数据跨境流通的法律监管

数据跨境流通，是指数据在境内外服务器之间的传递，流通对象包括公民个人信息、政府信息、商业信息等。在如今的大数据时代，信息又被称为“数字时代的石油”，不仅具备极高的商业价值，甚至可能涉及国家安全和社会公共利益。完全放任数据跨境流通抑或过分限制数据跨境流通，均可能造成极其严重的后果，如何在保护数据信息安全和促进企业合理发展之间达成一个平衡至关重要。近些年，世界多国纷纷开展了数据领域的立法、修法工作，使数据跨境流通中各方权益的保障能够与时俱进，包括 2016 年 4 月 14 日欧盟通过《通用数据保护条例》(General Data Protection Regulation，简称“GDPR”)，2018 年 3 月美国通过《澄清域外合法使用数据法》（the Clarifying Lawful Overseas Use of Data Act，CLOUD Act）等。本文将重点围绕中国法律和 GDPR 中对具有涉外业务的中国企业或在华外企可能面临的数据跨境流通法律问题进行阐述。

一、中国数据跨境流通的法律监管及典型案例

2016 年 11 月 7 日，全国人大常委会表决通过了《中华人民共和国网络安全法》（以下称《网络安全法》），并于 2017 年 6 月 1 日起正式实施。该法是我国网络安全管理领域的基础性法律，对数据保护和数据跨境流通等问题做出了规定。《网络安全法》通过后，谁需要按照法律规定进行数据境内存储和数据出境安全评估，以及如何开展数据出境安全评估，成为了实务中备受关注的问题。

- **谁需要进行数据出境安全评估**

《网络安全法》将网络运营者分为关键信息基础设施运营者和关键信息基础设施以外的网络运营者，并对关键信息基础设施运营者提出了（1）数据境内存储，和（2）数据出境需开展安全评估的法律要求；而对于关键信息基础设施以外的运营者则并没有强制性要求。《网络安全法》第三十七条：**关键信息基础设施的运营者**在中华人民共和国境内运营中**收集和产生**的**个人信息和重要数据**应当在**境内存储**。因业务需要，确需**向境外提供**的，应当按照国家网信部门会同国务院有关部门制定的办法**进行安全评估**；法律、行政法规另有规定的，依照其规定。

有人质疑此举会限制数据跨境流通并对国际贸易产生不利影响，对此网信办负责人作出回应称，此项规定只是出于国家安全的考虑，对关键信息

基础设施的运营者针对个人信息和重要数据的保护提出要求，而且境内留存并不等同于禁止数据的跨境流动。

2017 年 4 月 11 日国家互联网信息办公室发布《个人信息和重要数据出境安全评估办法（征求意见稿）》（尚未正式出台），将需要进行数据境内存储和出境评估的对象扩大为“网络运营者”，而不局限于关键信息基础设施的运营者。当然，也有不少人质疑这种扩大化要求是否符合《网络安全法》的规定。

- **什么是关键信息基础设施运营者**

《网络安全法》第三十一条明确了“关键信息基础设施”的定义：国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的**关键信息基础设施**，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

《网络安全法》也明确了关键信息基础设施的具体范围和安全保护办法由国务院制定。《关键信息基础设施安全保护条例（征求意见稿）》第十八条明确了“应当纳入关键信息基础设施保护范围”的单位：下列单位运行、管理的网络设施和信息系统，一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的，应当纳入关键信息基础设施保护范围：（一）政府机关和能源、金融、交通、水利、卫生医疗、教育、社保、环境保护、公用事业等行业领域的单位；（二）电信网、广播电视网、互联网等信息网络，以及提供云计算、大数据和其他大型公共信息网络服务的单位；（三）国防科工、大型装备、化工、食品药品等行业领域科研生产单位；（四）广播电台、电视台、通讯社等新闻单位；（五）其他重点单位。

同时，《关键信息基础设施安全保护条例（征求意见稿）》第十九条明确了由国家网信部门会同国务院电信主管部门、公安部门等部门制定关键信息基础设施识别指南。国家行业主管或监管部门按照关键信息基础设施识别指南，组织识别本行业、本领域的关键信息基础设施，并按程序报送识别结果。

- **什么数据需要境内存储和出境评估——个人信息和重要数据**

《网络安全法》将需要境内存储和出境评估的数据定义为在中华人民共和国境内运营中收集和产生的“个人信息”和“重要数据”，同时明确“个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身

份证件号码、个人生物识别信息、住址、电话号码等。”该法没有对“重要数据”进行界定，而 2017 年 4 月 11 日国家互联网信息办公室发布的《个人信息和重要数据出境安全评估办法（征求意见稿）》明确：“重要数据，是指与国家安全、经济发展，以及社会公共利益密切相关的数据，具体范围参照国家有关标准和重要数据识别指南。”因此，什么数据会被认定为“重要数据”仍有待国家进一步明确。

