DXCon 2021

国际数字化转型最佳实践管理峰会

– 4月16日 •上海 –

DPO知识体系从理解到实践

上海傲彤信息技术服务有限公司
首席安全官　顾源

主办方：EXIN BEST PRACTICE

讲师个人资料介绍

- 毕业于华东理工大学，计算机管理专业。
- 十余年信息安全咨询顾问从业经验。
- 精通各种国内外信息安全标准（网络安全法、等级保护、ISO27001、GDPR、ISO27701、ISO27017、ISO38505-1等）。
- 现任上海傲彤信息技术服务有限公司首席安全官。
- 获取证书：CCIE&RS、CCIE&SEC、CISA、CISM、CISP、CISSP、ISO27701 、ISO27001 LA、PDPF、PDPP、DPO等。

丰富的安全架构和安全管理经验，有过大量国内知名大型企业的安全架构规划及安全管理咨询工作，多年信息安全领域技术架构设计与信息安全领域咨询管理经验。精通信息安全防护管理技术及信息安全管理体系咨询。

服务客户部分名录：

欧莱雅 L'ORÉAL　中国平安 PING AN　SMIC　Roche

数云 shuyun　康师傅　圆通速递　得物 识货

GDPR出台的意义

制定和出台《通用数据保护条例》的现实需求

适应IT技术发展
客观需要

大数据、云计算、移动互联网、社交网络以及各种智能终端的普及使得个人数据无处遁形。为了应对数字时代个人数据的新挑战，并且确保欧盟规则的前瞻性。

法律规则
统一的必要性

95指令不协调和失衡的法律适用严重影响数据保护的实际效果和欧盟内的数据自由流动，公众开始普遍怀疑在线活动的安全性，数据保护法已经开始阻碍产业的成长。

技术和贸易
全球化发展需要

网络的开放性和包容性使得个人数据更加公开化和全球化，强化了自然人的数据保护权，协调了现有的各类数据保护规则，简化了跨国公司法规遵从的程序。

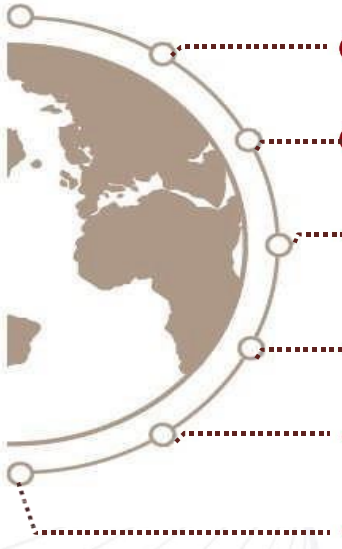
GDPR概念总结

GDPR聚焦的核心议题在于数据主体的各项权利，规则中对于数据及相关处理技术的使用加大了关注。

基于GDPR：

- **更多的企业实体将会被监管**，其中包括单纯的数据处理方及非欧盟企业实体在内
- 合规的要求将会被**扩展到隐私影响评估、隐私设计、被遗忘权、数据传输保护**等方面
- 更加严格的透明机制要求了清晰的**授权同意书及信息泄露**的通报
- 随着扩大监管力而增加的法律法**规风险**，例如：高额的罚金、集体诉讼及赔偿要求等

GDPR的关键要素：



- **被遗忘权**：客户有权要求组织删除其原始目的不再需要的个人资料
- **数据可携权**：客户有权因为变更公司而要求将他们的个人资料从一个组织转移到另一个组织，组织机构有义务帮助实现该要求
- **透明机制**：公司对于处理个人数据的授权同意书需清晰明确
- **数据泄露通报**：公司将仅有72小时向监管机构披露个人信息方面的泄露，在某些情况下会同时向受影响的个人披露
- **数据存储**：客户及监管机构有权了解所有数据存储位置
- **默认隐私设计**：组织机构将被要求尽可能减少收集和使用个人数据，并且在设计新产品和服务时，自动遵循此要求
- **数据保护责任**：GDPR强制要求按一定标准雇用数据保护官（DPO）

你是否了解

- 可高达**全球年营业额4%**的罚款
- **用户行为**的直接权利
- **72小时内**报告信息泄露
- 适用于**非欧盟企业实体**
- 对于数据的定义拓展为：
  - 原始数据
  - RFID标签
  - 虚拟匿名化数据
  - IP地址
  - Cookie缓存

GDPR合规难点

管辖广

- **欧盟企业：**设于欧盟成员国的企业均受GDPR管辖。
- **设于欧盟以外的企业：**

1. 为了向欧盟境内可识别的自然人提供商品和服务而收集、处理他们的信息；

或

2. 为了监控欧盟境内可识别的自然人的活动而收集、处理他们的信息。

注：个人信息的“ 处理” 包括：收集、储、组织、修改、恢复、使用、转移、传播、保护以及销毁等。

合规难度大

业界4大GDPR合规挑战及实施工作：

1. 研发阶段即需部署隐私保护体系（privacy by design）
2. 数据跨境传输限制（cross-border data transfer）
3. 要求实现数据在企业的全生命周期管理（data lifecycle management）
4. 涵盖合作方的数据保护责任（data processor accountability）

