2019第三届顺丰信息安全峰会

2019 THE 3rd SF INFORMATION SECURITY SUMMIT

GDPR-风险和误读

李学庆

Himan

历史 History

- 中国移动飞信
- 京东安全第一人
- 摩拜高级安全总监

Consultant

出行　智能

通信　生物

教育　IOT

壹

1400万 Verizon

2017年7月的ZDNet的一份报道称，有超过1400万Verizon客户的个人数据遭到泄露，这次事件突出了将数据保护实践迁移到云的重要性。

据称，这次安全失误涉及技术提供商Nice Systems，它让Verizon客户数据在AWS S3存储实例上处于未被保护的状态。数据包含姓名、电话号码以及可能被用于访问其Verizon账户的PIN码。多达1400万订阅用户受到影响，占到Verizon公司1.8亿总订阅用户的10%，受影响的订阅用户主要是那些在最近6个月中调用了Verizon客户服务的人。

5700万 Uber

Uber在2017年11月发现，黑客在2016年一次大规模数据泄露事件中窃取了来自5700万名乘客和司机的信息，同时，Uber在2016年10月向黑客支付了10万美元用于删除数据并对泄露事件保密。

Uber公司首席执行官Dara Khosrowshani表示，被黑客盗取的乘客和司机信息中包含来自第三方服务器的电话号码、电子邮件地址、以及姓名，而向盗贼支付费用这件事情是前首席安全官Joe Sullivan决定的，后者已被解雇。

1.43亿 Equifax

Equifax在2017年9月份透露，一次规模庞大的数据泄露导致其1.43亿信用和信息服务客户受到影响。这些事件最早是在7月29日发现的，该事件是由美国网络应用的一个漏洞导致，漏洞允许黑客访问某些特定文件。

泄露的信息包含姓名、出生日期、社会保障号码、地址和一些驾照号码信息，此外还有20多万个信用卡号码和近20万个其他带有个人身份信息的文件。就在该泄露事件发生不到三周之后，该公司宣布首席执行官Richard Smith将退休。

52GB D&B

世界著名的商业信息服务机构Dun & Bradstreet经历了一起严重的数据泄露事件，一个大小为52GB的数据库意外在线泄露，影响了包括AT&T、沃尔玛、Wells Fargo，甚至美国国防部等在内的3300多万员工，泄露信息包含详细的联系方式、职位名称、邮箱地址、电话号码以及雇主信息等。

据了解，D&B的全球商业数据库覆盖了超过1亿条企业信息，可见，目前商业网站仍是黑客攻击的主要目标之一。

5000万 Facebook

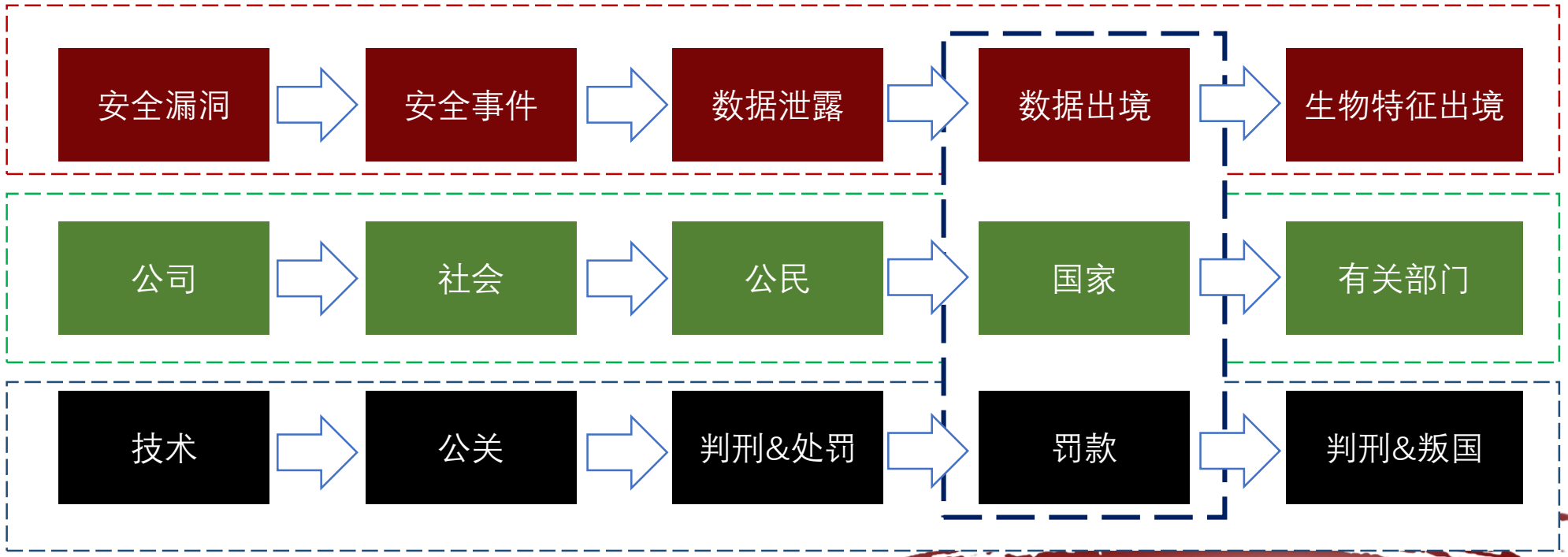
2018年3月16日，Facebook被曝在2014年有超过5000万名用户（接近Facebook
户总数的三分之一，美国选民人数的四分之一）的个人信息遭剑桥分析公司非法用
广告，部分媒体将其视为Facebook有史以来遭遇的最大型数据泄露事件，但Faceb
否认这是一起数据泄露事件。

