CHINA LEGAL
Executive Council

GDPR一周年回顾
——典型案例梳理以及合规的平衡点分析

主讲人：

斐石国际律师事务所中国区 管理合伙人 周照峰博士

斐石国际律师事务所中国区 高级律师 张德昊

目录

01 数据跨境传输

GDPR下的数据跨境传输

1）欧盟标准传输协议（低级别）

2）BCRs（需要执法机关批准）

数据跨境传输的豁免情形：目前已经有欧洲企业实施：

GDPR第49条（数据跨境传输安排的例外/豁免情形）

中国法下的数据跨境传输

（1）数据本地化与数据跨境传输的关系

- 两个处理行为
- 但有联系

（2）是否禁止企业传输数据出中国?

- 只有极少数类别：遗传基因、网约车、共享单车、 地图等；
- CII 的定义：未能明确其范围，如何判断?
- 关于《个人信息和重要数据出境安全评估办法》
- （征求意见稿）中，将义务主体扩展?

02 数据共享/数据传输

GDPR下数据共享/传输

关键点Keypoint

中国数据共享/传输

→ 网安法：选择同意原则

→ 个人信息安全规范：例外情形

→ 用户授权+平台授权+用户授权三重授权原则

03 案例分析

GDPR案例

法国CNIL - 谷歌罚款案

- 目前影响最大、罚款金额最高的案件

谷歌违反GDPR：

1）违反透明度原则和信息告知义务

- “碎片化”展示信息、不充分告知用户处理活动

2）违反GDPR下对同意的规定

- 要求用户一揽子同意其隐私政策内所展示的所有的处 理活动。

程序上：

- 谷歌被认为决策权在美国，因此不适用一站式执法， 目前瑞士等多个欧洲国家在考虑对其采取执法措施。

GDPR案例

德国Knuddels.de案

- 案情简介

德国Knuddels.de社交软件被黑客攻击后数据泄露。公司向LfDI报告，其中大约有33万名用户密码和电子邮件 地址被盗。该公司并未加密密码形式，而是以纯文本（明文）形式储存并因此违反了GDPR第32条—未达到 处理过程的安全性。

在得知数据泄露之后，Knuddels.de立即要求所有的用户变更密码，并向德国的数据保护执法机关提出报告。

- 处罚

原则上，该公司可被处罚1000万欧元或者是上一财政年度全球营业额的2%。但该公司表现出强烈的合作和 配合意愿 最终LfDI视情况给予了较低的罚金：2万欧元。

GDPR案例

奥地利监控案

- 2018 年 9 月 19 日， 在 GDPR 实 施 4 个 月 后， 奥 地 利 数 据 保 护 机 构 （Datenschutzbehörde，简称为DSB）开出了首张GDPR罚 单，对违规的企业罚款4800欧元。

- 被罚的企业在其建筑物前安装了一台闭路电视摄像机，该摄 像机覆盖了人行道的大部分区域。DSB认为企业违反了GDPR 的规定，因为GDPR不允许对公共场所进行大规模的监控。 另外，摄像机没有清楚标示正在执行视频监控，这也违反了透明义务。

- 此次罚款金额不高。奥地利DSB代理负责人Matthias Schmidl 称：罚款应当遵循比例原则，数据保护机构不会对一个年收 入为4万欧元的数据控制者开具2000万欧元的罚单的。

GDPR案例

荷兰单因素登录案

- 荷兰执法机关对某人事社保机构做出了处罚，罚款为每月15　万欧，但是给了整改期限：到2019年10月31号整改完毕，　否则会执行罚款。
- 主要的原因是因为该机构的技术措施上，采取单因素认证登 录的方式，荷兰执法机关认为，单因素认证不足以保障健康 数据这一敏感数据，要求采取多因素认证的方式。
- 荷兰执法机关提出至少两种验证方式结合，比如密码+短信 验证码方式。

GDPR案例

荷兰单因素登录案

- 荷兰执法机关对某人事社保机构做出了处罚，罚款为每月15万欧，但是给了整改期限：到2019年10月31号整改完毕，否则会执行罚款。
- 主要的原因是因为该机构的技术措施上，采取单因素认证登录的方式，荷兰执法机关认为，单因素认证不足以保障健康数据这一敏感数据，要求采取多因素认证的方式。
- 荷兰执法机关提出至少两种验证方式结合，比如密码+短信 验证码方式。

