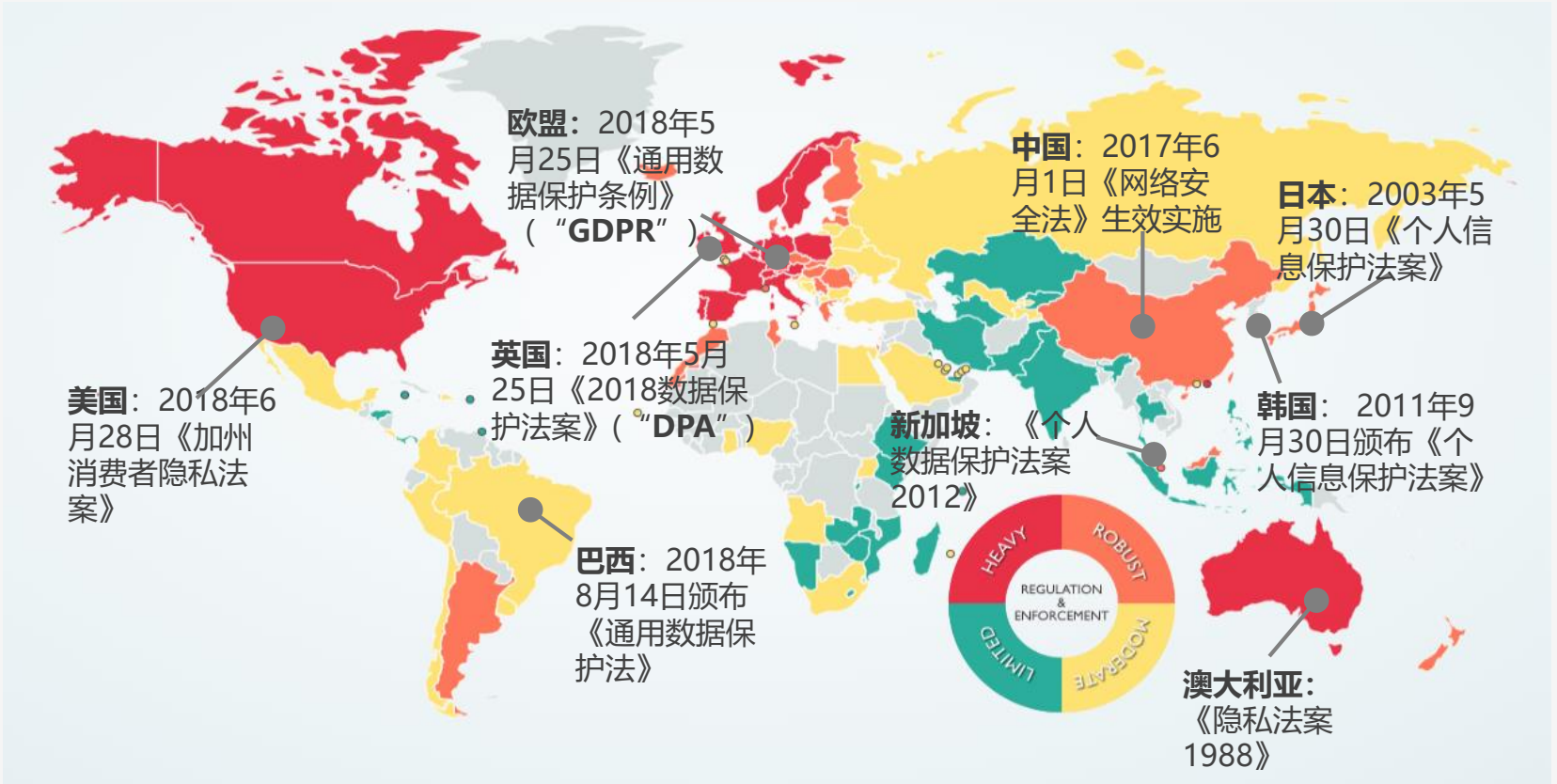
金杜律师事务所
KING&WOOD
MALLESONS

GDPR数据保护合规

北京市金杜律师事务所
网络安全与数据合规团队

全球数据保护立法趋势


欧盟：2018年5月25日《通用数据保护条例》（“GDPR”）
中国：2017年6月1日《网络安全法》生效实施
日本：2003年5月30日《个人信息保护法案》
美国：2018年6月28日《加州消费者隐私法案》
英国：2018年5月25日《2018数据保护法案》（“DPA”）
新加坡：《个人数据保护法案2012》
韩国：2011年9月30日颁布《个人信息保护法案》
巴西：2018年8月14日颁布《通用数据保护法》
HEAVY
ROBUST
REGULATION & ENFORCEMENT
LIMITED
MODERATE
澳大利亚：《隐私法案1988》

