关于《一般数据保护条例》适用的地域范围的指南

欧洲数据保护委员会　发布，敖海静　译

〔**译者按语**〕2018 年 5 月，欧盟《一般数据保护条例》（GDPR）正式生效，极大地改变了有关数据保护的国际法律格局。此后，如何正确理解和适用 GDPR 成为学术界和实务界关注的焦点问题。而就非欧盟国家而言，尤为关注 GDPR 的域外效力。在这个意义上，正确理解和澄清规定了 GDPR 适用的地域范围的第 3 条的含义就成为至为关键的研究议题。然而众所周知，对于 GDPR 的解释和实施，欧洲数据保护委员会（EDPB）及其前身——第 29 条工作组——所发布的指南最为权威。2018 年 11 月 16 日，欧洲数据保护委员会发布了《关于〈一般数据保护条例〉适用的地域范围的指南》（征求意见稿），经广泛征求公众意见，并于 2019 年 11 月 12 日发布了修订后的正式官方版本，十分详尽地阐释和澄清了确定 GDPR 适用的地域范围的标准。在全球经济和互联网愈发开放融合的背景下，GDPR 也将对中国的相关数据保护实践产生重大影响。中国的跨国企业等主体在启动 GDPR 合规项目时，首先需要评估的事项就是哪些数据处理活动将受到 GDPR 的约束。正如欧洲数据保护委员会所说，本指南对于欧盟境内外的数据控制者和处理者非常重要，他们可以据此评估其是否需要遵守 GDPR。

关键词：GDPR；适用的地域范围；机构标准；目标标准；代表

［**中图分类号**］D912.8　　［**文献识别码**］A　　［**文章编号**］2096-6180（2020）02-0135-24

鉴于欧洲议会和欧盟理事会 2016 年 4 月 27 日制定的，关于个人数据处理中的自然人保护和个人数据自由流动，同时废除《95/46/EC 指令》的《2016/679/EU 条例》第 70 条第 1 款 e 项之规定，欧洲数据保护委员会（EDPB）特采纳本指南。

导论

欧盟《一般数据保护条例》（GDPR）[1] 第 3 条规定了适用该条例的地域范围，和《95/46/EC

［作者简介］敖海静，法学博士，中国人民大学法学院博士后，讲师。

［基金项目］科技部司法专项“公共安全风险防控与应急技术装备”课题四“法律援助律师服务质量评价模型与智能推荐技术”（项目批准号：2018YFC0830904）。

〔1〕欧洲议会和欧盟理事会 2016 年 4 月 27 日制定的关于个人数据处理中的自然人保护和个人数据自由流动，同时废除《95/46/EC 指令》的《2016/679/EU 条例》（《一般数据保护条例》）。

指令》（下称《指令》）[2] 相比，这一规定体现了欧盟数据保护法的重大变化。某种程度上，GDPR 确认了欧盟立法者和欧盟法院在《指令》背景下的选择。但是，新的重要元素已经被引入了。最重要的是，《指令》第 4 条的目标是界定哪个成员国的国内法是可以适用的，GDPR 第 3 条则规定了直接适用该条例的地域范围。此外，虽然《指令》第 4 条将在欧盟境内“使用设备”作为“不在共同体（即欧盟——译者注）境内设立”的数据控制者纳入欧盟数据保护法适用范围的依据，但这一具体规定并没有出现在 GDPR 第 3 条当中。

GDPR 第 3 条体现了立法者的如下意图：确保欧盟境内数据主体的权利得到全面保护，并且根据数据保护要求，在全球数据流动的背景下，为活跃在欧盟市场的公司营造公平竞争的环境。

GDPR 第 3 条根据如下两项标准规定了该条例适用的地域范围：第 3 条第 1 款的“机构”标准和第 3 条第 2 款的“目标”标准。如果符合这两项标准中的任何一项，GDPR 的相关规定就将适用于有关控制者或处理者对个人数据的相关处理。第 3 条第 3 款则确认了 GDPR 对基于国际公法成员国法律有管辖权的数据处理的适用性。

通过欧盟境内数据保护机构的统一解释，本指南旨在确保在评估控制者或处理者的特定处理是否属于新的欧盟法律框架的范围时 GDPR 的一致适用。在本指南当中，欧洲数据保护委员会规定并阐明了决定 GDPR 适用的地域范围的标准。不论对欧盟境内，还是境外的控制者和处理者，这种统一解释都是完全必要的。如此一来，他们就可以评估对于既定的处理活动，是否需要遵守 GDPR。

由于不在欧盟所设立，但从事第 3 条第 2 款规定的处理活动的控制者或处理者必须在欧盟境内委任一名代表，因此，本指南还将阐明根据第 27 条委任该代表的程序及其责任和义务。

作为一般原则，欧洲数据保护委员会宣称，如果个人数据处理处在 GDPR 适用的地域范围之内，则 GDPR 的所有条款都可适用于这一处理。本指南将根据处理活动的类型、实施这些处理活动的实体，以及这些实体的所在地，具体列明可能出现的各种情况，同时详细阐释适用于每种情况的法律条款。因此，数据控制者或处理者，尤其是在全球层面提供商品和服务的控制者或处理者，必须对其处理活动进行仔细和具体的评估，以确定相关个人数据处理是否属于 GDPR 的适用范围。

欧洲数据保护委员会强调，第 3 条的适用旨在确定某一特定处理活动，而不是某个人（不论是法人，还是自然人）是否属于 GDPR 的适用范围。因此，某个控制者或处理者对个人数据的某些处理可能属于 GDPR 的适用范围，但同时其另一些处理则不属于这个范围，具体结果取决于处理活动。

本指南最初由欧洲数据保护委员会在 2018 年 11 月 16 日制定，且于同年 11 月 23 日至 2019 年 1 月 18 日提交公众咨询，并根据反馈意见进行了修订。

（2）欧洲议会和欧盟理事会 1995 年 10 月 24 日制定的关于个人数据处理中的自然人保护和个人数据自由流动的《95/46/EC 指令》。

一、机构标准的适用——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设有机构的数据控制者或处理者，在该机构活动范围内对个人数据的处理，不论其数据处理是否发生在欧盟内部。"

GDPR 第 3 条第 1 款不仅提到了控制者的机构，还提到了处理者的机构。因此，如果处理者在欧盟境内设有机构，那么其对个人数据的处理仍有可能要受欧盟法的管辖。

第 3 条第 1 款确保了 GDPR 适用于某个控制者或处理者在其设在欧盟境内机构的活动范围之内进行的处理，而不论该处理的实际发生地在哪里。因此，欧洲数据保护委员会建议采用"三步检验法"来确定个人数据处理是否属于 GDPR 第 3 条第 1 款规定的地域范围。

以下各小节将对机构标准的适用进行阐释。首先考察欧盟数据保护法意义上的欧盟境内机构的定义；其次考察"在欧盟境内机构的活动范围内处理"是什么意思；最后确认无论在该机构活动范围内的处理是否发生在欧盟内部，GDPR 都将适用。

a）"欧盟境内设有机构"

在考察"欧盟境内设有机构"的含义之前，首先有必要确定谁才是既定处理活动的控制者或处理者。根据 GDPR 第 4 条第 7 项，控制者是指"那些决定——不论是单独决定还是与他人共同决定——个人数据处理目的与方式的自然人或法人、公共机构、代理人或其他实体"。根据 GDPR 第 4 条第 8 项，处理者是指"为了数据控制者而处理个人数据的自然人或法人、公共机构、代理人或其他实体"。正如欧盟法院相关判例和之前的 WP29 意见所确立的[3]，根据欧盟数据保护法，确定一个实体是否构成控制者或处理者，是评估 GDPR 对所涉个人数据处理的适用性的关键因素。

虽然第 4 条第 16 项界定了"主要机构"的概念[4]，但 GDPR 并没有为第 3 条提供"机构"的定义。然而，说明部分第 22 段解释说[5]，"机构意味着通过稳定安排存在有效且真实的经营活动。这种安排的法律形式，是否通过具有法人人格的分支机构或子公司并不是决定性因素"。

这一措辞和《指令》的说明部分第 19 段如出一辙，欧盟法院在几项裁决中都引用了这一措辞，

---

〔3〕G29 WP169 - Opinion 1/2010 on the concepts of "controller" and "processor", adopted on 16th February 2010 and under revision by the EDPB.

〔4〕"主要机构"的定义和根据 GDPR 第 56 条确定领导性监管机构的职权有关。*See* the WP29 Guidelines for the identifying a controller or processor's lead supervisory authority（16/EN WP 244 rev.01）- endorsed by the EDPB.

