2022 年 3 月 16 日

GDPR 下不同数据跨境转移工具之评析

2022 年 2 月 22 日，欧盟数据保护委员会（“EDPB”）发布了《行为守则作为数据跨境转移工具的 04/2021 号指南》（“《04/2021 指南》”），对欧盟《一般数据保护条例》（“GDPR”）第 46 条项下，以行为守则作为数据跨境转移工具的适用以及行为守则的制定程序和内容等提供了相关指引。在此之前，标准合同条款（“SCCs”）和有约束力的企业规则（“BCRs”）是最常用的数据跨境转移工具。本文将借此机会梳理 GDPR 下的数据跨境转移途径并对不同数据跨境转移工具的适用场景和特点进行评析。

GDPR 原则性地规定，个人数据不得向欧盟以外的国家或地区转移，除非该国家或地区确保对数据主体有关个人数据处理的权利与自由实行与欧盟等同的保护水平。然而，在以下三种情况下个人数据可以合法出境：

1. 向欧盟认定具有同等保护水平的国家或地区转移；

2. 向提供了适当保障，确保充分数据保护的国家或地区转移；或

3. 依据豁免情形转移。

一、向欧盟认定具有同等保护水平的国家或地区转移

根据 GDPR 第 45 条的规定，个人数据可以向欧盟认可的已经提供“足够的数据保护水平”的第三国或国际组织进行跨境转移而无需再获得任何批准。截至目前，欧盟委员会已认定安道尔、阿根廷、加拿大（仅适用于商业机构）、法罗群岛、根西岛、以色列、马恩岛、泽西岛、新西兰、瑞士、乌拉圭、日本、韩国以及英国具有同等保护水平。也就是说，个人数据可以自由地从欧盟、欧盟经济区转移至该等国家而无需采取额外的保障措施。

二、向提供适当保障，确保充分数据保护的国家或地区转移

尽管有第 45 条的规定，大多数的情况下个人数据会被转移至未被欧盟认可具有“足够的数据保护水平”的国家或地区。GDPR 的第 46 条提供了几项机制，允许个人数据在满足特定条件的情况下，向未被欧盟认定为具有“足够的数据保护水平”的国家、地区或国际组织转移。该等机制包括：（a）基于公共机构之间具有约束力和可执行力的协议进行跨境转移；（b）企业制定 BCRs，且该 BCRs 获得了数据保护机关的批准；（c）数据出口方与数据进口方签署了 SCCs；（d）基于经批准的行为守则（codeofconduct）进行转移；以及（e）基于经批准的认证机制进行转移。

在过去几年中，SCCs 和 BCRs 是企业最常使用的数据跨境转移工具。特别是 SCCs 广泛地被使用在涉及欧盟/欧洲经济区的数据跨境转移场景中。BCRs 由于必须获得数据保护机关的批准才可以采用，因此目前仅有少量大型跨国企业采用了 BCRs 工具进行数据跨境转移。EDPB 的网站列出了所有经批

准的 BCRs。通过行为守则作为数据跨境转移工具的情况也较为少见，我们注意到目前仅有德国、荷兰、西班牙的个别组织获批了行为守则。EDPB 近期发布的《04/2021 指南》可能会推动以行为守则作为数据跨境转移工具的使用。

1. SCCs

SCCs 的目的是确保个人数据在转移至欧盟经济区以外的第三国/地区时，位于第三国/地区的数据接收方仍然能够通过合同义务的方式对数据主体的个人数据实行与欧盟同等水平的保护。最新版的 SCCs 分为控制者到控制者、控制者到处理者、处理者到控制者以及处理者到处理者四个版本，根据具体的数据跨境转移中数据出口方和数据进口方分属的角色不同而签署。