数据保护重要性日益提升

2018年是数据保护具有里程碑意义的年份。自2018年5月25日欧盟GDPR生效以来，深刻影响欧盟乃至全球范围内个人数据保护和数字经济发展态势。

巨额罚金造成损失

- 截止19年9月，22个国家DPA对87件案件共做出**373,650,857** 欧元的行政处罚决定。
- 其中共开出**6**件超过**50万**欧元罚款的行政处罚，最大罚单超**2亿欧元**。
- 经过一段时间的适应期，2019年以来，各国DPA 处罚力度明显加大。

个人数据权利意识提高

- 随着GDPR 执法的深入，公众对数据保护规则及个人权利的了解有了很大提升，向DPA咨询GDPR和提出申诉的人日益增多。
- 同时，非营利组织代表个人发起的申诉也开始出现。

企业合规成本高昂

- GDPR让美国财富500强企业在实施前就花费了**78亿美元**合规成本。
- 对中型企业来说，两年平均花掉的合规成本为**55万美元。**
- 68%的公司预计将花费**100万到1000万美元**的投入。

GDPR概况

➢ **基本情况**

- GDPR共99个条文，全文共263页。
- 为应对快速的科技发展对个人数据保护带来的全新挑战，GDPR对1995年的《欧盟数据保护指令》（95/46/EC）进行了大刀阔斧的改革，全面提升了对个人数据的保护力度，堪称史上最高标准的数据保护条例。

➢ **立法目的——GDPR第2条**

- 保护自然人的基本权利及自由，尤其是自然人保护个人数据的权利。
- 不能以在个人数据加工领域保护个人权利为由，阻碍或限制欧盟范围个人数据的自由流动。

此前

- 1995年《欧盟数据保护指令》及一系列配套措施；

2016年4月27日

- 欧洲议会及欧盟理事会共同颁布GDPR文本，设定两年过渡期；

2018年5月25日

- GDPR正式生效，替代施行了二十余年的《欧盟数据保护指令》。

GDPR的适用

➢ **适用对象：数据处理**

- 对个人数据进行的任何操作（无论是否自动化），例如收集、记录、组合、建构、存储、修改、使用、披露、传输、或以其它方式使用。

➢ **需要转化为成员国国内法?**

- GDPR可直接约束相关主体行为，**无需**转化。
- 在不与其发生冲突的前提下，GDPR允许成员国进行更为细化、具体的国内立法。

- **欧盟内**建立的控制者及处理者：无论数据处理行为是否发生在欧盟境内。
- 即便控制者和处理者设立在**欧盟外**，GDPR也适用于：
  - 向欧盟境内数据主体**提供商品和服务**的，如向产品销往欧盟的电商平台、设有欧盟分公司/分支机构的企业等；
  - **监控**数据主体在欧盟境内行为的；
  - 根据国际公法适用**成员国法律**的。

GDPR中的“个人数据”