〔5〕GDPR 说明部分第 22 段规定："只要控制者或处理者的机构在欧盟境内，任何在该机构活动范围内进行的个人数据处理都应该遵守本条例的规定，无论处理活动本身是否发生在欧盟境内。机构意味着通过稳定安排存在有效且真实的经营活动。这种安排的法律形式，是否通过具有法人人格的分支机构或子公司并不是决定性因素。"

扩大了对“机构”一词的解释，不同于机构仅指在企业注册地设立的这一形式主义认定方法。[6] 事实上，欧盟法院裁决，机构的概念延伸到通过稳定安排存在有效且真实的经营活动，哪怕是极其微小的活动。[7] 为了确定一个设在欧盟以外的实体是否在一个成员国设有机构，必须根据有关经营活动和服务的具体性质，考量这些安排的稳定度和在该成员国有效开展经营活动的程度。对于专门通过互联网提供服务的企业来说尤其如此。[8]

当控制者的主要活动涉及在线服务时，“稳定安排”[9] 实际上可能是个相当低的门槛。因此，在某些情况下，即便是非欧盟实体在欧盟境内的单个雇员或代理人，只要他的行为具备足够的稳定性，可能就足以构成一项稳定的安排（就第 3 条第 1 款而言，相当于一个“机构”）。相反，即便雇员位于欧盟境内，但处理不属于该雇员的活动范围（例如，处理与设在欧盟境外的控制者的活动有关），那么仅仅只是存在欧盟境内的雇员并不足以导致 GDPR 适用于该处理。换言之，仅仅存在欧盟境内的雇员尚不足以构成 GDPR 的适用前提，因为要使有关处理属于 GDPR 的适用范围，这一处理还必须是在该雇员的活动范围内进行的。

虽然负责数据处理的非欧盟实体在成员国没有分支机构或子公司，但这一事实并不排除其在该国设立欧盟数据保护法意义上的机构。虽然机构的概念很宽泛，但也不是毫无限制。不能仅仅因为非欧盟实体的网站可以在欧盟境内访问，就认为该实体在欧盟境内设有机构。[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全资分公司，负责其在欧洲的所有业务，包括营销和广告。

比利时分公司可以被认为是一个稳定安排，它根据汽车制造公司的经济活动性质，开展有效真实的经营活动。因此，比利时分公司可以被视为 GDPR 意义上的欧盟境内机构。

一旦认为某控制者或处理者设立在欧盟境内，接下来就应该对相关处理是不是在该机构活动范围内进行展开具体分析，以确定是否适用第 3 条第 1 款。如果设在欧盟之外的控制者或处理者通过“稳定安排”在成员国境内开展了“有效且真实的经营活动，哪怕是极其微小的活动”，无论其法律形式如何（如子公司、分支机构、办事处……），该控制者或处理者都可以被视为在该成员国设有机构。[11] 因此，正如说明部分第 22 段所强调的，重要的是要考察个人数据处理是否处于这一机构的“活动范围”之内。

---

〔6〕 *See* in particular Google Spain SL，*Google Inc. v. AEPD*，Mario Costeja González （C-131/12），*Weltimmo v. NAIH*（C-230/14），*Verein für Konsumenteninformation v. Amazon EU*（C-191/15）and Wirtschaftsakademie Schleswig-Holstein（C-210/16）.

〔7〕 Weltimmo，paragraph 31.

〔8〕 *Id.*，at 29.

〔9〕 *Id.*，at 31.

〔10〕 CJEU，*Verein für Konsumenteninformation v. Amazon EU Sarl*，Case C-191/15，28 July 2016，paragraph 76（Verein für Konsumenteninformation）.

〔11〕 特别参见 Weltimmo，paragraph 29，这一段强调了对“机构”概念进行灵活界定，并解释说，“必须根据有关经济活动和提供服务的具体特征来解释安排的稳定程度和在该成员国经营活动的有效性”。

b）在机构的“活动范围内”进行个人数据处理

第 3 条第 1 款确认，有关处理不必“由”相关欧盟境内机构自身进行；只要该处理是在相关欧盟境内机构的“活动范围内”进行的，控制者或处理者就将承担 GDPR 规定的责任。欧洲数据保护委员会建议，就第 3 条第 1 款来说，处理是不是在控制者或处理者设在欧盟境内机构的活动范围内进行的，应当逐案具体分析。每一种情形都必须根据其本身的是非曲直加以评估，并且考虑案件的具体事实。

就第 3 条第 1 款来说，欧洲数据保护委员会认为，应当根据相关判例来理解“在控制者或处理者所设机构的活动范围内处理”的含义。一方面，为了实现全面有效的保护，不能对在“机构的活动范围内”作限缩性解释。[12] 另一方面，不应该将存在 GDPR 意义上的机构解释得太过宽泛，以至于认为欧盟境内的任何存在，哪怕和非欧盟实体的数据处理活动之间只有最微弱的关联，也足以将这一处理纳入欧盟数据保护法的适用范围。事实上，非欧盟实体在某成员国的一些商业活动可能离该实体进行的个人数据处理还很遥远，因此，在欧盟境内存在商业活动这一事实还不足以将非欧盟实体的数据处理纳入欧盟数据保护法的适用范围。[13]

以下两个因素可能有助于确定控制者或处理者的处理是不是在其设于欧盟境内机构的活动范围内进行的：

i）欧盟境外的数据控制者或处理者与其欧盟境内机构之间的关系

设立在欧盟境外的数据控制者或处理者的数据处理活动可能和某成员国当地机构有着不可分割的联系，这就可能导致适用欧盟法律，即便就数据处理本身来说，当地机构实际上没有发挥任何作用。[14] 如果对事实的逐案分析表明，非欧盟控制者或处理者对个人数据的处理和欧盟境内机构有着不可分割的联系，那么欧盟法律就将适用于非欧盟实体的处理，无论欧盟境内机构是否在该处理中发挥了作用。[15]

ii）欧盟境内的增收

如果在某种程度上可以认为，当地机构在欧盟境内的增收和欧盟境外的个人数据处理，以及境内个人之间有着“不可分割的联系”，那么这一增收就可能表明非欧盟控制者或处理者的处理是在“欧盟境内机构的活动范围内”进行的，并且足以导致对该处理适用欧盟法律。[16]

欧洲数据保护委员会建议非欧盟组织对其处理活动进行评估，首先确定自身是否正在处理个人数据，其次辨别数据处理活动和该组织在欧盟境内任何机构的活动之间的潜在联系。一旦确定

---

〔12〕 *Supra* note〔7〕, at 29；Google Spain，paragraph 53.

〔13〕 G29 WP 179 update-Update of Opinion 8/2010 on applicable law in light of the CJEU judgment in Google Spain，16th December 2015.

〔14〕 CJEU，Google Spain，Case C-131/12.

〔15〕 *Supra* note〔13〕.

〔16〕 对于任何在欧盟设有销售办事处或其他机构的外国运营商来说，这种情况都是可能出现的。即便该办事处在实际的数据处理——特别是发生在欧盟内的销售活动范围内的处理，以及该机构针对其所在欧盟成员国居民的活动范围内的处理——中没有发挥任何作用，仍然可能出现这种情况。

了这一联系，这一联系的性质将是决定 GDPR 是否适用于相关处理的关键，必须根据上述两个因素加以评估。

示例 2：一家中国公司运营着一个电子商务网站。该公司的个人数据处理活动只在中国进行。该公司在柏林设立了欧洲办事处，以领导和实施面向欧盟市场的商业开发和市场营销。

在这种情况下，就面向欧盟市场的商业开发和市场营销显著地使该电子商务网站提供的服务有利可图这一点而言，可以认为驻柏林的欧洲办事处与中国电子商务网站进行的个人数据处理存在不可分割的联系。中国公司进行的和在欧盟的销售活动有关的个人数据处理确确实实和驻柏林的欧洲办事处面向欧盟市场开展的商业开发和市场营销存在不可分割的联系。因此，中国公司处理和在欧盟的销售活动有关的个人数据可被视为是在作为欧盟境内机构的欧洲办事处的活动范围内进行的。因此，根据 GDPR 第 3 条第 1 款，中国公司将受到 GDPR 的约束。

示例 3：南非的一家连锁度假酒店通过其网站提供一揽子交易，网站有英语、德语、法语和西班牙语版本。该公司在欧盟没有任何办事处、代表或稳定安排。

在这种情况下，酒店在欧盟境内没有任何代表或稳定安排，看来似乎不存在任何和这个南非的数据控制者有关的实体可以作为 GDPR 意义上的欧盟境内的机构。因此，根据第 3 条第 1 款，这一处理不受 GDPR 的约束。

但是，还必须根据第 3 条第 2 款对设在欧盟之外的数据控制者的处理是否受到 GDPR 的约束进行具体分析。

c）GDPR 适用于控制者或处理者在欧盟境内设立的机构，不论其处理是否发生在欧盟内部

根据第 3 条第 1 款，在控制者或处理者设在欧盟境内机构的活动范围内的个人数据处理会导致 GDPR 的适用，并且让有关的数据控制者或处理者承担相关责任。

GDPR 的文本明确规定其适用于在欧盟境内机构的活动范围内进行的处理，“不论其数据处理是否发生在欧盟内部”。正是数据控制者或处理者在欧盟境内的机构，以及在这一机构的活动范围内进行数据处理的事实，导致 GDPR 适用于它的处理活动。因此，处理发生的地点和确定在欧盟境内机构的活动范围内进行的处理是否属于 GDPR 的适用范围没有关系。

