Deloitte.
德勤

# 欧盟GDPR
# 对企业的影响及隐私与安全保护应对

# 目录 / CONTENTS


PART 01

**隐私相关信息解读**

- 什么是隐私
- 什么是GDPR

PART 02

**如何满足GDPR**

- GDPR业务影响
- 符合GDRP的机制

# 何为隐私?

## 隐私资料是一个非常广的概念:

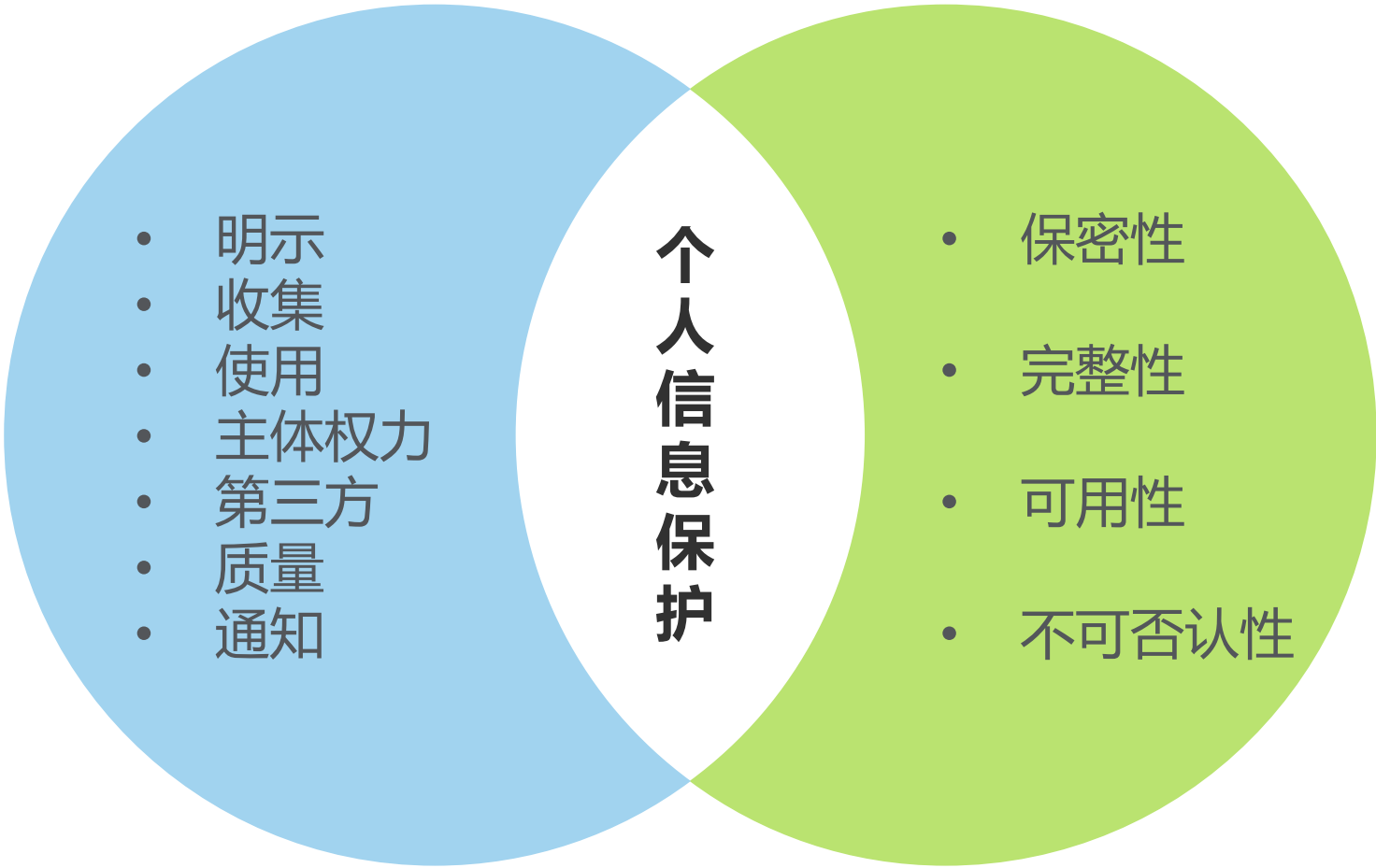
只要是任何信息可以直接识别或间接识别到一自然人，如:

