

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GDPR的机制

何为隐私？

隐私资料是一个非常广的概念：

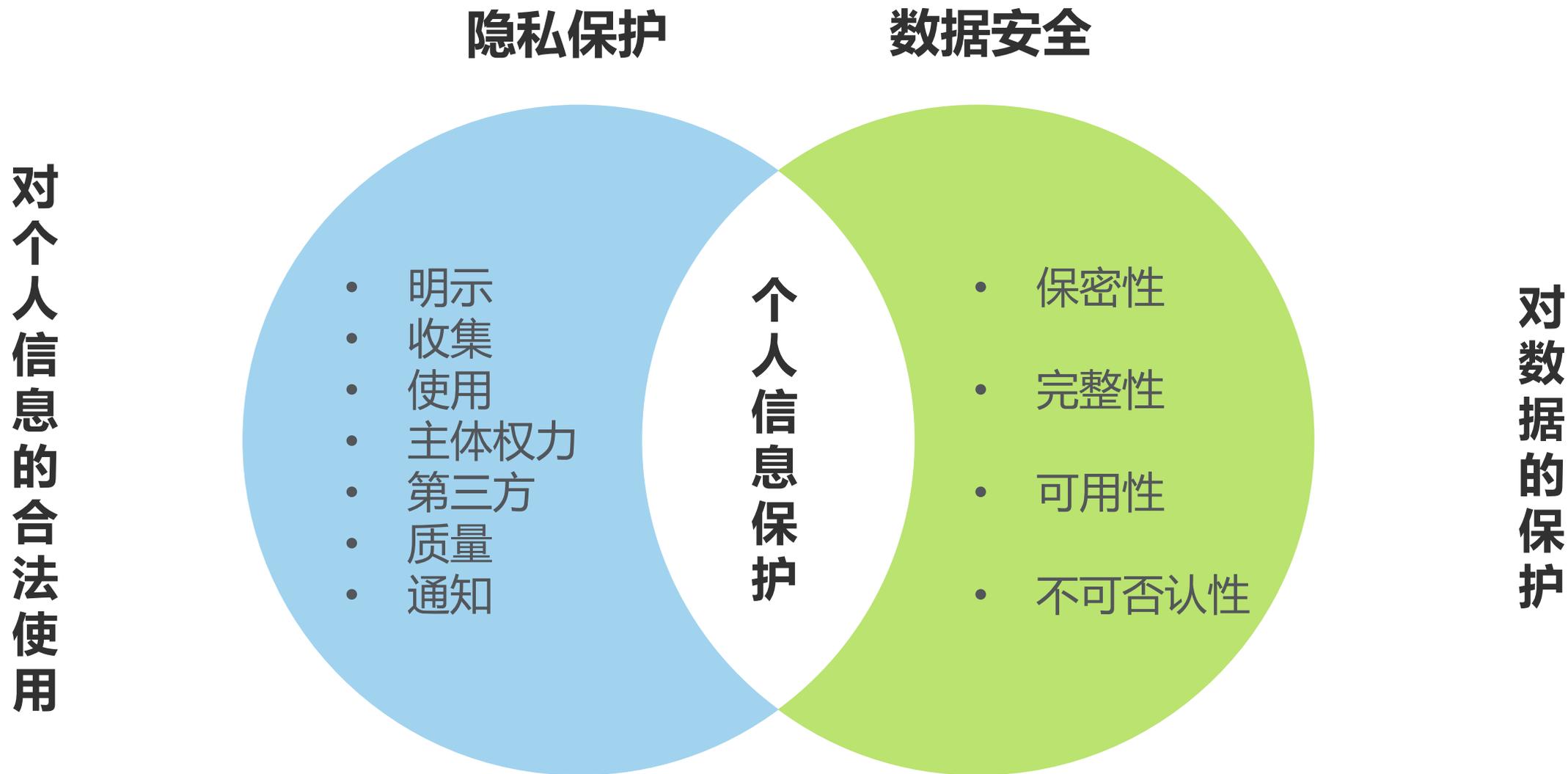
只要是任何信息可以直接识别或间接识别到一自然人，如：