权利广

GDPR的监管机构 “Supervisory authority”接受关于违法的投诉后，有权 调查可能的违法情形，并进行相应的处罚， 其拥有各项权力：

- **调查权**
  1. 有权要求个人信息的“ 控制者”以及“ 处理者” 提供任何所需资料并展开调查
  2. 有权进入“ 控制者” 以及“ 处理者” 的任何营业场所，调查 其内的任何数据处理设备。
- **处罚权**
  1. 有权强制性执行暂时或永久性的限制性措施， 例如：禁止个人信息的处理；
  2. 有权强制性执行行政罚款
- **其他权力（授权、咨询等）**

违法处罚严厉

赔偿责任

1. 每个个人均拥有向GDPR监管机构 提出投诉、并获得有效的法律补偿方法的权利。
2. 由于违反GDPR相关规定而导致个 人受到严重的或其他不同程度的损失，该个人有权向企业获取相关赔偿。如果个人信息的处理涉及多家企业或组织。每家企业均有责任赔偿该个人的相关损失。

最大处罚金额：根据所触犯条款的不同，GDPR设置了两个阶段的最大处罚金额，分别为：

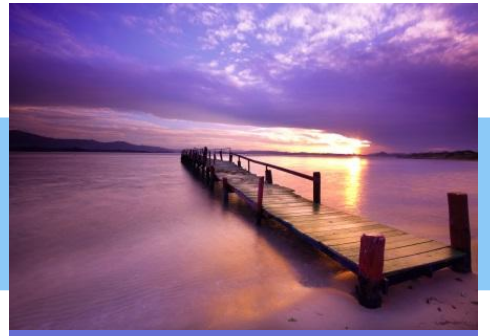
3. 最大处罚金额1000万欧元或是企业全球年度收入的2%（**选其中较高的数字**）；
4. 以及最大处罚金额2000万欧元或是企业全球年度收入的4%（**选其中较高的数字**）

案例分享-某电动车制造商GDPR合规需求分析

企业出海规划

背景介绍：

- 中国内智能电动车制造业
- 产品出口至几个欧盟国家
- 自行车有定位芯片，提供服务
- 车主需要注册并收集个人信息
- 由经销商进行销售，收集注册信息
- 计划在德国开设分公司



合规需求分析

合规需求：

- 公司组织架构规划（分公司/独立）
- 隐私保护监管机构（德国哪州监管）
- IT架构设计（机房选址/应用架构）
- 保护组织确定（隐私保护职责）
- 隐私保护政策确定
- 领导力、支持、沟通、资源