剑桥分析公司的丑闻对Facebook的公司品牌造成了巨大损害。如今要想恢复公众对
Facebook在隐私保护和数据安全上的信任，需要付出更为巨大的努力。

M

现　　状

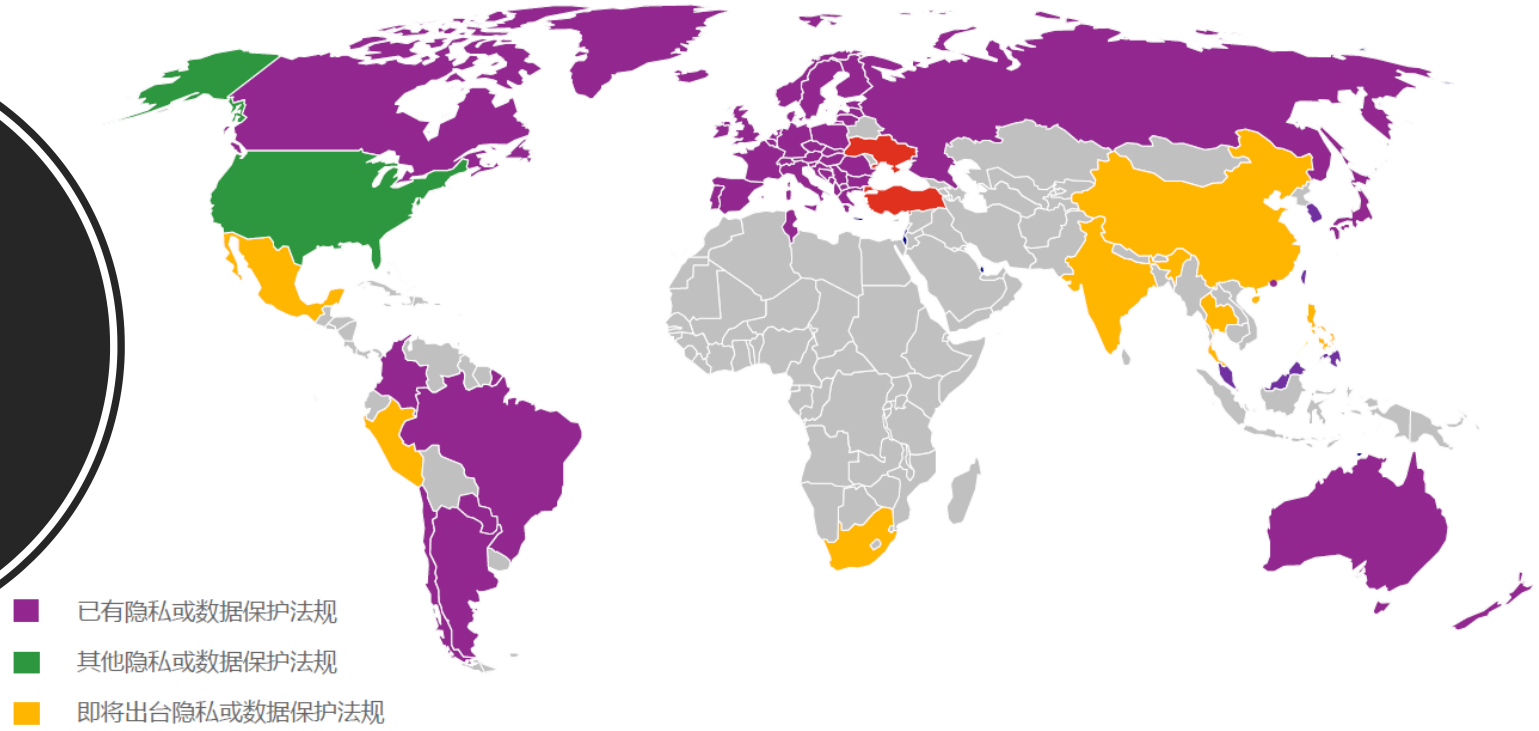
没有网络安全，就没有国家安全



现　　状

- GDPR于2018年5月25日生效
- 整个欧盟（EU）范围经营
- 高达2000万欧元的罚款威胁或全球年营业额超过GDPR 4%的威胁
- 企业别无选择，评估处理个人数据的措施

立法现状



贰

欧盟原则

- 合法性（lawfulness）
- 公平性（fairness）
- 目的限制性（purpose limitation）
- 透明性（transparency）
- 问责制（accountability）

数据盘点

数据分类	示例及描述
个人基本信息	姓名 | 生日 | 性别 | 民族 | 国籍 | 家庭关系 | 住址 | 电话号码 | 电子邮箱
个人身份信息	身份证 | 护照 | 驾驶证
系统或网络标识信息	User ID（真实ID、伪名ID） | IP地址 | Cookie数据 | RFID标签 | 系统密码及口令 | 个人证书等
个人文化社会信息	职业 | 职位 | 雇主 | 学历 | 教育经历 | 工作经历 | 培训记录 | 成绩单
个人经济信息	银行帐号 | 存款信息 | 房产信息 | 贷款记录 | 消费记录 | 信用记录 | 流水信息 | 虚拟货币信息
个人位置信息	行踪轨迹 | 定位信息 | 经纬度