- 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。

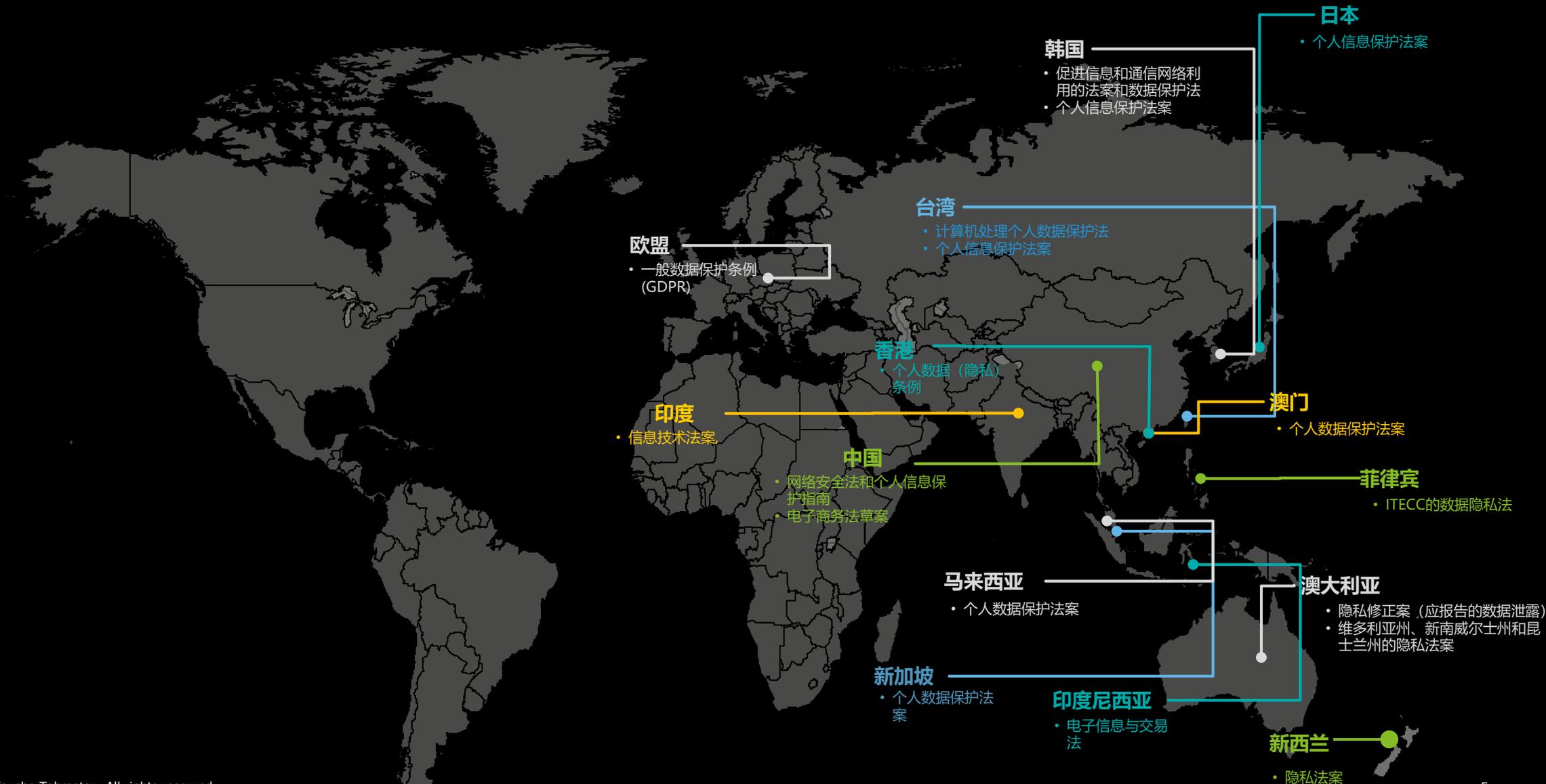
姓名	指纹、虹膜	信用卡卡号/支付宝账号	儿童个人信息
生日	婚姻状态	社会活动	宗教信仰
身份证号码	家庭情形	应用使用纪录	政治观点
护照号码	教育状态	账户活动	基因数据
联络信息	职业	违法犯罪信息	性生活

