公益翻译小组荣誉出品

EDPB《GDPR 域外适用指南》中译本

译校者：陈昕、李璐瑶、柯恬恬、于雪、李为

2019 年 12 月 3 日

译者简介及工作分工：

陈昕（1-1(d)(i)），北京大学国际法学院硕士研究生

李璐瑶（1(d)(ii)-2(a)），在线途游（北京）科技有限公司海外法务专员

柯恬恬（2(b)-2(c)），鸿鹄律师事务所伦敦办公室律师助理

于雪（简介及2(d)-3），中国社会科学院大学法硕研究生

李为（第四节），现任职于广东国智律师事务所

序言

2019 年 11 月 12 日，欧洲数据保护委员会（European Data Protection Board, “EDPB”）对外发布了针对《通用数据保护条例》（GDPR）域外适用效力的最终指南。GDPR 作为欧盟统一法规，旨在促进各类组织改变处理数据隐私的方式，保护欧盟公民的个人信息数据权，以回应公众和立法者对各类组织，尤其是企业无限制收集和处理欧盟公民个人信息行为的担忧。根据 GDPR 的规定，企业违规将被处以最高 2000 万欧元的罚款或上一财政年度全球年营业额的 4%的较高者。因此，了解 GDPR 的适用范围，对于跨国公司及具有开拓国际市场意向的企业而言具有重要意义。

基于此，本译组对《通用数据保护条例》第 3 条，即地域适用范围条款及说明进行全文翻译，以期为实务界及数据法研究的各位同仁提供参考。

基于欧洲议会和欧盟委员会于 2016 年 4 月 27 日共同通过的《2016/679/EU 条例》（有关个人数据保护及数据自由流通，和《95/46/EC 指令》的废止）的第 70 条第 1 款第 e 项的规定，欧盟数据保护委员会（EDPB）通过了如下指南：

简介

《通用数据保护条例》[1]（下称“GDPR”或者《条例》）第 3 条规定了其地域适用范围，与《95/46/EC 指令》[2]所定义的框架相比，这是欧洲数据保护法的重大发展。GDPR 在一定程度上承认了欧盟立法者和欧盟法院（CJEU）在《95/46/EC 指令》生效期内作出的决定。同时，GDPR 也规定了新的重要内容。其中最重要的是，《指令》第 4 条主要规定哪些成员国的国内法是可适用的，而 GDPR 第 3 条则是规定《条例》可直接适用的地域范围。此外，《指令》第 4 条引入在欧盟境内“使用设备（use of equipment）”这一概念，从而把“未在欧盟境内设立”的控制者纳入欧盟数据保护法的调整范围，但是这一概念在 GDPR 第 3 条中没有体现。

GDPR 第 3 条反映出，立法者想要在欧盟境内确保对数据主体的全面保护，并尝试，在全球数据流动的背景下，基于数据保护要求，为活跃在欧洲市场的公司营造公平竞争的环境。

GDPR 第 3 条基于两个主要标准确定了《条例》的地域适用范围：一是第 3 条第 1 款规定的“实体（establishment）”标准；二是第 3 条第 2 款规定的“针对性”标准。如果相关的数据控制者或者处理者满足其中一个条件，GDPR 的有关条款就适用于其对个人数据的相关处理。此外，第 3 条第 3 款规定，若根据国际公法，成员国法律适用于某一数据处理行为，则 GDPR 也同样适用。

根据欧盟数据保护机构的通用解释，指南旨在评估控制者或者处理者的某一数据处理行为是否应受欧盟法律框架调整时，确保 GDPR 适用的一致性。在指南中，

[1]欧盟议会和欧盟法院在 2016 年 4 月 27 日通过《（欧盟）2016/679 条例》，该条例旨在针对自然人的个人数据处理和自由流动进行保护。同时，废止 95/46/EC 指令（《通用数据保护条例》）。

[2]欧盟议会和欧盟法院在 1995 年 10 月 24 日通过《95/46/EC 指令》，该指令旨在针对自然人的个人数据处理和自由流动进行保护。

EDPB 提出并解释了确定 GDPR 适用地域范围的各项标准。欧盟境内外的数据控制者和处理者都需评估其某一数据处理行为是否需要遵循 GDPR，所以这一通用解释对他们来说都至关重要。

因为未在欧盟境内设立实体的控制者或处理者参与到第 3 条第 2 款所规定的数据处理活动时被要求在欧盟境内派驻代表，所以指南也将在第 27 条具体阐明派驻代表的程序，以及代表的责任和义务。

EDPB 主张，只要个人数据处理行为发生在 GDPR 的适用地域范围，那么《条例》的全部条款都适用于该行为。根据处理行为的类型、实施处理行为的主体、主体所在地，指南将可能发生的多种情形进行分类，详述每一情形适用的条款。因此，对于控制者和处理者，尤其是涉及提供跨国商品和服务的控制者和处理者，为判断其相关个人数据处理行为是否受 GDPR 调整，对自身处理行为进行细致、具体的评估就至关重要。

EDPB 强调第 3 条是用来判断某一处理行为而不是个人（法人或自然人）是否受 GDPR 调整。所以，同一控制者或处理者的某些个人数据处理行为属于《条例》的调整范围的同时，也会有些行为不在其调整范围。

本指南，由 EDPB 会在 11 月 16 日首次公布，2018 年 11 月 23 日到 2019 年 1 月 18 日之间征求公众意见，经充分考虑接收到的意见和反馈后，更新制定。

1. 实体标准的适用—第3条第1款

GDPR 第 3 条第 1 款规定：“本条例适用于在欧盟境内有实体的控制者或处理者，在其活动范围内对个人数据的处理行为，无论该处理行为是否在欧盟境内进行。”

GDPR 第 3 条第 1 款不仅提到了控制者的实体，还提到了处理者的实体。因此，在欧盟境内有实体的处理者，在对个人数据进行处理时可能也需遵守欧盟法律。

第 3 条第 1 款确保 GDPR 适用于在欧盟境内有实体的控制者或处理者在其实体活动范围内对个人数据的处理，无论数据处理行为实际发生在何处。EDPB 因此提出“三步法”来判定对个人数据的处理行为是否落入第 3 条第 1 款所规定的适用范围。

以下各节阐明了“实体标准”的应用。首先确认该“实体”是否落入欧盟数据保护法所定义的欧盟“实体”范围内，其次判断该实体是否“在其活动范围内对个人数据进行处理”。一旦满足前两点，则确认 GDPR 适用于此种情况，而无论该处理行为是否在欧盟境内进行。

a) 在欧盟境内的实体

在判断“在欧盟境内的实体”之前，首先必须确定谁是数据处理行为的控制者或处理者。根据GDPR第4条第（7）款的定义，控制者是指“单独或与他人共同决定处理个人数据目的和方式的自然人或法人、公共权力机构、代理人或其他机构。”根据GDPR第4条第（8）款的规定，处理者是指“代表控制者处理个人数据的自然人或法人，公共权力机构、代理人或其他机构”。根据相关的CJEU判例法和WP29的观点[3]，确定实体是否是欧盟数据保护法规定的控制者或处理者，是评估该实体处理个人数据的行为能否适用GDPR的关键要素。

尽管GDPR第4条第16款中定义了“主要实体”，但并未对第3条中的“实体”作出定义[4]。但是，序言第22条[5]阐明，“‘实体’意味着通过稳定的安排（stable arrangements）

[3]G 29 WP169 ,《关于“控制者”和“处理者”概念的 1/2010 号意见(Opinion 1/2010 on the concepts of "controller" and "processor" 》, 于 2010 年 2 月 16 日通过，并由 EDPB 进行修订。

[4]“主要实体”的定义主要与 GDPR 第 56 条规定的确定有关监管机构的权限有关。请参阅经 ED29 批准的

实施真实有效的数据处理活动（theeffectiveandreal exercise of activities）。无论是以分支机构还是具有法人资格的子公司的结构形式，都不是确定实体的决定性因素。”

此措辞与第95/46 / EC号指令序言第19条一致，并被CJEU许多判决引用，以扩大对“实体”一词的解释。这种解释偏离了形式主义分析路径。形式主义分析方法认为只有在注册地成立的才能被称为“实体”[6]。欧盟法院判决认为，“实体”概念扩展到通过稳定形式进行的任何实际有效活动的组织，即使是规模最小（minimal）的活动[7]。为了确定欧盟境外的主体在成员国中是否设有实体，必须根据经济活动的特殊性和服务行为来考虑其经济活动安排的稳定性和在该成员国有效开展活动的程度。这种考量尤其适用于仅通过网络提供服务的企业[8]。