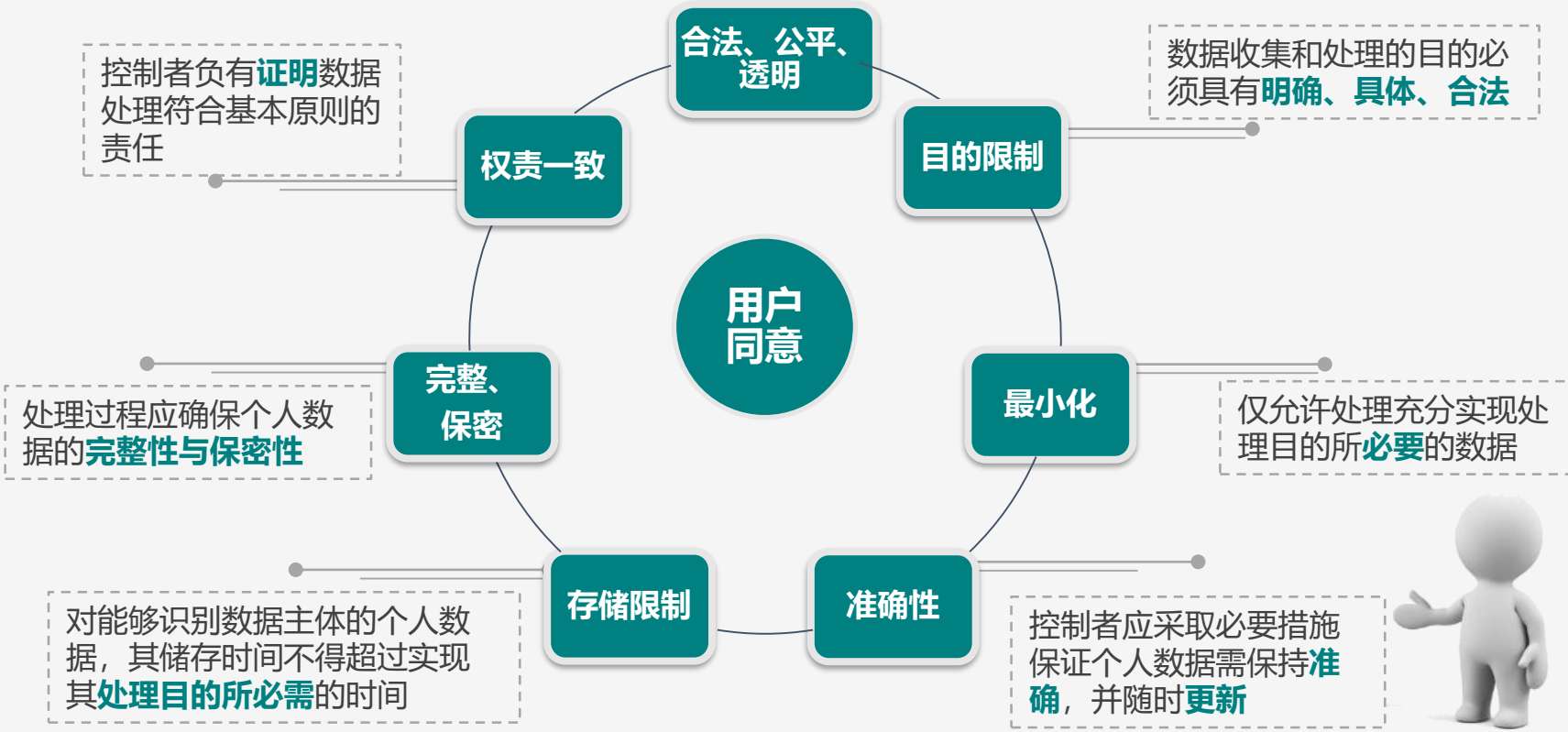
- **“个人数据”**，指**一切指向数据主体的信息**，诸如姓名、身份证号码、定位数据、在线身份识别，或是针对该自然人一个或多个如物理、生理、遗传、心理、经济、文化或社会身份的要素。
  - IMEI（国际移动设备识别码）、设备MAC地址?
  - 网上浏览行为记录?
  - 社交软件的好友列表?

- **“数据主体”**，指一个**已识别（identified）**或**可被识别的（identifiable）**自然人。拥有一个人的信息越多，这个人就越有可能被识别，数据处理则存在更多的风险。

- **“特殊类型个人数据”——GDPR第9条**

  表明自然人种族或族裔、政治观点、宗教或信仰、工会会员资格的，或基因数据、生物识别数据等可唯一识别自然人的，或与个人健康状况、性生活或性取向相关的数据。 **（原则上禁止处理）**

个人数据处理的基本原则



数据主体的基本权利

权利	内容	条款	具体实现
获取权	数据主体有权要求控制者告知个人数据是否被处理，处理目的、保留时间、跨境传输的安全措施等。	第15条	控制者应提供访问接口、交互界面，或以隐私政策、弹窗、邮件、短信、电话等方式告知
被遗忘权	数据主体有权要求控制者及时删除其个人数据	第17条	控制者应提供撤回同意、注销账号或要求删除的申请方式，并告知数据主体
修改权	数据主体有权要求控制者及时修改不准确的个人数据，有权补充不完整的个人数据	第16条	控制者应提供数据主体反馈意见的渠道，并及时作出响应
限制处理权	数据主体有权限制数据控制者处理其个人数据	第18条	
可携权	数据主体有权获取其个人数据，并且有权将这些数据转移到另一个控制者	第20条	
异议权	数据主体有权反对处理其个人数据	第21条	
自动化决策	数据主体有权不受基于自动化处理行为得出的决定的制约，当产生法律效果或者其他类似重大影响时	第22条	在基于自动化处理行为作出决策前，取得用户同意或确认是否为签订、履行与用户之间的合同之必要