合规风险评估

风险评估：

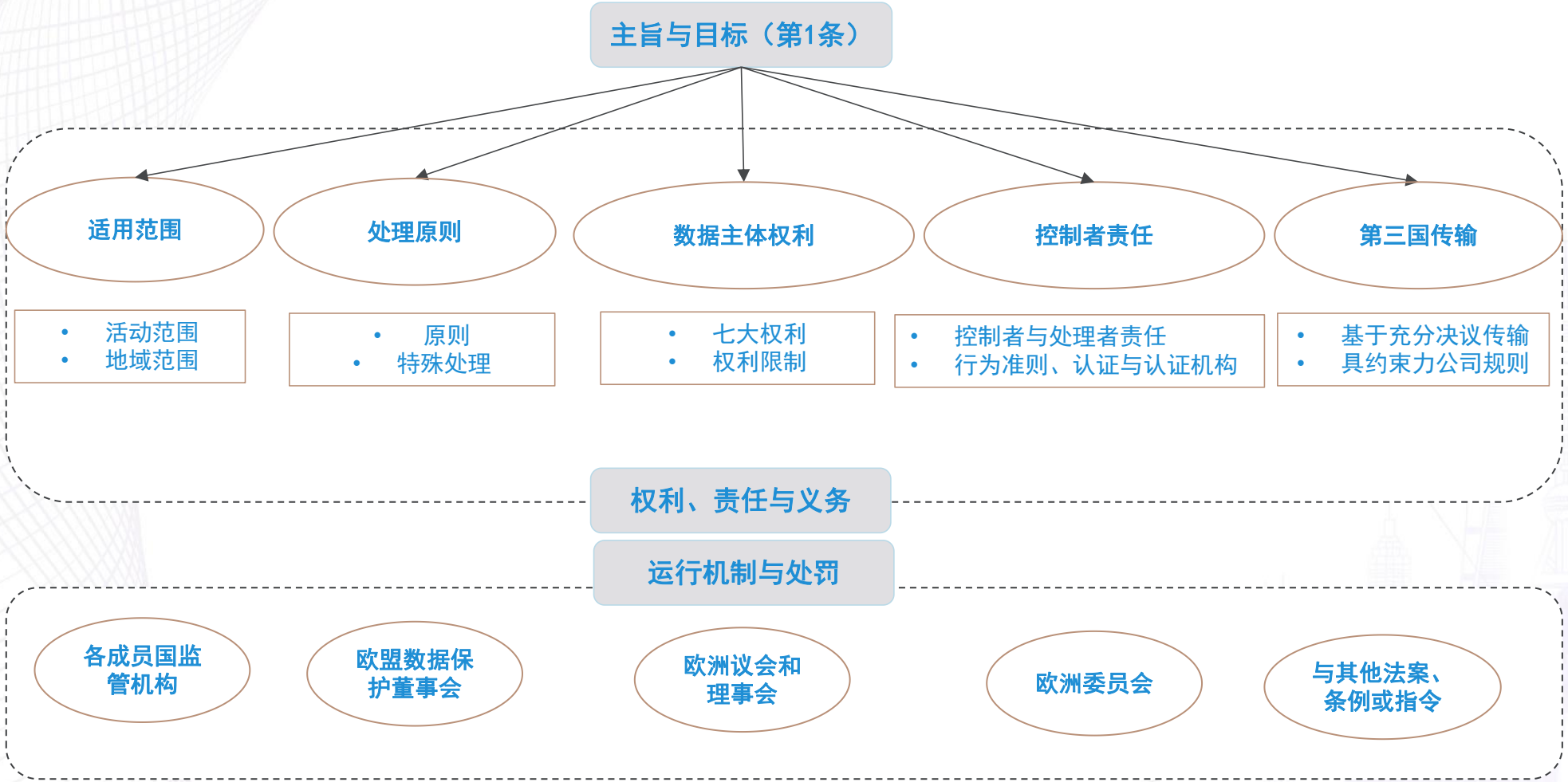
- 构建风险评估实施环境（参考标准、接受标准等）
- 隐私保护默认设计
- 隐私数据资产识别、形成清单
- 隐私数据威胁及脆弱性分析
- 隐私风险计算及处置建议

数据处理规则

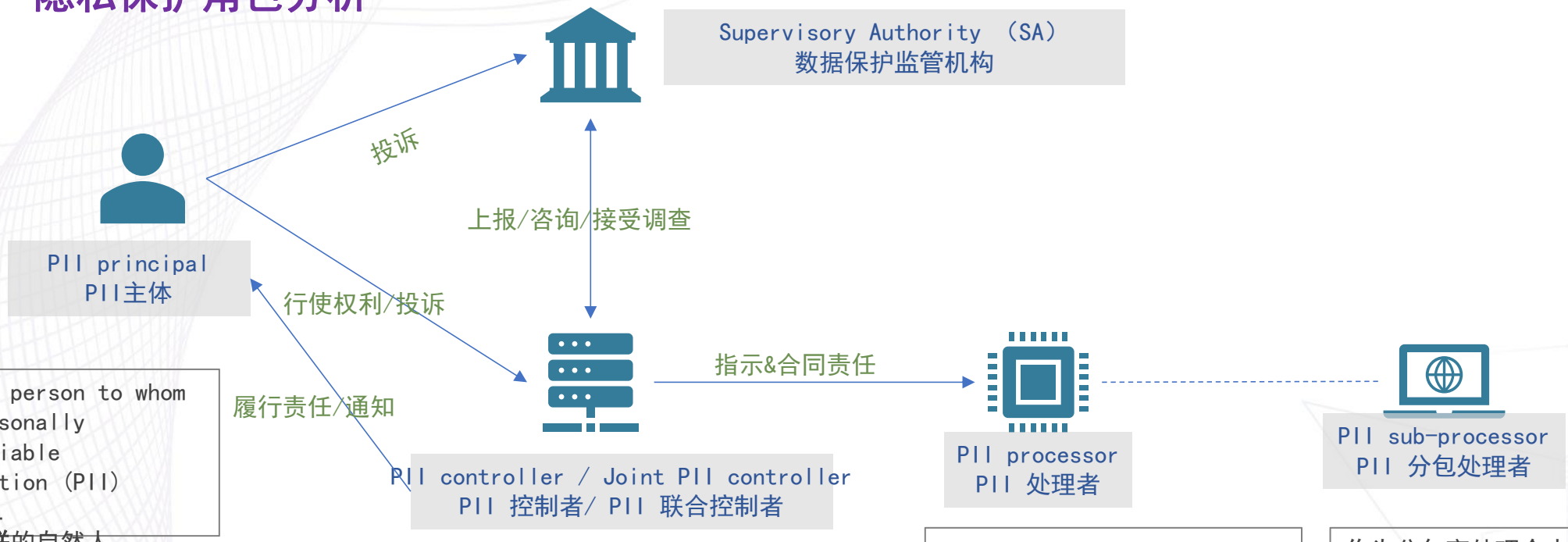
隐私规则：

- 隐私保护意识培训
- 数据采集和传输
- 数据保存及使用
- 数据共享（BI数据分析脱敏）
- 隐私泄露通报流程
- 日常运维操作

企业出海GDPR合规分析



隐私保护角色分析



Natural person to whom the personally identifiable information (PII) relates.
PII 关联的自然人

