互联网时代企业如何应对欧盟通用数据保护条例（GDPR）

普华永道网络安全与合规咨询服务 高级经理 童磊

2018年6月7日

pwc

普华永道

普华永道是全球领先的专业服务机构

覆盖全球的网络组织

普华永道**1849年**创立于英国伦敦，经过近**170年**的发展，已经成为一家全球性运营的专业服务机构网络。截至2016年底，普华永道成员所已经覆盖全球六大洲，在世界上**158个**国家拥有超过**236,000人**组成的全球网络。

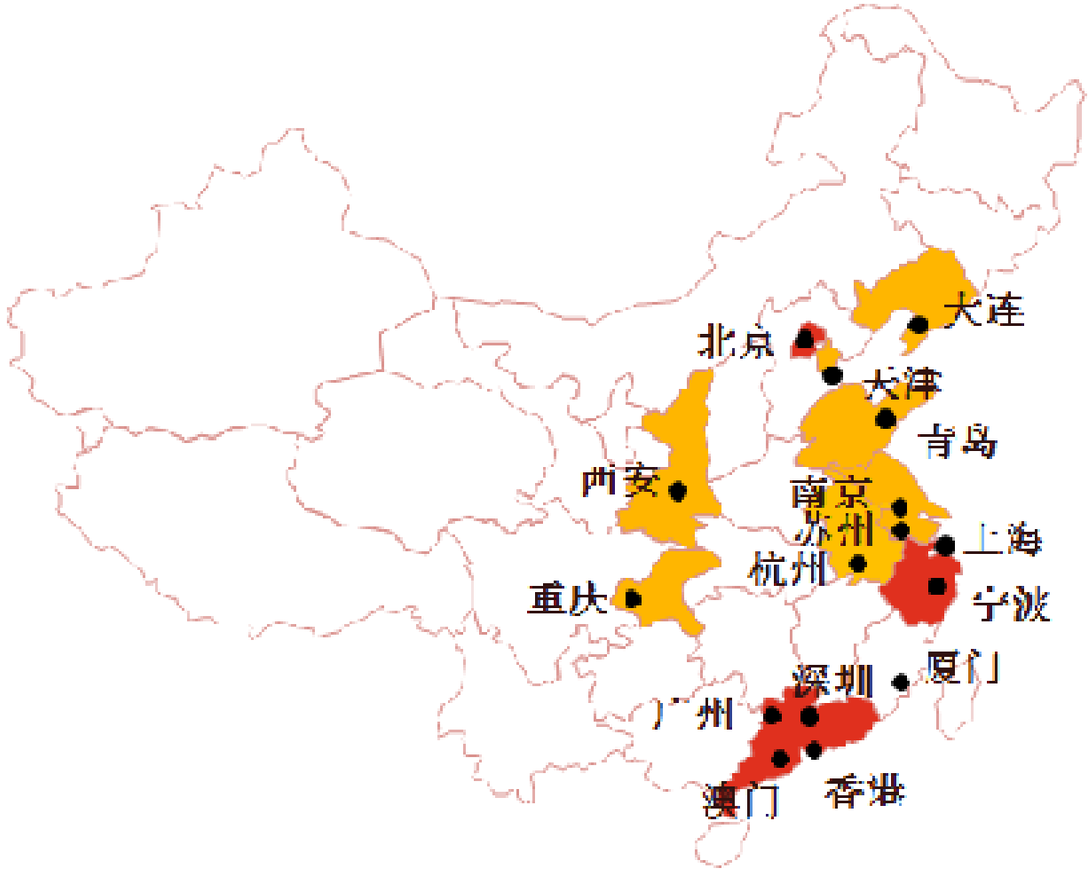
扎根本土的专业服务

普华永道于1949年进入中国，是当时第11家被授予营业执照的外国公司，**也是4大会计师事务所中第一家在中国获得营业执照**。

普华永道1979年重新进入中国内地市场，如今在中国内地拥有最为雄厚的实力和最为广大的地域覆盖。

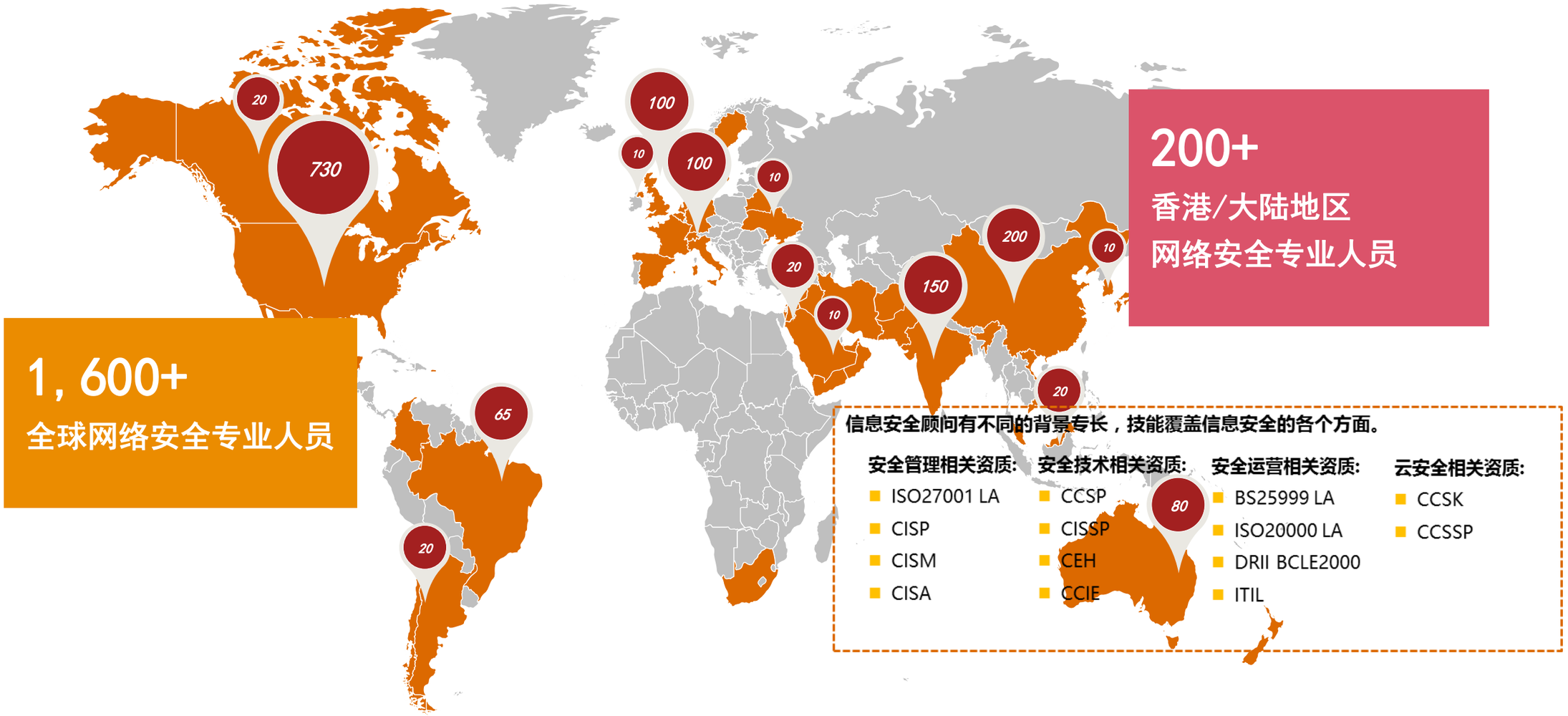
如今已经在中国大陆**23个**城市开设了分支机构，共有**18,000名**员工。

从2003年至今，在中注协百强会计师事务所排名中持续**15年名列第一**。



普华永道网络安全与隐私合规咨询服务

普华永道的网络安全团队在全球拥有**超过1600名**的信息科技风险和信息安全专家，我们可以帮助客户了解不断变化的信息安全挑战，适应并响应商业生态系统的固有风险，优先识别并保护企业最有价值的资产，以支持企业的经营战略。