示例 4：一家法国公司开发了一个专门面向摩洛哥、阿尔及利亚和突尼斯客户的共享汽车应用程序。这项服务只在这三个国家开展，但所有个人数据处理活动都由数据控制者在法国进行。

虽然个人数据的收集是在非欧盟国家进行的，但该情形下后续的个人数据处理都是在数据控制者在欧盟境内机构的活动范围内进行的，因此，尽管处理涉及的是非欧盟数据主体的个人数据，但是根据第 3 条第 1 款，GDPR 对这家法国公司进行的数据处理仍然是适用的。

示例 5：一家总部位于斯德哥尔摩的制药公司将其所有涉及临床试验数据的个人数据处理活动都放在新加坡的分公司进行。

在这种情况下，虽然处理活动发生在新加坡，但却是在位于斯德哥尔摩的制药公司，也就是一家设在欧盟境内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 适用于这一处理活动。

在确定 GDPR 适用的地域范围时，根据第 3 条第 1 款，地理位置对下列机构的设立地至关重要：

* 控制者或处理者自身（是设立在欧盟境内还是境外）；

* 非欧盟控制者或处理者的任何业务存在（其是否在欧盟境内设有机构）。

但是，就第 3 条第 1 款而言，地理位置对于数据处理发生的地点，或有关数据主体所在地点并不重要。

第 3 条第 1 款的文本并没有将 GDPR 的适用限制在针对欧盟境内的人的个人数据处理上。因此，欧洲数据保护委员会认为，任何处于控制者或处理者在欧盟境内所设机构活动范围内的个人数据处理都处在 GDPR 的适用范围之内，不论个人数据受到处理的数据主体在什么地方，属哪国国籍。这种解释也得到了 GDPR 说明部分第 14 段的支持，该段规定“本条例提供的保护应当适用于其个人数据受到处理的自然人，不论其国籍和居住地”。

d）机构标准对控制者和处理者的适用

就第 3 条第 1 款范围内的处理活动而言，欧洲数据保护委员会认为，如果控制者和处理者的处理活动是在各自设在欧盟境内机构的活动范围内，那么这些规定就适用于他们。虽然承认建立控制者和处理者之间关系的要求[17]不因控制者或处理者所设机构的地理位置而有所不同，但欧洲数据保护委员会认为，当根据第 3 条第 1 款涉及由 GDPR 的适用性引发的不同责任时，各实体的处理必须单独考量。

GDPR 设想了适用于数据控制者和处理者各不相同、专门的规定或责任，因此，如果根据第 3 条第 1 款，数据控制者或处理者应受 GDPR 的约束，那么他们将分别承担相关责任。在这种情况下，欧洲数据保护委员会特别指出，欧盟境内的处理者不应仅仅因为其作为代表控制者的处理者身份，而被视为第 3 条第 1 款意义上的数据控制者的所设机构。

如果控制者和处理者这两个实体中的一个不是设在欧盟境内，那么两者间关系的存在不一定引起 GDPR 的适用。

一个代表另一个组织（客户公司），并根据该客户公司的指示进行数据处理的组织，将成为这家客户公司（控制者）的处理者。如果处理者设在欧盟境内，他就必须承担 GDPR 赋予处理者的法律责任（“GDPR 处理者责任”）。如果指示处理者的控制者也位于欧盟境内，则控制者也必须承担 GDPR 赋予其的法律责任（“GDPR 控制者责任”）。当控制者实施的处理活动根据第 3 条第 1

〔17〕 根据第 28 条，欧洲数据保护委员会回顾说，处理者代表控制者进行的处理活动应受根据欧盟法或成员国法律制定的合同或其他法律行为的约束，对控制者来说，该合同或法律行为对处理者具有约束力，而且控制者只能选用有充分保证的、可采取合适技术和组织措施的、其处理方式符合本条例要求并且保障数据主体权利的处理者。

款属于 GDPR 的适用范围时，这一处理不会仅仅因为控制者指示了位于欧盟境外的处理者代表自己进行该处理就越出了 GDPR 的适用范围。

i）欧盟境内的控制者指示境外的处理者进行处理

如果受 GDPR 约束的控制者选择利用位于欧盟境外的处理者进行所涉的处理活动，那么控制者仍有必要通过合同或其他法律行为确保处理者对数据的处理符合 GDPR 的规定。第 28 条第 3 款规定，处理者进行的处理应受合同或其他法律行为的约束。因此，控制者必须保证和处理者签订符合第 28 条第 3 款所有要求的合同。此外，为了确保自己遵守了第 28 条第 1 款规定的责任——只能选用有充分保证的、可采取合适技术和组织措施的、其处理方式符合 GDPR 要求并且保障数据主体权利的处理者——控制者可能需要考虑通过合同将 GDPR 规定的责任加诸处理者。换言之，控制者必须确保不受 GDPR 约束的处理者承担第 28 条第 3 款规定的责任，而这些责任要受到根据欧盟法或成员国法律制定的合同或其他法律行为的约束。

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受 GDPR 约束的控制者施加的某些责任的约束。此外，GDPR 第 5 章的规定也可能适用。

示例 6：一个研究萨米人的芬兰研究所启动了一个只涉及俄罗斯萨米人的研究项目。在这个项目中，该研究所使用的处理者位于加拿大。

芬兰控制者有义务选用有充分保证的、可采取合适技术和组织措施的、其处理方式符合 GDPR 要求并且保障数据主体权利的处理者。芬兰控制者需要和加拿大处理者签订数据处理协议，以规定该处理者的责任。

ii）在处理者设在欧盟境内机构的活动范围内处理

通过相关判例，我们已经清楚地了解了在控制者设在欧盟境内机构的活动范围内的处理的效果，但对在处理者设在欧盟境内机构的活动范围内的处理的效果尚不太清楚。

欧洲数据保护委员会强调，在确定控制者和处理者各自所设机构是否“设在欧盟境内”时，对各方进行分别考量是很重要的。

第一个问题是，控制者自身是否在欧盟境内设有机构，并在该机构的活动范围内进行处理。假定控制者未被视为在其设于欧盟境内机构的活动范围内进行处理，那么控制者将不受第 3 条第 1 款规定的 GDPR 控制者责任的约束（尽管其仍可能受到第 3 条第 2 款的约束）。除非有其他原因，否则处理者设在欧盟境内的机构将不会被视为控制者的机构。

紧接着出现的第二个问题是，处理者是否在其设于欧盟境内机构的活动范围内进行处理。如果答案是肯定的，处理者就要受到第 3 条第 1 款规定的 GDPR 处理者责任的约束。但是，这并不会导致非欧盟控制者受到 GDPR 控制者责任的约束。也就是说，一个“非欧盟”控制者（如前所述）不会仅仅因为选用了欧盟境内的处理者就受到 GDPR 的约束。

通过指示欧盟境内的处理者，不受 GDPR 约束的控制者没有“在欧盟境内的处理者的活动范围内”进行处理。处理是在控制者自身的活动范围内进行的；处理者不过只是提供了和控制者的

活动没有“不可分割的联系”的处理服务。[18] 如前所述，在欧洲数据保护委员会看来，对于设在欧盟的数据处理者代表欧盟境外，且根据第 3 条第 2 款不受 GDPR 约束的数据控制者进行处理的情况，数据控制者的处理活动不会仅仅因为是由设在欧盟境内的处理者代表其进行的就被认为属于 GDPR 适用的地域范围。然而，即便数据控制者不是设在欧盟境内，并且根据第 3 条第 2 款也不受 GDPR 的约束，但设在欧盟境内的数据处理者将根据第 3 条第 1 款受到 GDPR 相关规定的约束。

示例 7：一家墨西哥零售公司和一个设在西班牙的处理者签订合同，委托其处理和墨西哥公司的客户有关的个人数据。墨西哥公司专门向墨西哥市场提供服务，而且其处理对象也仅限于欧盟境外的数据主体。

在这种情况下，墨西哥零售公司既没有通过提供货物或服务将目标客户锁定在欧盟境内，也没有监控欧盟境内人员的行为。因此，根据第 3 条第 2 款，设在欧盟境外的数据控制者的处理不受 GDPR 的约束。

由于数据控制者不是在欧盟境内机构的活动范围内处理个人数据，因此，根据第 3 条第 1 款，GDPR 的规定不适用于该控制者。然而由于数据处理者设在西班牙，因此，根据第 3 条第 1 款，它的处理属于 GDPR 的适用范围。就其活动范围内的任何处理来说，处理者必须承担该条例赋予的处理者责任。