Privacy stakeholder (or privacy stakeholders) that determines the purposes and means for PII other than natural persons who use data for personal purposes.
PII 控制者： 决定PII处理目的和方法的**隐私权利益相关方**。
因个人目的使用数据的自然人不在此列。

PII controller that determine the purposes and means of the processing of PII jointly with one or more other PII controllers.
PII 联合控制者：与一个或多个其他的PII控制者**共同决定PII处理目的和处理方法**的PII控制者。

Sometimes instructs others to process PII on its behalf while the responsibility for the processing remains with the PII controller.
有时会指示其他PII处理者，代表PII控制者处理PII，但**责任仍归属与PII控制者**。

Privacy stakeholder that processes PII on behalf of and in accordance with the instructions of a PII controller.
代表PII控制者，并按PII控制者的指示对PII进行处理的隐私权利益相关方。

作为分包商处理个人数据的PII处理者。

隐私保护政策设计

政策内容

- 解释为什么需要的正当性
- 策略涵盖哪些主题和范围
- 采取的保护措施及方式
- 联系人的定义及其职责
- 违规处理的程序
- 数据主体的权利保障

默认设计

- 主动而不是被动;预防而不是补救
- 作为默认设置的隐私
- 设计中的隐私嵌入
- 全功能性——正和，而非零和
- 端到端安全性——全生命周期保护
- 可见性和透明度——保持开放
- 尊重用户隐私——以用户为中心