1，600+

全球网络安全专业人员

200+

香港/大陆地区

网络安全专业人员

信息安全顾问有不同的背景专长，技能覆盖信息安全的各个方面。

安全管理相关资质:	安全技术相关资质:	安全运营相关资质:	云安全相关资质:
ISO27001 LA	CCSP	BS25999 LA	CCSK
CISP	CISSP	ISO20000 LA	CCSSP
CISM	CEH	DRII BCLE2000	
CISA	CCIE	ITIL	

网络安全与隐私合规咨询领域

全球信息安全事件

Facebook——全球最大的社交网站之一

2018年3月17日，美国《纽约时报》和英国《观察家报》报道，有超过5000万Facebook用户（这一人数接近脸书美国活跃用户总数1/3）的私人信息被一家名为“剑桥分析公司”的数据分析公司以不正当方式获取，该公司可能以这些数据为基础**预测并影响了全球多地政治活动中公众的选择**，其中包括2016年美国总统选举以及英国“脱欧”公投。

美国联邦贸易委员会(FTC)针对Facebook展开调查，其获将面临2万亿美元最高罚款。路透社分析今年5月GDPR生效后，Facebook的广告定向投放业务届时将受影响，如若Facebook违反这一法规，将面临最高相当于年收入4%的罚款。