当控制者的核心业务涉及在线服务时，“稳定安排”[9]的门槛实际上可能会很低。在某些情况下，即使该实体并未在欧盟境内注册，若其一名雇员或代理人在欧盟境内有稳定持续的行为就可能构成“稳定安排”（相当于第3条第1款的“实体”）。相反，如果某个雇员位于欧盟境内，但数据处理与该雇员在欧盟境内的活动范围无关（即，该处理行为仅与控制者在欧盟境外的活动有联系），那么该处理行为并不会因为欧盟境内存在雇员这一事实而落入GDPR的管辖。换句话说，单凭欧盟境内存在雇员这一事实还不足以触发GDPR的适用，相关数据处理行为还必须发生在欧盟雇员的活动范围之内。

负责数据处理的非欧盟实体在成员国中没有分支机构或子公司的事实并不排除其拥有欧盟数据保护法所指的实体机构。但尽管实体的概念很广泛，并非没有限

《WP29 关于识别控制者或处理者的主导监管机构指南》（ 16 / EN WP 244 rev.01 ）。

[5] GDPR 第 22 条规定：“在欧盟境内设有实体的控制者或处理者在该实体的活动范围内进行的任何个人数据处理行为都应遵守本法规，无论处理行为本身是否在欧盟境内进行。实体指通过稳定的安排有效，真实地开展活动。无论是以分支机构还是以具有法人资格的子公司的形式来体现这样的安排，都不是确定实体的决定性因素。”

[6]请特别参阅 Google Spain SL, Google Inc. v AEPD, Mario Costeja Gonz ́alez (C-131/12), Weltimmo v NAIH (C-230/14), Verein f ̈ur Konsumenteninformation v Amazon EU (C-191/15) and Wirtschaftsakademie Schleswig-Holstein (C-210/16).

[7] Weltimmo, para. 31

[8] Weltimmo, para. 29

[9] Weltimmo, para. 31

制。不能仅仅因为可在欧盟境内访问某经营主体的网站而得出该非欧盟主体在欧盟境内已设立实体的结论[10]。

示例1：一家总部位于美国的汽车制造公司，在布鲁塞尔设有一家全资分支机构。该分支机构负责监督包括营销和广告业务在内的所有欧洲业务。

这个比利时机构根据汽车制造公司经济活动的性质进行着真实有效的经济行为，因此可以被认为是一个“稳定安排”。按照GDPR的定义，该比利时机构也因此可以被视为汽车制造公司在欧盟境内的实体。

一旦确定控制者或处理者是在欧盟境内设立的（即在欧盟境内有实体），接下来就应具体分析数据处理行为是否发生在该实体的经营活动范围之内，以确定是否能适用第3条第1款。在欧盟境外设立的控制者或处理者无论以何种法律形式（比如，子公司、分支机构、办公室等）通过“稳定安排”在欧盟境内进行“一项真实有效的活动，即使活动规模很小”，就可以被视为该控制者或处理者在该成员国中设有实体[11]。因此，正如序言第22条强调的，重要的是要考虑个人数据处理行为是否发生在实体的“活动”范围内。

b）在实体“活动范围内”进行的个人数据处理行为

第3条第1款规定，数据处理行为并不必然由欧盟境内实体本身进行；只要处理行为发生“在欧盟境内实体的活动范围内”，那么控制者或处理者就需要承担GDPR规定的义务。EDPB建议，在基于第3条第1款确定数据处理行为是否发生在“在欧盟境内设立的控制者和处理者的实体活动范围内”时，应根据个案，具体情况具体分析。每种情形都必须基于具体案件事实进行评估。

EDPB认为，就第3条第1款而言，应根据相关判例来理解“在控制者或处理者的实体活动范围内进行数据处理”的含义。一方面，为了实现有效和全面的保护，不能对“在控制者或处理者的实体活动范围内进行数据处理”进行限制性解释[12]。另一方面，不应将GDPR规定的“实体”解释得过于宽泛，以致使欧盟境外主体

[10] CJEU, Verein für Konsumenteninformation v. Amazon EU Sarl, C- 191/15, 2016 年 7 月 28 日, para. 76 (下称“Verein für Konsumenteninformation”).

[11]特别参考 Weltimmo 判决的第 29 段，该段强调了“实体”概念的灵活定义，并澄清了“必须根据经济活动的特殊性质和有关服务行为来解释安排的稳定程度和活动的有效开展程度”。

[12] Weltimmo, para. 25 和 Google Spain, para.53。

的数据处理行为与欧盟境内实体存在任何联系，甚至是微弱关联时，都使此数据处理行为落入欧盟数据保护法的管辖范围。非欧盟主体在某个成员国中进行的某些商业活动可能实际上确实与该主体的个人数据处理行为并无联系，所以在欧盟境内存在商业活动这一事实并不足以让其数据处理行为也落入GDPR的适用范围[13]。

考虑以下两个因素可能有助于确定数据处理行为是否发生在控制者或处理者的欧盟境内实体的活动范围之内。

i）欧盟境外数据控制者或处理者与其欧盟境内实体的关系

在欧盟境外设立的数据控制者或处理者的数据处理行为可能与成员国境内的一个本地实体的活动密不可分。在这种情况下，即使该本地实体实际上并没有在数据处理活动中扮演任何角色，该处理行为也可能触发欧盟数据保护法的适用[14]。如果基于事实进行个案分析后发现，非欧盟控制者或处理者对个人数据的处理行为与欧盟境内实体的活动之间有着密不可分的联系，那么无论该欧盟境内实体是否在数据处理过程中发挥作用，该数据处理行为都将适用欧盟法律。[15]

ii）欧盟境内收入增加

当欧盟境外的控制者或处理者在欧盟境外的个人数据处理行为，与欧盟境内实体的活动存在“不可分割的联系”，且该实体在欧盟内的收入由于该活动增加，则境外控制者或处理者在欧盟境外的个人数据处理行为可能会被认定为在“欧盟境内实体的活动范围内”，从而落入欧盟法律的管辖。[16]

EDPB建议非欧盟境内组织对其数据处理行为进行评估，首先是确定处理的是否是个人数据，其次是确定数据处理行为与任何欧盟实体之间的潜在关联。如果存

[13] G29 WP 179 更新-根据 CJEU 对 Google Spain 一案的判决，更新了有关适用法律的第 8/2010 号意见，2015 年 12 月 16 日。

[14] CJEU, Google Spain, C- 131/12

[15] G29 WP 179 更新-根据 CJEU 对 Google Spain 一案的判决，更新了有关适用法律的第 8/2010 号意见，2015 年 12 月 16 日。

[16]例如，可能的例子包括任何外国运营者在欧盟境内设立销售办公室或者其他形式的实体存在（即使该办公室在实际数据处理过程中未起任何作用），特别是该处理活动发生于欧盟境内的销售活动范围内，且该实体的活动针对该实体所在的成员国居民。

在类似关联，则该关联的性质将是确定GDPR是否适用于该数据处理行为关键，并且上述两个要素将被用于评估之中。

示例2：一家运营电子商务网站的中国公司。该公司的个人数据处理行为仅在中国进行。这家中国公司已在柏林设立了欧洲办事处，以领导并实施针对欧盟市场的商业开发和营销活动。

在这种情况下，只要该驻柏林欧洲办事处针对欧盟市场的商业开发和市场营销活动促进了该电子商务网站服务的收入增加，就可以认为该办事处的活动与中国公司进行的、有关欧盟销售的个人数据处理行为有不可分割的联系。因此，可以认为中国公司进行的、与欧盟境内的商业开发和市场营销活动有关的个人数据是在欧洲办事处（欧盟境内实体）的活动范围内进行的。中国公司因此需在GDPR第3条第1款的规定下处理个人数据。

示例3：一家南非连锁旅馆度假村品牌通过其网站提供套餐服务，其网站提供英语，德语，法语和西班牙语等语言。该公司在欧盟没有任何办事处、代表处或稳定安排。

在此情况下，该南非连锁度假村品牌在欧洲境内没有任何代表或稳定安排，从表面来看，没有任何与该南非数据控制者有联系的实体，符合GDPR中的“欧盟境内实体”标准。根据第3条第1款，该南非数据控制者对个人数据的处理行为不受GDPR指南的管辖。

