EU General Data Protection Regulation (GDPR)

欧盟通用数据保护条例介绍

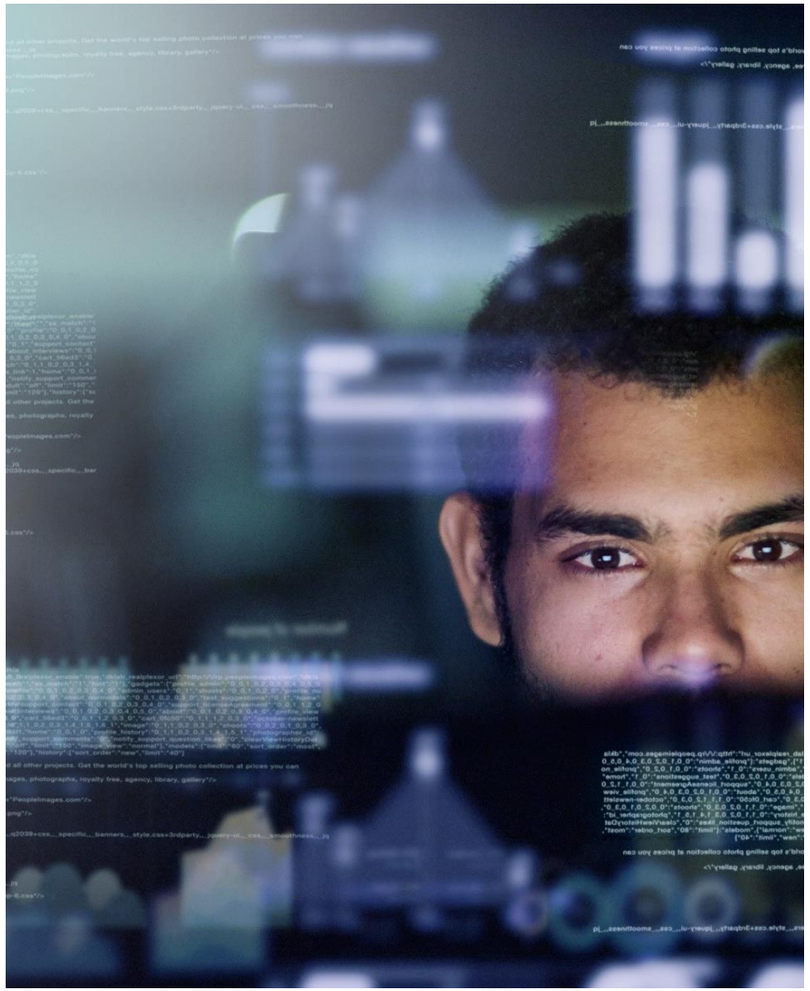
Building a better working world

目录

背景

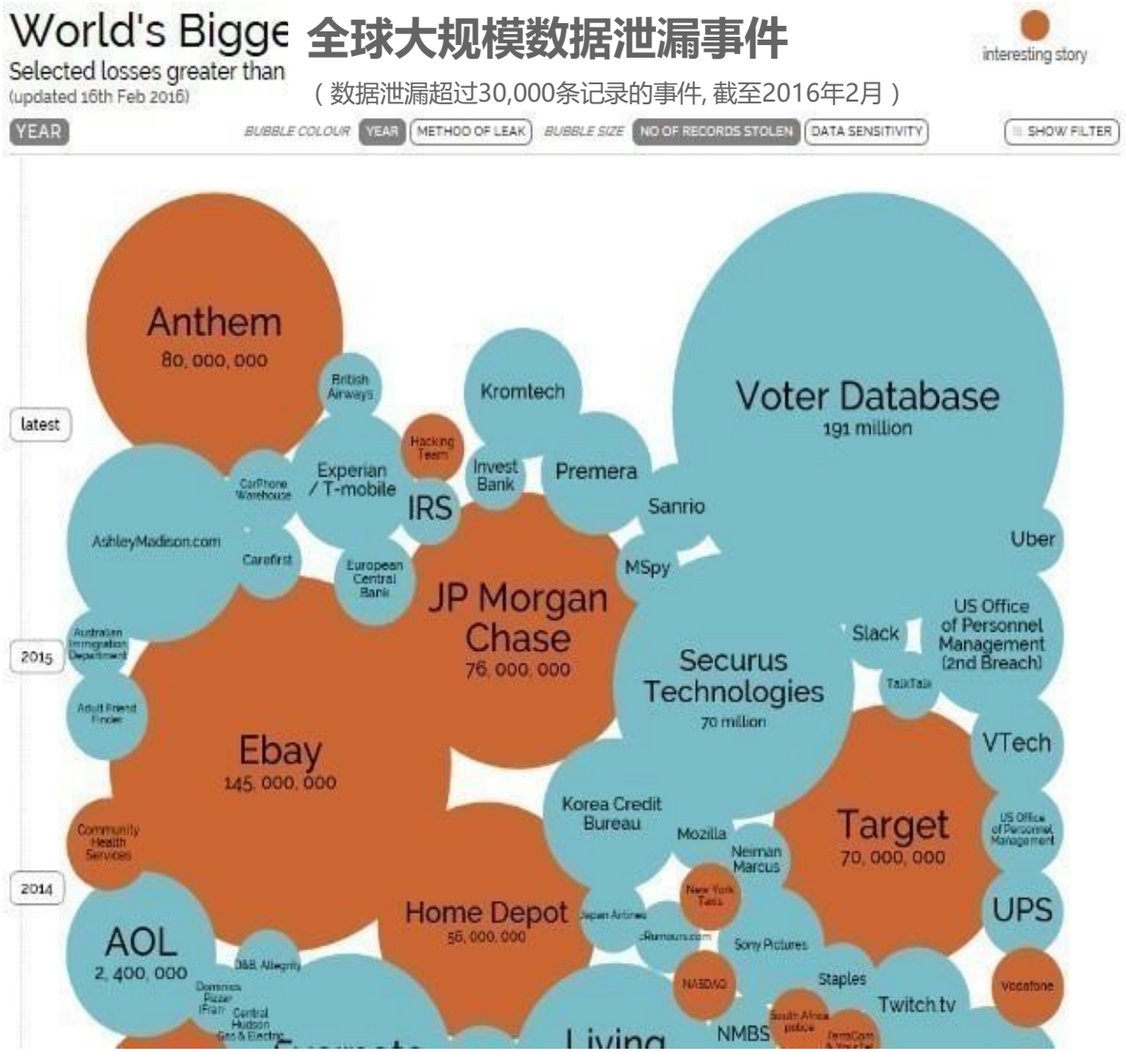
01

我们为何需要GDPR？



- 欧盟分散的数据保护制度
- 国家监管机构采用不同的标准
- 技术发展形成了公民隐私的新类型威胁
- 在欧盟之外也保护欧洲公民的隐私
- 促进欧盟内部的数据流动

为何聚焦数据保护领域？



资料来源：http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

2015年10月6日，欧盟法院 (ECJ) 宣布美国安全港协议 (the US Safe Harbor agreement) 正式失效

欧盟数据保护条例

Council of the European Union

Brussels, 15 December 2015
(OR. en)

15039/15

Interinstitutional File:
2012/0011 (COD)

LIMITE

DATAPROTECT 229
JAI 976
MI 786
DIGIT 108
DAPIX 235
FREMP 295
COMIX 663
CODEC 1676

NOTE

From:	Presidency
To:	Permanent Representatives Committee
No. prev. doc.:	9565/15, 14936/15, 14901/15, 14902/15
No. Cion doc.:	5853/12
Subject:	Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [first reading] - Analysis of the final compromise text with a view to agreement

欧盟通用数据保护条例发展历程

1995年数据保护指令（95/46/CE）

- 国家法律的拼凑
- 欧盟各国的数据保护水平不同
- 执法选项非常有限
- 新技术的开发和数据传输的巨大增长

通用数据保护条例

- 欧盟的统一保护水平
- 增加欧盟公民对其私人数据的控制
- 法律确定性和执法选择的改善

时间线

2012	2013	2014	2015	2016	2017	2018
2012年1月欧洲委员会(EC) 提议撰写GDPR		2014年3月 欧盟议会通过 一份中间版本	2015年12月15日 GDPR条例正式被通过	2016年4月14日 欧盟议会正式批准发布GDPR		2018年5月25日 GDPR正式生效