隐私政策

数据保护隐私政策的主要目的是就企业对个人数据的收集、使用、处理、披露、监视等方面的数据隐私事宜，提供通用准则。

SDLC + Privacy by Design

需求评审，商业论证
隐私与安全合规评审

需求分析与设计
隐私与安全需求分析
隐私与安全设计检查

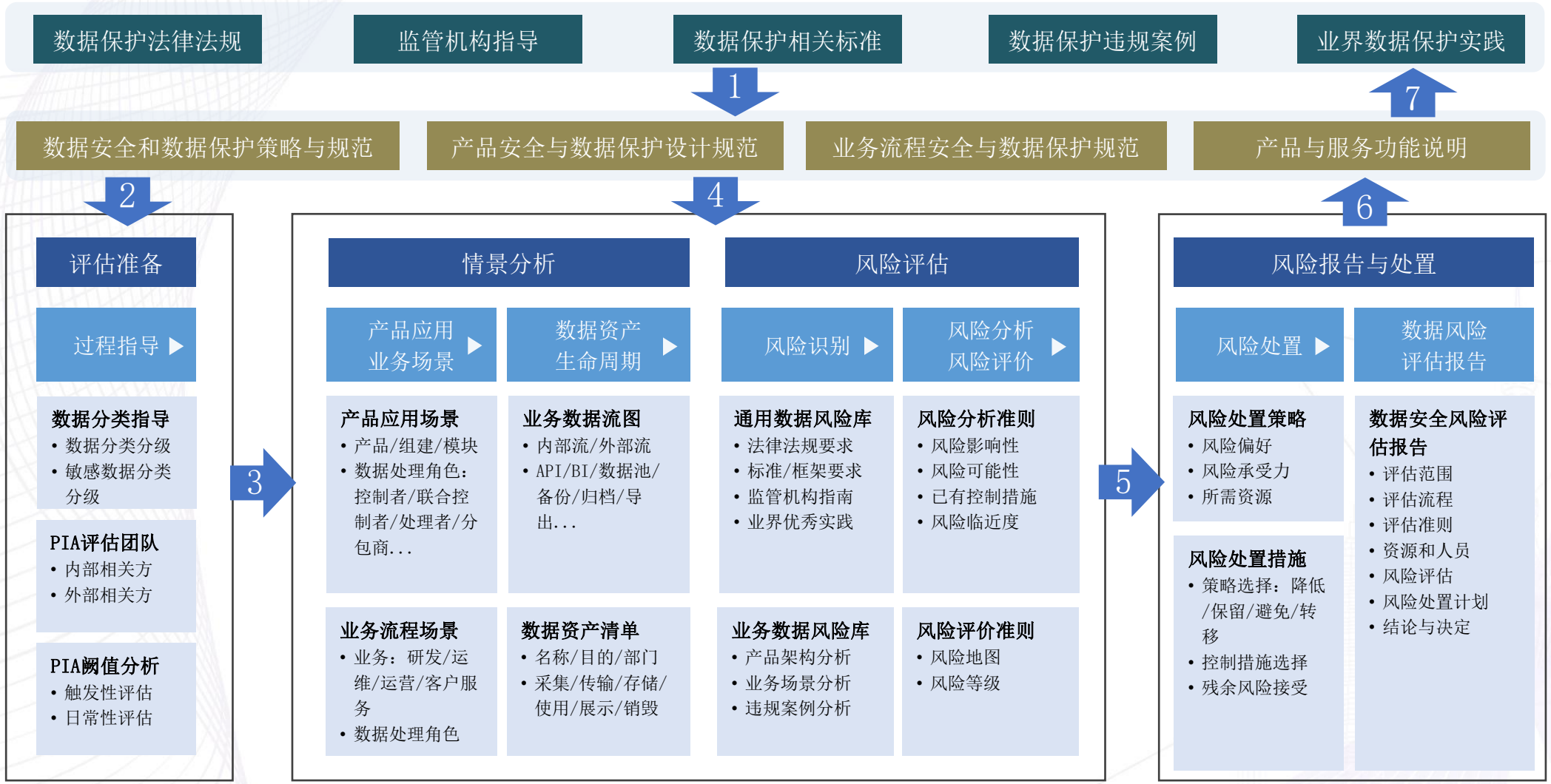
代码编码开发设计
隐私增强技术
隐私功能实现
安全编码规范
代码白盒检测

软件功能测试
隐私与安全功能测试

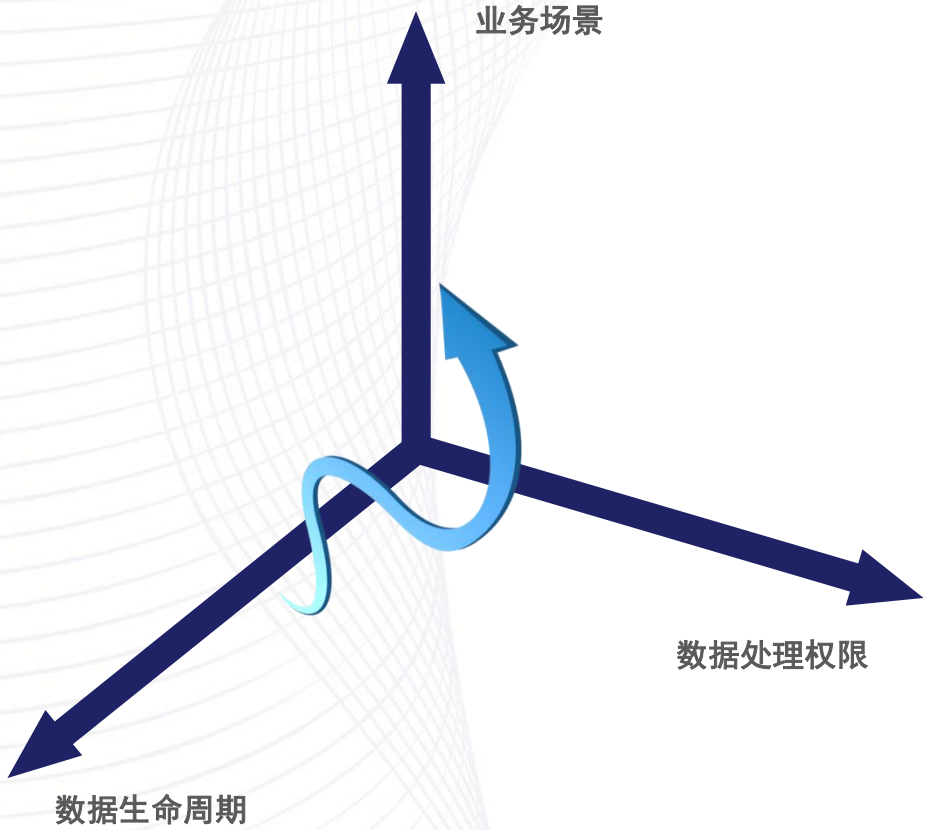
软件发布上线
安全黑盒测试
隐私合规测试
隐私合规评审
隐私政策更新

软件持续运行
持续安全检测
持续合规评估

隐私保护影响评估DPIA



隐私保护业务数据流梳理



业务场景：

1. 公司有哪些*业务场景（产品/服务、业务流程、信息系统/功能模块）*？
2. 上述业务场景中的*数据处理目的*是什么？
3. 适用哪些*法律法规、监管条例、合同要求*？