但是，必须根据第3条第2款，对该南非数据控制者在欧盟境外的个人数据处理行为是否落入GDPR管辖进行具体分析。

c）GDPR 适用于在欧盟境内建立的控制者或处理者，而不论该个人数据处理行为是否在欧盟境内进行

根据第3条第1款，若控制者或处理者在欧盟建立了实体，则该实体在活动范围内进行的个人数据处理行为，会落入GDPR的管辖并需遵守有关数据控制者或处理者的相关义务。

GDPR规定，该指南适用于欧盟实体活动范围内的个人数据处理行为，而“无论该个人数据处理行为是否在欧盟进行”。数据控制者或处理者在欧盟境内建立实体，同时该实体在活动范围内进行了个人数据处理行为，使得该个人数据处理行

为落入GDPR管辖。因此，该数据处理行为发生的地理位置与该行为是否落入GDPR管辖范围无关。

示例4：一家法国公司开发了一种专门针对摩洛哥，阿尔及利亚和突尼斯的客户的汽车共享应用程序。该服务仅在这三个国家/地区可用，但所有个人数据处理活动均由法国的数据管理员执行。

尽管个人数据的收集是在欧盟境外进行的，但后续的个人数据行为是由控制者在欧盟实体的活动范围内进行的。因此，即使该行为涉及的数据主体位于欧盟境外，根据第3条第1款，GDPR的规定仍将适用于法国公司进行的个人数据处理行为。

示例5：一家总部位于斯德哥尔摩的制药公司，其新加坡分支机构负责处理与临床试验有关的个人数据。在这种情况下，虽然处理行为在新加坡进行，但该行为是在斯德哥尔摩制药公司，即，在欧盟境内有实体的数据控制者的活动范围内进行的。因此，根据第3条第1款，GDPR的规定适用于此类行为。

根据第3条第1款，如下与实体有关的地理位置在确定GDPR的领土范围时至关重要：

- 控制者或处理者本身（是在欧盟境内还是境外建立的？）；

- 与欧盟境外控制者或处理者的业务实体（在欧盟境内是否存在实体）。但是，第3条第1款并不关注数据处理行为或数据主体的地理位置。第3条第1款并未将GDPR的适用范围限制于对欧盟境内数据主体的个人数据的处理行为。因此，EDPB认为，在控制者或处理者的欧盟境内实体的活动范围内进行的任何个人数据处理行为都将落入GDPR的管辖，而不论数据主体的国籍或地理位置。GDPR序言第14条指出：“本指南保护与个人数据处理行为有关的自然人，无论该自然人的国籍或居住地为何地。”

d）实体标准对控制者和处理者的应用

对于落入第3条第1款范围内的数据处理行为，EDPB认为该规定适用于在欧盟各自实体的活动范围内进行个人数据处理活动的控制者和处理者。在确认控制者与处理者之间的关系与控制者或处理者所建立的实体的地理位置无关的同时，

EDPB认为，必须对每个实体的数据处理行为进行单独判断，从而确定是否应当适用GDPR第3条第1款规定的以下义务[17]。

GDPR对数据控制者和处理者有不同规定。因此，落入GDPR第3条第1款的管辖的数据控制者或处理者，应当承担不同义务。在这种情况下，EDPB特别指出，欧盟境内处理者不应仅因其代表控制者，就被认定为第3条第1款意义下的数据控制者的实体。

如果控制者或处理者二者之一未在欧盟境内建立实体，则控制者和处理者之间存在关系并不一定会使两者均落入GDPR管辖。

代表并根据另一组织（客户公司）的指令处理个人数据的组织，将作为该客户公司（控制者）的处理者。若该处理者在欧盟境内设立，它需遵守GDPR规定的处理者义务（“ GDPR处理者义务”）。如果指示处理者的控制者也位于欧盟境内，则该控制者必须遵守GDPR对控制者施加的义务（“ GDPR控制者义务”）。控制者进行的个人数据处理行为，若根据第3条第1款落入GDPR管辖，则不会因为该控制者指示欧洲境外处理者代表它进行数据处理行为，而免受本指南管辖。

i）欧盟境内控制者指示欧盟境外处理者进行个人数据处理行为

如果受GDPR管辖的控制者选择指示欧盟境外处理者进行给定的个人数据处理，则控制者仍然有必要通过合同或其他法律行为确保处理者根据GDPR来处理数据。第28条第3款规定，处理者的个人数据处理行为应受合同或其他法律行为的约束。因此，控制者需与处理者签订满足第28条第3款中所有规定的合同。此外，为了确保控制者遵守第28条第1款的义务—即其仅可能够使用提供足够保证，确保个人数据处理行为符合指南的要求并保护数据主体的权利的处理者—控制者需要考虑通过合同将GDPR所承担的义务加于受其约束的处理者。也就是说，根据第28条第3款，控制者必须确保不受GDPR约束的处理者，遵守由欧盟或成员国法律规定的合同或其他法律行为所约束的义务。

因此，根据第28条规定的合同安排，欧盟境外的处理者将间接受到由GDPR约束的控制者所施加的某些义务的约束。此外，GDPR第五章的规定可能同样适用。

[17]根据第 28 条，EDPB 重申处理者代表一控制者的处理活动应当受到合同或者其他欧盟或成员国法律文件的调整，对有关控制者而言，这些文件对处理者具有约束力，并且控制者应仅使用提供足够保证以实施适当的措施的处理者，以使处理能够满足 GDPR 的要求并确保保护数据主体的权利。

示例6：一家芬兰研究所发起了一个仅涉及俄罗斯萨米人的项目。该项目由位于加拿大的处理者进行。

芬兰控制者有责任仅使用能够提供足够保证以实施适当措施的处理者，使处理能符合GDPR的要求并确保保护数据主体的权利。芬兰控制者需要与加拿大处理者订立数据处理协议，该法律行为将规定处理者的职责。

ii）处理者在其欧盟境内实体的活动范围内进行的数据处理行为

尽管判例法使我们清晰地了解到控制者在其欧盟境内实体的活动范围内处理数据的效果，但处理者在其欧盟境内实体的活动范围内处理数据的效果并不明朗。

EDPB 强调，在确定控制者与处理者是否各自在欧盟境内设立时，必须将控制者与处理者的实体分开考虑。

首要问题是控制者本身在欧盟境内是否有一个实体，并且是否在这个实体活动范围内进行数据处理。假设控制者不被认定为在其自身实体的活动范围内进行数据处理，那么这个控制者就不受 GDPR 第 3 条第 1 款规定的控制者义务约束，但仍有可能适用第 3 条第 2 款。除非有其他因素影响，欧盟境内处理者的实体将不会被认定为是控制者的实体。

另一个由此产生的问题是处理者是否是在其欧盟境内实体的活动范围内进行数据处理。如果是，处理者将适用 GDPR 第 3 条第 1 款的规定。但是，这并不意味着非欧盟控制者将受 GDPR 规定的控制者义务的约束。换句话说，一个非欧盟控制者（如前所述）不会仅仅因为利用了欧盟境内的一个处理者而需要适用 GDPR。

控制者自身通过指示欧盟境内的处理者处理数据而不受 GDPR 约束。在这种情形下，控制者并不是在“欧盟境内处理者的活动范围内”进行数据处理。该处理是在控制者自己的活动范围内进行的；处理者仅仅是为控制者提供了一项处理服务[18]，且该服务并不必然与控制者的活动范围相联系。如上所述，当欧盟境内设

[18]在这种情况下，提供处理服务不能被视为向欧盟境内的数据主体提供服务。

立的数据处理者代表欧盟境外设立的控制者处理数据且不受 GDPR 第 3 条第 2 款的约束时，EDPB 并不会仅凭控制者与处理者之间的代理关系就认为该控制者的数据处理行为落入 GDPR 的地域适用范围之内。但是，即使控制者没有在欧盟境内设立，并且也不适用 GDPR 第 3 条第 2 款，欧盟境内设立的数据处理者将依据 GDPR 第 3 条第 1 款适用 GDPR 的相关规定。

例 7：一家墨西哥零售公司与在西班牙设立的数据处理者签订了一份合同，用以处理墨西哥公司客户的个人数据。该墨西哥公司只针对墨西哥市场提供服务，并且只处理欧盟境外主体的个人数据。

在这个案例中，这个墨西哥零售商既不会通过提供商品或服务将欧盟境内的个人作为目标，也没有监控欧盟境内个人的行为。因此，位于欧盟境外的控制者的数据处理行为将不会依据第 3 条第 2 款适用 GDPR。