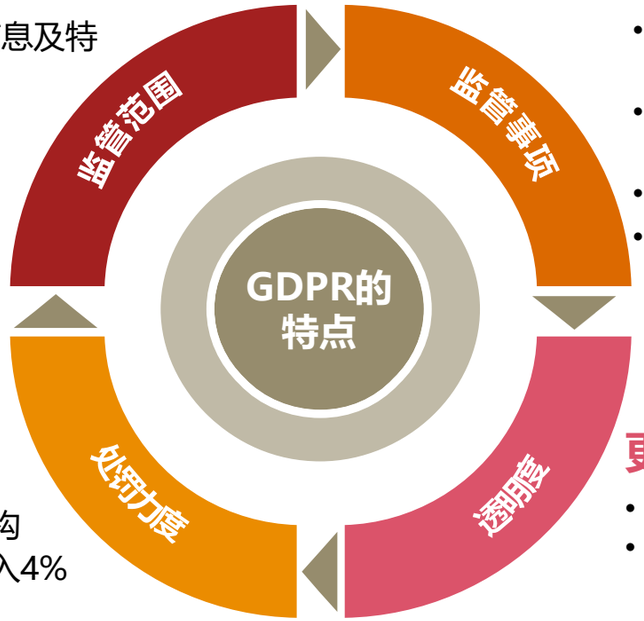
Reference: http://www.sohu.com/a/225896373_563945

GDPR概述

GDPR概述：GDPR 11个章节、99个条款

GDPR加强和统一了欧盟内部个人的数据保护，公司必须对其系统和业务进行所有必要的修改以满足新的合规要求

GDPR章节 (共99个条款)
一、一般规定
二、原则
三、数据主体权利
四、控制者和处理者
五、数据出境
六、独立监管机构
七、合作与一致性
八、权利、责任与罚则
九、特定处理情况
十、实施细则
十一、终章



更大的监管范围

- 监管范围更广(个人信息及特殊个人信息)
- 新增隐私保护要求
- 新增隐私保护7原则

更多的监管事项

- 研发过程隐私保护要求(Privacy by Design)
- 隐私影响分析(Privacy Impact Analysis)
- 被遗忘权和可转移权
- 隐私保护专员(DPO)

更严格的处罚

- 授权各国数据保护机构
- 最大罚款上限达年收入4%
- 侵权赔偿及集体诉讼

更广的透明度要求

- 明示同意
- 保护者两种不同角色及对应责任(Controller/Processor)
- 隐私政策公开
- 泄露事件72小时报告监管

GDPR重点内容

GDPR是关于信息管理良好实践的业务规则。这也是人权和消费者保护立法。

GDPR关注的关键问题，如数据主体的权利。该法规使人们更加关注数据（技术）的使用。

- GDPR涉及11个领域的管理，包括“同意”概念、个人敏感数据、问责机制、数据主体的权力、数据处理者、数据泄露的通知、数据保护者、数据处理者
- 更多实体将受到监管，包括纯数据处理公司和非欧盟实体
- 遵从义务将扩展到证据隐私影响评估、设计隐私权、被遗忘权和数据可移植性
- 要求更高的透明度，如明确同意、违约披露等条款
- 增加诉讼风险与扩大执法权力，如罚款，集体诉讼和增加赔偿索赔
- 2018.5.25 正式实施GDPR

关注点

- 罚款达到全球营业额的4%
- 公民直接诉权
- 72小时内报告数据泄露
- 属地主义转化成属人主义
- 定义扩展到：
  - 基因数据
  - IP地址
  - RFID标签
  - Cookie

如何存储：知道所有个人数据所存储的位置

设计隐私：尽量减少在设计阶段对新产品的个人数据和保障措施的使用

职责：任命数据保护官（DPO）

通报机制：违规72小时内向监管机构披露

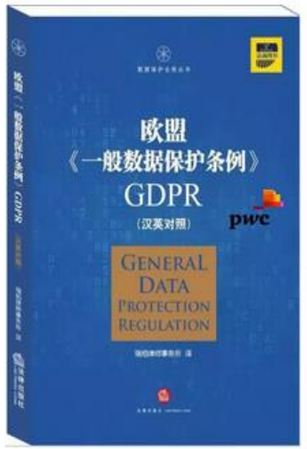
数据披露：必须要有处理个人数据的声明与授权

数据携带：将个人数据及时转移给其他所有者允许转移的公

被遗忘的权利：根据要求删除所有相关的个人数据。

数据的角色： 数据控制者 数据处理者

用户画像：数据主体明确同意授权或者是签订合同所必需的时候



GDPR的三个重要定义

个人数据

一个确定的或可识别的自然人相关的任何数据。特别是通过参考诸如姓名、身份号码、位置数据、等标识符，或参考与该自然人的身体、生理、遗传、心理、经济、文化或社会身份有关的一个或多个因素。