- 基本的身份信息，如姓名、地址和身份证号码等;
  (不论员工、客户、供应商或代理商)
- 网络数据，如位置、IP地址、Cookie数据和IMEI等;
- 医疗保健和遗传数据;
- 生物识别数据，如指纹、虹膜等;
- 种族或民族数据;
- 政治观点、性取向。


**基本原则为**
**只要能直接识别或间接识别到个人皆属隐私资料!**

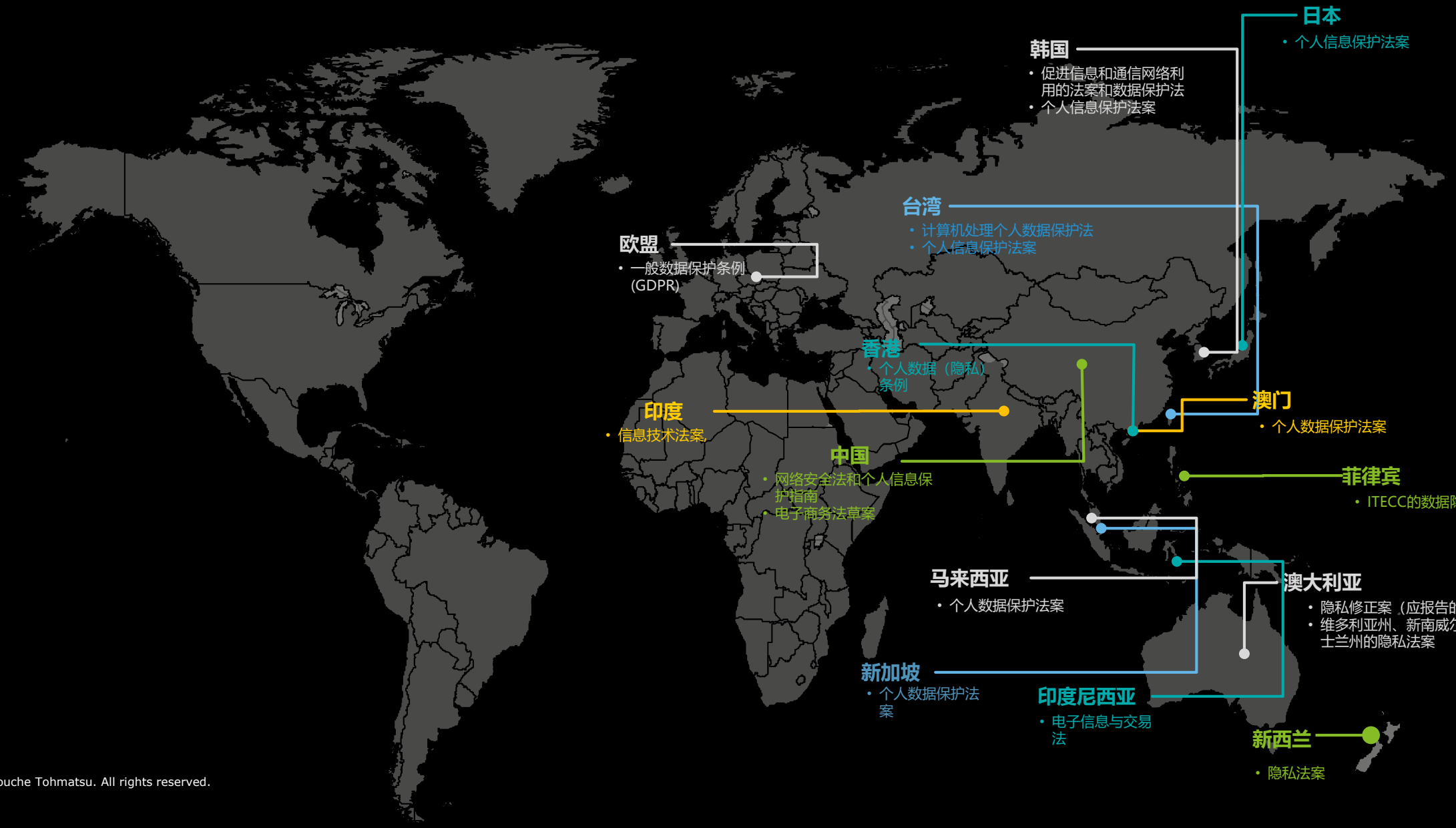
# 隐私与数据的有何区别?