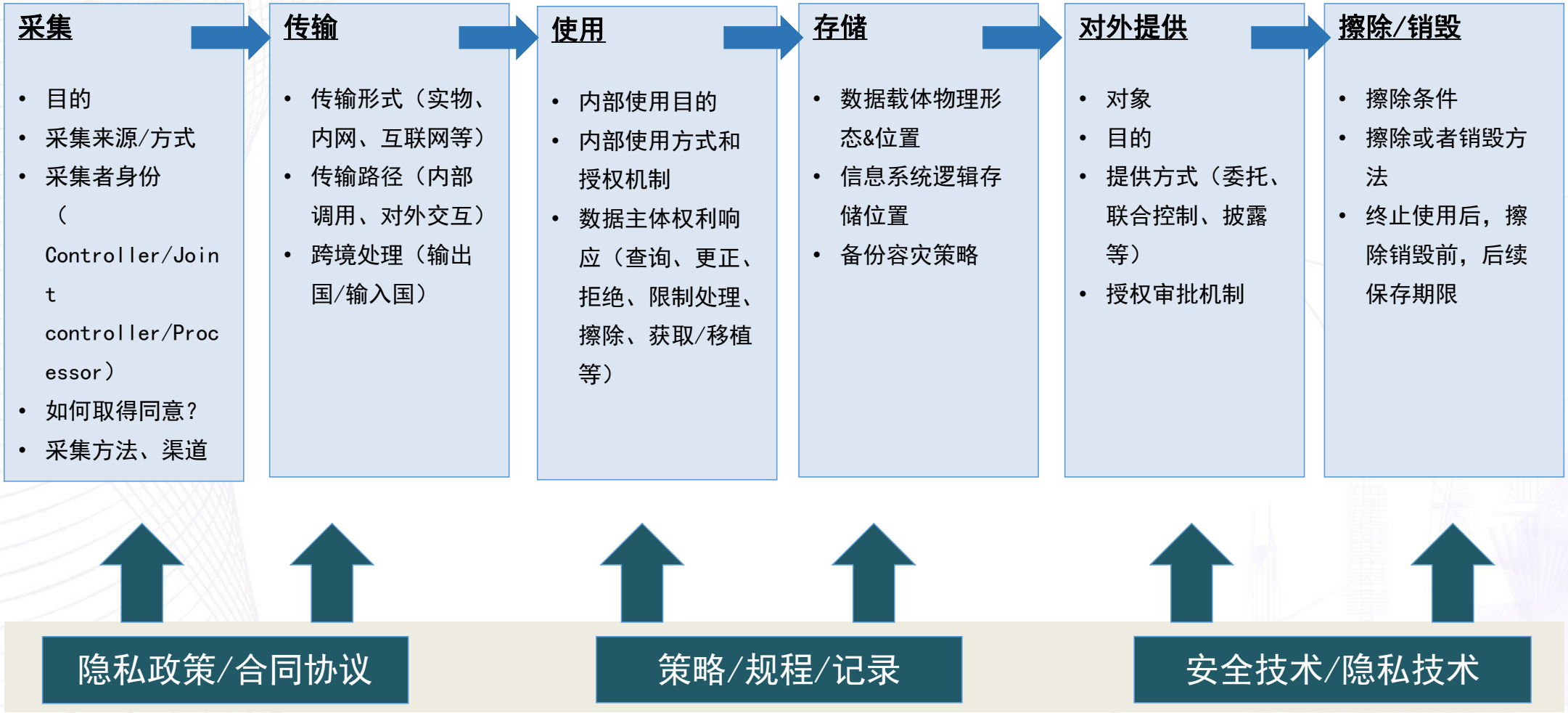
数据处理权限：

1. 各业务场景下的数据处理身份和责任？
2. 各身份和责任的权限控制？

数据生命周期：

1. 业务场景中收集处理哪些核心数据？
2. 对核心数据的分类分级，分级分类的标准？
3. 各业务场景下，在组织内部，数据流向是怎样的？数据责任者是谁？

隐私保护全生命周期管理



隐私保护相关注意点

- 用户身份验证
- 信息屏蔽或脱敏
- 查询限制和审计

信息展示

- 安全影响评估
- 数据保护责任
- 信息脱敏处理
- 防泄漏监控
- 信息监控和审计
- 导出操作访问控制
- 导出通讯安全
- 导出过程审核和记录

共享和转让

- 安全影响评估
- 披露情况记录

公开披露

- 主体授权同意
- 安全影响评估
- 处理过程记录
- 信息脱敏处理
- 对受委托者进行监督审计
- 对接入工具进行技术监测

委托处理

- 信息清洗和转换过程保护
- 加工后重新识别风险
- 加工记录防止泄露
- 信息滥用监控
- 处理操作的记录

加工处理

- 超范围后取得主体同意
- 汇聚融合后的安全影响评估

汇聚融合

- 环境隔离
- 测试脱敏

开发测试

收集

- 明确收集方案
- 信息来源可溯
- 隐私政策查阅

传输

- 链路加密
- 数据加密
- 身份认证
- 传输完整性校验

存储

- 数据防泄漏
- 存储加密
- 逻辑隔离
- 数据清除

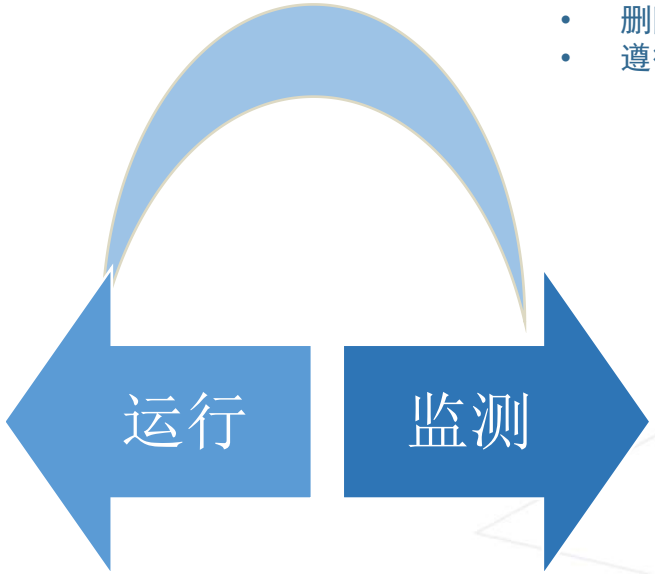
使用

删除

- 数据保存的期限
- 删除后不被访问
- 遵循法律法规要求

销毁

- 销毁过程监督与控制
- 销毁过程记录
- 介质销毁处理
- 信息销毁处理
- 云环境数据清除



- WEB系统安全评估
- 客户端评估
- 开发SDK评估
- 网络基础架构安全
- WEB应用防护
- WEB实时安全监测

- 数据操作审计
- 系统日志审计
- 恶意代码监测
- 网络流量安全监控
- 异常流量监测分析
- 安全事件应急响应

构建隐私保护管理体系PIMS

方针、策略、目标

个人隐私数据保护策略
（方针、目标、准则、原则）