- 如何进行数据出境安全评估

根据《网络安全法》第三十七条的规定，数据出境安全评估的具体办法将由国务院有关部门制定。2017 年 4 月 11 日，国家互联网信息办公室发布《个人信息和重要数据出境安全评估办法（征求意见稿）》。2017 年 5 月 27 日，全国信息安全标准化技术委员会发布《信息安全技术 数据出境安全评估指南（草案）》，同年 10 月发布《信息安全技术 数据出境安全评估指南（征求意见稿）》。虽然上述配套办法和国家标准均尚未正式出台，但可资借鉴，为将来正式实施做好准备。

根据《个人信息和重要数据出境安全评估办法（征求意见稿）》，网络运营者的数据出境安全评估分为“自行评估”和“应报请行业主管或监管部门组织安全评估”两种，当出现下列情形之一时，应该报请行业主管或监管部门组织安全评估：（一）含有或累计含有 50 万人以上的个人信息；（二）数据量超过 1000GB；（三）包含核设施、化学生物、国防军工、人口健康等领域数据，大型工程活动、海洋环境以及敏感地理信息数据等；（四）包含关键信息基础设施的系统漏洞、安全防护等网络安全信息；**（五）关键信息基础设施运营者向境外提供个人信息和重要数据；**（六）其他可能影响国家安全和社会公共利益，行业主管或监管部门认为应该评估。

值得注意的是，相比于《网络安全法》，《个人信息和重要数据出境安全评估办法（征求意见稿）》扩大了需要进行数据出境安全评估的对象（前者仅限于“关键信息基础设施运营者”，而后者是全部“网络运营者”），因此，《个人信息和重要数据出境安全评估办法（征求意见稿）》中规定“应报请行业主管或监管部门组织安全评估”的情况，除第（五）项“关键信息基础设施运营者向境外提供个人信息和重要数据”外，还有其他五种情况。

同时，《个人信息和重要数据出境安全评估办法（征求意见稿）》明确数据出境安全评估应重点评估以下内容：（一）数据出境的必要性；（二）涉及个人信息情况，包括个人信息的数量、范围、类型、敏感程度，以及个人信息主体是否同意其个人信息出境等；（三）涉及重要数据情况，包括重要数据的数量、范围、类型及其敏感程度等；（四）数据接收方的安全保护措施、能力和水平，以及所在国家和地区的网络安全环境等；（五）数据出

境及再转移后被泄露、毁损、篡改、滥用等风险；（六）数据出境及出境数据汇聚可能对国家安全、社会公共利益、个人合法利益带来的风险；（七）其他需要评估的重要事项。

此外，《个人信息和重要数据出境安全评估办法（征求意见稿）》还进一步明确了数据不得出境的三种情形：（一）个人信息出境未经个人信息主体同意，或可能侵害个人利益；（二）数据出境给国家政治、经济、科技、国防等安全带来风险，可能影响国家安全、损害社会公共利益；（三）其他经国家网信部门、公安部门、安全部门等有关部门认定不能出境的。

- **不开展数据出境安全评估的法律后果**

《网络安全法》第六十六条明确了关键信息基础设施的运营者违反数据境内存储或出境评估的法律后果：由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

除《网络安全法》外，早年颁布的《人类遗传资源管理暂行办法》（国办发〔1998〕36 号）就对人类遗传资源材料出境有非常严格的规定，擅自出境也将承担法律后果。

- **典型案例**

《网络安全法》实施后，苹果公司宣布与云上贵州公司合作建设 iCloud 贵安新区主数据中心，该数据中心由云上贵州运营，苹果公司提供技术支持。iCloud 涉及到手机数据的备份和存储，包含用户的大量个人信息，苹果公司此举即是对《网络安全法》第三十七条的遵守。

对于人类遗传资源材料出境的问题，科学技术部于 2015 年 9 月 7 日做出国科罚〔2015〕1 号和 2 号行政处罚决定书，对复旦大学附属华山医院和深圳华大基因科技服务有限公司做出处罚，原因是华山医院与深圳华大基因科技服务有限公司未经许可与英国牛津大学开展中国人类遗传资源国际合作研究（“中国女性单相抑郁症的大样本病例对照研究”），华山医院和华大科技未经许可**将部分人类遗传资源信息从网上传递出境**，违反了《人类遗传资源管理暂行办法》第四条、第十一条、第十六条规定。

此外，关于境外数据向境内流通的问题，《网络安全法》第五条规定，国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