当欧盟境内的机构代表没有在欧盟境内设立机构的数据控制者进行处理活动，同时根据第 3 条第 2 款不属于 GDPR 适用的地域范围时，该处理者应受到下列直接适用于数据处理者的 GDPR 相关规定的约束：

* 除了协助数据控制者履行 GDPR 规定的有关（控制者）义务的责任之外，还包括第 28 条第 2、3、4、5、6 款赋予处理者的责任，以及签订数据处理协议的责任；

* 根据第 29 条和第 32 条第 4 款，除非收到控制者的指示，处理者和任何在控制者或处理者授权下访问个人数据的人都不得处理这些数据，除非欧盟或成员国法律要求进行这种处理；

* 根据第 30 条第 2 款，如果适用的话，处理者应当保存代表控制者进行的所有类型的处理的记录；

* 根据第 31 条，如果适用的话，在监管机构的要求下，处理者应当在履行其任务时和监管机构合作；

* 根据第 32 条，处理者应当采取技术和组织措施，以确保和风险相称的安全水平；

* 根据第 33 条，处理者在获知个人数据泄露后，应当及时告知控制者；

* 根据第 37 条和第 38 条，如果适用的话，处理者应当委任一名数据保护官；

* 第 5 章有关将个人数据转移到第三国或国际组织的规定。

[18] 在这一范围内提供的处理服务不能被视为向欧盟境内的数据主体提供服务。

此外，由于此类处理将在欧盟境内机构的活动范围内进行，欧洲数据保护委员会再次强调，处理者还必须确保其处理就欧盟或成员国法律规定的其他义务来说仍然是合法的。第 28 条第 3 款还规定，“如果处理者认为某项指示违反了本条例或其他欧盟或成员国的数据保护条款，其应当立即告知控制者”。

与第 29 条工作组先前的立场一致，欧洲数据保护委员会认为，在诸如处理活动涉及不可接受的道德问题的情况下〔19〕，欧盟不能成为“数据安全港”。同时，对于那些欧盟数据保护法适用范围之外的法律义务，尤其是有关公共秩序的欧盟或成员国法律规则，任何欧盟境内的数据处理者在任何情况下都必须遵守，不论数据控制者位于哪里。这一观点还考虑到了这样一个事实，即通过执行欧盟法律，GDPR 和相关成员国的法律规定受到了《欧盟基本权利宪章》的约束。〔20〕但是，就不属于 GDPR 适用的地域范围的处理来说，这并不意味着给欧盟境外控制者强加额外的责任。

二、目标标准的适用——第 3 条第 2 款

没有在欧盟境内设立机构并不必然意味着第三国的数据控制者或处理者进行的处理活动就不属于 GDPR 的适用范围，因为第 3 条第 2 款规定了根据其具体的处理活动，GDPR 适用于设在欧盟境外的控制者或处理者的情况。

在这种情况下，欧洲数据保护委员会确认，当没有在欧盟境内设立机构时，控制者或处理者不能从 GDPR 第 56 条规定的一站式服务机制中受益。事实上，GDPR 的合作和一致性机制仅适用于在欧盟境内设有一个乃至多个机构的控制者和处理者。〔21〕

虽然本指南旨在阐明 GDPR 适用的地域范围，但欧洲数据保护委员会也希望强调，控制者和处理者还需要考量其他可适用的文本，比如欧盟或成员国的部门立法和国内法律。在某些领域或和特定处理有关的情形，GDPR 的某些规定确实允许成员国在国家层面引入附加条件，并定义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，并且遵守这些可能因成员国不同而各异的附加条件和框架。在有关 GDPR 第 8 条（规定儿童对信息社会服务处理其数据给予有效同意的年龄在 13 至 16 岁之间）、第 9 条（有关特殊类型个人数据的处理）、第 23 条（限制），以及第 9 章（表达和信息自由；公众对官方文件的访问；全国性身份识别号码；雇佣语境下的处理；为了实现公共利益、科学或历史研究或统计目的的处理；保密；教会和宗教团体）的规定内容方面，这种各成员国适用的数据保护规定间的差异表现得尤为明显。

第 3 条第 2 款规定：“本条例适用于控制者或处理者对欧盟境内数据主体的个人数据的如下处

〔19〕 *Supra* note〔3〕.

〔20〕 Charter of Fundamental Right of the European Union，2012/C 326/02.

〔21〕 G29 WP244 rev.1，13th December 2016， Guidelines for identifying a controller or processor’s lead supervisory authority-endorsed by the EDPB.

理，即使数据控制者或处理者不在欧盟设立：a. 为欧盟境内的数据主体提供商品或服务，不论是否要求数据主体支付对价；或 b. 对发生在欧盟境内的数据主体的行为进行监控。”

根据第 3 条第 2 款，如果欧盟境外的控制者或处理者进行的处理活动既和欧盟境内的数据主体有关，又属于该条款规定的两种不同的活动类型的任意一种，就将引发针对欧盟境内数据主体的“目标标准”的适用。除了适用于欧盟境外控制者或处理者进行的处理之外，目标标准主要关注“处理活动”和这两种活动类型的“相关性”，而这一点将通过个案考察予以确定。

欧洲数据保护委员会强调，控制者或处理者可能因自身某些处理活动而受 GDPR 的约束，但在另一些处理活动中则不受 GDPR 的约束。根据第 3 条第 2 款，GDPR 适用的地域范围的决定因素在于对相关处理活动的考量。

因此，在评估适用目标标准的条件时，欧洲数据保护委员会建议采用“两步检验法”：首先判断处理是否关涉欧盟境内数据主体的个人数据；然后确定处理是否涉及提供商品或服务，或监控数据主体在欧盟境内的行为。

a）欧盟境内的数据主体

由于第 3 条第 2 款的措辞是“欧盟境内数据主体的个人数据”，因此，目标标准的适用不受个人数据正被处理的数据主体的公民身份、居住地或其他法律身份的限制。GDPR 说明部分第 14 段确认了这一解释，该段指出，“本条例提供的保护应当适用于其个人数据受到处理的自然人，不论其国籍和居住地”。

因为《欧盟基本权利宪章》第 8 条规定个人数据受保护的权利的主体不是有限的，而是“所有人”[22]，GDPR 的这一规定表明，为个人数据保护规定了广泛范围的欧盟主要法律也不是只适用于欧盟公民。虽然根据第 3 条第 2 款，数据主体位于欧盟境内是适用目标标准的决定性因素，但欧洲数据保护委员会认为，欧盟境内数据主体的国籍或法律身份不能限定或限制本条例适用的地域范围。

在引起 GDPR 适用的相关处理活动发生时，也就是提供商品或服务，或监控行为发生时，不论这些行为持续多久，都必须对数据主体位于欧盟境内的要求进行评估。

然而就和提供服务有关的处理活动而言，欧洲数据保护委员会认为，该条款旨在针对那些特意，而非无意或偶然以欧盟境内个人为目标的处理活动。因此，如果处理和仅向欧盟境外个人提供的服务有关，即便这些人进入欧盟时服务并未取消，相关处理也不受 GDPR 约束。在这种情况下，处理不是特意针对欧盟境内的个人，而是针对欧盟境外的个人，而且不论这些人是在欧盟境外还是境内，这一处理活动都将继续。

示例 8：一家澳大利亚公司根据用户偏好和兴趣提供移动新闻和视频内容服务。用户可以每天或每周接受更新。此服务仅针对澳大利亚的用户，而且用户在订阅时必须提供澳大利

〔22〕《欧盟基本权利宪章》第 8 条第 1 款规定：“人人享有与其相关的个人数据受到保护的权利。”

亚电话号码。

一位澳大利亚订户前往德国度假，同时继续使用该服务。

虽然这位澳大利亚订户在欧盟期间将继续使用该服务，但该服务并不是“针对”欧盟境内的个人，而是仅针对澳大利亚的个人，因此这家澳大利亚公司对个人数据的处理不属于 GDPR 的适用范围。

示例 9：一家设在美国的初创企业为游客提供城市地图应用服务，但在欧盟没有任何业务或机构。一旦用户开始在游览的城市适用这款应用程序，它就将处理和用户（数据主体）所在位置有关的个人数据，以便为其提供有关游览地、餐厅、酒吧和酒店的针对性广告。这款应用程序可供游客在纽约、旧金山、多伦多、巴黎和罗马旅游时使用。

凭借其城市地图应用程序，这家美国初创企业专门针对在欧盟境内（即巴黎和罗马）的个人，在这些人旅欧期间向他们提供服务。根据第 3 条第 2 款 a 项，处理欧盟境内数据主体的和提供服务有关的个人数据属于 GDPR 的适用范围。此外，通过处理数据主体的位置数据，以便根据他们的位置提供有针对性的广告，处理活动还涉及对欧盟境内个人行为的监控。因此，根据第 3 条第 2 款 b 项，这家美国初创企业的处理也属于 GDPR 的适用范围。

