Bird&Bird&鸿鹄律师事务所

GDPR 何处适用？欧洲数据保护委员会的最终权衡

*久经酝酿，欧洲数据保护委员会(“**EDPB**”)公布了《关于2016/679通用数据保护条例(“**GDPR**”)的地域适用范围指引（征求意见稿）》（点击此处以查看本指引英文版原文）。我们对其中部分重点信息总结如下。如果您想对公众意见征求进行回复或进一步讨论，请与我们联络。*

提醒：GDPR 可通过以下两种方式适用于一个组织：(1) 因为该组织在欧盟境内设立营业地(*establishment*)（或欧盟法律适用的其他地方——例如大使馆），并且在该营业地的“活动范围内(*in the context of*)”进行个人数据处理；或(2)对于未在欧盟建立营业地的组织，因为其向欧盟境内的个人提供商品或服务或监控个人的行为。

点击下面的链接可跳转到每个部分:

1. EDPB 确认宽泛解释：一个组织何时被视为“已设立(established)”

为确定 GDPR 是否因一个组织的设立而得以适用，EDPB 提出了两步测试：第一，评估组织是否已设立；第二，确定该营业地的活动范围内是否进行个人数据处理。本指引表明，组织应宽泛理解这两个要求。

a) 设立营业地的门槛“非常低”——单个员工或代理人的存在即可能足以满足要求

根据 GDPR 前言第 22 条，“营业地意味着通过稳定的安排进行有效和真实的活动*(establishment implies the effective and real exercise of activities through stable arrangements)*”。本指引对此解释，“必须考虑到安排的稳定程度和该成员国的有效活动”。

这是一个十分针对具体事实的调查，要求一组织应考虑其与欧盟的联系和存在形式的属性。正如 GDPR 前言第 22 条所述，“此类安排的法律形式，无论是通过分支机构还是具有法人资格的子公司，都不是决定性因素”。

本指引与欧盟法院（“**CJEU**”）在 *Weltimmo* 案中提出的对营业地的定义相一致：欧盟法院判定，即使是“最小（*minimal*）”活动，也足以认定为营业地。然而，这个案例非常特定化：它是一家小公司（实际上是一人经营），公司所有者住在匈牙利，并且公司主要是为匈牙利市场服务，但刚好却是在其他地方成立。

本指引进一步为互联网组织扩展了这一原则，认定“当数据控制者的活动中心涉及提供在线服务时，‘稳定的安排’的门槛可以非常低”。在某些情况下，“具备单个员工或代理人即可认定具有足够的稳定性”。

b) *欧盟境内营业地具有收入就可满足要求，但仅可通过网站进行访问不足以认定*

对于视为在欧盟境内设立的组织，数据处理必须是在欧盟境内的“营业地的活动范围内*(in the context of the activities of an establishment)*”——但该营业地不需要参与处理。本指引确认，在“欧盟营业地的活动与非欧盟数据控制者执行的数据处理之间存在着不可分割的联系*(an inextricable link)*”的情况下，该条件得以满足。在此需要考虑的一个因素是，欧盟境内的营业地是否代表该非欧盟实体参与了实现收入的活动。

EDPB 提供了一个中国电商网站的例子：该电商网站在柏林设有办事处，负责向欧盟市场开展商业和营销活动。由于柏林办事处有助于使电商活动在欧盟获利，EDPB 认为，这足以认定该中国公司在其德国营业地的活动范围内处理个人数据。

本指引脚注第 16 条提供了最直接的阐述：“任何在欧盟设有销售办事处或其他存在形式的外国经营者，即使该办事处在实际数据处理中没有任何作用”，也可能受到 GDPR 的约束。同样，本指引反映了判例法中的广泛观点。在欧盟法院谷歌西班牙*(Google Spain)*案中，因为谷歌在西班牙设有销售的子公司，谷歌在美国的搜索业务被认为是已设立了欧盟境内的营业地，但也本可以更加狭义地理解该判决，因为该西班牙子公司出售了针对西班牙市场的母公司的广告产品。