数据控制者

指能够单独或联合决定个人数据处理目的和处理方式的自然人法人、公共机构行政机关其他非法人组织。

举例：
采集并存储用户数据的应用APP，如

- 解锁应用采集用户指纹
- 导航应用采集用户的地理位置信息
- 云存储运营提供商

数据处理者

代表控制者处理个人数据的自然人、法人公共机构、行政机关或其他非法人组织。

举例：
处理数据并有所行动的应用APP，如

- 导航应用处理数据后提供路线方案
- 电商通过搜索的数据分析为用户提供推荐商品

欧盟通用数据保护条例与网络安全法的联系

《GB/T 35273 2017信息安全技术　个人信息安全规范》——个人信息

附录A　　表A.1　个人身份和鉴别信息举例

个人基本资料	指对个人社会属性和自然属性进行描述的信息。包括但不限于生日、性别、职业、职位、民族、国籍、邮编、姓名、地址、工作单位等。
个人身份信息	指能单独、准确识别个人真实身份的影印件及其他信息。包括身份证、护照、驾驶证、社保卡、军官证、居住证及其他法定证件影印件及号码等与自然人法定身份紧密相关的数据。
生物识别信息	指与个人具有唯一对应关系的用户生理信息。包括但不限于基因、指纹、声纹、掌纹、耳廓、虹膜、面部特征等。
虚拟身份标识和鉴别信息	包括电话号码，社交类软件昵称、IP地址、邮箱地址及与前述有关的密码、口令、口令保护答案等。
	包括交易类软件账号、银行卡账号，证券账号，以及交易类软件账号的口令、用户个人数字证书等。

《信息安全技术 个人信息安全规范》

3.1个人信息

以电子或其他方式记录的能够单独或与其他信息结合识别自然人身份的各种信息，包括与确定自然人相关的生物特征、位置、行为等信息，如姓名、出生日期、身份证号、个人账号信息、住址、电话号码、指纹、虹膜等。

实施难点解析

GDPR 合规难点及应对措施----数据的发现

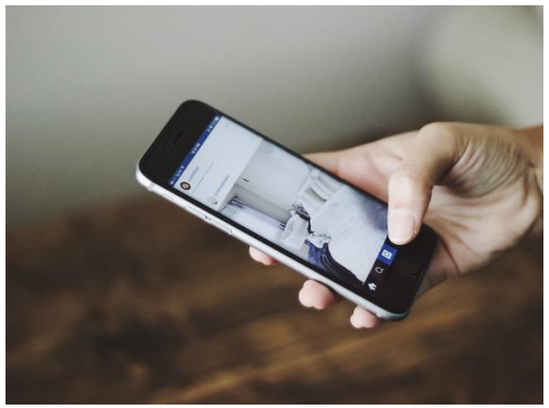
涉及的GDPR法规

(Chapter I, Article 4) 'personal data' means any information relating to **an identified or identifiable natural person** ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

本项GDPR合规落地难点、主要任务及影响	
涉及GDPR义务的角色	数据控制者和数据处理者
主要任务	• 依据个人数据的定义，归整产品(例如采集用户信息中的系统数据或相机应用数据）所涉及的可识别一般个人数据和特殊个人数据分类 • 修改服务合同，明确告知客户产品的数据搜集种类和将用于处理的目的以及客户所拥有的权限
落地完成本项工作后的收益是	• 明确客户权利、消除客户疑虑，同时降低客户的合规难度 • 满足数据合规收集要求

受影响业务场景的示例

例如：指纹识别数据
（属于特殊个人数据）



sample

一般个人数据如位置信息

私人助理 获取

- 根据GDPR的一般个人数据和**特殊个人数据（比如生物特征信息）**保护规定，对手机产品的各项功能会收集或处理的个人数据进行整理划分，归纳可能涉及的一般个人数据和特殊个人数据搜集清单，并总结一般个人数据和特殊个人数据的判定规则。根据GDPR的信息保护规定，定期更新收集清单和判定规则。
- 修改与客户的服务合同，在合同中明确告知客户，产品在数据收集、数据存储、数据处理过程中涉及的数据种类、处理目的和**需要明示同意**的内容，更好的符合GDPR相关条款规定。

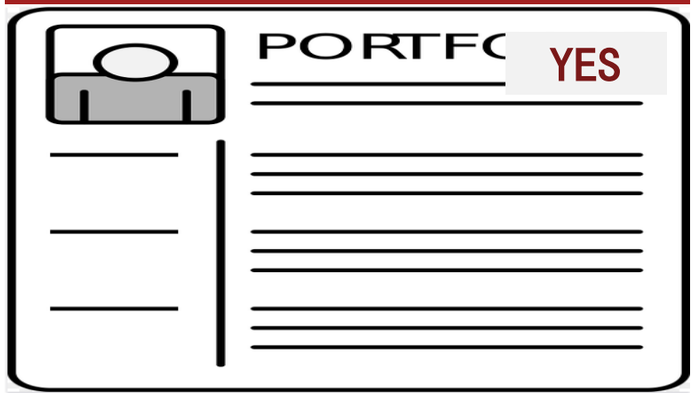
特定场景分析——GDPR定义的个人数据

VIN(车架识别号)