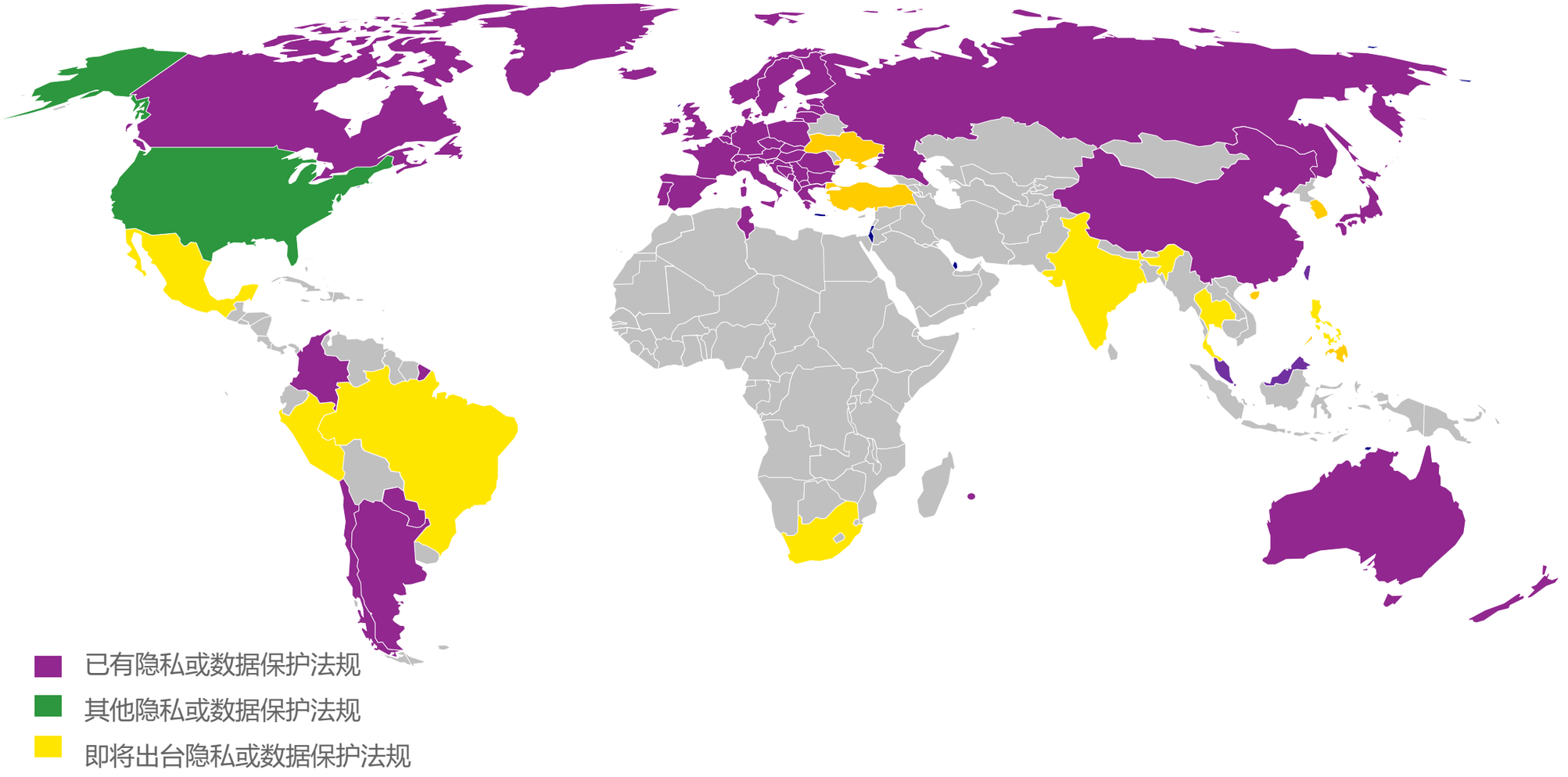
欧洲数据保护指令与GDPR比较

目前，于1995年颁布的欧洲数据保护指令积极保护公民隐私。但是，鉴于最近的技术发展，该指令不再提供足够的保护。与GDPR相比，该指令包含以下值得注意的方面：

指令：

- 将由当地数据保护机构（DPA）进行解释；
- 仅适用于在欧盟境内完成的加工；
- 不包括数据保护官（DPO）的需要；
- 不包含数据处理者的义务；
- 不包含处理属于儿童的个人资料的具体规定；
- 并不总是需要通知数据泄露；
- 允许较低的罚款（与GDPR相比）；
- 不需要使用隐私影响评估（PIA）。

全球隐私相关法律法规环境



全球隐私相关法律法规环境（续）

截至2016年, 全球已有80多个国家、地区和组织颁布了相关法规

《中华人民共和国网络安全法》

《个人资料保护法》（台湾）

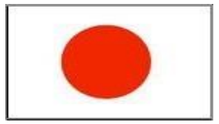
《个人资料（隐私）条例》（香港）

HIPPA（医疗保险和携带法案）

GLBA（金融现代化法案）

DPA 《隐私数据保护法案》

GDPR《通用隐私保护法规》



《个人信息保护法》

《个人信息保护及电子文件法案》

《个人信息保护法案》

《隐私法案》

此外，瑞典颁布了《个人数据法》；美国颁布了《隐私权法》、《电子通讯隐私法》、《互联网保护个人隐私的政策》；德国颁布了《联邦数据保护法》以及法国颁布了《数据处理，档案与自由法》等

适用性

02

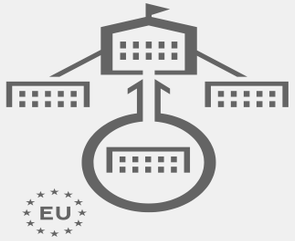
GDPR对于非欧盟公司的适用性

对中国大陆及香港企业的影响

1	中国大陆 / 香港的电商企业	**中国大陆及&香港电商提供在线销售业务** 中国大陆或香港电商通过在线渠道向欧盟中的个人提供商品，并收集相关的联系信息用于商品物流环节	EU www 电商
2	在欧盟境内有分支机构的中国大陆 / 香港公司	**分支机构 / 分公司提供产品或服务** 中国大陆或香港公司在欧盟设有分支机构或分公司的，并为欧盟中的个人提供商品或服务	
3	中国大陆 / 香港外包服务商 (数据处理者)	**外包服务提供商作为数据处理者** 中国大陆或香港公司为欧盟内的数据管理者提供涉及数据的外包服务时	数据处理者
4	中国大陆 / 香港公司	**数据收集用于调研 / 监控目的** 中国大陆或香港公司收集欧盟中的个人数据用于调研或监控用途	个人

GDPR对于非欧盟公司的适用性

潜在应用场景

场景		含义
	在欧盟无分支机构的中国及香港特别行政区组织在欧盟提供商品或服务，并处理居住在欧盟的客户个人信息	组织适用GDPR，并必须指定一位在欧盟的代表1)
	在欧盟有分支机构的中国及香港特别行政区组织在欧盟提供商品或服务，并处理居住在欧盟的客户个人信息	组织使用GDPR，且其在欧盟的分支机构可能承担责任
	中国和香港特别行政区组织在欧盟分支机构将居住在欧盟的客户的个人信息之处理外包给一服务提供商	中国和香港特别行政区组织的分支机构及服务提供商适用GDPR，且可能由其在欧盟的分支机构直接承担责任