对个人信息的合法使用




对数据的保护

# 数据隐私 趋紧



# GDPR条文要览

一、定义了条例范围、目的及名词解释

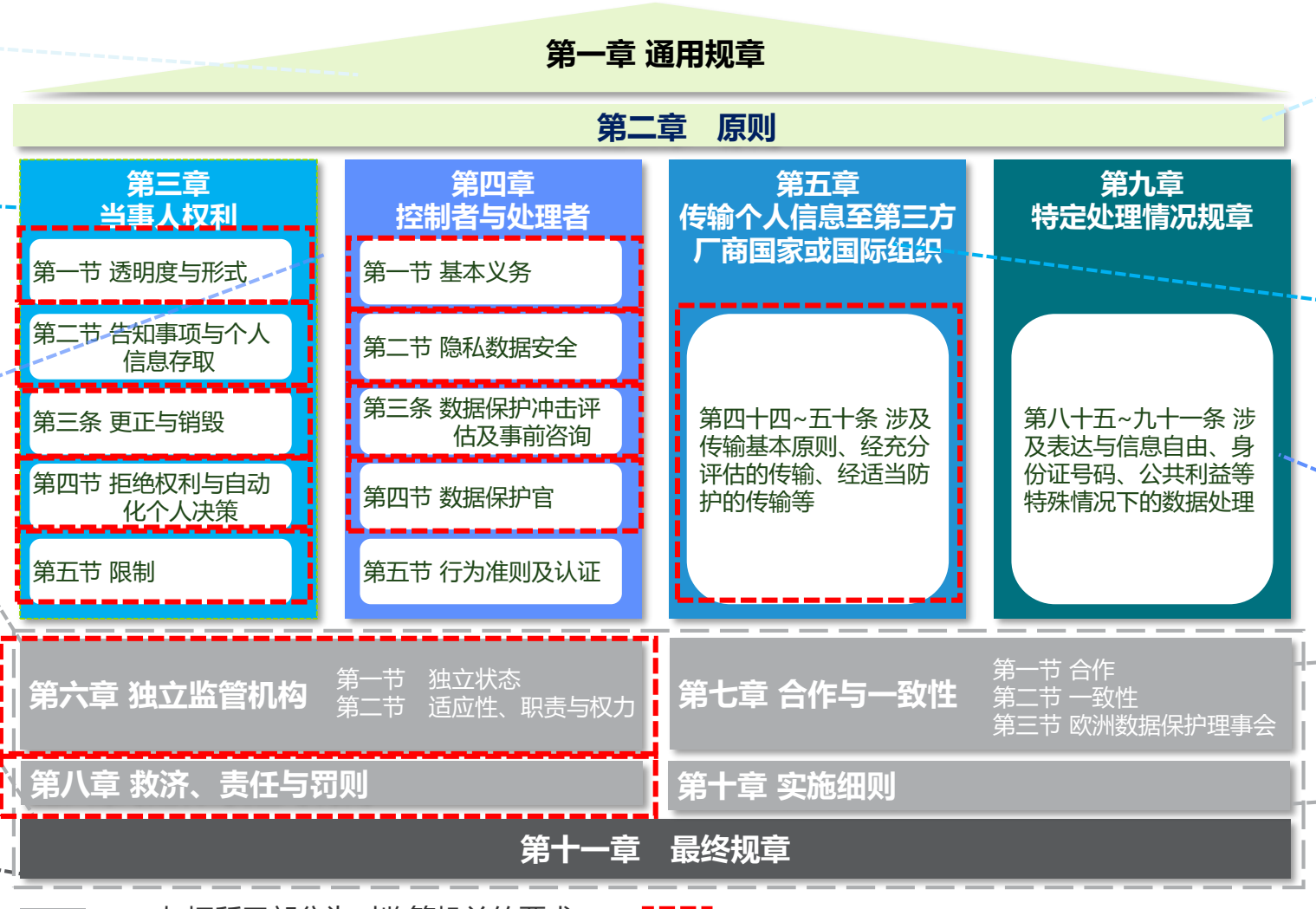
三、介绍当事人可行使的权利内容及要求

四、介绍当事人可行使的权利内容及要求

六、对监管机构的独立性要求及权责说明

八、监管机关对数据主体申诉的处理

十一、法规的废止与生效




二、1）定义了个人数据处理的基本原则，如最小搜集原则；2）处理的合法性规定，如获取当事人同意；3）特殊类型个人数据处理

五、介绍对于个人数据传输至第三国的要求

九、介绍特殊情况下数据处理的规定

七、监管机关间的合作及争议解决等管理办法

十、法规授权

❖ 灰框所示部分为对监管机关的要求

❖ **为GDPR项目实施过程中的主要关注重点内容，也是数据处理者和数据所有者的主要关注内容**

# 目录 / CONTENTS


PART 01
**隐私相关解读**

- 什么是隐私
- 什么是GDPR

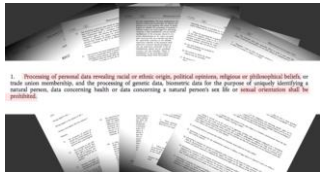
PART 02
**如何满足GDPR**

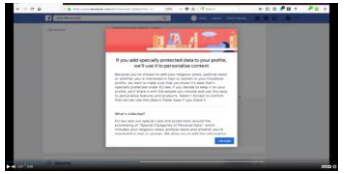
- GDPR的业务影响
- 符合GDRP的机制

# GDPR不合规的影响冲击和影响

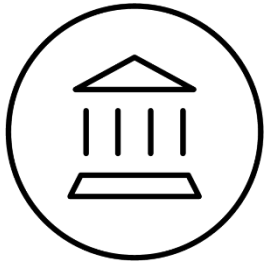