**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?



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

第一章 通用规章

第二章 原则

第三章 当事人权利

第一节 透明度与形式

第二节 告知事项与个人信息存取

第三节 更正与销毁

第四节 拒绝权利与自动化个人决策

第五节 限制

第四章 控制者与处理者

第一节 基本义务

第二节 隐私数据安全

第三节 数据保护冲击评估及事前咨询

第四节 数据保护官

第五节 行为准则及认证

第五章 传输个人信息至第三方厂商国家或国际组织

第四十四~五十条 涉及传输基本原则、经充分评估的传输、经适当防护的传输等

第九章 特定处理情况规章

第八十五~九十一条 涉及表达与信息自由、身份号码、公共利益等特殊情况下的数据处理

第六章 独立监管机构

第一节 独立状态
第二节 适应性、职责与权力

第七章 合作与一致性

第一节 合作
第二节 一致性
第三节 欧洲数据保护理事会

第八章 救济、责任与罚则

第十章 实施细则

第十一章 最终规章

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构的要求

❖ 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

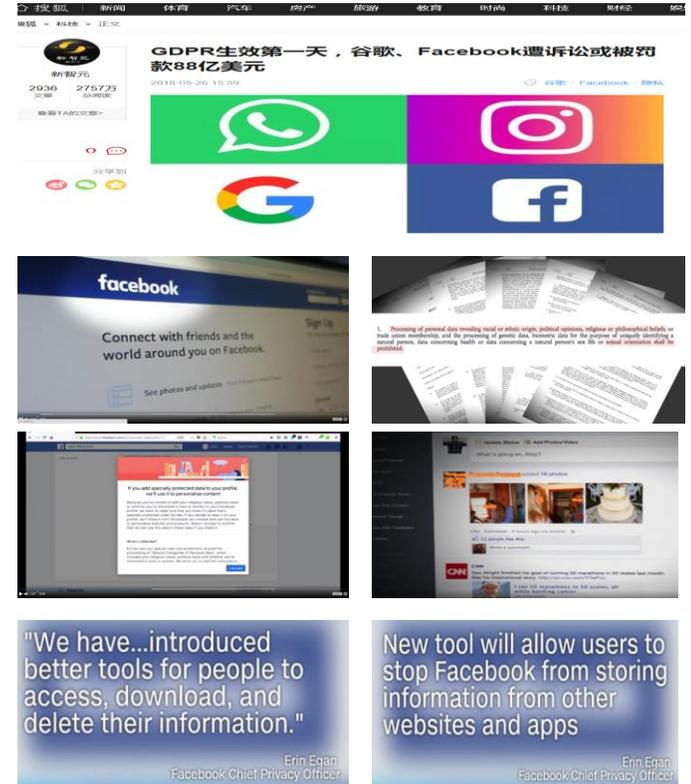
- 什么是隐私
- 什么是GDPR

PART 02 如何满足GDPR

- GDPR的业务影响
- 符合GDPR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
<p>时间：2018.5.25 企业：Facebook、谷歌</p> <p>“Noyb.eu”对Facebook和Google发起4项投诉。指控其强迫用户同意共享个人数据。</p> <ul style="list-style-type: none"> 针对Google的Android系统向法国监管机构CNIL投诉：37亿欧元 针对Facebook旗下Instagram向比利时监管机构DPA投诉：13亿欧元 针对Facebook旗下Whats App德国监管机构HmbBfDI投诉：13亿欧元 针对Facebook向奥地利监管机构DSB进行投诉：13亿欧元 	<p>巨额罚款：</p> <p>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</p>	<p>核心要求：告知及当事人同意</p> <p>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。</p> <p>应对措施：</p> <ul style="list-style-type: none"> 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； 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	隐私事件应急处理机制
--------------	------------	---------------	-----------	--------------	------------	------------

应对方案

隐私数据管理

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
<ul style="list-style-type: none"> • 评估收集的目的及合法性; • 设计隐私声明告知和同意方式 • 调整/优化系统和产品功能 	<ul style="list-style-type: none"> • 确定DPIA执行时机和执行范围 • 开展隐私影响评估 • 制定和落实风险改善建议和计划 	<ul style="list-style-type: none"> • 系统/产品开发的需求分析阶段嵌入适用隐私保护需求或 • 系统/产品开发的测试阶段验证隐私保护需求的实现。 	<ul style="list-style-type: none"> • 落实隐私权行使流程 • 配置权利请求受理、处理岗位 • 调整/优化系统及产品功能 • 加强第三方供应商管理, 协同处理权利请求 	<ul style="list-style-type: none"> • 对受委托的第三方单位开展隐私保护评估 • 合同管理 • 管理第三方单位对个人数据的访问、处理 	<ul style="list-style-type: none"> • 确定隐私数据跨境涉及的业务场景及接受方; • 分析适用的合法跨境传输依据 • 签署标准合同条款 (SCC) 或 • 申请有约束力的公司规则 (BCRS) 	<ul style="list-style-type: none"> • 落实和优化应急处理流程 • 加强与主管机关的联系 • 定期开展应急演练 • 加强员工隐私安全培训