相比之下，本指引澄清了仅因网站具有可访问性并不视为设立了欧盟境内营业地。这也反映了判例法——VKI 诉亚马逊案*(VKI v Amazon)*——该案之前认定网站不是营业地。EDPB 提供了一个针对欧盟消费者、但在欧盟没有任何存在形式的连锁酒店的例子。GDPR 第 3 条第(2)款（域外规定）才是其准确的分析依据，而不是第 3 条第(1)款。

c) *GDPR 适用于数据处理活动——一个组织可能存在的某些活动才受到约束的情况*

本指引确认，仅仅因为一个组织可能被认为是“已设立营业地”，并不会使其所有活动都受 GDPR 的约束。因此，国际组织必须根据具体情况考虑其活动。本指引提供了一家总部位于美国的汽车制造商的例子，该公司在比利时拥有一家全资分支机构以负责营销。该公司的比利时分机构可能会使其美国公司的某些面向客户的活动受到 GDPR 的约束，但这并不意味着 GDPR 适用于美国员工数据。

2. EDPB 尝试对 GDPR 的域外适用进行限制

在以下相关个人数据处理活动中，GDPR 适用于非欧盟成立的组织：(a)在欧盟境内提供商品或服务；或(b)监控欧盟境内数据主体的活动。

a) *提供意味着提供，且需具备意图*

在本指引发布之前存在的一个重要问题是，“提供(*offering)*”商品和服务是否也包括“已提供(*providing)*”服务——或者是否只有提供之时的具有意图才与之相关。

本指引明确规定，“无论提供或进行监测的时间长短，都必须在提供商品或服务之时，或在监控行为之时，对数据主体是否位于欧盟境内这一要求进行评估(*the requirement that the data subject be located in the Union must be assessed at the moment of offering goods or services or the moment when the behaviour is monitored, regardless of the duration of the offer made or the monitoring undertaken*)”。

这意味着，不计划在欧盟提供服务但可能在欧盟被访问的组织将不受 GDPR 的约束。例如，一个组织意图面向美国提供某款 APP，将不会仅因为其某些美国用户在欧洲旅行时访问该 APP，而受到 GDPR 的约束。

GDPR 的适用必须具有“针对性(*targeting)*”。判断该针对性的相关因素包括：

- 在宣传材料中提及欧盟或一成员国；
- 向一搜索引擎运营商支付费用以便于用户在欧盟境内访问该网站，或推进针对欧盟受众的营销活动；
- 该活动具有国际性，例如与旅游有关的活动；
- 提供与产品或服务相关的本地电话号码或地址；
- 使用涉及欧盟或一成员国的顶层域名（例如“.eu”或“.de”）；
- 提供来自一成员国的旅行指示；
- 在宣传材料中提及国际用户或提供用户推荐（特别是在用户位于欧盟的情况）；
- 使用欧盟语言或货币；以及
- 在欧盟提供送货服务。

本指引并未规定 GDPR 适用时必须存在任何或所有这些因素，但是这些是数据保护机构在判断是否具有针对欧盟个人的足够意图时所考虑的各种指标。

以苏黎世的瑞士大学为例。瑞士大学的招生对任何具有足够英语或德语知识的学生开放。在这种情况下，GDPR 将不适用，因为“在申请或选拔的过程中，没有对欧盟的学生进行区别或规范”。但是，瑞士大学的国际关系暑期课程专门向德国和奥地利大学进行广告宣传，这将使得 GDPR 适用于任何与此相关的数据处理活动。

b) *监控须具有目的性*

与提供商品和服务相反，GDPR 第 3 条第二款中涉及的监控并没有特别要求表示出任何意图。但是，本指引规定，“监控(*monitoring)*”一词的使用表明“数据控制者具有对数据主体在欧盟境内行为的相关数据进行收集并后续再利用的特定目的”。

识别监控的“主要考虑因素”是存在“任何后续行为分析或用户画像(*profiling)*技术”。GDPR 所定义的用户画像，要求对“与自然人有关的个人方面”进行自动数据处理以及评估，比如预测健康状况、个人偏好、经济状况、工作表现、位置或行踪等。

换言之，对涉及某时间段内在欧盟境内的数据主体行为个人数据被动收集并不足以构成监控——而是必须同时具有评估目的。本指引提供了一系列例子，包括：

- 精准行为广告投放和内容的地理定位（特别是用于广告目的）；

- 通过使用 cookie 或指纹识别设备进行在线跟踪；
- 在线个性化饮食和健康分析服务；
- 闭路电视监控；
- 基于个人用户画像进行的市场调查和其他行为研究；以及
- 监测或定期报告个人的健康状况。