定义

03

个人数据处理的定义

个人数据的定义

GDPR中，个人数据是指——**任何指向一个已识别或可识别的自然人（“数据主体”）的信息**”。该可识别的自然人能够被直接或间接地识别，尤其是通过参照诸如姓名、身份证号码、定位数据、在线身份识别这类标识，或者是通过参照针对该自然人一个或多个如物理、生理、遗传、心理、经济、文化或社会身份的要素。

你拥有一个人的信息越多，这个人就越有可能被识别，并且数据的处理拥有更多的风险。GDPR中，数据处理指“**在个人数据上执行的任何操作**”。

个人敏感数据

敏感的个人数据的处理有点类似于在数据保护指令下处理这样的数据，但仅在GDPR中提及了“遗传数据”和“生物特征数据”。

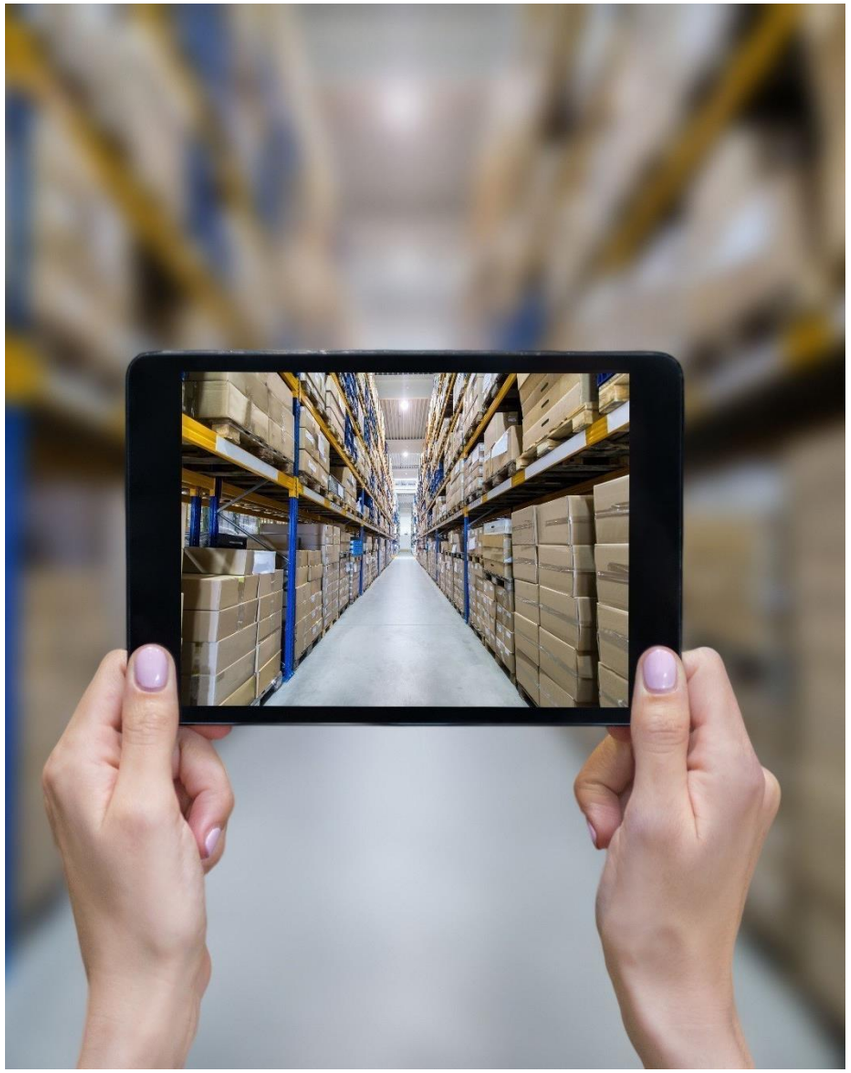
匿名数据：

与已识别或可识别的自然人无关的数据，而不受数据保护法的影响。

化名数据：

特定方面与已识别或可识别的自然人分离的数据，该数据受数据保护法的约束。

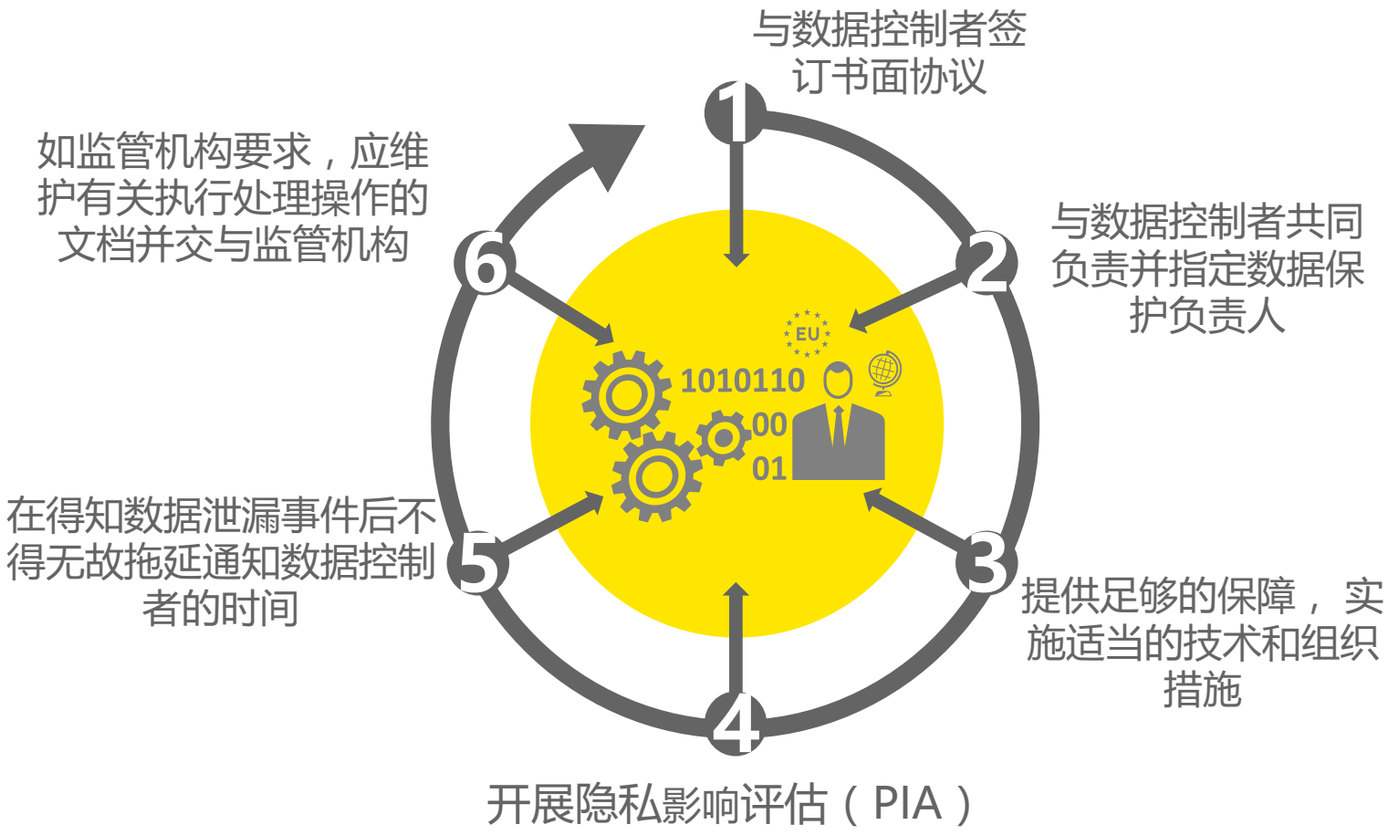
个人数据处理的原则



- GDPR包含处理个人数据的原则，这些原则如下：
- 数据处理应**合法、公正**，并对数据主体**透明**
- 收集数据的**目的**应是明确的和合法的
- 个人数据存储期受限严格限制
- 确保适当的**安全和保密**
- **责任制**：制定政策和实施适当的措施，确保个人数据在整个数据生命周期的安全

个人数据处理者的责任

数据处理者的（新）责任



数据控制者：

能决定个人数据处理目的和处理方式的个人或组织。

数据处理者：

实际处理个人数据的组织或个人。

GDPR的要点

04

GDPR的要点

高达4%全球营业额的罚金	违反GDPR的罚金是巨大的。监管机构可征收高达4%全球年度营业额或2,000万欧元，以较高者为准