可直接关联到车主的身份

员工卡号

在办公环境下，通过工号可以关联到个人身份



个人照片（无其他信息）

使用特殊技术可识别出个人身份

同事或老板走过切换到邮件选项

在雇佣关系场景下，个人意见或针对他们的意图

Identifier

Art.4

(Personal data about the Data Subject)

- Name
- Address
- Email Address
- Passport Number
- Financial & Bank Info
- Date of Birth
- Healthcare Data
- Biometric Data
- Employee ID
- Phone Number

Online Identifier

Rec.30

("...online identifier[Personal data] provided by their[Data Subject's] devices, applications, tools and protocols")

- IP address, static and dynamic
- MAC addresses
- Cookies
- International Mobile Equipment IDs(IMEI)
- International Mobile Subscriber Identity(IMSI)
- Advertising IDs
- GPS or other location data
- Log files
- Browser fingerprints

Special Category Identifier

Art.9

(Special Categories of Personal Data about the Data Subject)

- Biometric Data
- (for the purpose of uniquely identifying a natural person)
- Religious of Philosophical Beliefs
- Trade Union Memberships
- Processing of Genetic Data
- Race
- Ethnic Origin
- Political Opinions
- Health
- Sex Life
- Sexual Orientation

GDPR 合规难点及应对措施----数据处理知情权

涉及的GDPR法规

(Chapter II, Article 6) Lawfulness of processing 1.Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject **has given consent to the processing** of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject……

本项GDPR合规落地难点、主要任务及影响	
涉及GDPR义务的角色	数据控制者和数据处理者
主要任务	• 收集个人信息的产品(例如手机系统指纹解锁或面部识别功能所收集的信息、照相功能)，需要增加供客户可以灵活配置产品中隐私协议条款的功能 • 手机开机画面应该明确与客户的服务合同，确保客户明确授权
落地完成本项工作后的收益是	• 符合欧盟GDPR和相关法律（如合同法相关规定）的合规要求 • 提升品牌合规形象，提升合规保障水平

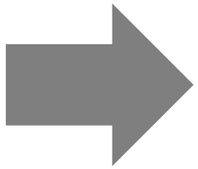
受影响业务场景的示例

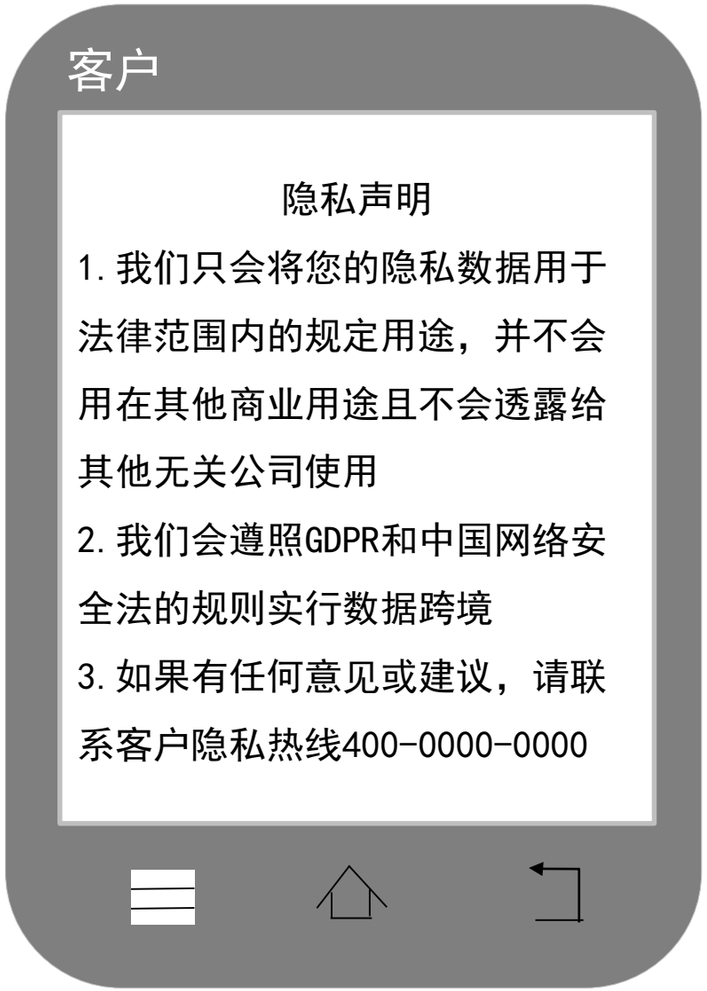
sample

例如：开机页面明确用户服务条款
并在个人数据收集和处理权限上设置可勾选项

- 根据GDPR对数据处理的明确要求进行数据保护，包括对数据处理的合法性、公平性、透明性；以及收集目的的特定性、明确性；数据收集的最小化原则；个人资料的准确性以及储存限制；数据存储的完整性和机密性要求。
- 与客户的服务合同，在其中增加GDPR**允许处理和明示用户权利的条款**，并提供选择**同意选项**（如明确手机可对用户提供可携带权，但由此所造成的风险应由其个人负责等内容），以确保业务的正常、合规开展。