个人设备信息	MAC | 唯一设备号（IMEI/Andriod ID/IDFA/GUID/IMSI）
服务内容	如通话记录、短信、传输的数据文件和邮件内容；个人在手机、电脑等终端或云端上存储的图片、文本等私有资料；个人对特定用户群体发布的社交信息，如群组内发布内容等
服务记录	通过日志储存的用户的操作记录、服务内容信息记录等，包括消费记录、游戏记录、视频操作流水记录、点击日志、业务日志等
联系人及关系链信息	指个人在电话、即时聊天工具、邮件中的联系人信息，包括相应的账号、用户名、头像等信息。关系链包括但不限于通讯录联系人、好友列表、关注对象列表
个人生物识别信息	个人基因 | 指纹 | 声纹 | 掌纹 | 虹膜 | 面部特征
个人健康信息	身高 | 体重 | 病症 | 病例 | 检验报告 | 用药记录 | 过敏信息 | 家族病史
个人其他隐私信息	种族或民族出身 | 政治观点 | 宗教或哲学信仰 | 党派或工会信息 | 性取向

数据主体权利

- **知情权**

数据控制者从数据主体或其他来源处收集个人信息时，应当提供相应的信息确保数据主体对其自身权利以及救济途径得以充分知晓，包括但不限于数据控制者及数据保护官的身份信息和联系方式、个人数据处理目的及其合法基础、数据储存期限、数据种类、数据主体享有的权利、向监管机构投诉的途径等。

第13、14条

- **访问权**

数据主体有权从数据控制者处获得关于其个人数据是否被处理的结果，同时有权了解处理的目的、类别、存储期限、救济途径、安全保障措施等，数据主体还可获得正在处理的其个人数据副本。