SCCs 可以在集团内部各关联公司之间签署，也可以与集团外部的第三方签署。如果 SCCs 在集团内部关联公司之间签署，通常集团内部会签署一份集团内数据跨境转移协议（并将 SCCs 整合到其中），以避免各关联公司交叉签署单独的 SCCs。由于 SCCs 可以在集团内签署，且无需再次经数据保护机关批准，因此对于跨国企业来说是最为便利的选择。尽管 BCRs 也是跨国企业内部使用的机制，但使用 BCRs 需获得数据主管机关的批准，需要花费较大的经济和时间成本。

值得注意的是，欧盟法院于 2020 年 7 月做出 SchremsII 案件判决，该判决除了裁定欧盟-美国“隐私盾”计划无效之外，其确认了 SCCs 的合法性，但提出了仅依赖 SCCs 进行数据跨境转移是不足够的，采用 SCCs 的企业还必须进行额外的尽职调查并采取适当的补充措施，以确保个人数据在转出欧洲经济区之外仍能受到欧盟实质同等的保护水平。

EDPB 于 2021 年 6 月发布了相关指南，就如何采取“补充措施”提供了最终建议。该最终建议提出了六个步骤。即，第一步：梳理自身数据跨境转移的情况；第二步：识别数据跨境转移所依赖的转移工具（即是依赖 SCCs,BCRs，行为准则还是其他工具）；第三步：评估第三国的法律或实践是否妨碍该数据转移工具的有效性；第四步：若经评估后认为第三国的法律或实践妨碍了数据转移工具的有效性，则采取补充措施（指南的附件中列举了补充措施的例子）；第五步：采取正式的程序性步骤实施补充措施；第六步：定期重新评估。

2. BCRs

如果跨国企业内部制定了一套 BCRs，且该 BCRs 获得了数据保护机关的批准，则该跨国集团将个人数据从位于欧洲经济区内的实体转移至位于欧洲经济区之外的关联实体是允许的。BCRs 仅适用于关联企业之间的数据跨境转移，不适用于与第三方（例如服务提供商、客户、供应商等）之间的数据跨境转移，并且采用 BCRs 工具要求跨国企业必须在欧洲经济区内有实体。由于 BCRs 需要获得数据保护机关的批准，其实施成本较高，因此并未被大量地使用。

此外，需要注意的是，尽管上述章节中提及的 SchremsII 案判决侧重于 SCCs，但在使用 BCRs 进行数据跨境转移时，上述观点应同样适用，即企业除了实施 BCRs 以外，还应进行额外的尽职调查和采取适当的保护措施，以确保对个人数据进行足够的保护。

3. 行为守则

若位于第三国/地区的数据接收方通过具有约束力和可执行的方式（通常以签署协议的方式），承诺其会遵守特定行为守则以保护其接收到的来自欧洲经济区的个人数据，且该行为守则是经批准通过的，则该数据跨境转移是在 GDPR 下允许的。

行为守则与 SCCs 和 BCRs 在程序、内容和适用情形方面都有所不同，它旨在鼓励行业协会或组织制定符合其数据处理活动特征的规则，从而实现在其行业或部门内部进行数据跨境转移的目的。行为守则需要通过特定的审批流程，经所在成员国的主管机关批准并由欧盟委员会通过颁布实施法案的形式认可该行为守则在欧洲经济区内具有通用有效性后才可以实施。如果行为守则涉及多个成员国的数据处理活动，则在欧盟委员会颁布实施法案认可该行为守则在欧洲经济区内的通用有效性之前，还需将行为守则提交给 EDPB 由其提供意见。

行为守则作为数据跨境转移的工具，具有以下几个特征：

1） 行为守则既可以代表一个行业的机构拟定（例如银行金融业协会、保险协会、教育协会等），也可以为不同部门但具有相同的数据处理特征的某项数据处理活动而拟定（例如人力资源专业协会制定专门的人力资源行为守则）；