根据第 3 条第 1 款，GDPR 的规定也不适用于本案的数据控制者，因为不属于控制者自身在欧盟境内实体的活动范围内处理个人数据的情形。本案中的数据处理者在西班牙成立，因此根据第 3 条第 1 款，其数据处理行为将适用 GDPR。对于在其活动范围内进行的任何处理行为，该处理者将被要求遵守 GDPR 规定的处理者义务。

当在欧盟境内设立的数据处理者代表在欧盟境内没有实体的数据控制者进行数据处理，且这种情形不适用 GDPR 第 3 条第 2 款时，处理者将直接适用以下 GDPR 的相关规定：

-根据第 28 条第 2 款，第 3 款，第 4 款，第 5 款和第 6 款的规定，除了协助数据控制人遵守 GDPR 规定的控制人义务的情形，处理者被要求订立数据处理协议。

-根据第 29 条和第 32 条第 4 款的规定，处理者和在控制者或处理者授权下采取行动的有权访问个人数据的任何人，除非欧盟法或成员国法律另有要求，否则不得在没有控制者指示的情况下处理这些个人数据。

-根据第 30 条第 2 款的规定，在适用的情形下，处理者应当保留代表控制者进行的所有数据处理类别的记录。

-根据第 31 条的规定，在适用的情形下，应监管当局要求，处理者应与其合作执行任务。

-根据第 32 条的规定，处理者应采取技术和管理措施以确保适当的安全性。

-根据第 33 条的规定，处理者应在得知个人数据泄露后立即通知控制者，不得过分延迟。

-根据第 37 条和第 38 条的规定，在适用的情形下，处理者应指派一名数据保护人员。

-第五章有关向第三方国家或国际组织转移个人数据的规定。

此外，由于此类数据处理将发生在欧盟境内设立的处理者的活动范围内，EDPB 再次强调，处理者必须确保其处理行为仍然符合其他欧盟或成员国国家的法律规定。GDPR 第 28 条第 3 款也规定："如果处理者认为控制者的指令违反了本条例或其他欧盟或成员国的数据保护规定，则处理者应立即通知控制者。"

根据第 29 条工作组先前的立场，EDPB 认为，不能将地域适用范围用作"安全港"。例如，当数据处理行为涉及严重的道德问题[19]，并且涉及的法律责任远比欧盟数据保护法的适用更重要时，尤其涉及欧盟及各成员国关于公共秩序的法规时，无论数据控制者在何处设立，数据处理者都必须尊重并遵守欧盟和各成员国的这些规定。这个结论还考虑到了这样一个事实，即通过执行欧盟法律，GDPR 和成员国相关法律所产生的规定就会遵守《欧盟基本权利宪章》[20]。但这并不会对不属于 GDPR 地域适用范围内的控制者施加额外的义务。

2. "针对性标准"（targeting criterion）的适用—第3条第2款

在欧盟境内没有实体并不意味着在第三方国家设立的控制者或者处理者进行的数据处理将被排除适用 GDPR 的规定，因为第 3 条第 2 款依据数据处理行为规定了欧盟境外设立的控制者或处理者适用 GDPR 的情形。

在这类情形中，EDPB 确认，若在欧盟境内没有实体，控制者或处理者将无法从 GDPR 第 56 条规定的一站式服务机制中受益。的确，GDPR 的合作机制仅适用于在欧盟境内拥有一个或多个实体的控制者和处理者[21]。

[19] G29 WP169-《关于"控制者"和"处理者"概念的 1/2010 号意见》，于 2010 年 2 月 16 日通过，并由 EDPB 修订。

[20]《欧盟基本权利宪章》，2012/C 326/02 。

[21]G29 WP244，《识别控制者或处理者主导监督机构的指南》，2016 年 12 月 13 日，修订版 1，由 EDPB 批

尽管本指南旨在阐明 GDPR 的地域适用范围，但 EDPB 同样希望，控制者和处理者也将顾及其他可适用的法律法规，比如欧盟或成员国的部门立法和国家法律。GDPR 的很多规定也确实允许成员国增加其他条件，以及在某些领域或在特定情况下，在各成员国国家层面制定具体的数据保护框架。因此，控制者和处理者必须确保他们了解并遵守因国家而异的条件和框架。这种差异尤其体现在第 8 条（规定儿童就信息服务提供商处理其个人数据给予有效同意的年龄可以在 13 到 16 岁之间），第 9 条（与处理特殊种类的数据有关），第 23 条（限制规定），或者 GDPR 第 9 章的规定（言论和信息自由；公开获取官方文件；身份证号码；就业背景；出于公共利益、科学研究、历史研究或统计目的数据处理；保密；教堂和宗教团体）。

GDPR第3条第2款规定“本条例适用于处理欧盟境内数据主体的个人数据的行为，即使控制者和处理者没有在欧盟境内设立，只要其处理行为：(a) 发生在向欧盟境内的数据主体提供商品或服务的过程中，无论此项商品或服务是否需要数据主体支付对价；或(b) 是对数据主体发生在欧盟境内的行为进行监控的。”

根据第3条第2款，未在欧盟境内设立实体的控制者或处理者在处理欧盟境内数据主体的个人数据时，只要该数据处理行为与该条规定的任一活动类型有关，就需要适用这条“针对性标准”。除此之外，适用这条“针对性标准”很多大程度上还需要在个案中，具体判定处理行为与这些活动类型的“关联性”。

EDPB 强调，控制者或处理者可能只就其部分处理行为适用 GDPR。，适用 GDPR 第 3 条第 2 款的决定性因素在于对数据处理行为的考量。

因此，在评估适用“针对性标准”的条件时，EDPB 建议采取两步法，首先需要评估该数据处理行为是否欧盟境内数据主体的个人数据有关，其次评估该处理行为是否与提供商品或服务，或监视欧盟境内数据主体的行为有关。

a） 欧盟境内的数据主体

第 3 条第 2 款的措词是“欧盟境内数据主体的个人数据”。因此，“针对性标准”的适用并不局限于拥有国籍、合法居留或拥有合法身份的个人。GDPR 序言第 14 条证实了这一解释。序言规定：“本条例所提供的保护应适用于涉及处理自然人个人数据的情形，无论其国籍或居住地在何处”。

GDPR 的这一规定体现了欧盟的基本立法《欧盟基本权利宪章》的精神，该法律也为个人数据保护提供了不局限于欧盟公民的广泛的适用范围。该立法第 8 条规定，“个人信息的保护针对‘每个人’”[22]。

尽管“数据主体位于欧盟境内”是适用第 3 条第 2 款的决定因素，但 EDPB 认为，欧盟境内数据主体的国籍或法律地位不能限制 GDPR 的地域适用范围。

当数据主体位于欧盟境内时，无论提供商品或服务的行为以及监控行为持续多久，有关机构必须在这些行为发生时进行评估。

但是，EDPB 认为，就与提供服务有关的处理活动而言，第 3 条第 2 款旨在针对那些有意将欧盟境内的个人作为目标的数据处理行为。因此，如果某项与数据处理有关的服务仅针对欧盟境外的个人，当此类个人进入欧盟却未撤销该服务时，则相关数据处理行为将不受 GDPR 的约束。在这种情况中，数据处理行为并不是有意针对欧盟境内的个人，而是针对欧盟以外的个人，因为无论他们是在欧盟外还是进入欧盟内，这种处理行为都会持续进行。

例 8：:一家澳大利亚公司根据用户的喜好提供移动新闻和视频内容服务。用户可以接收每日或每周的最新内容。该服务只向位于澳大利亚的用户提供，用户在订阅时必须提供澳大利亚的电话号码。
一名澳大利亚用户在假日旅行时前往德国，并继续使用该服务。
尽管该澳大利亚用户将在欧盟境内使用该服务，但该服务并非“针对”欧盟境内的个人，而是针对位于澳大利亚的个人。因此，澳大利亚公司处理个人数据的行为不适用 GDPR。

[22]《欧盟基本权利宪章》第 8 条第 1 款规定，“每个人都有权保护与他或她有关的个人数据”。

例 9：在美国成立的一家初创企业，在欧盟没有任何业务或实体，为游客提供城市地图应用程序。一旦游客在访问的城市中使用该程序，该程序就会开始处理与客户（数据主体）位置有关的个人数据，以便为他们提供与景点，餐厅，酒吧和酒店有关的针对性广告。该应用程序可供游客在纽约，旧金山，多伦多，巴黎和罗马使用。