尽管 EDPB 表示监控并不一定于线上发生（例如，EDPB 明确举出可穿戴式技术和其他智能设备），有趣的是，EDPB 提供的大部分例子是关于在线跟踪的，并没有提及其他普遍使用的案例（比如反洗钱检查，员工邮件监控以及欺诈预防等）。EDPB 的以上列举情况在本指引的终稿中是否会得到扩大仍有待观察。

3. 即使数据控制者并不适用，位于欧盟境内的数据处理者仍必须遵守 GDPR——但是，这在数据输送的限制方面如何适用？

各个组织在遵守 GDPR 时遇到的棘手情况之一是，在不受 GDPR 约束的数据控制者聘用位于欧盟的数据处理者的情况下该怎么处理。由于数据处理协议的实施要求似乎同样适用于数据控制者和数据处理者，后者是否需要继续提供前者既不需要、也不想要的合同保护？

简而言之，是的。本指引阐明，如果数据处理者受 GDPR 的约束，即使数据控制者不受 GDPR 的约束，数据处理者仍必须遵守对其适用的所有规定，包括需要制定 GDPR 第 28 条规定的合规协议（除去协助数据控制者遵守 GDPR 规定下作为数据控制者义务相关的义务）。这与某些国家数据保护机构的 GDPR 指引中对数据处理者义务[例如，CNIL（法国信息与自由委员会），ICO（英国信息委员会办公室），Irish DPC（爱尔兰数据保护委员会）]的规定是一致的。与此同时，EDPB 本指引确认，仅仅在欧盟境内聘用数据处理者的事实不会使数据控制者也受 GDPR 的约束。这可助于向数据控制者确保可在不增加他们自己的法律风险的情况下达成此类协议。

除强制性合同外，本指引还规定了位于欧盟的数据处理者还必须遵守 GDPR 的数据处理者义务，例如对数据输送的限制。然而，数据处理者究竟该如何遵守还不清晰：

- 首先，如果数据处理者将数据发送回数据控制者，是否需要在数据控制者和欧盟内的数据处理者之间建立数据传输机制？导致的这一结果似乎是异常的，因为(a)目前不存在从欧盟数据处理者输送到非欧盟数据控制者的标准合同条款（“**SCCs**”）；以及(b)我们通常认为数据控制者是发起数据转移的数据控制者，因为他们决定了目的和手段。因此，这可能不是来自欧盟的数据输送，而只是输送到欧盟——这并不是受到限制的情况。对这一问题，有待 EDPB 的澄清。
- 其次，即使 EDPB 仅意在解决下游数据传输（即从欧盟数据处理者到非欧盟分数据处理者），SCCs 条款仍然是一个难以适用的工具。欧盟委员会曾试图起草数据处理者—数据处理者条款(processor-processor clauses)的尝试已以失败告终，但由于数据输送条款直接适用于欧盟数据处理者，因此当前该需要更加紧迫。

4. 组织注册事项——谨慎选择您的船旗和其他特殊情况

如营业地标准所述，GDPR 不仅限于位于欧盟境内的数据主体的个人数据处理。相反，GDPR 适用于收集自然人（无论其国籍或居住地）的个人数据的欧盟组织。EDPB 明确证实了这一点，并列举了一家法国公司的例子：该法国公司运营一款针对摩洛哥、阿尔及利亚和突尼斯的用户的共享汽车 APP，该服务仅在这三个国家/地区提供，但所有个人数据处理活动均由法国的数据

控制者进行。在这种情况下，即使处理涉及不在欧盟的 APP 用户的个人数据，GDPR 的规定也适用于法国公司进行的数据处理活动。这一结果可能使某些仅在非欧盟市场运营的欧盟境内组织重新考虑其组织的注册国家的决定。

另外，GDPR 还适用于根据国际公法，欧盟或一成员国法律得以适用的地方建立的组织，例如大使馆和领事馆。根据本指引，在国际水域中悬挂德国国旗（因其注册地为德国）的游轮也将受到 GDPR 的约束。这一情况同样适用于航空器。

