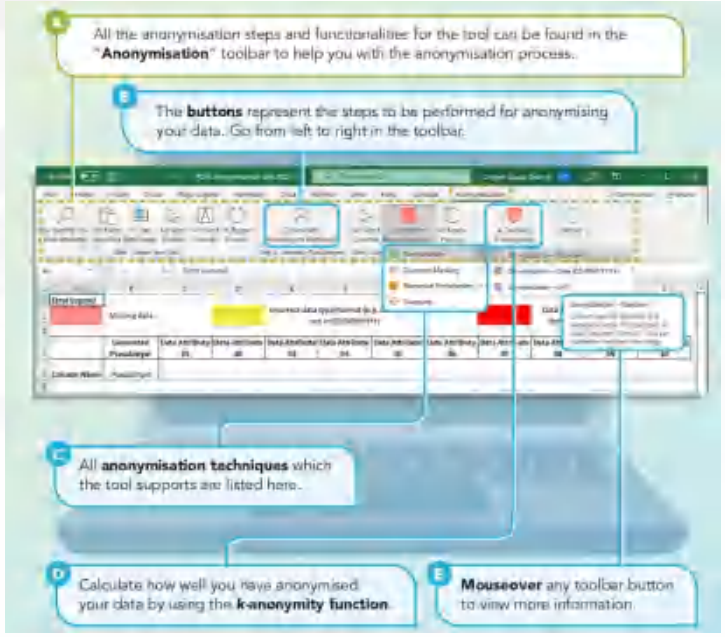

5.1.9.1.3 L-多样性匿名模型

L-多样性匿名的做法是在 K 匿名的基础之上，对敏感属性进行多样化处理，这样看在准标识符满足 K-匿名模型的情况下，在需保护的敏感属性数据上要包含至少 L 中不同的属性值，至之前 K 类名的数据集里面，考虑加入另外一条记录，它的敏感属性是糖尿病，这种情况下，我们就称 K=4（前四行年龄均为 90 的等价类）的匿名数据集满足 L=3（感冒、骨质疏松、糖尿病）的多样性。在这种情况下，要推断张三患有什么疾病要更加困难。

表12. L-多样性匿名数据集

姓名（直接标识符）	年龄（准标识符）	地址（准标识符）	职位（准标识符）	疾病或症状（敏感属性）
A	90	A 大学	教授	感冒
*	90	A 大学	教授	骨质疏松
*	90	A 大学	教授	糖尿病


5.1.9.1.4 T-接近性匿名模型



04 Q & A

问答环节

欢迎交流，共同提升

欢迎实名加微信交流

谢谢各位！