参考ISO/IEC27701：2019

制度、办法、规范

- ✓ 个人隐私数据分类分级管理制度
- ✓ 个人隐私数据生命周期管理制度
- ✓ （收集，传输，存储，使用，删除，销毁）
- ✓ 信息系统分级授权管理制度
- ✓ 个人隐私数据脱敏管理制度
- ✓ 个人隐私数据安全影响评估制度
- ✓ 外包服务机构与外部合作机构管理制度
- ✓ 个人隐私数据安全检查与监督制度
- ✓ 个人隐私数据投诉与申诉处理制度
- ✓ 人员及岗位安全管理制度
- ✓ 人员、岗位、保密管理制度
- ✓ 安全培训及考核管理制度

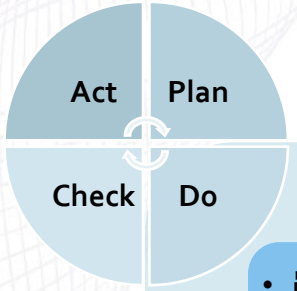
操作流程、实施细则

- ✓ 个人隐私数据生命周期各阶段管理操作流程
- ✓ 个人隐私数据脱敏管理流程
- ✓ 个人隐私数据安全影响评估实施细则
- ✓ 信息系统安全评估实施细则
- ✓ 个人隐私数据投诉与申诉处理流程
- ✓ 安全事件处置流程和应急预案
- ✓ 个人信息保护隐私政策
- ✓ 人员入职、离职、离岗流程
- ✓ 安全手册、培训文档

隐私数据保护建设蓝图


隐私信息防护体系框架
策略
隐私信息保护策略
隐私信息保护准则
方针、目标和原则
组织架构制度体系
隐私信息保护组织架构及职责
隐私信息保护制度体系
防护体系运行
人员、岗位、保密安全管理
分类分级管理
投诉与申诉管理
生命周期管理
系统分级授权管理
数据脱敏管理
安全事件处置管理
外包服务机构与外部合作机构管理
安全培训及考核管理
安全检查及监督管理
传输存储加密
信息显示屏蔽
数据脱敏
信息销毁
环境隔离
基础网络安全
WEB防护
主机安全防护
数据防泄漏
数据库审计
恶意代码监测
身份认证
访问策略
权限控制
流量监控
日志记录
操作审计
物理访控
分级分类
信息收集
信息传输
信息存储
信息使用
信息删除
信息销毁
大数据安全智能分析
综合审计分析
威胁预警、流量安全监测分析
安全应急响应
评估改进
隐私信息安全影响评估
系统安全检查或评估
隐私信息安全合规评估
信息泄露事件后的安全检查与评估
隐私安全管理体系
治理终端
治理系统
治理网络
治理数据
管理人员
内外部机构外联
法律和