2） 行为守则不必须在集团内的关联实体之间使用（与 BCRs 不同），其可以与外部第三方之间使用。例如，某总部设在意大利且在欧盟其他国家有分支机构的企业，为了管理集团使用的 IT 工具，使用了位于第三国的云服务提供商，该提供商在欧盟没有实体。作为 IT 工具使用的一部分，个人数据需要从意大利以及其他分支机构所在的欧盟国家转移至第三国储存。该第三国的云服务提供商将遵守行为守则作为 GDPR 下数据跨境转移的工具。则该公司可以依赖云服务提供商遵守行为准则这一途径进行数据跨境转移。在此情况下，BCRs 工具无法适用，因为 BCRs 仅能在集团内关联实体之间使用；

3） 采用行为守则的方式无需数据进口方在欧洲经济区内有实体。该项与 BCRs 不同，BCRs 的使用要求该跨境集团必须在欧洲经济区内有实体；

4） 行为守则只要求位于第三国的数据进口方承诺遵守用于数据跨境转移的行为守则，而受 GDPR 约束的数据出口方不一定必须遵守此行为守则；

5） 行为守则还具有使用一个传输工具可以解决多次数据跨境转移的优势。

行为守则的使用需要位于第三国的数据接收方通过有约束力和可执行的方式承诺遵守行为守则，签署协议是最直接和方便的选择。需要注意的是，有约束力和可执行性是需要基于欧盟法律来判定，并且数据主体可以通过“第三方受益权（third-partybeneficiaries）”执行该协议。因此协议应当适用认可第三方受益权的法律作为管辖法。中国的法律不认可第三方受益权，一般情况下建议选择欧盟成员国法律或者英国法作为管辖法。

尽管 SchremsII 案中关于签署 SCCs 需采取补充措施的判决是否同样适用于行为守则并不是非常明确，但从其逻辑来看，我们认为使用行为守则进行数据跨境转移时很可能同样适用。

《04/2021 指南》还对行为守则应当包含什么内容及其制定的参与者、审批程序、监督机构做出了详细的指引。预计在该指南发布后，可能会有更多的组织、机构参与制定行为守则并使用该守则作为数据跨境转移的工具。

无论是适用 SCCs,BCRs 还是行为守则作为数据跨境转移的工具，企业应当根据自身的情况选择最适当的工具进行跨境转移，并完成相应的尽职调查和采取适当的补充措施，确保对数据的足够保护。

三、依据豁免情形转移

若上述两种数据跨境转移机制均无法达成，GDPR 还规定了一些例外情形也可以作为数据跨境转移的途径。包括

1） 数据主体明确同意将其个人数据转移至欧洲经济区以外的地方，且前提是数据转移可能产生的潜在风险已经如实告知数据主体；

2） 数据跨境转移是为了履行数据主体作为一方的合同义务所必须，或者合同虽不是数据主体为一方签署，但是该合同是代表数据主体利益签署的；

3） 数据跨境转移是为了基于保护公共利益的重要理由；

4） 数据跨境转移是为了建立、行使或抗辩法律主张；

5） 数据跨境转移是为了保护数据主体的重大利益；以及

6） 跨境传送公共注册登记机构的部分数据。

然而，上述豁免情形的适用条件非常有限，通常只适用于一次性的转让，不能用于重复的连续性的转让行为。

GDPR 下的数据跨境转移不仅是欧盟企业应当关注的问题，也是许多中国企业（无论是跨国企业还是国内企业）应当关注的问题。即使中国企业在欧盟境内没有实体，也有可能因为 GDPR 的域外效力从而受到 GDPR 的约束，因而也需要遵守 GDPR 下关于数据跨境转移的规定。即使中国企业本身不受 GDPR 的约束，也有可能因为接收来自位于欧盟的受 GDPR 约束的企业的个人数据，从而被该企业要求遵守 GDPR 的跨境数据转移规定，包括与该等企业签署 SCCs，配合进行尽职调查和采取补充措施等。因此，了解 GDPR 下的数据跨境转移机制对于该等企业而言也尤为重要。

陆斯珮 电话：86 21 2208 6250 邮箱地址：lusp@junhe.com