二、境外数据跨境流通的法律监管及典型案例

2018 年 5 月 25 日，欧盟《通用数据保护条例》（GDPR）正式全面实施，成为近年来影响全球数据保护最大的法规。GDPR 整合了隐私保护指令、电子通信隐私保护指令及欧盟公民权力指令，要求只要是核心业务直接或间接和欧洲民众个人数据的搜集、处理和利用有关的企业或自然人，从内部系统到数据安全，都必须符合 GDPR 对于个人数据保护的规范和要求。欧盟重视公众数据隐私，因此 GDPR 核心在于强化数据保护和隐私权。比如，GDPR 规定公民享有个人数据删除权，即如果公民想收回个人数据处理权限，而持有单位无正当理由继续保存该数据，则须予以删除，如果单位认为数据有留存必要，则须由单位举证。GDPR 还规定企业收集资料时须充分且明确告知收集个人数据资料的所有用途，公民也可以基于任何理由随时撤销同意或将数据转移至另一单位。在企业责任方面，GDPR 要求企业应根据业务程序发展，制定符合需求的个人数据保护政策，并指派个人数据保护负责人（Data Protection Officer，DPO），从而使企业自发将保护公民个人数据作为一项义务来实行。

对于个人数据从欧盟境内向欧盟以外的国家转移，GDPR 也做了专章规定。以下对此进行专门介绍。

- **谁会受到 GDPR 的监管**

GDPR 的管辖范围很宽泛，一是对主体的管辖，由于采用了数据“控制者（controller）”和“处理者（processor）”的概念，GDPR 将数据控制者和处理者在欧盟境内的实体的活动都纳入监管；二是对行为的管辖，**即使控制者或处理者不在欧盟境内，但只要处理了欧盟境内数据主体的个人数据，并且处理活动有关于向欧盟境内的数据主体提供商品或服务（不论是否收费），或者监视了欧盟境内数据主体在欧盟内发生的行为，也同样会受到 GDPR 的监管。**[1]

- **GDPR 项下数据出境的一般原则**

GDPR 第五章“个人数据向第三方国家或国际组织转移”对数据出境进行了规定，共七个条文（第 44 条至第 50 条）。首先，GDPR 第 44 条规定了

“转移的一般原则”，即“个人数据的任何转移（包括正在被处理的或者在转移至第三方国家或国际组织后将会被处理的个人数据），只有在满足本《条例》其他条款的前提下，当本章所列条件均被控制者和处理者遵守时，才得以发生，包括个人数据从第三方国家或国际组织向上转移至另一个第三方国家或另一个国际组织的情形。本章所有条款应当适用，**以确保本《条例》所保障的对自然人的保护程度不会被削弱。**”[2]本条确立了欧盟对个人数据转移的保护原则，由于 GDPR 本身对个人数据设定了比较高的保护标准，为更好地保护个人数据，欧盟不希望个人数据一经转移出境，其保护程度就受到减损。

- GDPR 项下数据出境的前提条件

GDPR 在第 45 至 49 条，规定了数据在从欧盟出境前，需要满足的条件；不符合所列条件的，数据不得出境，否则构成对这些条款的违反，将会面临相应的法律责任。总体而言，有三种方式可以满足数据出境的要求：一是接收个人数据的国家或地区经欧盟评估后获得了欧盟的“充分性决定”，二是数据的控制者或处理者（即数据的转移方）采取了适当的保障措施，三是符合可以减轻保护程度的七种特定情形之一。[3]

1.充分性决定（adequacy decision）[4]

欧盟委员会会对第三方国家、某地区、第三方国家内的一个或多个特定领域、或国际组织进行评估，评估其对个人数据的保护程度，然后对保护程度是否具有充分性做出决定。如果这个第三方国家被欧盟认定具有充分的保护并作出了相应的决定，那么个人数据向这些国家或组织转移，就无需再获得任何具体核准（authorization）。

充分性决定，因而被认为是白名单制度。满足条件的国家或国际组织会出现在欧盟委员会的充分性认定国家清单中，截止 2019 年 3 月 28 日，该清单上仅有十三个国家和地区，包括安道尔、阿根廷、加拿大（商业组织）、法罗群岛、根西岛、以色列、马恩岛、日本、泽西岛、新西兰、瑞士、乌拉圭和美国（限于隐私保护框架）[5]。中国尚没有在名单内。

2.适当的保障措施（appropriate safeguards）[6]

在没有获得 GDPR 第 45 条的充分性决定的情况下，数据控制者或者处理者也可以采取适当的保障措施，使得个人数据可以向那些没有获得“充分性决定”的第三方国家转移。依照采取保障措施后，是否还需获得“监管当局（supervisory authority[7]）”的具体核准才能转移个人数据，可以分为下面两种情况：