这家美国初创公司通过其城市地图应用程序有针对性地为欧盟境内（即巴黎和罗马）的个人提供服务。根据第 3 条第 2 款（a）项的规定，在提供服务的前提下，与这类服务相关的处理欧盟境内个人数据的行为应当适用 GDPR。此外，通过处理数据主体的位置信息以便根据其位置提供有针对性的广告，也涉嫌监控欧盟境内个人的行为。因此，根据第 3 条第 2 款（b）项的规定，该美国初创企业的数据处理行为也属于 GDPR 的适用范围之内。

EDPB 还强调，有针对性地处理欧盟境内个人的数据并不足以让在欧盟境外设立实体的控制者或处理者适用 GDPR 的规定。这个针对行为的要素必须同时包含了提供商品、服务或监控行为（如下所述）。

例 10：一位美国公民在假期期间要穿越欧洲。在欧洲期间，他下载并使用了一家美国公司提供的新闻应用程序。从该应用程序的使用条款和以美元作为唯一可付款货币可知，该应用程序只针对美国市场。因此，该美国公司通过应用程序收集美国游客个人数据的行为不受 GDPR 约束。

此外，应注意的是，当在第三方国家处理欧盟公民或居民的个人数据时，只要该数据处理行为与针对欧盟境内个人提供的具体服务没有联系，也不涉及监控欧盟境内个人的行为，就不会受 GDPR 的约束。

例 11：台湾一家银行的客户居住在台湾，但拥有德国国籍。该银行只针对台湾市场提供服务，不涉足欧盟市场。因此，该银行处理其德国客户个人数据的行为不受 GDPR 约束。

例 12：加拿大移民局在欧盟公民进入加拿大领土时会处理他们的个人数据，以检查其签证申请。此处理行为不受 GDPR 约束。

b) **向欧盟境内的数据主体提供商品或服务，无论是否需要该数据主体支付对价**

触发适用第 3 条第 2 款的第一项活动是“提供商品或服务”。这一概念已在欧盟法律和判例法中得到进一步强调，并在适用“针对性（targeting）”标准时应予以考虑。服务提供还包括提供信息社会服务，在欧盟 2015/1535 指令[23]第 1 条第 1 款（b）项中定义为“信息社会服务，通常指通过电子方式并应服务接受者的个人要求，以一定距离获得报酬的服务”。

第 3 条第 2 款（a）项规定，无论数据主体是否支付对价，与提供商品或服务有关的数据处理行为均适用针对性标准。因此，是否将未在欧盟境内设立实体的控制者或处理者的活动视为提供商品或服务，并不取决于是否通过付款来交换该商品或服务。[24]

示例 13：一家美国公司（在欧盟境内没有任何实体）处理其赴法国、比利时和荷兰进行临时商务旅行的员工的个人数据，以用于人力资源管理，尤其是为了支付员工的住宿费用以及他们的每日津贴。这些费用的具体金额取决于他们所在的国家。

在这种情况下，虽然处理活动与欧盟境内的个人（即暂时在法国，比利时和荷兰的员工）特别相关，但并不是向这些个人提供服务，而是雇主履行与个人雇佣相关的合同义务和人力资源职责相关的必要处理的一部分。该数据处理活动与提供服务无关，因此 GDPR 第 3 条第 2 款（a）项不适用。

在确定是否可以满足第 3 条第 2 款 a 项针对性标准时要评估的另一个关键要素是，商品或服务的提供是否针对欧盟中的某个人。换句话说，决定了数据处理方式和目的的控制者的部分行为，是否表明了其向欧盟境内数据主体提供商品或服务的意图。 GDPR 序言第 23 条确实阐明了“为了确定这样的控制者或处理者是否正在向欧盟境内数据主体提供商品或服务，应确定控制者或处理者是否显然

[23]欧洲议会和理事会于 2015 年 9 月 9 日发布的关于规定在技术法规和信息社会服务规则领域提供信息的程序的（欧盟）2015/1535 指令（Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.）。

[24]特别参见，欧盟法院, C-352/85, Bond van Adverteerders and Others vs. The Netherlands State, 26 April 1988, par. 16)，以及欧盟法院, C-109/92, Wirth [1993] Racc. I-6447, par. 15.

打算向位于一个或多个欧盟成员国的数据主体提供服务。”
序言进一步规定：“可在欧盟境内访问控制者、处理者或中介的网站、电子邮件地址或其他联系方式，或使用控制者所在的第三国通常使用的语言，都不足以确定这种意图。但其他因素，例如使用一个或多个成员国通常使用的一种语言或货币，并有可能以该种语言订购商品和服务，或者提及欧盟境内的客户或用户，可能会明显表明控制者有意图向欧盟中的数据主体提供商品或服务。”

序言第 23 条的标准与以欧盟理事会第 44/2001 号条例[25]（关于管辖权以及民用和商业事务中的判决的承认和执行），尤其是其第 15 条 1 款 c 项为基础的 CJEU 判例法相呼应，并与之相符。在 *Pammer 诉 Reederei Karl Schlüter GmbH&Co* 和 *Hotel Alpenhof 诉 Heller*（共案 C-585/08 和 C-144/09）中，法院被要求澄清第 44/2001 号条例（《布鲁塞尔 I 号条例》）第 15 条第 1 款第 c 项所指的“引导活动（direct activity）”的含义。欧盟法院认为，为了确定交易者是否可以视为符合《布鲁塞尔 I 号条例》第 15 条第 1 款第 c 项规定的将其活动“引导”到消费者居住的成员国，交易者必须已经表明了与此类消费者建立商业关系的意图。在这种情况下，CJEU 认为有证据表明该交易者正在设想与一个成员国内的消费者开展业务。

尽管“引导性活动”的概念与“提供商品或服务”不同，但 EDPB 认为，*Pammer 诉 Reederei KarlSchlüterGmbH&Co* 和 *Hotel Alpenhof 诉 Heller* 案中（共案 C-585/08 号和 C-144/09 号）[26]对于判断是否向欧盟中的数据主体提供商品或服务可能会有所帮助。因此，在考虑到案件的具体事实时，除其他外，可以考虑以下因素（可能相互结合）：

-提供的商品或服务中至少提及欧盟或至少一个成员国；
-数据控制者或处理者向搜索引擎运营商支付互联网检索服务的费用，以便欧盟境内的消费者访问其网站；控制者或处理者针对欧盟国家的受众发起了营销和广告活动

[25]理事会于 2000 年 12 月 22 日颁布的关于民事和商业事务中的管辖权以及判决的承认和执行（EC）第 44/2001 号条例（Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters）。
[26]更重要的是，根据欧洲议会和理事会于 2008 年 6 月 17 日颁布的关于适用于合同义务的法律（罗马 I）的（EC）第 593/2008 号条例第 6 条，在没有法律选择的情况下，在将消费者的经常居住地的法律指定为适用于合同的法律时，考虑到了“将活动指向消费者经常居住地的国家”的标准。

-有关活动具有国际性质，例如某些旅游活动；

-提到可联系的欧盟国家/地区的专用地址或电话号码；

-使用除控制者或处理者所在的第三国家/地区以外的顶级域名，例如“.de”，或使用中立的顶级域名，例如“.eu”；

-从一个或多个欧盟成员国到服务提供所在地的旅行说明的介绍；

-提及由多个欧盟成员国的客户组成的国际客户，特别是通过展示此类客户撰写的理由；

-使用交易者所在国家/地区以外的其他语言或货币，特别是一个或多个欧盟成员国的语言或货币；

-数据控制者可在欧盟成员国内交付货物。

如前所述，如果单独考虑上述所列因素可能不足以明确表明数据控制者向欧盟境内数据主体提供商品或服务的意图，但是，在具体分析与数据控制者商业活动有关的多个因素的组合是否可以共同去证明向欧盟境内数据主体提供商品或服务的意图时，每个因素都应被纳入考虑，。

但重要的是，序言第 23 条确认了仅可以访问欧盟境内控制者、处理者或中介的网站，在网站上提及其电子邮件或地理位置，或其没有国际代码的电话号码，本身并未提供足够的证据来证明控制者或处理者打算向位于欧盟境内的数据主体提供商品或服务的意图。在这种情况下，EDPB 回顾，如果无意或偶然地向欧盟境内的个人提供了商品或服务，则有关个人数据的处理行为将不属于 GDPR 的范围。

例 14：在土耳其建立和管理的一网站提供创建、编辑、打印和运输个性化家庭相册的服务。该网站提供英语、法语、荷兰语和德语版本，并且可以欧元付款。该网站表明，相册只能在法国、比荷卢三国和德国以邮寄方式送达。