GDPR下主要的法律义务主体（一）：数据控制者

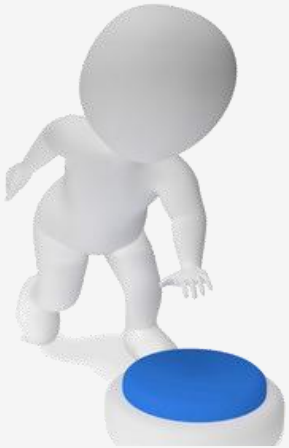
数据控制者作为个人数据收集、使用等过程的主导角色，决定了数据处理目的和方式等关键因素；为此，欧盟GDPR体系下，数据控制者承担了最为严格的数据合规义务。

GDPR中对（共同）数据控制者的定义：

“控制者”是指，能单独或者共同决定个人数据处理的目的和方式的自然人、法人、公共机构、行政机关或者其他主体。（第4条）

“共同控制者”是指，当由两个或两个以上的控制者共同决定数据处理的目的和方式时，这些控制者构成共同控制者。（第26条）

相应地，共同控制者之间应当以一种透明的方式，决定其各自应当履行的GDPR下的数据合规义务以及相应承担的责任，尤其是与数据主体权利实施相关和根据数据主体权利而各自需要提供信息的职责。



GDPR下主要的法律义务主体（一）：数据控制者

主体要素

•自然人或法人、公共机构、行政机关或其他任何实体

能力要素

- “**决定**”
- “**目的**”和“**方式**”

数量要素

•单一：数据控制者

•多个：共同控制者

➢ **“决定”**

- *明示的法律能力导致的控制*

  例如，国家法律明文授权公共安全部门对户籍 进行建档、收集和管理；

- *默示的法律能力导致的控制*

  例如，雇主对雇员信息的处理；

- *事实影响导致的控制*

  对复杂合同关系的分析、评估。

➢ **“目的”和“方式”**——决定的内容

- 对“目的”的决定是控制者专享的权利，即数据处理发生的原因；
- 而对“方式”的决定则不尽然，控制者应当完全知晓或者被通知用以实现处理目的的处理方式，但具体的细节可以由处理者决定。例如，使用何种IT系统进行数据收集、数据安全保障措施的技术细节、个人数据进行传输的具体方式、确保数据主体删除权实现的技术机制等。

GDPR下主要的法律义务主体（二）：数据处理者

数据处理者不会参与到数据处理的目的决定过程，而是通过向控制者提供处理服务的方式，以数据控制者的名义进行数据处理。因此，数据处理者承担的数据合规义务和责任低于数据控制者，但仍需遵守数据安全保障等相关义务。

GDPR下对于数据处理者的定义

“数据处理者”是指以控制者名义处理个人数据的自然人、法人、公共机构、行政机关或其他主体。因此，数据处理者的出现取决于数据控制者的选择。

因此，数据处理者的外部特点，决定了其判断依然存在主体层面的要求，即属于法律上独立的实体。除此之外，处理者判断的一个核心，即是**“以控制者的名义”**：

- 数据处理者的数据处理行为，并非服务于其自身利益，而是**基于委托行为服务于他人**；
- 处理者应当基于控制者的指示进行处理，“指示”则至少包括**数据处理的目的及处理方式的基本要求**。

数据处理中的主要义务（适用于控制者和/或处理者）

- **数据控制者**作为数据处理的决定性角色，在GDPR下**承担义务最重、责任范围最大**：

  实施适当的技术和组织措施保护数据主体的权利，确保数据处理符合相关规定

- 此外，**数据处理者**应：
  - 提供足够的安全保障
  - 未经控制者同意，不得再次委托数据处理
  - 发生安全事件时，及时告知控制者
  - 处理服务终止时，应删除、匿名化或返还全部数据

记录处理活动	通知数据泄露	数据保护影响评估	设置数据保护官	配合监管机构
• 依职责保存处理活动的记录 • 记录内容如目的、主体类别、控制者联系方式等	• 72小时内通知监管部门 • 及时通知受到实质影响的用户	• 采用新技术，可能影响自然人的权利和自由时，进行相应的影响评估	• 如有必要，应委任数据保护官员	• 如监管机构要求，应配合监管机构，提交文档、记录等