持续的隐私安全评估和检查

跨部门团队协作合作 (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

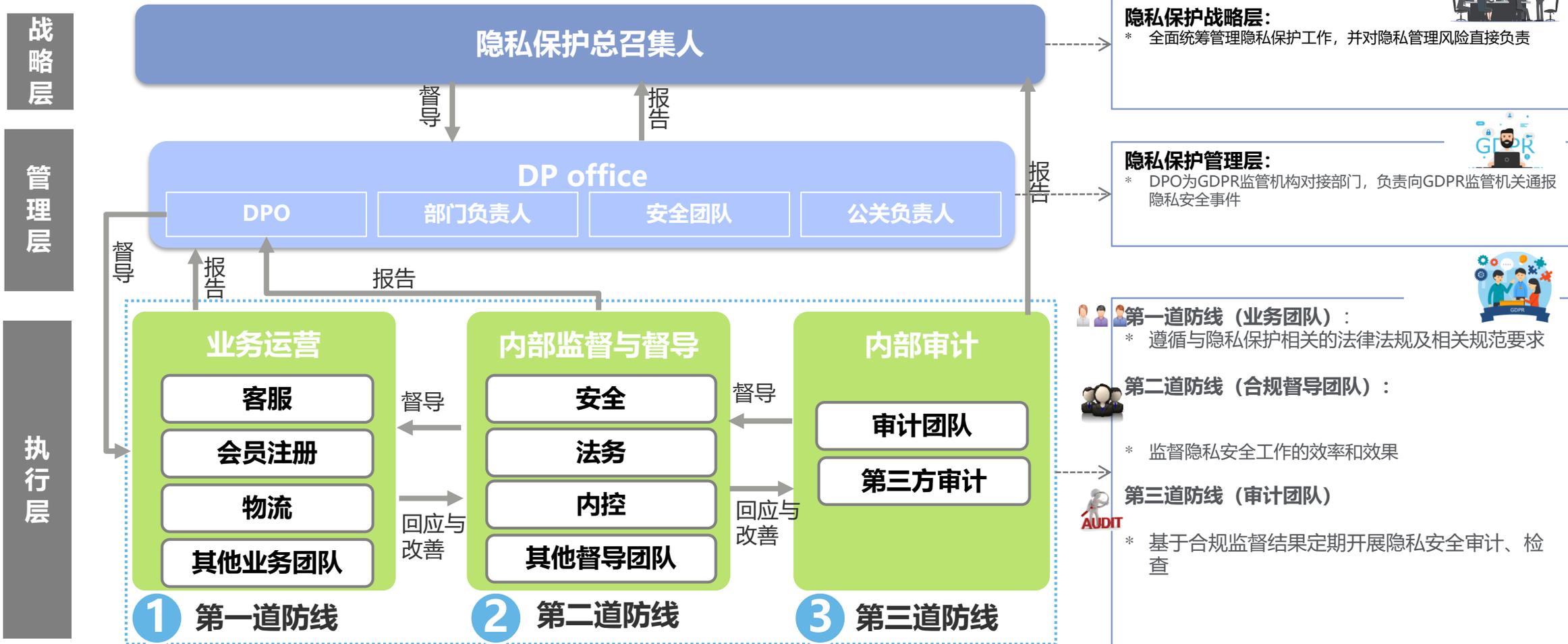
2- 隐私运营

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，需要跨部门团队协作合作。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。





肖腾飞

德勤中国网络安全服务合伙人

电话：13581962223

邮件：frankxiao@deloitte.com

关于德勤全球

Deloitte ("德勤") 泛指德勤有限公司 (一家根据英国法律组成的私人担保有限公司, 以下称德勤有限公司("DTTL")), 以及其一家或多家会员所。每一个会员所均为具有独立法律地位之法律实体。德勤有限公司 (亦称"德勤全球") 并不向客户提供服务。请参阅 www.deloitte.com/about 中有关德勤有限公司及其会员所法律结构的详细描述。德勤为各行各业之上市及非上市客户提供审计、税务、风险咨询、管理顾问及财务顾问服务。德勤联盟遍及全球逾150个国家, 凭借其世界一流和优质专业服务, 为客户提供应对其最复杂业务挑战所需之深入见解。德勤约220,000 名专业人士致力于追求卓越, 树立典范。

关于德勤大中华

作为其中一所具领导地位的专业服务事务所, 我们在大中华设有22个办事处分布于北京、香港、上海、台北、成都、重庆、大连、广州、杭州、哈尔滨、新竹、济南、高雄、澳门、南京、北京、苏州、台中、台南、天津、武汉和厦门。我们拥有近13,500名员工, 按照当地适用法规以协作方式服务客户。

关于德勤中国

德勤品牌随着在1917年设立上海办事处而首次进入中国。目前德勤中国的事务所网络, 在德勤全球网络的支持下, 为中国的本地、跨国及高增长企业客户提供全面的审计、税务、企业管理咨询及财务咨询服务。在中国, 我们拥有丰富的经验, 一直为中国的会计准则、税务制度与本地专业会计师的发展贡献所长。

本出版物系依一般性信息编写而成, 仅供读者参考之用。德勤有限公司、会员所及其关联机构 (统称"德勤联盟") 不因本出版物而被视为对任何人提供专业意见或服务。对信赖本出版物而导致损失之任何人, 德勤联盟之任一个体均不对其损失负任何责任。

© 2019 德勤版权所有 保留一切权利