在这种情况下，很明显，个性化家庭相册的创建、编辑和打印构成了欧盟法律范围内的服务。该网站以欧盟的四种语言提供服务，并且可以在六个欧盟成员国内邮寄相册，这表明该土耳其网站有意向欧盟的个人提供服务。

因此，很明显，土耳其网站作为数据控制者所进行的处理行为涉及向欧盟境内数据主体提供服务，因此根据第 3 条第 2 款（a）项要遵守 GDPR 的义务和规定。

根据第 27 条，该数据控制者必须在欧盟境内指派一名代表。

例 15：位于摩纳哥的一家私营公司为了支付工资而处理其员工的个人数据。该公司大量员工是法国和意大利居民。

在这种情况下，尽管公司执行的数据处理与来自法国和意大利的数据主体有关，但并不是在提供商品或服务。确实，人力资源管理，包括第三国公司的薪水支付，不能被视为第 3 条第 2 款（a）项所指的服务提供。该处理与向欧盟境内数据主体提供商品或服务无关（也与行为监控无关），因此，不受第 3 条所述的 GDPR 规定的约束。

此项评估不影响有关第三国的适用法律。

例 16：苏黎世的一所瑞士大学通过提供一个在线平台，使候选人可以上传其简历和求职信以及联系方式，来进行其硕士学位选择程序。选拔过程对拥有足够德语和英语水平且拥有学士学位的任何学生开放。该大学没有专门向欧盟大学的学生做广告，仅以瑞士货币付款。

由于在此硕士学位的申请和选择过程中，没有对来自欧盟的学生进行任何区分或特别规定，因此无法确定瑞士大学有意针对特定欧盟成员国的学生。具备通用水平的德语和英语是一项通用要求，适用于任何申请人，无论是瑞士居民、瑞士联邦人士还是来自第三国的学生。如果没有其他因素表明其针对欧盟成员国学生，那么就不能确定所涉及的处理与向欧盟数据主体提供教育服务有关，因此此类处理将不受 GDPR 规定。

瑞士大学还提供暑期国际关系课程，并专门在德国和奥地利的大学中宣传此课程，以最大程度地提高课程的参与率。在这种情况下，瑞士大学明确打算向欧盟中的数据主体提供此类服务，GDPR 将适用于相关的处理活动。

c）监控数据主体的行为

触发适用第 3 条第 2 款的第二项活动是监视数据主体在欧盟境内的行为。

序言第 24 条澄清，“由在欧盟中设立实体的控制者或处理者处理欧盟境内数据主体的个人数据，在与监控此类数据主体行为有关时，只要该行为发生在欧盟境内，也应受本法规的约束。”

为适用 GDPR 第 3 条第 2 款，所监视的行为必须首先与欧盟境内数据主体相关，同时，所监视的行为必须在欧盟境内发生。

序言 24 条进一步规定了可以被视为行为监控的处理活动的性质，其中指出："为了确定是否可以将处理活动视为监控数据主体的行为，应确定自然人是否在互联网上被跟踪，包括后续可能使用的个人数据处理技术，其中包括对自然人进行用户画像，特别是为了做出有关她或他的决定，或分析或预测她或他的个人喜好、行为和态度。"尽管序言第 24 条完全与通过在互联网追踪一个人的监视行为有关，认为在确定处理活动是否等同于行为监控时，也应考虑通过其他类型网络或技术进行的涉及个人数据处理的跟踪监视行为，例如通过可穿戴设备和其他智能设备。

与第 3 条第 2 款（a）项相反，第 3 条第 2 款（b）项和序言第 24 条都没有明确规定数据控制者或处理者必须有一定的"针对意图"，以确定监视活动是否将触发适用 GDPR。但是，"监视"一词的使用意味着控制者有一个特定的目的，即收集和随后复用有关个人在欧盟境内行为的相关数据。EDPB 认为，在欧盟对个人数据的任何在线收集或分析都不会自动计为"监视"。必须考虑控制者处理数据的目的，尤其是涉及该数据的任何后续行为分析或性能分析技术。EDPB 考虑了序言第 24 条的措辞，该措辞表明互联网上对自然人的追踪（包括随后可能使用的分析技术）是确定数据处理行为是否涉及监视数据主体的一个关键考虑因素。

因此，第 3 条第 2 款（b）项对数据控制者或处理者监视欧盟境内数据主体的行为的适用可能包括广泛的监视活动，特别是：

-行为广告
-地理定位活动，尤其是用于营销目的
-通过使用 Cookie 或其他跟踪技术（例如指纹识别）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(CCTV)
-根据用户画像进行市场调查和其他行为研究
-监视或定期报告个人的健康状况

例 17：在美国成立的一家零售咨询公司，通过对 Wi-Fi 跟踪收集的一法国购物中心内顾客的活动进行分析，向该购物中心提供有关零售布局的建议。
通过 Wi-Fi 跟踪技术对顾客在购物中心内的运动进行分析将构成对个人行为的监控。在这种情况下，由于购物中心位于法国，因此数据主体的行为发生在欧盟境内。因此，作为数据控制者的咨询公司的数据处理活动根据 GDPR 第 3 条第 2 款（b）项受到 GDPR 的约束。
根据第 27 条，数据控制者必须在欧盟境内指定一名代表。

例 18：根据第 3 条第 2 款（b）项，在加拿大成立但未在欧盟境内设立实体的应用程序开发者监视欧盟境内数据主体的行为，要遵守 GDPR。开发者使用在美国设立的处理者进行应用程序优化和维护。

就此处理而言，根据第 28 条，加拿大控制者有义务仅使用适当的处理者，并确保其自身与美国处理者之间的合同或法律行为中能体现 GDPR 规定的相关义务。

d） 未在欧盟境内设立实体的处理者

若处理行为与第 3 条第 2 款规定的针对性活动“有关”，则其受 GDPR 约束。EDPB 认为处理行为与提供商品和服务之间应当存在联系，但是控制者和处理者的处理行为均是有关的并应均纳入考虑。

当判断在欧盟境外设立的数据处理者的处理行为是否应根据第 3 条第 2 款适用 GDPR 时，有必要查看该处理者的处理行为是否与控制者的针对性活动相联系。

EDPB 认为，在控制者的处理行为与提供商品和服务存在联系，或者与监控欧盟境内个人行为（“针对性”）相关联的情形中，任何受到指示以控制者名义实施处理行为的处理者，都应基于其处理行为，依照第 3 条第 2 款，受到 GDPR 的调整。

处理行为的“针对性”特征与行为目的和方式有关。只有作为控制者的主体才能做出将欧盟境内个人作为目标的决定。但这一阐释并不排除处理者可能会积极参

加并实施与针对性标准有关的处理行为（即，处理者提供商品或服务，或者以控制者的名义或受到控制者的指示实施监控行为）。

因此，EDPB 认为，应当重点关注处理者实施的处理行为与数据控制者实施的针对性活动的关联性。

例 19：一家线上经营食物原材料和当地食谱的巴西公司，在法国、西班牙、葡萄牙通过投放广告、提供配送向欧盟境内的个人出售商品。此背景下，该公司要求同样设立在巴西的一数据处理者，根据法国、西班牙、葡萄牙的消费者的先前订单，进行相关数据处理，从而发展针对这些消费者的特定服务。

在数据控制者的指示下，处理者对欧盟境内的商品交易数据进行处理。此外，为发展特定消费服务，数据处理者直接监控欧盟境内的数据主体。因此根据第 3 条第 2 款，该处理者的处理行为应受到 GDPR 的调整。

例 20：一开发健康状况和生活方式应用程序的美国公司，允许用户使用该公司应用程序去记录其个人数据（睡眠时间、体重、血压、心跳，等等）。程序会为用户提供每日饮食和运动建议。相关数据由一美国数据控制者进行处理。该应用程序针对并被欧盟境内个人使用。为实现数据存储，该美国公司使用了设立在美国的处理者（云服务提供商）。

只要该美国公司涉及监控欧盟境内个人的行为，就会被视为在其运行应用程序的过程中“针对”欧盟境内个人。所以根据第 3 条第 2 款，该公司处理欧盟境内个人数据的行为应当受到 GDPR 的调整。

在该美国公司的指示下，云服务提供商/处理者以该美国公司的名义实施的处理活动与控制者针对欧盟境内个人的处理活动有关。因此根据第 3 条第 2 款，该处理者以控制者名义实施的处理活动也受到 GDPR 的调整。