扩大范围	适用于所有处理欧盟居民信息的在欧盟的数据控制者、处理者和组织机构
数据保护官(DPO)	如果一个组织进行大规模的系统监测或处理大量敏感的个人数据，数据保护官需被指派
责任制	组织需证明他们具有以下责任机制： ▸ 建立一监测，审查和评估数据处理程序 ▸ 最少化数据处理和数据保留 ▸ 为数据处理活动建立保障 ▸ 记录数据保护监管机构所需要的数据处理策略、程序和操作
隐私影响分析 Privacy Impact Assessment(PIA)	当进行有风险的或大规模个人数据处理时，组织必须进行隐私影响评估

GDPR的要点

同意	▸ 消费者同意企业处理数据必须是自由作出的决定并且是为了具体的目的 ▸ 消费者能取消同意的权利必须被告知 ▸ 企业在涉及敏感的个人数据或数据传输的情况下处理数据，必须获得消费者明确的同意
强制的数据外泄通告机制	▸ 组织在发生数据外泄时必须“没有不当延误”地或在72小时之内通知监管当局，除非这次数据外泄对个人没有风险 ▸ 如果会给个人带来高风险，那些可能遭遇风险的人也必须被告知
隐私设计Privacy by Design (PbD) 成为正式要求	▸ 组织应在使得PbD成为组织的一种文化，在组织提供的各类服务、产品的每个环节，充分考虑隐私要求，使隐私考虑成为组织工作当中一个自发的、默认的、必不可少的环节
新的权利	▸ 被遗忘权 — 个人有权要求数据控制者在特定情况下没有不当延误地删除所有个人数据 ▸ 数据可移植权 — 在技术可行的情况下，当个人已向某个服务供应商提供数据，他们可以要求该服务提供商将数据传输给另一服务提供商 ▸ 反对数据画像的权利 — 有权不接受仅在通过自动化数据处理建立的决策的支配
跨境数据传输	▸ 允许数据传输到由欧盟视为其法律制度可以提供个人数据保护适当水平的国家