隐私数据保护意识培训



Plan：根据安全意识现状设计意识宣惯和推广方案

Do：按计划实施意识宣惯和推广方案

Check：进行意识推广绩效评价，分析总结

Act：采取后续措施，继续推广意识持续提升

现场培训学习

- 员工信息安全意识培训
- 安全专员引导性培训
- 案例分析学习等

在线教育考试

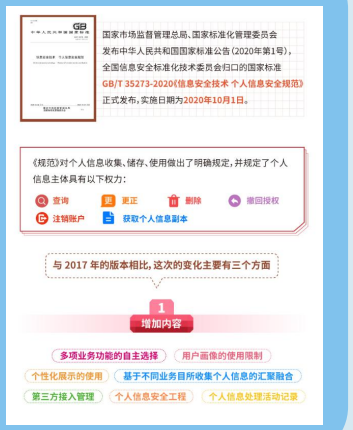
- 信息安全知识库构建
- 在线学习
- 在线考试

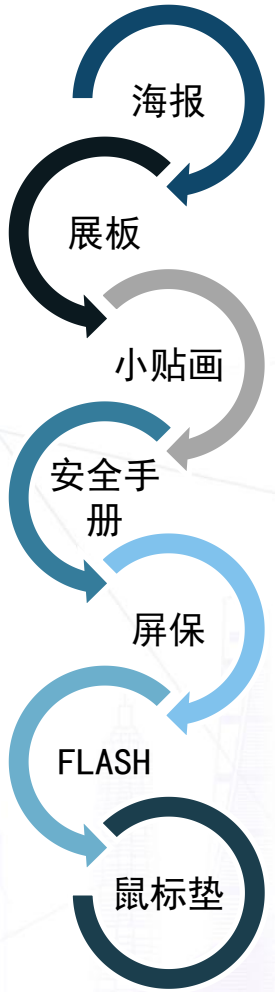
多媒体推广

- 影视大片
- 新闻视频
- 媒体消息
- 屏幕保护
- Flash短片
- 电子期刊

立体方式宣传

- 大型海报
- 小招贴画
- 桌面帖示
- 实物招贴
- 台历挂历
- 鼠标垫
- 宣传手册





管理类
意识宣传

技能类
技能宣传

意识类
培训宣传

某电动车制造商GDPR合规建设里程碑

Value

第一阶段：6个月左右
构建隐私信息合规环境

目标：结合法律法规要求，建构隐私信息合规环境。
- 识别欧盟主要法律法规标准GDPR规范要求。
- 对GDPR要求进行解读，并结合ISO/IEC 27701要求。
- 公司架构设计，德国为独立分公司运作。
- 确定德国主监管机构为巴伐利亚州。
- 应用APP确定为德国微软云平台架构，构建Saas服务。
- 确定隐私政策内容，并进行细化。
- 确定DPO本地人选，并建立隐私保护管理机构。
- 进行隐私保护正式立项，并提供资金等资源。

第二阶段：1年左右
隐私保护默认设计及风险评估

目标：结合GDPR合规要求进行业务流程默认设计及隐私保护影响评估，识别风险并为后续整改提供依据。
- 识别企业的业务流程，标记各环节设及的隐私信息。
- 构建隐私保护风险环境（参考标准、接受标准等）。
- 构建欧盟版APP业务，将隐私默认设计嵌入。
- 绘制隐私数据DataFlow数据流。
- 对PII数据基于数据流生命周期的风险评估。
- 识别和描述PII会员信息的风险， 进行风险计算。
- 制定风险处置控制措施以及风险处置计划。

第三阶段：1年左右
隐私保护体系建设

目标：结合风险评估内容，进行控制措施增强，并建立隐私保护管理体系，进行全员意识培训。
- 按风险处置计划进行增强控制。
- 进行隐私保护风险再评估，验证控制措施的有效性。
- 构建隐私保护管理体系PIMS。
- 进行全员隐私保护意识培训，并定期考核。
- 取得ISO/IEC 27701证书，标准为UKAS。
- 构建隐私保护全生命周期蓝图。

持续进行信息安全建设：日常

定期进行隐私保护维护建设，包括定期安全评估、安全基线检查，安全应急演练，安全漏洞扫描，安全巡检，应用系统安全渗透测试等，进行全员信息安全意识教育培训。

Innovation

DXCon 2021

国际数字化转型最佳实践管理峰会

– 4月16日•上海 –

Thanks

感 谢 聆 听

主办方: EXIN BEST PRACTICE