例 21：一家提供中东文化旅游服务的土耳其公司，旗下拥有英语、法语和西班牙语导游。该旅游服务在网络上以三种语言进行大力宣传，并允许用欧元和英镑进行网上预定和支付。为进行市场和商业前景调查，该公司指示一家设立于突尼斯的客户服务中心作为数据处理者，，联系爱尔兰、法国、比利时和西班牙的客户，询问他们先前旅行的反馈并介绍新的服务和旅行地。根据第 3 条第 2 款，因为该控制者有针对性地为欧盟境内个人提供服务，所以应适用 GDPR。
为提升控制者面向欧盟境内个人提供服务的质量，突尼斯处理者所实施的处理行为与控制者提供的服务有关，所以根据第 3 条第 2 款，该处理者的处理行为也适用 GDPR。此外，在本案中，该突尼斯处理者在土耳其控制者的指示下并以土耳其控制者的名义，通过提供服务积极地参与了有针对性的的数据处理活动。

e) 与 GDPR 其他条款与其他法律的相互影响

EDPB 将会进一步评估 GDPR 第 3 条规定的地域适用范围与第 5 章有关国际数据转移之间的相互作用。并就这一点而言，有必要增加指南内容。

未设立在欧盟境内的控制者或处理者需遵守第三国国内有关个人数据处理的规定。然而，根据第 3 条第 2 款，当处理行为针对欧盟境内个人时，控制者在遵守第三国国内法律之外，还必须遵守 GDPR。无论处理行为是否是在履行第三国的法律义务下实施的，控制者都须遵守 GDPR。

3. 基于国际公法适用成员国法律的处理行为

第 3 条第 3 款规定：“本条例适用于虽在欧盟境外设立，但基于国际公法仍适用成员国法律的控制者的个人数据处理行为。”这一规定在序言第 25 条得到进一步解释：“本条例适用于在欧盟外设立的，但基于国际法仍适用成员国法律的地域，例如：成员国大使馆或领事馆。”

因此，EDPB 认为，根据第 3 条第 3 款，欧盟成员国位于欧盟境外的大使馆和领事馆的个人数据处理行为仍然适用 GDPR。作为数据控制者和处理者的各成员国大使馆和领事馆，因此要遵守 GDPR 的相关规定，其中包括数据主体权利、控制者和处理者的一般义务以及向第三国或者国际组织传输个人数据。

例 22：位于牙买加金斯顿的荷兰领事馆因管理需要开通招聘当地工作人员的网上申请。
尽管位于牙买加金斯顿的荷兰领事馆为设立在欧盟境外，但根据第 3 条第 3 款，基于国际公法适用欧盟成员国法律的的成员国领事馆的个人数据处理行为，也应当适用 GDPR。

例 23：一艘航行在公海领域的德国游轮，为策划游轮内娱乐休闲服务，对客人数据进行处理。
尽管这艘游轮在公海领域，未在欧盟境内，但根据第 3 条第 3 款的规定，德国国籍游轮意味着，该个人数据处理行为也将依据国际公法适用 GDPR。

尽管与第3条第3款的适用无关，还存在着一种特殊情况：基于国际公法，依照《1961年维也纳国际关系公约》[27]、《1963年维也纳领事关系公约》或者包括国际组织之间、国际组织位于欧盟内的所在国之间签订的总部协定，设立在欧盟境内的的特定主体、机构和组织享有特权和豁免权。就此情况，EDPB重申GDPR的适用不妨碍国际公法的条款效力，例如规定非欧盟大使馆、领事馆和国际组织的特权和豁免权的条款效力。同时，有必要重申任何受GDPR约束的控制者或处理者的处理行为，在上述主体、机构和组织交换个人数据时也须遵守GDPR，包括适用有关向第三国或国际组织传输个人数据的规定。

4. 欧盟境外控制者或处理者的代表人

根据 GDPR 第 3 条第 2 款，数据控制者或处理者有义务指定一位欧盟代表。未在欧盟境内设立却受 GDPR 约束的控制者或处理者，如未能指派欧盟代表，就违反 GDPR。

[27] http://legal.un.org/lic/texts/instruments/english/convention/9_1_1961.pdf

由于欧盟数据保护指令 95/46/EC（Directive 95/46/EC）已规定类似义务，故本条款并非新规。根据指令，本条款所涉及的是，基于个人数据处理目的在成员国境内使用自动化或其他设备，且设立在欧盟境外的控制者。GDPR 要求，除非满足第 27（2）条所列的豁免条件，适用第 3 条第 2 款规定的所有控制者或处理者有义务指定一位欧盟代表。为促进该具体条款的适用，EDPB 认为需要对第 27 条所规定的欧盟代表人的指定程序、实体义务和责任作进一步的指引。

值得注意的是，已经根据 GDPR 第 27 条书面指定了欧盟代表的欧盟境外控制者或处理者不属于第 3 条第 1 款的管辖范畴。这意味着，根据第 3 条第 1 款的规定，欧盟代表的存在不构成控制者或处理者的“实体”。

1） 代表的指定

序言第 80 条阐明，“代表人代表控制者或处理者履行与本规定有关的义务，应当有控制者或处理者明示的书面授权。该代表人的指定不影响控制者或处理者在本规定下的责任或义务。该代表人应根据控制者或处理者的授权履行职责，包括与主要监管机构就任何为符合本规定所需采取的行动进行合作。”

因此，序言第 80 条中提到的书面授权应当适用于欧盟代表人与欧盟境外数据控制者或处理者之间的关系和义务，而不影响控制者或处理者的义务或责任。欧盟代表人可以是设立在欧盟内的、能够代表欧盟境外数据控制者或处理者行使其各自在 GDPR 项下的义务的自然人或法人。

实践中，欧盟代表人可以基于个人或组织签订的服务合同来行使其职能，故可以由诸如律师事务所、咨询机构、私人公司等设立在欧盟内的商业或非商业实体担任。一个代表人可以同时代表多个欧盟外控制者或处理者。

当由公司或其他类型的组织承担代表人职能时，建议为每一个被代表的独立控制者或处理者指定一位自然人作为其主要联系人或负责人。通常，在服务合同中约定该类要点也十分有用。

与 GDPR 相同的是，EDPB 确认当一个控制者或处理者的多个处理行为均处于 GDPR 第 3 条第 2 款的规定范围内（且不存在第 27 条第 2 款所规定的豁免情形），控制者或处理者无需为每一个处于第 3 条第 2 款规定范围内的处理行为指定代表人。EDPB 不认为欧盟代表人职能可以与欧盟内的外部数据保护官（“DPO”）相协调。第 38 条第 3 款确立的一些基本条款保证了数据保护官们能够在组织内享有充分的自主权以执行其任务。尤其，控制者或处理者应当确保数据保护官“不会收到与他/她执行的任务有关的任何指示”。序言第 97 条补充，数据保护官“无论是否是控制者的雇员，都应当独立履行他们的职责和任务”[28]。这种对数据保护官的独立性和高度自主权的要求显然难以与欧盟代表人的职能相兼容。代表人，实际上是根据控制者或处理者的授权，依据其直接指示并代表其开展行动[29]。代表人由其代表的控制者或处理者授权，以其名义执行任务，这种身份无法与独立承担职责和任务的数据保护官相比。

此外，为完善其解释，EDPB 回顾了工作组（WP29）采取的立场，强调“比如涉及数据保护纠纷，外部数据保护官被要求作为控制者或处理者的法庭代表时，利益冲突很可能会发生”[30]。

同样，考虑到执行过程中可能出现的义务和利益冲突，对于同一数据控制者而言，EDPB 不认为其欧盟代表人的职能可以与数据处理者的角色兼容，尤其涉及到各自的责任和合规的遵守度上。

尽管 GDPR 未给数据控制者或代表人本身施加将指定后者这一事实告知监管机构的义务，但 EDPB 重申道，作为他们信息义务的一部分，根据第 13 条第 1 款 a 项和第 14 条第 1 款 a 项控制者应当向数据主体提供与其欧盟代表人身份有关的信息。例如，这种信息应当被包含在数据主体作数据收集时向其提供的（隐私通知和）前期信息之中。符合第 3 条第 2 款的欧盟境外的控制者未能将其欧盟代表人的身份信息告知数据主体的，根据 GDPR 规定将违反透明义务。而且，该种信息应易于监管机构取得，为促进联络以备合作需要。

[28]WP29 数据保护官指南(Guidelines on Data Protection Officers (‘DPOs’)) ,WP 243 修订版 01 - 由 EDPB 批准。