GDPR案例

波兰：关于自公开渠道获取个人信息的告知义务

- 波兰数据保护执法机构（UODO）罚款事由：

针对某数据控制者从公开来源上收集到600万人的个人信息， 没有告知给个人，更没有告知其处理活动和处理目的。

- 罚款金额：约22万欧元

数据控制者抗辩事由：600万人的人数太多，无法一一履行 告知义务。

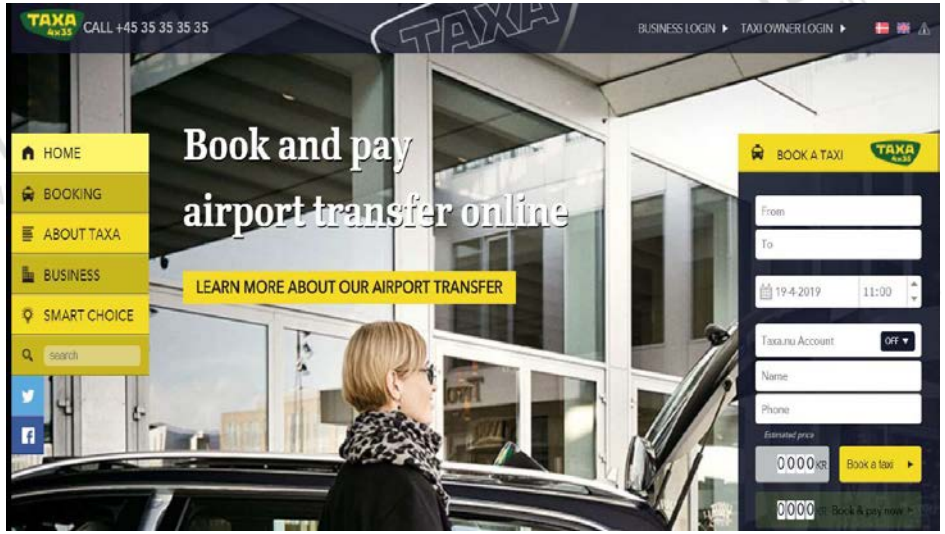
- 波兰UODO：

这是借口，应该通过公开渠道上获取的这些个 人的联系方式去告知给每一个涉及到的个人。否则违反GDPR第14条的强制性规定（信息告知义务）。

GDPR案例

丹麦：出租车数据删除案

- 案由：出租车公司在完成订单的两年后， 仅删除了用车记录中的乘客姓名，未删除 其他记录。
- 丹麦数据保护执法机关的罚款建议：120 万克隆，约€160,754，约合该公司年收入 的2.8%
- 该案体现了在GDPR下：如果不需要保存 记录时，仍不删除个人数据，或者删除的 数据不能成立匿名化（无法辨识出个人且 不能恢复），则将构成违法。



GDPR案例

立陶宛Mister Tango数据泄露案

2019年5月16日，立陶宛数据保护监管机构（State Data Protection Inspectorate）对互联网支付公司MisterTango违反《通用数据保护条例》（General Data Protection Regulation，GDPR）的行为处以61500欧元的罚款，这是立陶宛的首张GDPR罚单。

Mister Tango此次受处罚的原因有不恰当处理数据、泄露个人信息以及未向监管机构报告数据泄露事件。2018年7月，MisterTango公司用户的个人信息以及9000张网络支付交易截图被非法披露在互联网上，该数据泄露事件发生后72小时内公司亦未向监管机 构报告。此外，Mister Tango提供支付服务时，违反GDPR超出必要限度读取并收集用户的个人信息。

中国个人信息保护案例

庞先生诉东航、去哪儿网隐私权纠纷案

庞先生诉中国东方航空股份有限公司（“东航”）、北京趣拿信息技术有限公司（“去哪儿网”）隐私权纠纷案

庞某、鲁某买票，预留的联系方式是鲁某手机号

非东航及去哪儿网之外 的其他人直接向庞某自 己的手机号发送信息告 知航班取消

首次核实时，东航客服人员否认航班取消，并确认了庞某的手机号。此后东航官方向庞某手机上发送短信告知航班延误的信息，鲁某电话咨询东航，得知航班取消。

中国个人信息保护案例

庞先生诉东航、去哪儿网隐私权纠纷案

法院认为：争议焦点有四个：

①本案涉及的姓名、电话号码及行程安排等事项是否可以通过隐私权纠纷而寻求救济—是的

② 根据现有证据能否认定涉案隐私信息是由东航和趣拿公司泄露—东航和去哪儿网被认为有高度可能性，首先，从整个 案情来看，法院首先排除庞某以故意泄露个人信息进行虚假诉讼的可能；其次，在现有条件下，一般人无法确凿地举 证证明具体的泄露数据的人；再次，已经有多家媒体质疑东航、去哪儿网、中航信等数据泄露，强化了东航与去哪儿 网的数据泄露的可能性。

③ 在东航和去哪儿网有泄露庞某隐私信息的高度可能之下，其是否应当承担责任—在多家媒体质疑后，并未采取相应措 施，具备过错，应当承担责任。

④ 东航和去哪儿网所提出的中航信更有可能泄露庞理鹏信息的责任抗辩事由是否有效成立—不真正连带责任下，中航信 并非必须一并承担责任，旅客起诉了东航未起诉中航信，有理由认为旅客行使了选择权；其次，旅客订票有理由认为 其是向东航订的票，对外关系上东航应当先承担责任。