特定场景分析(1)——隐私声明举例





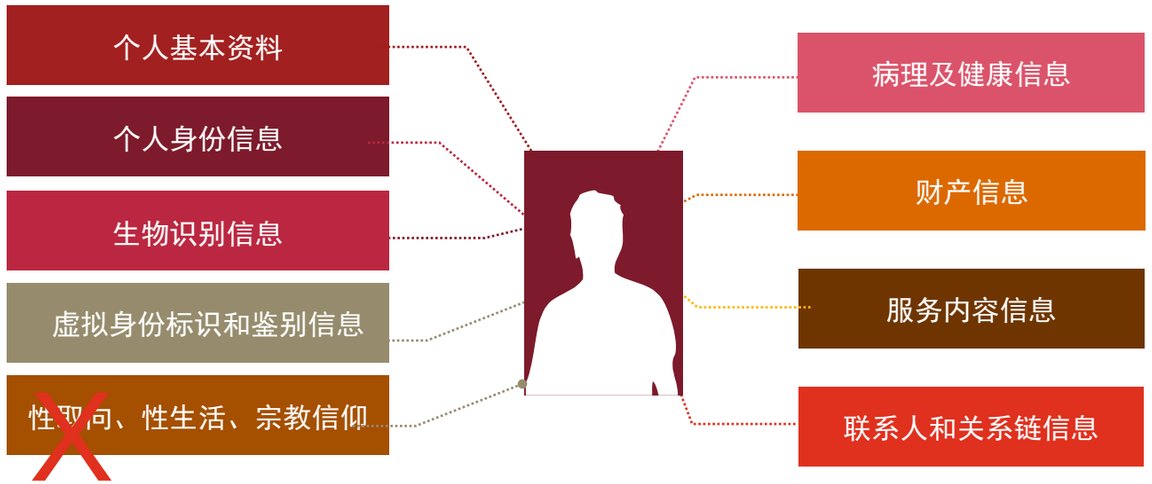
GDPR 合规难点及应对措施----大数据处理的规范

涉及的GDPR法规

（ Chapter I, Article 4) **‘profiling’** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person‘s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, **location or movements**.

本项GDPR合规落地难点、主要任务及影响	
涉及GDPR义务的角色	数据控制者和数据处理者
主要任务	• 收集、存储个人数据的系统需要配置对个人数据匿名化、去标识化的功能 • 修改与客户的合同，增加获取用户画像、特征处理的客户明示同意条款 • 明确哪些特殊个人数据不可处理 • 遵从数据的最小化原则
落地完成本项工作后的收益是	• 符合欧盟GDPR和相关法律（如合同法相关规定）的合规要求 • 提升品牌合规形象，提升合规保障水平

受影响业务场景的示例



- 不能够采集敏感信息，例如性取向、性生活、宗教信仰、政治信仰等
- 梳理目前所涉及的智能分析、用户画像等功能的服务合同，增加提示共享平台、直营店与服务站告知客户所搜集数据的使用目的和进行特征分析处理需客户明示同意的条款，协助提供合同条款模板条款供客户参考并更新合同
- 针对数据的分析必须是一次性，如果需要二次分析，需要进行二次授权确认
- 遵循数据采集最小化原则

GDPR 合规难点及应对措施----数据全生命周期管理

涉及的GDPR法规

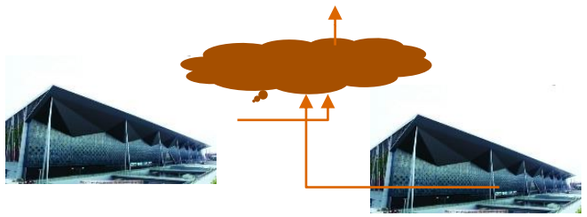
processed in a manner that ensures appropriate **security of the personal data**, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures **('integrity and confidentiality')**

本项GDPR合规落地难点、主要任务及影响	
涉及GDPR义务的角色	数据控制者(与客户的客户有关)
主要任务	• 保证系统的安全性，满足对个人数据的保护的要求 • 在产品中实现设计安全策略和措施
落地完成本项工作后的收益是	• 符合合规要求 • 增强市场竞争优势

受影响业务场景的示例

例如：
智能销售和服务系统

客户



例如：用户、手机
厂商与运营商

- 加强数据安全，降低系统被入侵而导致数据泄露的风险，设计数据保护策略，安全传输方案，应急响应措施。以此来达到GDPR要求的安全保护需求。
- 将相关安全策略及措施用技术开发手段加入产品中实现落地。
- 应该做出数据保护的动作，如数据的匿名化存储、数据存储的加密，并且全流程留痕记录处理，数据动作全流程审计