[29]兼任代表的外部数据保护官不可处在例如以下的情况：作为代表人，其依据指示与数据主体沟通控制者或处理者的决定或采取的措施，但是他/她作为数据保护官已经认为该决定或措施不符合且违反了 GDPR 的规定。

[30]WP29 数据保护官指南(Guidelines on Data Protection Officers (‘DPOs’)) ,WP 243 修订版 01 - 由 EDPB 批准。

例 24：例 12 所涉网站的注册地和经营地均位于土耳其，该网站提供个性化家庭相册的创建、编辑、打印和运输服务。网站语言可选择英语、法语、荷兰语、德语，可用欧元或英镑完成支付。该网站指明，家庭相册只能在法国、比荷卢三国和德国内邮寄送交。该网站受 GDPR 第 3 条第 2 款（a）项的约束，故数据控制者必须指定欧盟代表人。

代表人必须在可提供服务的成员国之中建立，在此可为法国、比利时、荷兰、卢森堡或德国。一旦他们通过创建相册来使用他们的服务，数据控制者及其欧盟代表人的名称或联系人详情就应成为数据主体在网上能够获取的信息的一部分。同样，这些信息也应显示在网站的一般隐私通知中。

2）指定义务的豁免[31]

尽管第 3 条第 2 款的适用会使欧盟境外控制者或处理者产生指定欧盟代表人的义务，但第 27 条第 2 款规定了两种得以免除强制指定欧盟代表人的情形：

- **处理是“偶然的，不包括大规模地处理第 9 条第 1 款所述的特殊类别信息和处理与第 10 条所述的刑事犯罪和违法行为有关的个人信息”，且该种处理“在综合考虑其性质、背景、范围和目的后，对自然人的权利和自由造成影响的可能性较小”。**

与工作组 29（WP29）此前立场相同，EDPB 认为只有在处理行为是不定期的、以及发生在控制者或处理者保留的常规业务或活动范围之外的情况下才能被认为是“偶然的”[32]。

此外，尽管 GDPR 未定义何为大规模的处理，但此前工作组 29 条（WP29）已经在工作组 243 条（WP243）中建议数据保护官在认定处理行为是否为大规模进行时从以下几个因素进行考虑：涉及的数据主体数量 - 具体的数字或相关人

[31]EDPB 批准的 G29 WP 243 修订版 1（数据保护官）中规定的部分标准和解释可以用作指定义务的豁免基础。

[32]WP29 关于依据 GDPR 第 30（5）条对处理行为记录义务的减损的立场文件。

口的比例；数据量或正在处理的不同数据项的跨度；数据处理活动的持续时间或持久性；处理活动的地理范围[33]。

最后，EDPB 强调第 27 条所述的豁免指定义务是指“对自然人的权利和自由造成影响的可能性较小”的处理行为[34]，因此，豁免的范围不限于让数据主体的权利和自由产生高风险的可能性较低的处理行为。根据序言第 75 条，评估数据主体的权利和自由所存在的风险时，应同时考虑风险的可能性和严重性。

或者

- **处理行为由“公共机构或主体”作出**

对于设立在欧盟外的实体，会由监管机构根据具体情况评估其“公共机构或主体”的资质[35]。EDPB 指出，考虑到他们的职责和任务性质，对于第三国公共机构或主体向欧盟数据主体提供商品或服务的行为、及其对欧盟内发生的自身行为的监控，可能会作出一定限制。c)设立在处理其个人数据的数据主体所在的成员国。

第 27 条第 3 款预料，“代表人设立之处，应当是被提供商品或服务且相关个人数据被处理的数据主体所在地，或者是行为被监控的数据主体所在地。如果处理个人数据的大部分数据主体都位于某个特定的成员国，则 EDPB 建议将代表人设立在同一个成员国更妥当。但是，对于尚未设立代表人、又已开始提供商品或服务或监控数据主体行为的情形，必须保持有一位欧盟境内代表人能够让数据主体易于联络。

EDPB 确认，欧盟代表人设立的标准是个人数据正在被处理的数据主体的所在地。即使处理者在另一成员国，该处理行为发生地在本规定中并非是认定代表人设立地的有关要素。

---

[33]WP29 数据保护官指南(Guidelines on Data Protection Officers (‘DPOs’))，于 2016 年 12 月 13 日批准，2017 年 4 月 5 日最后修订，WP243 修订版 01 - 由 EDPB 批准。

[34] GDPR 第 27 条第 2 款（a）项。

[35] GDPR 未定义何为“公共机构或主体”。EDPB 认为该概念应当由国内法认定。据此，公共机构或主体包括了全国性、地区性以及当地的机关，但在现行适用的国内法下，其概念通常还包括一定范围内由公法管辖的其他主体

示例 25：一家在欧盟境外设立和经营的印度医药公司，依据 GDPR 第 3 条第 2 款的规定，对位于比利时、卢森堡和荷兰的研究人员（医院）开展的临床试验进行赞助。大部分参与临床试验的病人都位于比利时。

作为数据控制者，印度医药公司应当在病人、即数据主体参与临床试验的三个成员国（比利时、卢森堡或荷兰）中指定一个欧盟代表人。鉴于大部分病人是比利时居民，我们建议代表人设立在比利时。而且在这种情况下，比利时代表人还应当易于被荷兰和卢森堡的数据主体和监管机构联系。

在这种特定情况下，依据（欧盟）536/2014 条例第 74 条有关临床试验的规定，欧盟代表人可以是赞助商在欧盟内的法定代表人，前提是代表人未以数据处理者的身份代表临床试验赞助商行动，且代表人设立在三个成员国之一中，以及代表人与赞助商的职能均适用并符合各自国家的法律体系。

3) 代表人的义务和责任

欧盟代表人代表控制者或处理者行动，它代表的是控制者或处理者在 GDPR 项下的义务。这清楚地表明代表人与行使数据主体权利有关的义务，，以及正如此前所述，根据第 13 条和第 14 条的规定，代表人的身份与联系信息都必须提供给数据主体。虽然代表本身无须遵循数据主体的权利，但代表必须促进数据主体和其代表的控制者或处理者之间的沟通以使数据主体能够高效行使自身权利。

根据第 30 条，控制者或处理者的代表人应当特别保留控制者或处理者负有责任的处理行为的记录。EDPB 认为，虽然这种记录保留是强加给控制者或处理者及其代表人的义务，但欧盟境外的控制者或处理者应当对记录的主要内容和更新负责，必须即时向代表人提供所有精确的、最新的信息以便代表人可随时随地留存、取用。同时，这也是第 27 条规定的属于代表人自身的责任，比如，当监管机构根据第 27 条第 4 款作出处理时，代表人的责任。

如序言第 80 条所述，代表人应当根据控制者或处理者的授权履行其职责，包括

与主要监管机构就任何为符合本规定所需采取的行动进行合作。实践中，这代表着监管机构会与代表人就与欧盟境外控制者或处理者合规义务有关的事宜进行联系，代表人应当能够促进监管机构与欧盟境外控制者或处理者的信息或程序性交换。

因此，必要时，在团队的帮助下，欧盟代表人必须能够有效地与数据主体沟通和与有关监管机构合作。这意味着，这一沟通原则上应当采用监管机构或有关数据主体的语言或者其所使用的语言，或者，若这样沟通效率不高，代表人应当采取其他途径或技巧以确保沟通的高效进行。因此，为了确保数据主体和监管机构能够与欧盟境外控制者或处理者轻易地建立联系，一位可靠的代表人十分重要。根据序言第 80 条和第 27 条第 5 款，欧盟代表人的指定不影响控制者或处理者在 GDPR 下的义务或责任，且不影响本可对控制者或处理者采取的任何法律手段。GDPR 不会给代表人设立一个替代责任制度来取代其所代表的控制者或处理者所应承担的责任。

然而，应当注意的是，准确引入代表人的概念是为了促进 GDPR 第 3 条第 2 款的控制者和处理者的联络并确保 GDPR 对其的有效适用。据此，旨在使监管机构能够通过欧盟境外控制者或处理者指定的代表人开展执法程序。这包括监管机构能够根据 GDPR 第 58 条第 2 款和第 83 条的规定，通过代表人对欧盟境外的控制者或处理者作出纠正措施或行政罚款和惩罚措施。但是，代表人直接承担责任的可能性亦仅限于 GDPR 第 30 条和 58 条第 1 款所涉及的直接义务。

EDPB 进一步强调，GDPR 第 50 条的主要目的是促进有关第三国和国际组织法规的适用，并且目前正考虑进一步发展该方面的国际合作机制。