GDPR的要点
监管与处罚

GDPR介绍了欧洲数据保护委员会（EDPB）。委员会的任务是：

- 监督GDPR在整个联盟中的统一应用
- 对GDPR相关事项给出建议
- 检查指导方针、建议、最佳实践以及其他问题
- 提供争端解决方案
- 制作数据保护年度报告

在GDPR下，地方数据保护机构通过使用行政罚款获得更大的权力来执行合规性。监管机构可征收高达**4%**全球年度营业额或**2,000万欧元**，罚款金额取决于以下因素：

- 性质、严重性和持续时间
- 数据加工的性质、范围和目的
- 涉及的数据主体数
- 意图
- 先前侵权行为
- 与数据保护机构的合作

GDPR的要点

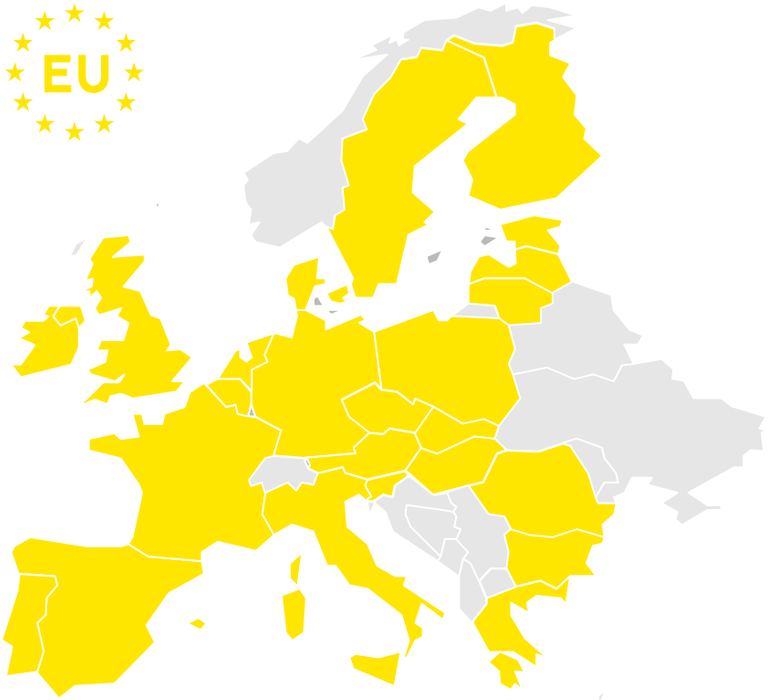
扩大范围 — 非欧盟企业的责任

非欧盟企业的责任

GDPR可应用到欧盟以外的数据处理活动，如果数据处理的目的为：

- 产品提供给在欧盟的个人信息权利人或在欧盟提供支持服务（例如：在线商店、IT服务供应商、外包合伙人、处理欧盟内的个人信息权利人数据的处理者）；或
- 监控欧盟居民个人信息权利人的互联网活动，如数据画像（例如：监控购物行为）
- 作为“处理者”处理欧盟内个人信息权利人的个人数据

例如，中国香港的企业实体向欧盟公民和/或在欧盟的一个分支机构提供服务时，将会被要求遵守通用数据保护条例，以及当地特定的法律及数据保护法律



GDPR的要点
数据保护官（DPO）

DPO
(DPO在公司是二道防线的一部分）

- DPO应适当并及时地参与与保护个人数据有关的所有问题。
- DPO必须得到业务部门的支持，提供执行这些任务所需的资源并获得个人数据和处理操作，并保持其专业知识。
- DPO应独立工作，不得接受外部指示。在执行任务时不得被业务单位解雇或处罚。
- 根据联盟或成员国法律，DPO应对其履行其任务保密。

公司一道防线、二道防线，共同保护个人信息，支持DPO工作

DPO的责任（第39条）

1. 通知并告知公司其与数据保护相关的义务
2. 与监督机构合作，并作为监督机构的联络人
3. 向数据主体提供与处理其个人数据有关的所有问题以及根据规定行使其权利的建议
4. 深入了解所有相关的数据保护和数据安全法规，并且必须对如何实施这些法规提供指导

GDPR的要点
责任制

“责任制” 原则

- 责任制需要数据控制者在他们的数据处理活动中，主动通过一定的手段促进和保障数据保护（例如：数据最少化、使用假名技术）。
- 数据控制者有责任遵守GDPR来进行处理操作。
- 数据控制者应有证明文件并且能在任何时候向个人信息权利人、公众和监管机构证明自己遵守了数据保护条例。

