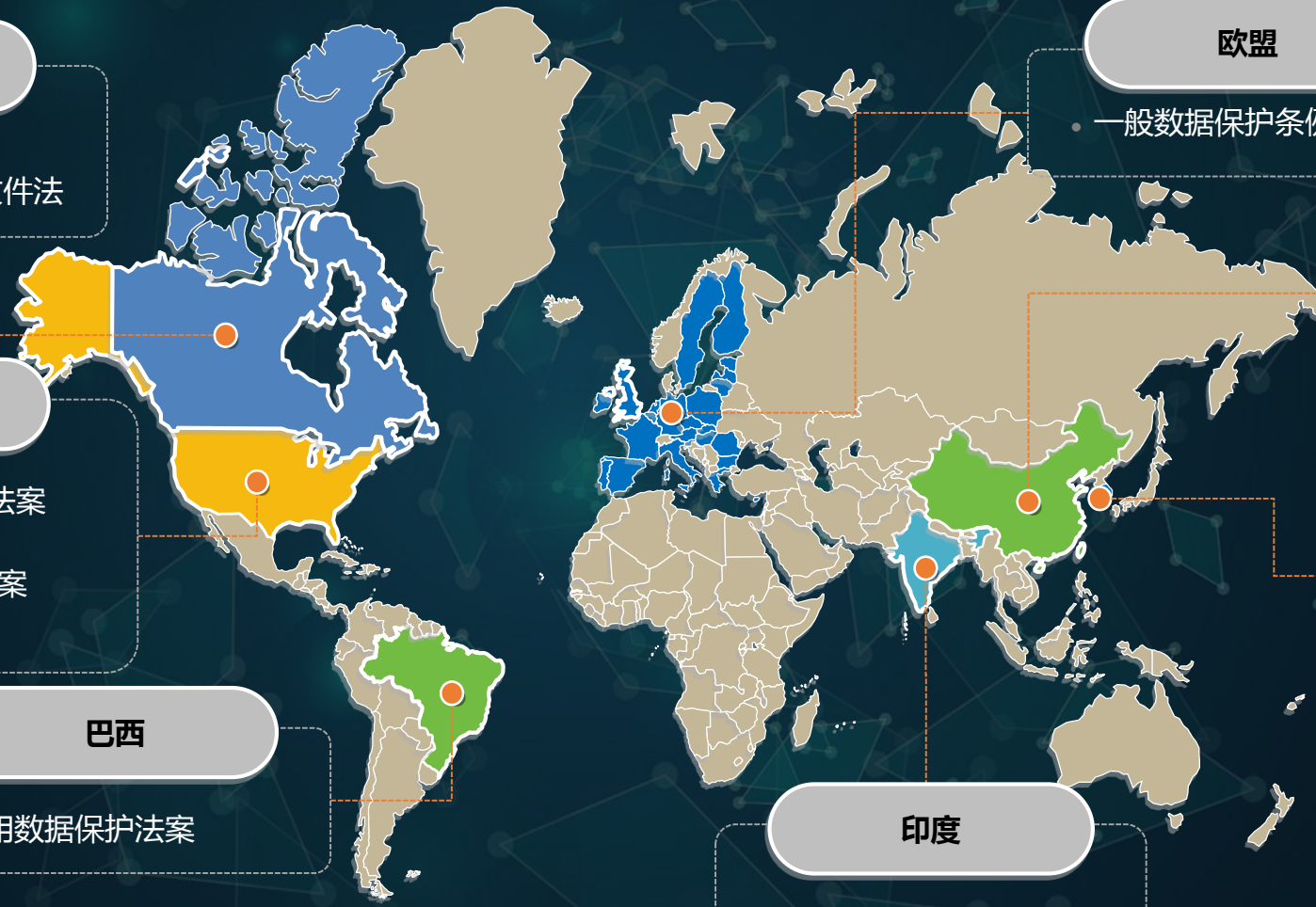
个人数据保护实践

携程信息安全部 / 胡立平

目录

全球个人信息保护法律法规概况



加拿大

- 个人信息保护法案
- 个人信息保护和电子文件法

美国

- 格雷姆-里奇-比利雷法案
- HIPPA
- 儿童在线隐私保护法案
- 加州消费者隐私法案

巴西

- 通用数据保护法案

欧盟

- 一般数据保护条例

中国

- 网络安全法
- 消费者权益保护法
- 民法总则
- 电子商务法

韩国

- 个人信息保护法案

印度

- 信息技术法案
- 个人数据保护法案-草案

从全球来看，超过80%的发达国家/地区以及超过80个国家/地区已经颁布和实施了隐私保护法规。

GDPR合规实践

GDPR介绍

《一般数据保护条例》（GDPR）是一项综合性的数据保护法，将于2018年5月25日生效。本法适用于控制或处理欧盟居民数据的任何组织，无论其地理位置。

4% 全球收入

除了潜在的处罚外，企业名誉也会遭受重创。

属人主义原则

从属地到属人，实现长臂管理，不合规意味着可能要失去拥有5亿多人口的欧盟市场。

用户新权利

保障数据主体的新权利(删除权，访问权，可携带权) 方面的不确定性带来更多的人力物力投入。

72小时响应

事件响应的有效管理至关重要，企业必须确保其组织完全履行合规义务。

数据控制者&处理者职责

对数据控制者和处理者需要承担更多的职责，包括数据安全官、数据影响评估、对数据建立安全措施等。

数据处理原则

企业在数据处理时需要遵守合法、公平透明、目的最小化等原则。

GDPR合规实践

携程GDPR合规思路

业务场景

- 涉及哪些业务部门
- 对风险的态度

法律要求

- 司法解释
- 法律诉讼
- 不合规的案例
- 咨询机构

重点关注

- 数据主体反馈
- 数据处理活动
- 跨境数据传输
- 人是最关键因素

应对方案

- 职责分配
- GDPR项目
- 外部资源
- 流程、工具
- 培训、意识
- 行业对标

GDPR合规实践

携程GDPR合规实践

网络安全法合规实践

携程作为网络运营者的落地重点

- 第二十一条：国家实行网络安全等级保护制度
- 第二十四条：用户评论实名制要求
- 第四十一至四十四条：个人信息安全要求

隐私政策　数据安全　等级保护　实名认证　内容安全

网络安全法合规实践

隐私政策

- 隐私政策更新和发布
- 隐私政策增强性告知
- 隐私政策专项评审

数据安全

- 用户数据收集
- 用户数据存储
- 用户数据使用
- 用户需求回应

等级保护

- 等保测评
- 备案业务
- 等保2.0

实名认证

- 注册认证
- 绑定手机
- 实名认证组件

内容安全

- 先审后发
- UGC敏感词过滤

敏感信息安全管理

敏感信息安全规范

生成	访问	传输	显示	存储	销毁
☐用户自主生成 ☐后台应用生成	☐保密协议 ☐授权记录 ☐权限回收	☐加密传输	☐掩码显示	☐加密 ☐密钥定期更新	☐定期销毁 ☐存储介质 ☐禁止供应商维修

敏感信息通用原则

敏感信息分类分级

敏感信息是指公司和员工从法律要求，社会义务等层面上要求得到保护的数据，该类数据只能在公司内部或某些授权合作方使用，一旦被泄露和破坏会对公司运营、客户利益、公司财务和声誉造成影响，可能导致违反法律法规和客户隐私侵犯，引发外界对企业的信任危机以及遭受法律制裁。


THANKS