5. 欧盟境内代表也不能同时是数据控制者的数据处理者，他们承担责任并且可能会扩大其作用

a) *欧盟境内代表不能也是非欧盟数据控制者的数据处理者*

鉴于执法过程中可能存在义务和利益冲突，本指引规定数据处理者不能作为数据控制者的代表。

这可能会影响欧盟境内数据处理者，这些数据处理者也提供代表性服务以及代表非欧盟数据控制者处理个人数据，例如同时向非欧盟赞助商提供代表性服务的临床试验提供商。

b) *代表的责任——迫切需要澄清*

GDPR 前言第 80 条表明，代表可以代表外国数据控制者或数据处理者承担责任。这似乎违背了一般法律原则，即人们只能对自己的作为或不作为承担责任；同时，鉴于前言不具有法律约束力，许多人想知道数据保护机构是否会对代表行使执行权。

本指引规定代表可能要承担责任，但并未明确该责任的范围。在本指引的最后一句中，EDPB 指出“*目的是使执法者能够以与数据控制者或数据处理者相同的方式对代表进行执行。其中包括可能施加行政罚款和处罚，并要求代表承担责任*”，但没有进行进一步解释。

显然，代表可能要对未能履行自己的职责承担责任。但这是否也意味着授权数据保护机构对因数据控制者或数据处理器者的行为对其代表进行罚款？我们希望 EDPB 在发布最终指引时能够明确其立场。承担全球年收入 4%或 2000 万欧元罚款的风险可能使得很难找到担任这个角色的代表。

c) *EDPB 将欧盟境内代表的职责扩展到 GDPR 的要求之外*

本指引进一步详细说明了代表的职责的其他方面：

- 代表性职责不同于与外部数据保护官(DPO)的职责，因为这会引起利益冲突
- 虽然代表可以是一个组织而不一定是一个人，但指引建议让一位主管人员担任该职位
- 在隐私声明中需要提供代表的姓名，但不需要专门通知数据保护机构
- 代表必须位于数据主体所在的成员国，并且最佳实践中，应该位于数据主体最密集的地方
- 代表必须促进数据控制者/数据处理者与数据主体或数据保护机构之间的通信。为此，EDPB 指出“通信必须以监管机构或有关数据主体使用的语言进行”
- 本指引规定，维护处理记录是数据控制者/数据处理者和代表的“共同义务”

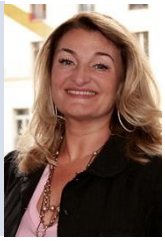
其中一些要求似乎超出了 GDPR 第 27 条的范围，对许多组织来说将是繁重的义务——特别是如果因上述责任承担问题使得难以找到合格的代表候选人。但是，本指引同时建议各方

可以通过合作履行职责。订立一份将某些任务委托给数据控制者或数据处理者的详细协议，可以是满足上述标准、而无需设立一重要的欧盟境内存在形式的一种方式。

联系人

Ariane Mole
合伙人, 法国

Tel: +33142686304
ariane.mole@twobirds.com



Gabriel Voisin
合伙人, 英国

Tel: +442079056236
gabriel.voisin@twobirds.com

Gabe Maldoff
律师, 英国

Tel: +442079826442
gabe.maldoff@twobirds.com

Alexander Shepherd
合伙人, 新加坡

Tel: +6564289487
alexander.shepherd@twobirds.com

余绚雯(Clarice Yue)
顾问律师, 中国

Tel: +85222486113
clarice.yue@twobirds.com

Lisa Vanderwal
顾问律师, 澳大利亚

Tel: +61292269832
lisa.vanderwal@twobirds.com

Ruth Boardman
合伙人，英国

Tel: +442074156018
ruth.boardman@twobirds.com

柯恬恬
律师助理，英国

Tel: +442079826515
tiantian.ke@twobirds.com

twobirds.com

阿姆斯特丹 & 阿布扎比 & 北京 & 布拉迪斯拉发 & 布鲁塞尔 & 布达佩斯 & 哥本哈根 & 迪拜 & 杜塞尔多夫 & 法兰克福 & 海牙 & 汉堡 & 赫尔辛基 & 香港 & 伦敦 & 卢森堡 & 里昂 & 马德里 & 米兰 & 慕尼黑 & 巴黎 & 布拉格 & 罗马 & 旧金山 & 上海 & 新加坡 & 斯德哥尔摩 & 悉尼 & 华沙