中国个人信息保护案例

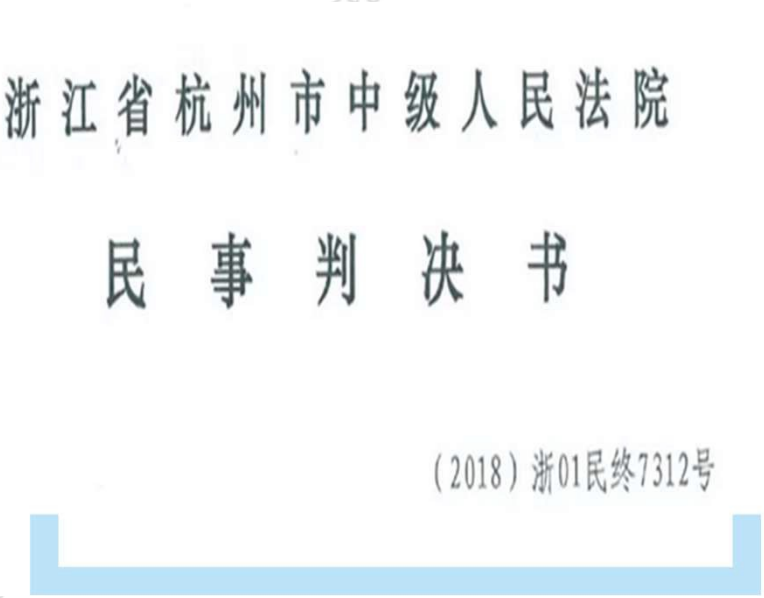
申女士诉携程和支付宝隐私权纠纷案

- 法庭上，携程公司提交的2018年敏感信息管理规则显示，订单信息属于一级信息，内部传输可不加密。
- 携程公司未向法庭提供内部员工授权进行访问涉案订 单的人员范围、访问敏感信息的授权记录、监控情况、 操作记录、内外部传输审批情况的相关证据。
- 在携程应用界面及短信确认内容中也没有充分明显地告知消费者对于航班信息诈骗的注意。

图示：“航空诈骗信息”

中国个人信息保护案例

淘宝中国诉安徽美景信息案


浙江省杭州市中级人民法院

民事判决书

（2018）浙01民终7312号

2018年12月18日，杭州市中级人民法院作出二审判决，确认淘宝对大数据产品“生意参谋”数据 享有**竞争性财产权益**，安徽美景信息科技有限公司需**停止涉案不正当竞争行为**，并赔偿淘宝经济损失及为制止不正当竞争行为所支付的合理费用共计200 万元。

作为大数据产品第一案，案件的裁判不仅有力打击了针对大数据产品的黑灰产与不正当竞争行为，对于整个大数据行业的发展，对于大数据产品研发人员以及**大数据产品运营主体的行为激励来说，都有直接现实的价值。**

中国个人信息保护案例

针对APP违规的大规模执法活动

- 2019年1月23日，网信办、工信部、公安部、国 家市场监督管理总局四部委联合下发《关于开展APP违法违规收集使用个人信息专项治理的公告》，就APP违法违规收集个人信息开展大规模 的执法活动。
- 2019年3月29日，上海市消保委已经通报了包括 聚美优品、穷游、百度糯米、神州租车等多个APP，要求整改，并对整改后的APP再次进行检查。

分享嘉宾介绍

周照峰博士

斐石律师事务所中国区 管理合伙人

周照峰博士是斐石律师事务所中国区管理合伙人。他的执业领域集中在反垄断法和数据保护方面。

在反垄断法领域，周照峰博士是国内目前为数极少的即具有深厚反垄断法理论基础又具有丰富实践经验的反垄断法律师。作为中国最早从事中国反垄断法研究和实务的中国律师之一，周博士曾经参与过多起在中国反垄断法发展史上具有里程碑意义的反垄断项目，例如商务部受理的第一起航空行业的集中申报和中国反垄断法实施后的第一起收购被剥离资产的项目。在数据保护领域，周博士带领其中国团队凭借斐石欧洲办公室的支持为多家大型央企提供欧盟个人数据保护GDPR的合规服务，是极少数真正具有指导中国企业全面合规GDPR的中国律师。

周博士所涉及的领域涵盖了多个行业，其中包括航空、飞机制造、汽车、互联网、矿用机器制造、新能源、医药和TMT等领域。

分享嘉宾介绍

张德昊

斐石律师事务所中国区 高级律师

张德昊律师的服务经验集中于数据保护以及网络安全，企业合规。他既有为客户提供GDPR下的全程全面服务的经验，又有为客户提供中国网络安全法和个人信息保护方面的经验，对部分欧盟成员国的员工数据保护方面的问题解决也有较为丰富的经验，并且能够同时为客户提供在GDPR、中国法等方面结合的具有实践意义的最优做法。

张德昊律师的主要客户是在客运航空、旅行方面。此外，他曾向TMT，教育，医疗，金融，环保以及汽车等领域的诸多公司提供过法律服务。

THANKYOU!