欧洲数据保护委员会还希望强调，仅有处理欧盟境内个人的个人数据这一事实尚不足以导致将 GDPR 适用于欧盟境外的控制者或处理者的处理活动。此外，以欧盟境内的个人为“目标”这一要素，不论是对向他们提供商品或服务的情形，还是对监控他们的行为的情形，都必须始终存在。

示例 10：一位美国公民正在欧洲旅游度假。旅欧期间，他下载使用了一家美国公司提供的新闻应用程序。从该款应用程序的使用条款和指定美元作为唯一支付货币可明显看出其专门针对美国市场。这家美国公司通过应用程序收集美国游客的个人数据的行为不受 GDPR 的约束。

此外，应当指出的是，只要处理既不涉及为欧盟境内个人提供商品或服务，也不是对他们在欧盟境内行为的监控，那么在第三国处理欧盟公民或居民的个人数据就不会导致 GDPR 的适用。

示例 11：中国台湾一家银行的客户住在台湾，但拥有德国国籍。该行仅在台湾开展业务，其经营活动也不针对欧盟市场。该行对其德国客户个人数据的处理就不受 GDPR 的约束。

示例 12：当欧盟公民进入加拿大领土时，为了审查这些人的签证申请，加拿大移民局会处理他们的个人数据。这种处理不受 GDPR 的约束。

b）为欧盟境内的数据主体提供商品或服务，不论是否要求数据主体支付对价

导致第 3 条第 2 款适用的第一种活动是“提供商品或服务”。欧盟法律和判例进一步厘清了这一概念，在适用目标标准时应予以考虑。提供服务还包括提供信息社会服务，而欧盟第 2015/1535

号指令[23]第1条第1款b项将之界定为“任何信息社会服务，即通常应服务接受者的个别要求，依靠电子手段提供的任何远程有偿服务”。

第3条第2款a项明确规定，不论是否需要数据主体支付对价，关于提供商品或服务的目标标准都适用。因此，欧盟境外的控制者或处理者的活动是否应被视为提供商品或服务并不取决于是否支付了对价。[24]

示例13：一家未在欧盟设立任何机构的美国公司，出于人力资源的目的，处理临时赴法国、比利时和荷兰的员工的个人数据，特别是根据他们所在的国家持续为他们报销差旅、支付津贴。

在这种情况下，虽然处理活动和欧盟领土上的人（即暂时在法国、比利时和荷兰的员工）存在特殊关系，但它和向这些人提供服务没有关系，不过是雇主履行其合同义务和人力资源方面的职责所必需的处理的一部分。处理活动不涉及提供服务，因此根据第3条第2款a项，不受GDPR规定的约束。

在确定是否满足第3条第2款a项的目标标准时，另一个需要评估的关键因素是，商品或服务的提供是不是针对欧盟境内的人，或者说，控制者一方的行为——它决定了处理的手段和目的——是不是表明他有意向位于欧盟的数据主体提供商品或服务。GDPR说明部分第23段对此明确说到：“为判断该控制者或处理者是否向位于欧盟境内的数据主体提供商品或服务，应确认控制者或处理者是否明显企图向位于欧盟境内一个或多个成员国的数据主体提供服务。”

说明部分进一步明确指出：“如果控制者网站、处理者网站或其他中介网站仅能获取邮件地址或其他联系方式，或者使用了控制者所在地的第三国的通用语言，不足以确认其提供服务的意图，一些判断因素可辨明控制者企图向欧盟境内相关数据主体提供服务的意图，例如使用一个或多个欧盟成员国的通用语言或货币用于订购以其他语言标识的商品和服务，或涉及欧盟境内的客户或用户。”

GDPR说明部分第23段规定的要素和欧盟法院根据欧盟理事会《关于民商事案件管辖与判决的承认和执行的第44/2001号条例》[25]尤其是其中的第15条第1款c项作出的判例是一致的。在帕尔默诉卡尔·施卢特航运公司案和阿尔本霍夫酒店诉海勒案（合并审理案件编号C-585/08和C-144/09）中，欧盟法院被要求就第44/2001号条例（《布鲁塞尔第一条例》）第15条第1款语境中的“指向性活动”作出解释。欧盟法院认为，根据《布鲁塞尔第一条例》第15条第1款c项，为了确定交易者是否能被视作将其活动指向消费者住所所在的成员国，交易者必须已表明和消费

【23】欧洲议会和欧盟理事会2015年9月9日第2015/1535号指令规定了在技术法规和信息社会服务规则领域提供信息的程序。

【24】*See* in particular，CJEU，C-352/85，*Bond van Adverteerders and Others vs. The Netherlands State*，26 April 1988，par. 16，and CJEU，C-109/92，Wirth［1993］Racc. I-6447，par. 15.

【25】Council Regulation（EU）No 44/2001 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

者建立商业关系的意图。在这一背景下，欧盟法院认为有证据表明，该交易者正打算和居住在某成员国的消费者做生意。

虽然“指向性活动”的概念不同于“提供商品或服务”，但欧洲数据保护委员会认为，在考虑是否构成向欧盟境内的数据主体提供商品或服务时，帕尔默诉卡尔·施卢特航运公司案和阿尔本霍夫酒店诉海勒案（合并审理案件编号 C-585/08 和 C-144/09）[26] 中的判例规则可能有所帮助。因此，在考量案件具体事实时，除了其他因素外，还可以将下列因素结合起来考量：

* 根据提供的商品或服务，欧盟或至少一个成员国被点名；

* 为了方便用户访问网站，数据控制者或处理者向搜索引擎运营商支付互联网指引服务的费用；或者控制者或处理者已针对某成员国受众发起营销和广告活动；

* 相关活动如某些旅游活动的国际性质；

* 提及某欧盟成员国的专用地址或电话号码；

* 使用控制者或处理者所在的第三国之外的顶级域名，如“.de”，或适用中性顶级域名，如“.eu”；

* 从一个或多个欧盟成员国到服务提供地的旅行说明；

* 提及由居住在多个成员国的消费者组成的国际客户，尤其是通过出示这些消费者的书面解释；

* 使用的语言或货币不是交易者所在国，特别是一个或多个欧盟成员国的通用语言或货币；

* 数据控制者在欧盟成员国交付商品。

如前所述，对于上述因素，如果单独考量，可能并不意味着数据控制者打算向欧盟境内的数据主体提供商品或服务。但是，为了确定和数据控制者的商业活动有关的多项因素的组合是否能证明为欧盟境内数据主体提供商品或服务，在任何具体分析中，都应当考量所有这些因素。

然而必须牢记的是，说明部分第 23 段确认，控制者、处理者或某中介在欧盟的网站仅能获取其邮件或地理地址，或没有国际电码的电话号码，那么其本身尚不足以证明控制者或处理者有意向欧盟境内的数据主体提供商品或服务。由此，欧洲数据保护委员会回顾说，如果向欧盟领土上的人提供商品或服务是一种无意或偶然的行为，那么相关的个人数据处理就不属于 GDPR 的适用范围。

示例 14：一家在土耳其设立和运营的网站为客户提供创建、编辑、印刷和运送个性化家庭相册的服务。该网站有英语、法语、荷兰语和德语版本，可以用欧元支付。该网站指出，在法国、比荷卢三国和德国，相册只能通过邮寄发送。

很明显，在这种情况下，创建、编辑和印刷个性化家庭相册是欧盟法律意义上的一项服

〔26〕更重要的是，根据欧洲议会和欧盟理事会 2008 年 6 月 17 日第 593/2008 号《关于合同责任的法律适用的条例（罗马第一条例）》第 6 条，在没有法律可供适用的情况下，考虑消费者经常居住国的“指向性活动”标准，将消费者经常居住地法律指定为适用于合同的法律。

务。该网站有四种欧盟语言版本；在六个欧盟成员国可以邮寄相册。这些事实都表明，这家土耳其网站有意向欧盟境内的个人提供服务。

因此，作为数据控制者，这家土耳其网站进行的处理显然涉及向欧盟境内数据主体提供服务。根据第 3 条第 2 款 a 项，这一处理必须遵守 GDPR 的规定。

同时，根据第 27 条，数据控制者还必须在欧盟委任一名代表。

示例 15：设在摩纳哥的一家私营公司为支付工资而处理员工的个人数据。该公司的大量员工都是法国和意大利居民。

在这一案例当中，虽然该公司进行的处理涉及法国和意大利的数据主体，但这种处理并非是在提供商品或服务的背景下进行的。事实上，人力资源管理包括第三国公司的工资支付都不能被视作第 3 条第 2 款 a 项所说的提供服务。相关处理不涉及向欧盟境内数据主体提供商品或服务（也不是对行为的监控），因此，根据第 3 条，不受 GDPR 规定的约束。