| 事件概述 | 影响冲击 | GDPR核心要求及应对措施 |
| --- | --- | --- |
| 时间：2018.5.25<br>企业：Facebook、谷歌<br><br>“Noyb.eu”对Facebook和Google发起4项投诉。<br>指控其**强迫用户同意共享个人数据。**<br><br>• 针对Google的Android系统向法国监管机构CNIL投诉：37亿欧元<br>• 针对Facebook旗下Instagram向比利时监管机构DPA投诉：13亿欧元<br>• 针对Facebook旗下Whats App德国监管机构HmbBfDI投诉：13亿欧元<br>• 针对Facebook向奥地利监管机构DSB进行投诉：13亿欧元 | **巨额罚款：**<br><br>如果欧洲监管机构同意诉讼，Facebook、Google将分别面临着39亿欧元和37亿欧元（共计约88亿美元）的罚款 | **核心要求：告知及当事人同意**<br><br>GDPR要求中规定，从用户处收集的任何个人数据，必须要有数据主体的同意和合法的使用理由，用户可以选择拒绝同意及随时撤销同意。<br><br>**应对措施：**<br><br>• Facebook CPO(首席隐私官)声称已开发引入升级工具，以便用户访问、下载、删除其个人数据；<br>• 新的工具平台允许用户“不同意”facebook在官网或其他网站对个人行为进行“碎片化搜集”并推断个人 |