个人数据跨境

- 以**充分保护**为原则，以基于**适当保护措施**的传输为例外

数据跨境的合规方式	优势	劣势	可能适用的情形
有约束力的公司准则 Binding Corporate Rules, “BCR”	• 正式的法律地位 • 认可的程序和内容标准有详细规定 • 一经建立，后续数据可自由跨境流动	• 制度设计、建设成本高 • 审批、认可的时间成本高（一般需要一年以上） • 存在不确定性	具有长期、频繁、大量的数据跨境传输需求的企业的最终选择
标准合同条款 Standard Contract Clause, “SCC”	• 能较为完整地满足GDPR合规要求 • 相较于BCR，成本更低 • 适用性强，对商业实践影响较小	• 合规风险残留，建议作为过渡措施 • SCC签订后GDPR下合规义务扩展至签约实体，可能带来沉重负担	存在较为频繁的数据跨境传输，却无法及时获得BCR认可的企业
用户同意 Explicit consent	• 不会对企业整体造成组织或制度层面的重大影响	• 可能造成大量业务流失 • 合规风险残留，不建议长期使用 • 获得同意的全面告知和机制设计存在困难	小规模、临时的数据跨境合规方式
选择性本地化 Selective Localization	• 本地化的数据处理过程无需履行个人数据跨境传输的相关义务	• 本地化成本较高 • 对商业实践带来影响较大 • 存在无法实施的情况：例如准入限制	欧盟业务规模较大且已有商业存在（如子公司等）的企业

违反GDPR的责任

➢ 行政责任（GDPR第83条）

- 各成员国内数据执法机构DPA**均有权**根据本条规定实施行政处罚。
- 视违法程度和具体行为，罚款数额分为两层：
  1. **一千万**欧元，或企业年度**全球营业额2%**，取其高者
  2. **两千万**欧元，或企业年度**全球营业额4%**，取其高者

➢ 法律救济途径

- **数据主体**：
  1. 有权向各监管机构递交投诉，并获知处理进度及结果（GDPR第77条）；对于处理结果或三个月内未处理的，有权向具有管辖权的成员国法院提起诉讼（GDPR第78条）
  2. 有权向具有管辖权的成员国法院起诉，寻求司法救济（GDPR第79条）
  3. 数据主体有权根据受损情况从控制者或处理者处获得相应赔偿（GDPR第82条）
- **控制者/处理者**：
  1. 有权针对监管机构作出的有法律拘束力的决定，向监管机构设立地的成员国法院寻求司法救济（GDPR第78条）

联系人

宁宣凤
高级合伙人
北京
Tel: +86 10 5878 5010
Fax: +86 10 5878 5599
susan.ning@cn.kwm.com

工作经历及教育背景

宁宣凤律师于1995年加入金杜律师事务所，现为金杜高级合伙人，并担任金杜合规业务部负责人。

宁宣凤律师毕业于北京大学，获法学学士学位；后就读于加拿大McGill大学，获法学硕士学位。

宁宣凤律师于1988年获得律师资格。

执业领域

宁宣凤律师是中国最早涉足网络安全与数据合规法律实务的律师之一，拥有一支具备跨学科背景的专业律师团队，能为客户提供网络安全自查、应对网络安全检查、数据合规培训、数据交易尽职调查、数据跨境传输合规等法律服务，提供综合性法律服务解决方案。

自2016年起，宁律师与金杜团队就为客户提供涉及网络安全与数据合规领域的优质全面的法律咨询和定制化的专项服务，并得到客户和业界的高度赞誉。宁律师的客户涵盖国内外知名跨国公司、传统实业及新兴互联网企业等，行业涉及银行金融、医疗科技、汽车制造、智能设备/家居、互联网出行、电子商务、酒店、能源、云服务、航空运输、日化产品、社交应用、线上游戏等众多领域。

为把握大数据立法的最新动态和监管趋势，金杜还加入了全国信息安全标准化技术委员会下的信息安全管理标准工作组、大数据标准工作组以及国家人工智能标准化总体组，积极参与大数据产业标准的制定。凭借国内外法律研究与实践能力，宁律师与金杜团队能够结合国内《网安法》、欧盟GDPR等为客户提供全方位的法律分析与咨询服务，助力客户在全球主要地区实现数据合规的无缝衔接，并结合行业最佳实践为客户量身打造综合性解决方案，协助客户从法律风险控制、产品方案规划、商业模式设计、公共关系应对等方面全方位应对网络安全与数据合规。

2019年，宁宣凤律师荣获LEGALBAND评选的中国网络安全与数据保护领域BAND 1执业律师。

金杜律师事务所
KING&WOOD MALLESONS

谢谢！