这一判断不影响有关第三国的准据法。

示例 16：位于苏黎世的一所瑞士大学正在开展其攻读硕士学位的遴选活动，考生可通过一个在线平台上传他们的简历、申请信和联系方式。任何拥有足够德语和英语水平，并持有学士学位的学生都可以参加遴选。这所大学没有专门向欧盟的大学的学生做广告，同时只接受用瑞士货币结算。

由于在该硕士学位的申请和遴选过程中没有对来自欧盟学生的区别对待，因此不能确定瑞士大学有意针对来自某个欧盟成员国的学生。足够的德语和英语水平也是一项一般性要求，适用于任何申请人，无论其为瑞士居民、欧盟的人，还是来自第三国的学生。因此，如果没有其他因素表明来自欧盟成员国的学生才是明确目标，就不能肯定相关处理涉及向欧盟境内数据主体提供教育服务，也就不受 GDPR 规定的约束。

这所瑞士大学还提供国际关系暑期课程，而且专门就这个项目向德国和奥地利的大学作宣讲，以最大化该课程的参与人数。在这种情况下，这所瑞士大学就有很明确的向欧盟境内的数据主体提供这项服务的意图，GDPR 也将适用于与此相关的处理活动。

c）监控数据主体的行为

导致第 3 条第 2 款适用的第二类活动是对发生在欧盟范围内的数据主体的行为进行监控。

说明部分第 24 段对此明确规定：“设在欧盟境外的控制者或处理者对欧盟境内数据主体的个人数据进行处理时，如果涉及对该数据主体发生在欧盟范围内的行为的监控，也应受到本条例的约束。”

就根据第 3 条第 2 款 b 项而适用 GDPR 的情况而言，受到监控的行为首先必须和欧盟境内的数据主体有关，其次，作为一项累计条件，受到监控的行为必须发生在欧盟境内。

说明部分第 24 段进一步明确规定了可被视为行为监控的处理活动的特征，其中规定：“为了判断处理活动是否可以被认定为是对数据主体在欧盟境内发生行为的监控，应查明是否可通过互

联网对自然人实施追踪，包括是否有可能后续运用个人数据处理技术描述出自然人的特征，或者对其个人偏好、行为或态度作出分析或预测。”虽然说明部分第 24 段仅涉及通过互联网对自然人实施追踪来监控行为，但欧洲数据保护委员会认为，在确定一项处理活动是否构成行为监控时，通过涉及个人数据处理的其他类型的网络或技术进行追踪，例如可穿戴的或其他智能设备，也应当纳入考量范围。

与第 3 条第 2 款 a 项不同，在确定监控活动是否会导致 GDPR 对处理活动的适用时，无论是第 3 条第 2 款 b 项，还是说明部分第 24 段都没有明确要求数据控制者或处理者要具备必要的“目标意图”。但是，“监控”一词的使用意味着控制者有一个特定的目的，即对自然人在欧盟境内行为的相关数据进行收集和随后再利用。但是，欧洲数据保护委员会并不认为，任何对欧盟境内自然人的个人数据的收集和分析都自动构成“监控”。有必要考量控制者处理数据的目的，尤其是涉及这些数据的后续行为分析或图谱技术。欧洲数据保护委员会考虑了说明部分第 24 段的措辞，该段措辞表明，就确定处理是否涉及对数据主体行为的监控来说，通过互联网对自然人实施追踪包括图谱技术的潜在后续应用是一个关键的考量因素。

因此，第 3 条第 2 款 b 项规定的数据控制者或处理者监控欧盟境内数据主体行为的情况可以涵盖范围广泛的监控活动，尤其包括以下诸项：

* 行为广告；
* 特别是用于营销目的的地理定位活动；
* 使用 Cookie 或其他追踪技术（如指纹识别）进行的在线追踪；
* 在线个性化饮食和健康分析服务；
* 闭路电视监控；
* 以个人资料为基础的市场调查和其他行为研究；
* 监测或定期报告个人的健康状况。

示例 17：根据对通过 Wi-Fi 追踪收集的一家法国购物中心的顾客活动的分析，美国的一家零售咨询公司为这家购物中心提供了零售布局方面的建议。

通过 Wi-Fi 追踪对购物中心顾客的活动进行分析就相当于对个人行为的监控。在这种情况下，因为购物中心位于法国，数据主体的行为就发生在欧盟。因此，根据第 3 条第 2 款 b 项，作为数据控制者，这家咨询公司为此目的进行的处理必须受到 GDPR 的约束。

根据第 27 条，数据控制者应在欧盟委任一名代表。

示例 18：未在欧盟境内设立机构的一家加拿大应用程序开发商监控了欧盟境内数据主体的行为，那么根据第 3 条第 2 款 b 项，这家开发商就要受到 GDPR 的约束。这家开发商利用设在美国的处理者进行应用程序的优化和维护。

就该处理而言，根据第 28 条，加拿大控制者有义务只选用适当的处理者，并确保其在 GDPR 项下的责任体现在管辖其与美国处理者关系的合同或法律行为当中。

d）处理者不设在欧盟境内

和引起第 3 条第 2 款适用的目标活动“相关”的活动属于 GDPR 适用的地域范围。欧洲数据保护委员会认为，处理活动和提供商品或服务之间需要有关联，但控制者和处理者的处理都是相关的，都需要纳入考量范围。

当涉及不设在欧盟境内的数据处理者时，为了确定其处理根据第 3 条第 2 款是否应受 GDPR 的约束，有必要研究处理者的处理活动是不是和控制者的目标活动“相关”。

欧洲数据保护委员会认为，如果控制者的处理活动和提供商品或服务，或者监控欧盟境内的个人行为（“目标”）相关，那么根据第 3 条第 2 款，任何被指示代表控制者实施处理活动的处理者，都会因为该处理活动而属于 GDPR 的适用范围。

处理活动的“目标”特征与其目的和手段有关；只有作为控制者的实体才能作出以欧盟境内的个人为目标的决定。这种解释并没有排除处理者可能积极参与和贯彻目标标准有关的处理活动（即处理者代表控制者，并根据其指示而提供商品或服务，或者实施监控活动）。

因此，在欧洲数据保护委员会看来，应当重点关注处理者实施的处理和数据控制者从事的目标活动之间的关联。

示例 19：一家巴西公司在网上销售食品配料和当地菜谱，通过在法国、西班牙和葡萄牙为这些产品做广告并提供配送，使欧盟境内的人可以获得这些商品。在这种背景下，该公司指示同样设在巴西的数据处理者在法国、西班牙和葡萄牙的消费者此前订单的基础上进行相关的数据处理，以为他们开发特价优惠。

在数据控制者的指示下，处理者的处理活动是和向欧盟境内数据主体提供商品相关的。此外，通过开发这些定制优惠，数据处理者直接监控了欧盟境内的数据主体。因此，根据第 3 条第 2 款，处理者的处理要受 GDPR 的约束。

示例 20：一家美国公司开发了一款关于健康和生活方式的应用程序，允许用户通过该应用程序记录他们的个人指标（睡眠时间、体重、血压、心跳等）。然后，该应用程序为用户提供每日饮食和运动建议。数据处理是由美国的数据控制者实施的。该应用程序可供欧盟境内的个人使用。为了存储数据，这家美国公司使用了设在美国的处理者（云服务提供商）。

这家美国公司正在监控欧盟境内个人的行为，从这一方面来看，在运营这款关于健康和生活方式的应用程序时，该公司将以欧盟境内的个人为“目标”。根据第 3 条第 2 款，它对欧盟境内个人的个人数据处理属于 GDPR 的适用范围。

在按照这家美国公司的指示，并以其名义实施处理时，云服务提供商/处理者正在实施一项和其控制者以欧盟境内个人为“目标”“相关”的处理活动。根据第 3 条第 2 款，处理者代表其控制者实施的这项处理活动属于 GDPR 的适用范围。

示例 21：一家土耳其公司提供中东文化旅游套餐，旗下导游说英语、法语和西班牙语。该旅游套餐特别通过一个包括三种语言的网站进行宣传和提供，并且接受在线预订，可以用

欧元和英镑支付。为了市场营销和商业前景，该公司指示设于突尼斯的数据处理者，也是一家呼叫中心，与爱尔兰、法国、比利时和西班牙的前客户联系，以获取他们对此前旅行的反馈意见，并告知最新的优惠和旅行地。控制者通过向欧盟境内的个人提供服务来“锁定目标”，其处理属于第 3 条第 2 款规定的情形。

突尼斯处理者的处理活动促进了控制者对欧盟境内个人的服务，也和控制者提供的服务相关，因此属于第 3 条第 2 款规定的情形。此外，通过代表土耳其控制者，并根据其指示，突尼斯处理者积极参与了和实施目标标准相关的处理活动。

e）和 GDPR 其他条款以及其他立法的互动

欧洲数据保护委员会还将进一步评估根据第 3 条适用 GDPR 的地域范围和第 5 章有关国际数据传输规定之间的互动关系。如有必要，可在这方面发布指南。

不设在欧盟境内的控制者或处理者将被要求遵守其本国有关个人数据处理的法律。但是，如果此类处理涉及针对欧盟境内的个人，根据第 3 条第 2 款，控制者不仅要受到本国法律的约束，还要遵守 GDPR。不论该处理是为了履行第三国规定的法律责任，还是仅仅只是控制者的选择，都必须遵守 GDPR。