第15条

- **更正权**

数据主体有权要求数据控制者立即更正与其有关的错误个人信息，包括以补充声明或其他方式补充其不完整的个人信息。

第16条

- **删除权（被遗忘权）**

当出现收集和处理数据已不再必要、数据主体撤销同意、数据主体行使拒绝权、个人数据被非法处理、基于法定义务需要删除等情形时，数据主体有权要求数据控制者立即删除其个人数据，数据控制者应当采取合理措施并告知正在处理该个人数据的其他控制者。

第17条

数据主体权利

- **限制处理权**

特定情形下，数据主体有权限制数据控制者的处理行为。例如，数据主体对其个人数据准确性提出质疑且控制者需要时间核实时；个人数据被非法处理但数据主体反对行使删除权时；相关个人数据虽然对于处理目的而言已不再必要，但为诉讼所必需的。

第18条

- **持续控制权**

数据主体有权要求数据控制者提供结构化、通用化和可机读的个人数据，并有权将上述数据转移给其他数据控制者，原数据控制者不得阻碍。

第20条

- **拒绝权**

数据主体有权基于其自身情况拒绝包括直销目的以及公众或第三方利益在内的个人数据处理行为。

第21条

- **自动化个人决策**

数据主体有权不受仅基于自动化处理行为得出的决定的制约，以避免对个人产生法律影响或类似影响，该自动化处理包括人物画像。

第22条

数据拥有者义务

- **数据系统保护和默认保护**

数据控制者应当采取适当的技术、组织措施（如匿名化等）确保数据处理符合GDPR要求的同时又保护数据主体的权利。此外，在默认（by default）情形下，该技术和组织措施应保证对个人数据的处理应在最小必要的原则下进行且不得被不特定自然人访问。

第25条

- **记录数据处理活动**

数据控制者和处理者应当保存由其负责的数据处理活动的记录，该记录应当采取书面形式，必要时向监管机构提供。

第30条

- **报告数据泄露事件**

数据控制者应自发现个人数据泄露事件之时起72个小时内向监管机构报告，报告中应阐明泄露数据的种类、数量、可能导致的后果以及建议采取的处理措施等。数据控制者还应提供数据泄露事件的完整记录以便监管机构之后的核实。

第33条

数据拥有者义务

- **数据保护影响评估**

数据控制者进行数据处理行为前，应当考虑处理行为的性质、范围、内容和目的以及可能对数据主体权利和自由产生的风险，并完成一份设想的处理行为给个人数据保护带来的影响的评估。
第35条

- **事先咨询**

若根据第35条制定的数据保护影响评估显示数据控制者的处理行为将导致高风险而缺乏有效风控措施时，控制者应当在处理前向监管机构进行咨询。监管机构应在规定期限内提供书面建议。
第36条

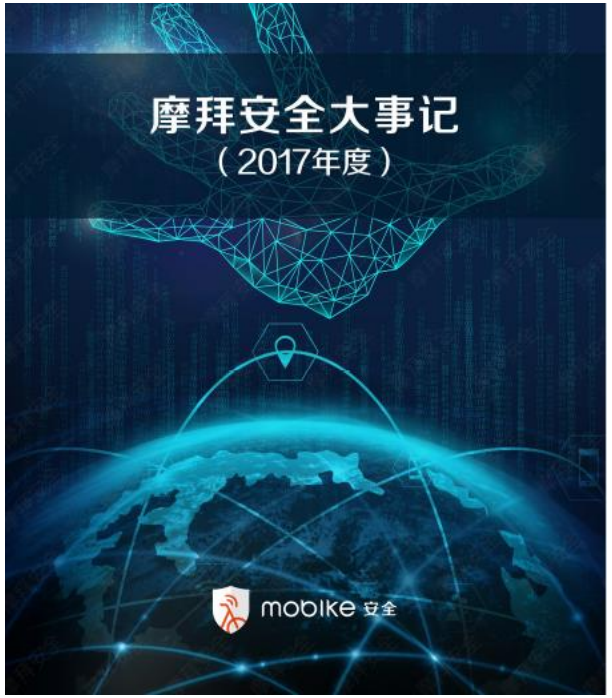
- **设立数据保护官**

数据控制者和处理者应当指定一名数据保护官的情形包括三种：一是数据控制者和处理者系行政机关或公共机构的；二是业务涉及的数据处理是定期、系统化且规模较大的；三是涉及处理敏感信息的。数据保护官应当具备专业素养，拥有数据保护法律的专业知识和实践经验。
第37-39条