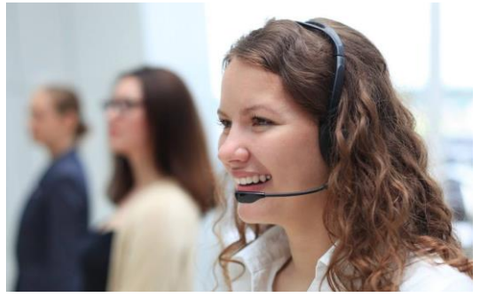
GDPR 合规难点及应对措施----数据遗忘权

涉及的GDPR法规

(Chapter III, Section 3, Article 17)) The data subject shall have the right to obtain from the controller **the erasure of personal data concerning him or her without undue delay** and the controller shall have the obligation to erase personal data without undue delay…

本项GDPR合规落地难点、主要任务及影响	
涉及GDPR义务的角色	数据控制者(主要与客户有关)
主要任务	• 设置数据定期清理或脱敏方案 • 收集客户信息时，需要增加供客户可以规范存储客户信息或删除的功能 • 确保客户和客户的沟通渠道畅通可用
落地完成本项工作后的收益是	• 低成本、全面、高效完成该领域合规 • 减少成本支出

受影响业务场景的示例



例如：
电话：400-----
邮箱：privacyissue@mail.com

客户有权要求删除关于客户自己的数据，除以下情况：

- ❑ 基于表达自由和信息自由；
- ❑ 基于公共利益和履行法律职责需要；
- ❑ 基于历史、统计和科学研究的目的；
- ❑ 出于提出、实施和保护合法权利的需要等

- **安全部门：**对存量数据设定数据清理周期，或脱敏策略，定期清除客户数据
- **研发和产品部：**的需要根据目标系统在使用过程中个人信息采集情况，在研发产品时，初始即分析和考虑未来该产品、系统需具备的个人数据存储和删除功能，从而在产品、系统中设计可供客户灵活地处置其中的个人数据，其中包括存储和删除功能，从而符合GDPR合规要求，可以检索出单个客户数据并予以删除的功能。。
- **客户接口部门：** 需要保持客户和客户沟通渠道畅通，当有客户希望立即删除自身个人数据时，由于现有技术手段限制和实施删除造成成本急剧增加导致无法立即删除。可与客户沟通表明定期删除的周期，并以现有的技术能力用合规的步骤删除个人数据。

GDPR 合规难点及应对措施----数据泄露应急处理

涉及的GDPR法规

(Chapter IV, Article 33) In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within **72 hours**, it shall be accompanied by reasons for the delay.

本项GDPR合规落地难点、主要任务及影响	
涉及GDPR义务的角色	数据控制者和数据处理者
主要任务	做好内部数据泄露事件应对计划，列明在发生数据泄露时须采取的行动，包括内部和外部主要联系人、检查清单和后续措施等内容
落地完成本项工作后的收益是	• 符合合规要求 • 完善个人信息保护管理体系

受影响业务场景的示例

1. 如在**72小时之内**不及时上报给**当地权威机构**进行妥善处理，数据泄露可能会使数据主体遭受身份盗用、欺诈、经济损失、名誉损失、保密性丧失等损失。

2. 除了通知监管机构外，数据控制者还有义务通知受影响的数据主体有关数据泄露的情况，不得无故拖延。

3. 数据控制者有义务记录包括与数据泄露相关的事实、数据泄露的影响以及所采取的任何补救措施等的所有有关数据泄露的情况。

4. 不遵守上述通知义务可能面临高达一千万欧元或相当于全球年营业总额百分之二的罚款（以其中较高者为准），不遵守监管机构的命令可能会面临高达两千万欧元或相当于全球年营业总额百分之四的罚款（以较高者为准）