遵守政策，并实施恰当的方法来**确保在整个数据生命周期中个人数据是有保障的**

个人数据生命周期管理

GDPR的要点
隐私影响分析（PIA）

- 隐私影响分析是一个可嵌入企业现有项目管理方法的一个流程；
- 通常在一个新项目启动的时候，或对现有项目或流程改变的时候会启动隐私影响分析；

1. 识别隐私影响分析需求

通过问题筛选或项目启动前的分析，来确定隐私影响分析是否为项目中所需的流程

2. 描述信息流

描述项目中所涉及的信息流。解释什么信息将被使用，用来做什么，信息从谁那边收集，将披露给谁，谁能访问及其他必要的信息

3. 识别隐私相关的风险

对个人的风险，如由于信息的不准确或泄漏造成的损失；

对企业的风险，如隐私泄露造成名誉及经济的损失；及合规风险，如GDPR等

4. 识别并评估隐私保护方案

解释如何消除或降低风险，使风险达到项目可接受水平；

评估每种方案的开销及收益，并考虑可用的资源

5. 确认并记录PIA的结果

隐私风险获取确认及批准；

PIA报告汇总降低隐私风险的步骤和方法，并记录管理层关于风险处置的决策；

披露报告，统一项目影响理解

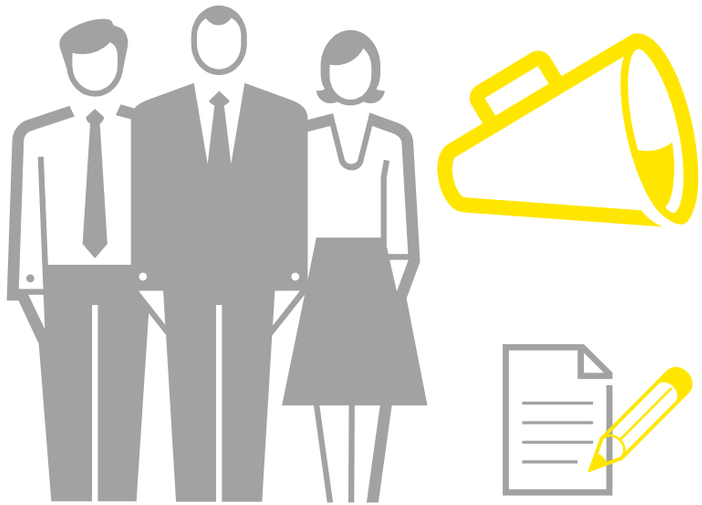
6. 将PIA结果整合，如项目计划

将PIA发现及整改措施融入项目计划，并在项目不同阶段重新审阅PIA结果；

项目过程中持续监控PIA的整改计划；

GDPR的要点
同意（Consent）

在GDPR中，“同意”被赋予了更多的条件



当把“同意”作为法律起诉的依据，必须确保满足额外要求：

- “同意”是被主动选择的，即不是通过默认的，静止的或提前勾选的框；
- “同意”数据被处理是可辨识的，清楚的并且不是与其他书面协定或声明捆绑在一起的；
- 当服务必须被提供时，服务条款是基于“同意”来制定的；
- 个人信息权利人应被告知他们有权随时取消同意的权利（通过简单的方法）；
- 不同的处理操作应获得独立的“同意”。
- 自由给予同意的权利

GDPR的要点
数据泄露通知

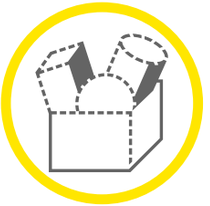
数据泄漏通知流程

- **数据处理者**必须向数据控制者报告个人数据泄漏
- **数据控制者**必须遵守GDPR具体的规定以及在影响到个人的某些情形下，向他们的监管当局**报告个人数据泄漏**事件
- 数据控制者必须**维护一个内部风险列表**
- 不遵守会导致**行政罚款**

GDPR的要点
隐私设计 (PbD)

“设计隐私”提出了以下观点：隐私的未来不能仅仅通过遵守监管框架来保证；相反，**隐私必须成为一个组织的默认操作方式**。

隐私设计



- 数据处理者以及IT系统生产商应该以数据最小化的方式和数据保护最友好的预设置来设计他们的服务
- 产品设计的原则应考虑仅能处理提供服务所需的数据
- 高安全标准
- 技术和组织措施的文件

默认数据保护

- 无需任何预调整的对数据主体的完整保护
- 不应收集额外的数据
- 向数据主体提供关于如何处理数据的清晰（说明性）的信息，包括安全标准，数据传输等。

GDPR的要点
数据主体的权利

1. **访问权（第12/15条）：**数据主体有权访问其被收集的所有数据。
2. **纠正权（第12/16/19条）：**数据主体有权纠正或完善数据。
3. **可移植权（第20条）：**数据主体有权从数据控制者接收可读格式的数据。
4. **删除权（被遗忘权）（第17条）：**数据主体有权要求数据控制者在某些情况下及时删除所有个人数据。
5. **数据加工限制（第18条）：**数据主体有权不受仅基于自动处理的决定限制
6. **反对加工处理的权利（第22条）：**不应仅基于自动处理的决定的权利
7. **知情权（第12/13/14条）：**告知数据主体数据如何使用的权利