GDPR误读

- 发现数据泄露后的72小时内向ICO（信息专员办公室）报告数据泄露
- 组织将面临高达其年营业额2%或1000万欧元的罚款
- 并如实报告受影响数据的性质，人数、后果以及采取了哪些措施
- 最高罚款为组织年营业额的4%，以目前最高者为准，即2000万欧元
- 如果是轻微违规，或者可以证明自己未违规，可以从轻处理

笃行·致远 2019第三届顺丰信息安全峰会



摩拜报告

叁

未来
Further

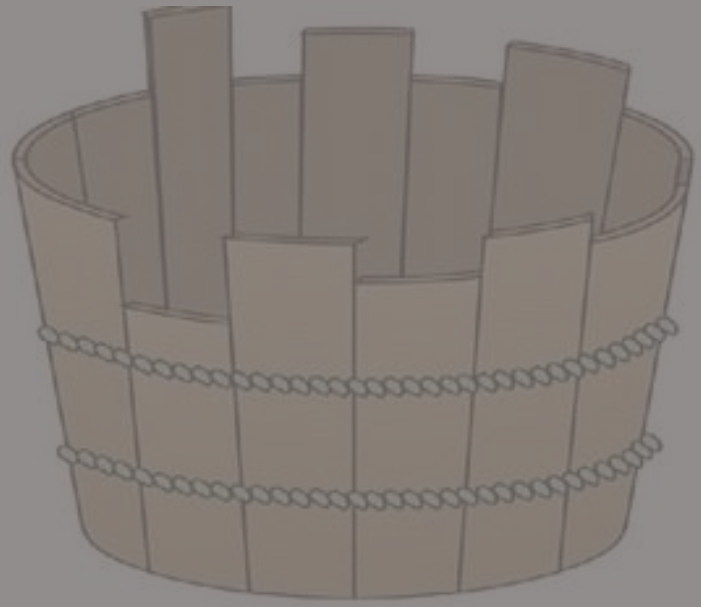
01 数据保护官

02 数据加密平台

03 数据权限平台

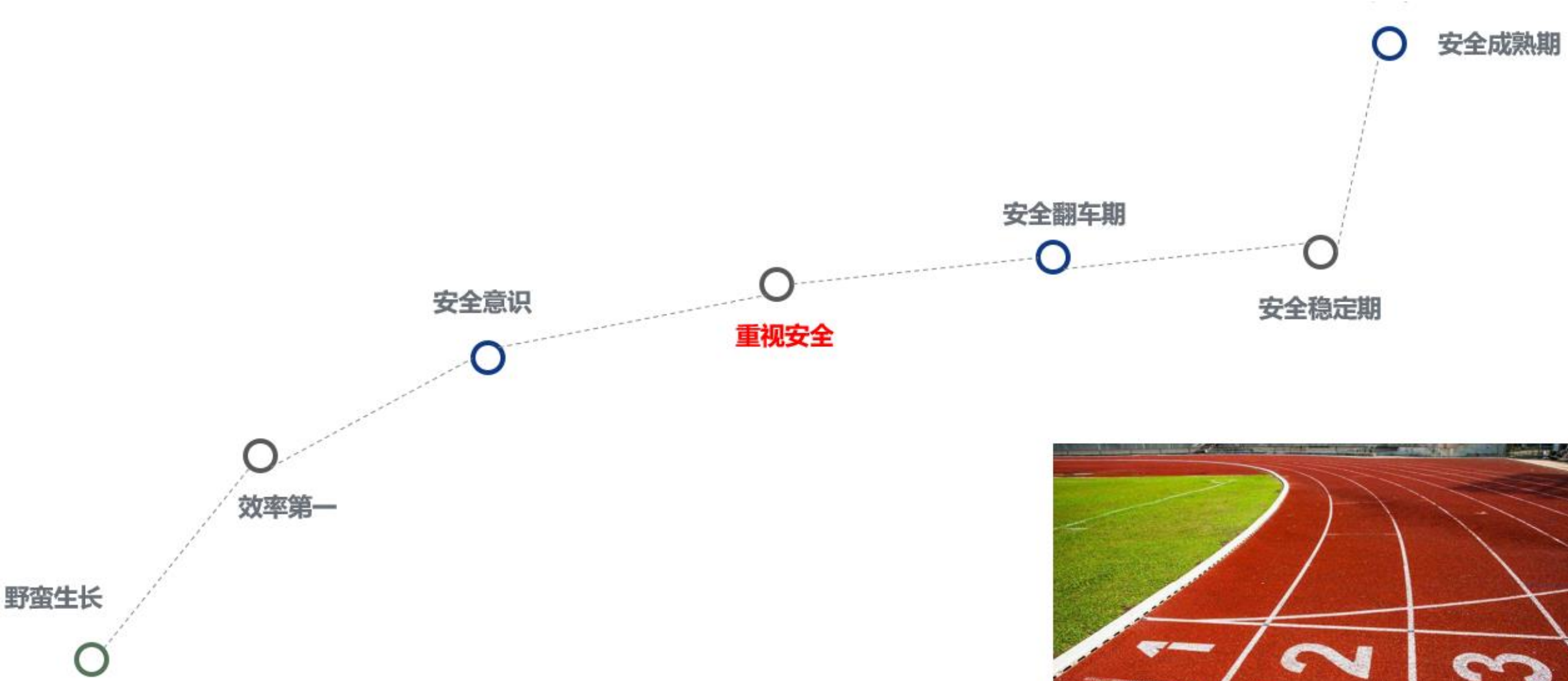
04 数据脉象平台

安全理念

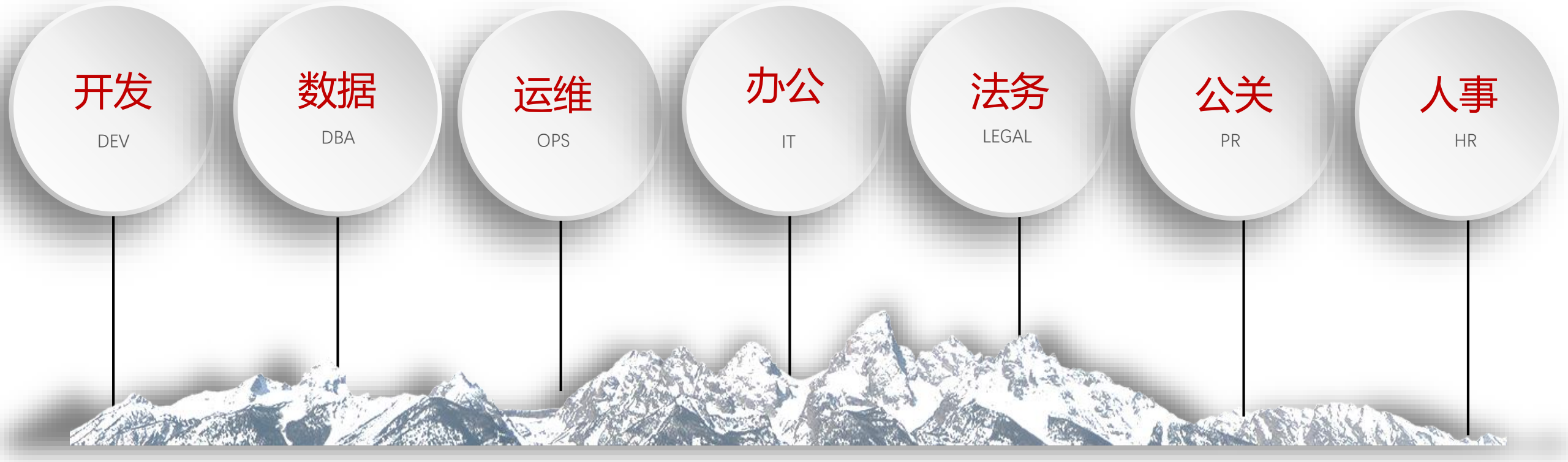


安全的木桶 可高低

安全理念



安全并不是一个人在战斗



牧羊犬理论


THANK YOU