## GDPR相关条款：

- 第6条 第7条 如数据主体通过书面声明的方式作出同意，且书面声明涉及其他事项，那么同意应以易于理解且与其他事项显著区别的形式呈现。构成违反本法的声明的任何部分，均不具约束力。
- 第83条 受到行政罚款最高2000万欧元，或根据企业具体情况，占前一个财政年度全球年营业额的4%，以较高者为准：(a)根据第5, 6, 7条和第9条处理的基本原则，包括取得用户同意；

# GDPR合规应对

## GDPR《一般数据保护条例》

| | | | | |
|---|---|---|---|---|
| 当事人权利 | 同意和告知 | 默认的隐私保护（PBD） | 第三方服务提供商管理 | 数据安全与处理活动记录 |
| 信息泄漏通知 | 隐私保护影响评估（DPIA） | 数据保护官（DPO） | 跨境数据传输 | 救济、责任与罚则 |

- **GDPR实施指南**
  - ✓ wp259-_rev.01：同意
  - ✓ wp251：自动化决策和用户画像
  - ✓ Wp250：个人数据泄露通知
  - ✓ WP248：隐私保护影响评估
  - ✓ WP243：数据保护官
  - ✓ WP242 _rev.01:数据可携权

## 隐私保护体系框架

| | | | | | | |
|---|---|---|---|---|---|---|
| 隐私数据收集同意告知机制 | 隐私保护影响评估机制 | 默认的隐私保护设计管理机制 | 当事人权利行使机制 | 第三方供应商安全管理机制 | 隐私数据跨境传输机制 | 隐私事件应变处理机制 |

隐私数据管理

**应对方案**

| 隐私数据收集同意告知机制 | 隐私保护影响评估机制 | 默认的隐私保护设计管理机制 | 当事人权利行使机制 | 第三方供应商安全管理机制 | 隐私数据跨境传输机制 | 隐私事件应急处理机制 |
|---|---|---|---|---|---|---|
| • 评估收集的目的及合法性；<br>• 设计隐私声明告知和同意方式<br>• 调整/优化系统和产品功能 | • 确定DPIA执行时机和执行范围<br>• 开展隐私影响评估<br>• 制定和落实风险改善建议和计划 | • 系统/产品开发的需求分析阶段嵌入适用隐私保护需求或<br>• 系统/产品开发的测试阶段验证隐私保护需求的实现。 | • 落实隐私权行使流程<br>• 配置权利请求受理、处理岗位<br>• 调整/优化系统及产品功能<br>• 加强第三方供应商管理，协同处理权利请求 | • 对受委托的第三方单位开展隐私保护评估<br>• 合同管理<br>• 管理第三方单位对个人数据的访问、处理 | • 确定隐私数据跨境涉及的业务场景及接受方；<br>• 分析适用的合法跨境传输依据<br>• 签署标准合同条款（SCC）或<br>• 申请有约束力的公司规则(BCRS) | • 落实和优化应急处理流程<br>• 加强与主管机关的联系<br>• 定期开展应急演练<br>• 加强员工隐私安全培训 |

持续的隐私安全评估和检查

**跨部门团队协同合作（包括业务、安全、法务、系统团队、大数据团队、产品和服务开发等）**

# GDPR合规应对措施概览


1- 专业团队

2- 隐私运营

3- 工具平台

# 隐私保护管理的组织架构

GDPR的合规落地，涉及到从**产品界面到后端数据库、再到制度流程**的全面排查和改造，需要跨部门团队协同合作。为了确保组织隐私保护体系的持续有效运行，组织需要**设置隐私保护架构和岗位**，以便在高级管理层的领导下，有效地推动隐私保护工作的落地和优化。

Deloitte.

肖腾飞
德勤中国网络安全服务合伙人
电话：13581962223
邮件：frankxiao@deloitte.com