GDPR的要点
跨境数据传输

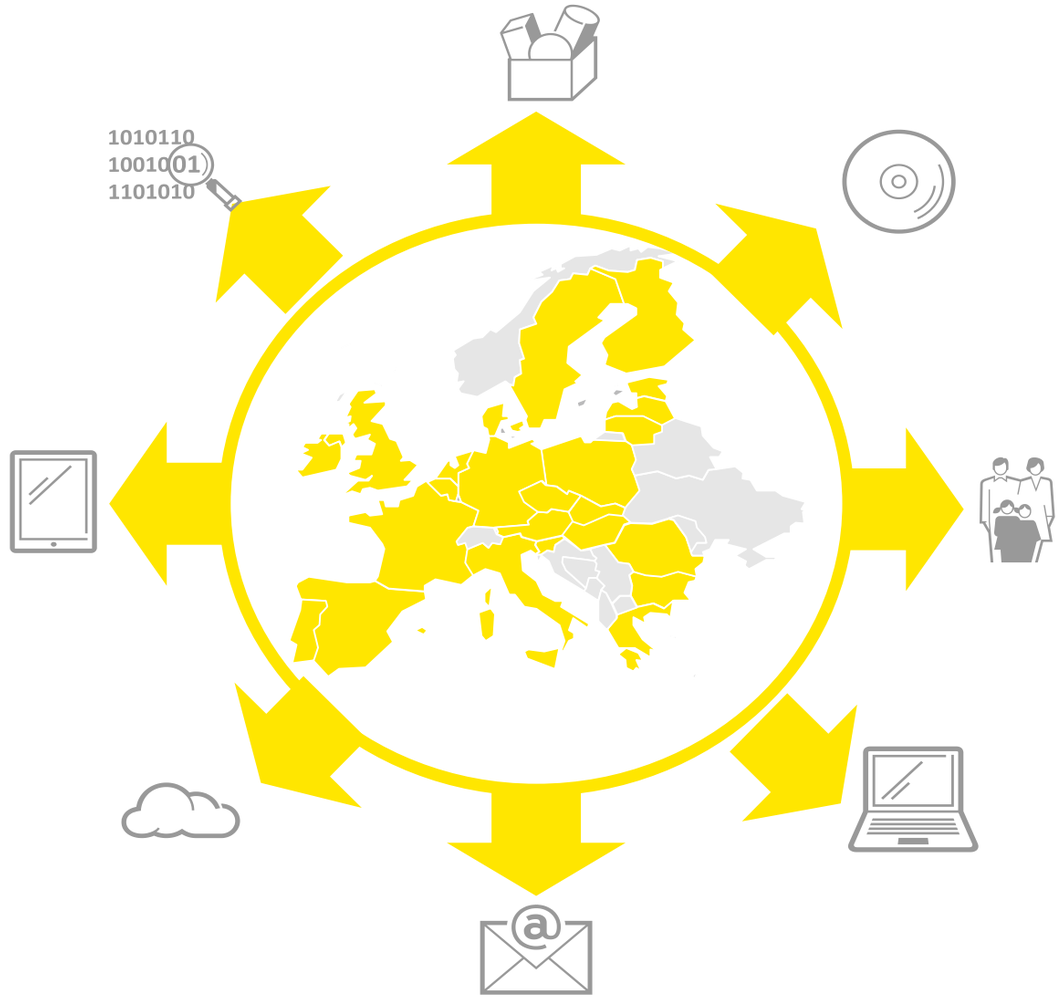
跨境数据传输

GDPR允许个人资料转移到第三国，但须**遵守相应的条件**，包括数据传输条件：

GDPR允许数据传输到由欧盟视为其法律制度可以提供**个人数据保护**达适当水平的国家。

如果适当的**保障措施**到位，允许向欧盟外部进行数据传输，例如：

- 标准的合同条款
- 有约束力公司规则 (BCRs)
- 批准的行为准则或认证机制（例如“欧洲数据保护认证”）



GDPR的要点
总结

罚款高达全球年营业额的
4%或
2000万欧元
以较大者为准

范围
扩展到欧盟和针对欧盟公民个人数据的组织中建立的所有数据管理者和加工者

问责制
在2018年5月28日生效后将成为今后数据保护取得成功的关键

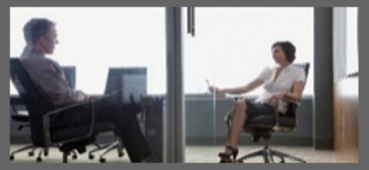
PIA
组织在进行有风险的或大规模的个人数据处理时必须进行隐私影响评估(PIA)

知情同意
必须清楚明确，并阐明目的

隐私设计
组织应该将数据保护设计为业务流程和新系统的开发的必要环节

DPO
如果组织进行大规模的监控或处理大量的个人数据，则必须任命数据保护官。

72 小时内必须将数据泄露事件通知监督机构，不得无故拖延，除非数据泄露行为对个人不构成威胁



新增权利

- 被遗忘权
- 数据可移植权
- 反对分析权

2018年5月28日
组织需要在生效日期前做好相关准备

EY 安永 | Assurance 审计 | Tax 税务 | Transactions 财务交易 | Advisory 咨询

关于安永
安永是全球领先的审计、税务、财务交易和咨询服务机构之一。我们的深刻洞察和优质服务有助全球各地资本市场和经济体建立信任和信心。我们致力培养杰出领导人才，通过团队协作落实我们对所有利益关联方的坚定承诺。因此，我们在为员工、客户及社会各界建设更美好的商业世界的过程中担当重要角色。

安永是指 Ernst & Young Global Limited 的全球组织，也可指其一家或以上的成员机构，各成员机构都是独立的法人实体。Ernst & Young Global Limited 是英国一家担保有限公司，并不向客户提供服务。如欲进一步了解安永，请浏览ey.com。

APAC NO. 03006622
ED

ey.com/china