场景一：IT系统遭黑客攻击

场景二：手机、笔记本、USB丢失

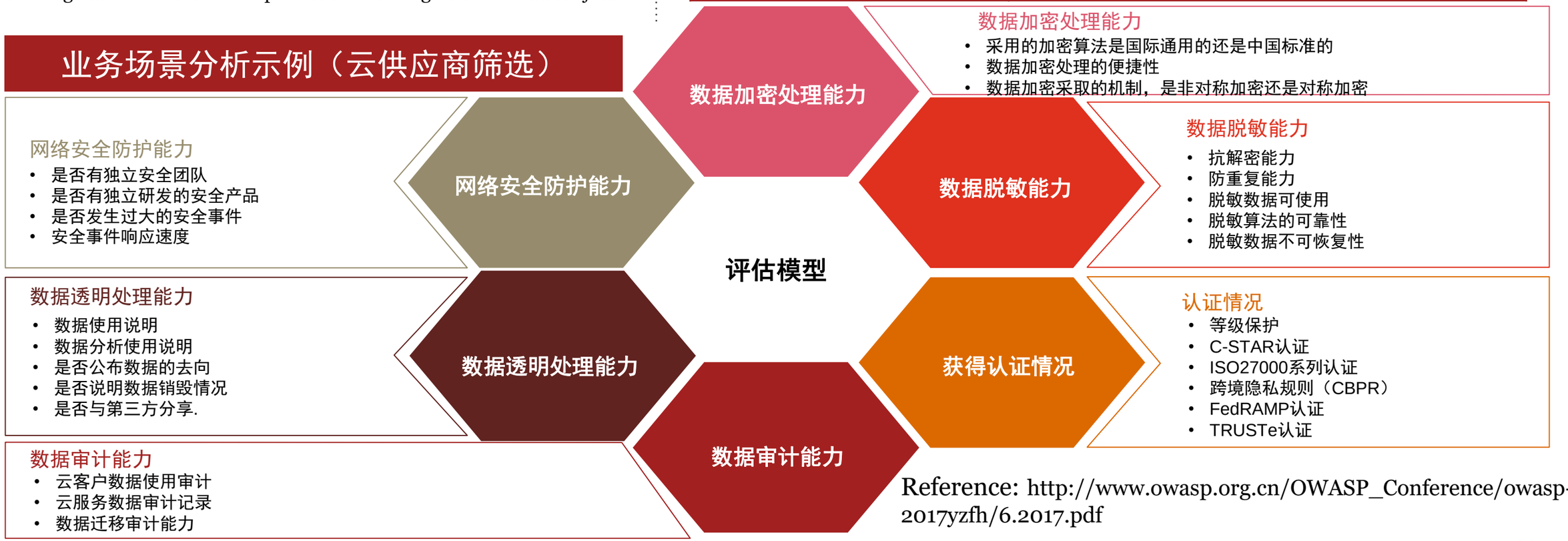
GDPR 合规难点及应对措施----外部供应商的筛选

涉及的GDPR法规

（Chapter IV, Article 28) 1.Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

本项GDPR合规落地难点、主要任务及影响	
涉及GDPR义务的角色	数据控制者和数据处理者
主要任务	供应商做为数据处理者也负有一些特定的责任，处理者代表控制者处理个人数据的(法)人，处理者并不负责决定处理目的和方式。一般而言，这涉及组织机构内部特定数据处理的外包， 例如，薪酬和员工管理、客户管理、云和托管服务或摄像头监控。 与供应商的合同内容要覆盖到GDPR的具体要求。
落地完成本项工作后的收益是	• 符合合规要求并完善供应商管理流程

业务场景分析示例（云供应商筛选）



Reference: http://www.owasp.org.cn/OWASP_Conference/owasp-2017yzfh/6.2017.pdf

GDPR 合规难点及应对措施----数据隐私评估

涉及的GDPR法规

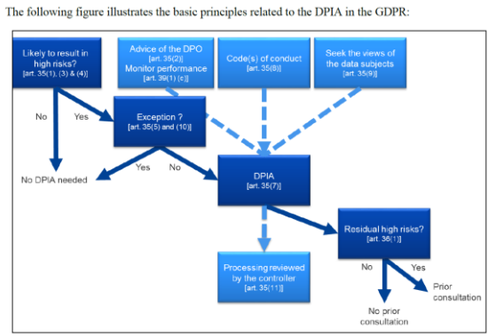
(Chapter IV, Article 35) Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

本项GDPR合规落地难点、主要任务及影响	
涉及GDPR义务的角色	数据控制者
主要任务	对单类数据处理过程，多类数据的处理过程和对数据保护有影响的技术产品都应进行DPIA
落地完成本项工作后的收益是	• 符合合规要求 • 完善个人信息保护和处理流程

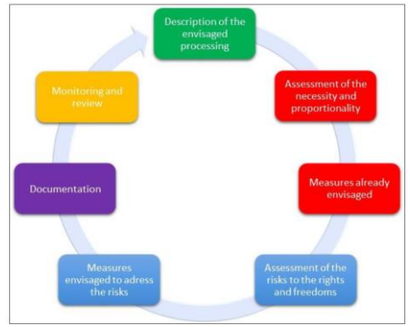
受影响业务场景的示例

DPIA评估的关键点

1. 目标系统的功能描述
2. 目标系统的数据量
3. 目标系统的业务流、信息流、数据流
4. 包含个人数据的类型及存储方式
5. 用户对于数据使用的知情状况
6. 数据修改、更新、删除



场景一：DPIA基本原则
（参考29工作组GDPR指南）



场景二：DPIA隐私评估流程
（参考29工作组GDPR指南）

GDPR 案例分享

普华永道网络安全与合规咨询　童磊

Richard.Tong@cn.pwc.com

欢迎联系咨询

谢谢!!!