三、依据国际公法适用成员国法律的处理

第 3 条第 3 款规定：“本条例适用于设在欧盟境外，但依据国际公法，成员国法律对其有管辖权的控制者进行的个人数据处理。”说明部分第 25 段对此进行了详细阐释，其规定：“如果依据国际公法应适用成员国法律的，则本条例同样适用于设在欧盟境外的控制者，例如成员国的使领馆。”

由于根据第 3 条第 3 款，成员国设在欧盟境外的使领馆进行的个人数据处理属于 GDPR 的适用范围，因此，欧洲数据保护委员会认为，GDPR 适用于此类处理。作为数据控制者或处理者，成员国的使领馆将受到所有 GDPR 相关条款包括涉及的数据主体的权利、关于控制者或处理者的一般性责任，以及关于向第三国或国际组织传输个人数据的一般性责任的约束。

示例 22：为支持自身的行政管理，荷兰驻牙买加金斯敦领事馆招聘了当地工作人员，并为此开通了在线申请程序。

虽然荷兰驻牙买加金斯敦领事馆不是设在欧盟境内，然而根据国际公法，该领事馆作为欧盟成员国的驻外领馆适用该成员国法律。因此，根据第 3 条第 3 款，GDPR 适用于该领事馆进行的个人数据处理。

示例 23：一艘航行在国际水域的德国邮轮正在处理船上游客的数据，以便调整船上的娱乐活动。

虽然该船位于欧盟境外的国际水域，但其为德国注册邮轮的事实意味着，基于国际公法的因素，根据第 3 条第 3 款，GDPR 适用于其对个人数据的处理。

虽然和第 3 条第 3 款的适用无关，但还有一种情况是，根据国际法，某些设在欧盟境内的实体、机构或组织享有 1961 年《维也纳外交关系公约》[27]、1963 年《维也纳领事关系公约》或国际组织和其欧盟驻在国订立的总部协议规定的特权和豁免。对此，欧洲数据保护委员会重申，GDPR 的适用不影响国际法的规定，例如关于非欧盟外交使领馆和国际组织享有特权和豁免的规定。然而与此同时，重要的是要记住，任何属于 GDPR 适用范围的特定处理活动的控制者或处理者，以及与此类实体、机构和组织进行数据交换的控制者或处理者，都必须遵守 GDPR，包括其中适用于向第三国或国际组织传输数据的规则。

四、不设在欧盟的控制者或处理者的代表

根据第 3 条第 2 款，受到 GDPR 约束的数据控制者或处理者有责任在欧盟委任一名代表。不设在欧盟境内，但受到 GDPR 约束的控制者或处理者没有在欧盟委任代表则会违反 GDPR。

这个规定不是新出台的，因为《指令》就已经规定了类似的义务。根据《指令》，这一规定涉及不是设在欧共体境内的控制者，为了处理个人数据，这些控制者使用了位于某个成员国的自动化或其他类型的设备。对任何属于第 3 条第 2 款范围内的控制者或处理者，GDPR 规定其有责任在欧盟境内委任一名代表，除非其符合第 27 条第 2 款规定的豁免标准。为了促进这一具体规定的适用，欧洲数据保护委员会认为，有必要根据第 27 条就驻欧盟代表的委任程序、机构义务和责任提供进一步指导。

值得注意的是，不设在欧盟境内的控制者或处理者根据 GDPR 第 27 条以书面形式委任驻欧盟代表的，不属于第 3 条第 1 款的适用范围。这就意味着驻欧盟代表的存在不构成第 3 条第 1 款意义上的控制者或处理者的“机构”。

a）委任代表

说明部分第 80 段解释说：“代表应通过控制者或处理者的书面授权明确加以委任，并代表控制者或处理者履行本条例规定的责任。此类代表的委任不影响本条例规定的控制者或处理者的责任或义务。代表应根据控制者或处理者的授权执行任务，包括为确保遵守本条例而采取的任何和监管机构的合作行动。”

因此，说明部分第 80 段所说的书面授权应规定驻欧盟代表和设在欧盟境外的数据控制者或处理者之间的关系和责任，但同时也不得影响控制者或处理者所承担的责任或义务。驻欧盟代表可以是欧盟境内的自然人或法人，应能代表设在欧盟境外的数据控制者或处理者履行各自所承担的 GDPR 上的责任。

---

〔27〕*Vienna Conventionon Diplomatic Relations*，https://legal.un.org/ilc/texts/instruments/english/conventions/9_1_1961.pdf（last visited Feb. 16，2020）.

实践中，驻欧盟代表的职能可以根据和个人或组织签订的服务合同加以履行，因此可以由范围广泛的商业和非商业实体如律师事务所、咨询公司、私营企业等来承担，只要这些实体设在欧盟境内。一名代表还可以代表数个非欧盟控制者和处理者。

当公司或其他类型的组织承担了代表职能时，有人建议为每个被代表的控制者或处理者单独指派一个人作为主要联系人和“负责”人。一般来说，在服务合同中将这些问题约定清楚也是很有用的。

根据 GDPR，欧洲数据保护委员会确认，当控制者或处理者的若干处理活动属于 GDPR 第 3 条第 2 款规定的情形（并且不适用第 27 条第 2 款规定的豁免）时，该控制者或处理者不必单独为每一项第 3 条第 2 款范围内的处理活动委任若干代表。在欧洲数据保护委员会看来，驻欧盟代表的职能和将设在欧盟境内的外部数据保护官（DPO）的角色并不一致。为了确保数据保护官在组织内部拥有足够的自主权执行其任务，第 38 条第 3 款确立了一些基本的保障措施。其中尤其要求控制者或处理者确保数据保护官“不会收到任何有关其执行任务的指示”。说明部分第 97 段还补充道，“不论他们是不是控制者的雇员，都应该以独立的方式履行他们的职责和任务”。[28] 这种针对数据保护官要有足够自主权和独立性的要求似乎并不符合驻欧盟代表的职能。事实上，该代表受制于控制者或处理者的委托授权，以其名义开展活动，并因此直接听命于他们的指示。[29] 驻欧盟代表由其所代表的控制者或处理者授权，因此要以控制者或处理者的名义执行其任务，这一角色无法与数据保护官以独立方式履行职责和任务相兼容。

此外，为了补充自己的解释，欧洲数据保护委员会还回顾了 WP29 先前已经采纳的立场，即强调“在涉及数据保护问题的案件中，要求外部数据保护官在法庭上代表控制者或处理者，也可能导致利益冲突”。[30]

同样地，鉴于执行程序中可能存在的责任和利益冲突，欧洲数据保护委员会认为，数据控制者驻欧盟代表的职能和其数据处理者的角色也是不兼容的，尤其在遵守他们各自的职责和合规性方面。

虽然 GDPR 没有要求数据控制者或其代表本身向监管机构通报代表委任事宜，但欧洲数据保护委员会重申，根据第 13 条第 1 款 a 项和第 14 条第 1 款 a 项，作为其告知义务的组成部分，控制者应当向数据主体提供其驻欧盟代表的身份信息。例如，这一信息应包含在数据收集时提供给数据主体的［隐私通知和］前期信息之中。不设在欧盟境内，但符合第 3 条第 2 款规定情形的控

〔28〕 WP 29 Guidelines on Data Protection Officers （“DPOs”），WP 243 rev.01-endorsed by the EDPB.

〔29〕 例如，在以下这种情况下，一个外部数据保护官不可能同时作为驻欧盟代表行事：作为代表，他被指示和数据主体就控制者或处理者采取的决定或措施进行沟通，然而对于这一决定或措施，作为数据保护官，他/她认为不符合 GDPR 的规定，并提出了反对意见。

〔30〕 *Supra* note〔28〕.

制者，如果没有向欧盟境内的数据主体告知其代表的身份，将违反根据 GDPR 承担的信息透明责任。此外，这些信息应便于监管机构查阅，以便建立合作所必要的联系。

示例 24：示例 14 中提及的网站设在土耳其，并且也在那里运营，其提供创建、编辑、印刷和运送个性化家庭相册的服务。该网站有英语、法语、荷兰语和德语版本，接受以欧元或英镑支付。该网站标明相册仅能在法国、比荷卢三国和德国寄送。根据第 3 条第 2 款 a 项，该网站受到 GDPR 的约束，数据控制者必须在欧盟委任一名代表。

代表必须设在可以接受服务的某个成员国。在这个案件当中，就是法国、比利时、荷兰、卢森堡或德国。一旦数据主体通过创建相册使用了这项服务，数据控制者及其驻欧盟代表的名称和联系方式就必须成为向他们在线开放的信息的构成部分。此外，这些信息还必须出现在网站的一般隐私声明当中。

b）委任责任的豁免[31]

虽然第 3 条第 2 款的适用引起了设在欧盟境外的控制者或处理者在欧盟委任代表的责任，但第 27 条第 2 款规定，在以下两种情况下，强制在欧盟委任代表的责任会得到豁免：

* 处理是“偶然发生的，并且不包括第 9 条第 1 款规定的特定类型数据的大规模处理，或者第 10 条所规定的和刑事定罪或违法相关的个人数据处理”，同时，“考虑到这种处理的性质、语境、范围和目的”，其“不太可能对自然人的权利和自由带来风险”。

根据第 29 条工作组此前的立场，欧洲数据保护委员会认为，处理活动只有是不定期进行，并且发生在控制者或处理者的通常业务和活动之外时，才会被认为是“偶然的”。[32]

此外，虽然 GDPR 没有界定什么是大规模处理，但 WP29 在其之前有关数据保护官的 WP243 指南中建议，在确定是否构成大规模处理时，以下因素尤其值得考量：有关数据主体的数量——要么是一个具体数目，要么是相关人口的一定比例；正在处理的数据量和/或不同数据项的范围；数据处理活动的持续时间或持久性；处理活动的地域范围。[33]

最后，欧洲数据保护委员会强调，第 27 条规定的豁免情形包括处理“不太可能对自然人的权利和自由带来风险”[34]，但并没有因此将豁免只限制于这种情形。根据说明部分第 75 段，在评估对自然人的权利和自由带来的风险时，应考量风险的可能性和严重性。

或者，

* 处理是由“公共机构或实体”实施的。

---

〔31〕 G29 WP243 第 1 版（数据保护官）中规定的部分标准和解释经 EDPB 认可，可作为豁免委任责任的依据。

〔32〕 WP29 关于豁免 GDPR 第 30 条第 5 款规定的保存处理活动记录的责任的立场文件。

〔33〕 WP29 guidelines on data protections officers（DPOs），adopted on 13th December 2016，as last revised on 5th April 2017，WP 243 rev.01-endorsed by the EDPB.

〔34〕 GDPR 第 27 条第 2 款 a 项。

对于设在欧盟境外的实体是否具备“公共机构或实体”的资质，需要由监管机构在个案中根据具体情况进行评估。[35] 欧洲数据保护委员会指出，鉴于第三国公共机构或实体的任务和使命的性质，当他们向欧盟境内数据主体提供商品或服务，或者监控这些数据主体在欧盟境内的行为时很可能会受到限制。

第 27 条第 3 款规定，“为数据主体提供相关商品或服务，或者监控数据主体的行为，应在数据主体的所在国之一设立代表”。如果个人数据受到处理的数据主体中的很大一部分都在某个特定的成员国，作为一种好的实践，欧洲数据保护委员会建议就在该国设立代表。但是，在未设代表的成员国，以及商品或服务提供地或者行为监控发生地所在的成员国，代表必须便于数据主体接触。

欧洲数据保护委员会确认，个人数据正被处理的数据主体所在的位置是设立驻欧盟代表的标准。处理地点——即便该处理是由设在另一个成员国的处理者实施的——在这里不是确定代表设立地点的相关因素。

示例 25：一家印度制药公司，既不在欧盟开展业务，也没有在欧盟设立机构，但赞助支持了比利时、卢森堡和荷兰的研究人员（医院）进行的临床试验，参加临床试验的大多数患者都在比利时。根据第 3 条第 2 款，这家印度制药公司要受到 GDPR 的约束。

作为数据控制者，这家印度制药公司应在患者作为数据主体参与临床试验的比荷卢三国中的一个设立驻欧盟代表。因为大多数患者都是比利时居民，因此建议将代表设在比利时。这样的话，荷兰和卢森堡的数据主体和监管机构也应该可以比较容易地接触到设在比利时的代表。

在这种特定情况下，根据欧盟《关于临床试验的第 536/2014 号条例》第 74 条，只要驻欧盟代表不作为临床试验赞助者的数据处理者，只要驻欧盟代表设这三个成员国中的一个，并且两种职能都受到各自所在国法律框架的约束，并以其为依据加以执行，驻欧盟代表就可以作为欧盟赞助者的法律代表。

c）代表的责任和义务

控制者或处理者在欧盟的代表将以其名义履行 GDPR 规定的控制者或处理者责任，尤其包括和数据主体行使权利有关的那些责任。如前所述，在这方面，必须根据第 13 条和第 14 条向数据主体提供代表的身份和联系方式。虽然代表本身不负责遵从数据主体的权利，但为了便于数据主体有效行使权利，他必须促进数据主体和其所代表的控制者或处理者之间的沟通。

根据第 30 条，控制者或处理者的代表尤其应当保存由控制者或处理者负责的处理活动的记录。欧洲数据保护委员会认为，虽然控制者或处理者，以及他们的代表都负有保存此类记录的责任，但设在欧盟境外的控制者或处理者对记录的主要内容和更新负有责任，同时必须向其代表提

〔35〕 GDPR 没有提供“公共机构或实体”的定义。欧洲数据保护委员会认为，这一概念应根据国内法来确定。因此，公共机构和实体包括全国性、区域性和地方性机构。但根据可适用的国内法，这一概念还包括一系列受公法调整的其他机构。

供所有准确和最新的信息，以便代表能随时保存和提供此类记录。与此同时，按照第 27 条的要求提供记录，例如根据第 27 条第 4 款，当监管机构要求时，也是代表自己的责任。

正如说明部分第 80 段所解释的那样，代表应根据控制者或处理者的授权执行任务，包括为确保遵守本条例而采取的任何和监管机构的合作行动。实践中，这意味着监管机构将就和欧盟境外的控制者或处理者的合规责任有关的任何事务联系代表，代表则应能促进提出请求的监管机构和欧盟境外的控制者或处理者之间的任何信息或程序交流。

因此，必要时在一个小组的帮助下，驻欧盟代表必须能和数据主体进行有效沟通，并和相关的监管机构展开合作。这意味着这种沟通交流原则上应以监管机构和相关数据主体使用的一种或数种语言进行，然而如果效果不佳，代表则应使用其他手段和技术来确保有效沟通。因此，为了保证数据主体和监管机构能较为方便地和非欧盟控制者或处理者建立联系，代表的存在是绝对必要的。根据说明部分第 80 段和第 27 条第 5 款，委任驻欧盟代表不影响控制者或处理者根据 GDPR 承担的责任和义务，也不影响可能针对控制者或处理者自身发起的法律诉讼。GDPR 也没有确立任何由驻欧盟代表代替其所代表的控制者或处理者承担责任的替代责任制度。

但是应当指出的是，引入代表的概念正是为了便利和第 3 条第 2 款规定情形中的控制者或处理者之间的联系，并确保 GDPR 的有效实施。为此，监管机构应当能够通过欧盟境外的控制者或处理者委任的代表来启动执法程序。这包括监管机构有可能将根据 GDPR 第 58 条第 2 款和第 83 条对设在欧盟境外的控制者或处理者发布的纠正措施或行政罚款和处罚向代表提出。但是，要求代表直接承担责任的情形仅限于 GDPR 第 30 条和第 58 条第 1 款 a 项规定的代表的直接责任。

欧洲数据保护委员会进一步强调，GDPR 第 50 条的主要目的是促进和第三国，以及国际组织有关的立法的实施，而且目前正在考虑进一步推进该领域的国际合作机制。

Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3)

EDPB (Author), AO Haijing (Translator)

Translator's Note: In May 2018, the EU's General Data Protection Regulation (GDPR) came into effect, which greatly changed the international legal pattern. Since then, how to correctly interpret and apply GDPR has become the focus of attention in academia and practice. For non-EU countries, particular attention is paid to the extraterritorial effectiveness of GDPR. In this sense, a proper interpretation and clarification of the meaning of Article 3, which defines the territorial scope to which the GDPR applies, has become a crucial research topic. However, it is well known that for the interpretation and implementation of the GDPR, the European Data Protection Board

(EDPB) and its predecessor, the Article 29 Working Group, have issued the most authoritative guidelines. On November 16, 2018, EDPB issued Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) (Adoption of the Guidelines for publication consultation), which was widely put forward for public consultation, and the revised official was released on November 12, 2019 Version, which elaborates and clarifies the criteria for determining the territorial scope to which the GDPR applies. In the context of the increasingly open and integrated global economy and the Internet, GDPR will also have a significant impact on China's relevant date protection practices. The main thing those Chinese multinational corporations and other entities need to evaluate when starting a GDPR compliance project is which data processing activities will be subject to GDPR. As stated by the EDPB, this guideline is very important for data controllers and processors within and outside the EU to assess whether they need to comply with GDPR.

Keywords: GDPR; Territorial Scope; Establishment Criterion; Targeting Criterion; Representative

（责任编辑：王乐兵）