1）采取下列任一保障措施，且无需再获得监管当局的任何具体核准：[8]

a） 公共主管当局或者公共机构具有法律约束力和执行力的文件；

b） 符合第 47 条要求的具有约束力的公司规则；

c） 欧盟委员会依照第 93 条第 2 款的审查程序采纳的标准数据保护条款；

d） 由监管当局采纳并由欧盟委员会依照第 93 条第 2 款的审查程序批准的标准数据保护条款；

e） 依照第 40 条批准的行为准则，和控制者或处理者做出的具有约束力和执行力的承诺，承诺其在第三方国家实施适当的保障措施，包括有关数据主体的权利的保障措施；

f） 依照第 42 条批准的认证机制，和控制者或处理者做出的具有约束力和执行力的承诺，承诺其在第三方国家实施适当的保障措施，包括有关数据主体的权利的保障措施。

2）采取下列任一保障措施后，还需获得有权的监管当局的核准：[9]

a） 控制者或处理者和第三方国家或国际组织中接收个人数据的控制者或处理者之间达成的合同条款；

b） 将被纳入公共主管当局或者公共机构之间的行政安排中的条款，其中包含了可执行和有效的数据主体权利。

3.可以减轻保护程度的特定情形（Derogations for specific situations）

当既不满足“充分性决定”，又没有采取“适当的保障措施”，只有符合以下七种情形之一，才可以向第三方国家转移个人数据：

a） 在数据主体被明确告知由于缺少“充分性决定”和“适当的保障措施”，该等转移可能会对数据主体有风险后，数据主体仍明确同意将要发生的数据转移；

b） 为履行数据主体和控制者之间的合同或者为履行数据主体请求采取的签约前措施，数据转移是必要的；

c） 为达成或履行控制者和另一个自然人或法人之间签订的为了数据主体利益的合同，数据转移是必要的；

d） 为了公共利益的重要理由，数据转移是必要的；

e） 为了合法的诉讼请求的建立、行使或辩护，数据转移是必要的；

f） 当数据主体物理意义上或法律意义上不能给予同意时，为保护数据主体或其他人的重要利益，数据转移是必要的；

g） 转移是从登记簿操作的，该登记簿是根据欧盟或欧盟成员国法律向公共提供信息的，并向公众整体或能够证明有合法权益的任何个人开放咨询，但仅限于欧盟或欧盟成员国法律中有关咨询的条件在个案中均得到满足。[10]

从上述内容可以看出，GDPR 对个人数据的保护力度是很高的，数据出境具有较高的前提条件。

- **不遵守 GDPR 的法律后果**

GDPR 的威力正在于其巨额的违法成本。如果违反 GDPR 有关个人数据出境的条款，则可能面临最高 20,000,000 欧元罚款，如果被处罚对象为企业，最高按其上一财年的全球年度营业额的 4%处罚，以两者中更高者计。[11]

GDPR 生效以来不到一年的时间里，欧盟多国已经开出了 GDPR 项下的罚单。

2019 年 1 月 21 日，法国数据保护机构 CNIL 宣布，对谷歌处以 5000 万欧元(约合 5700 万美元)的罚款，原因是谷歌违反了 GDPR 的两项义务，一是违反了透明和通知义务：用户无法轻易获得谷歌提供的通知，且有些通知不够清晰全面；二是谷歌向用户展示个性化广告没有取得用户有效同意：将数据用于个性化广告的通知分散在数份文件中，用户无法意识到它们的使用范围，并且谷歌收集的用户同意既不是“明确的”，也不是“清晰的”[12]。

2019 年 3 月 26 日，波兰数据保护监管局（*Urząd Ochrony Danych Osobowych*－UODO）宣布了第一张行政处罚的罚单，对一家位于华沙的公司处以 943,000 波兰兹罗提（约合 219,000 欧元）的罚款。[13]

2018 年 11 月 21 日，德国巴登-符腾堡州数据保护和信息自由委员会开出了德国的第一张 GDPR 罚单，一家社交媒体公司被处以 20,000 欧元的罚款。[14]

三、企业涉外业务需关注的数据合规风险及相应提示

不论是我国的《网络安全法》，还是欧盟的《通用数据保护条例》，均以开始发挥实质性作用。企业开展跨境业务，需要关注数据跨境的法律问题。数据合规已经成为企业合规工作中必不可少的一环。

- **总部位于中国但有涉外业务的企业**

对于总部设立在中国的企业，除本身需要遵守中国的法律法规包括《网络安全法》外，还需关注是否需要遵守境外的法律规定。如上文所述，GDPR 的管辖范围非常宽，既有对主体（控制者或处理者）的管辖，也有对行为的管辖。

即使企业没有在欧洲设立任何实体，也有可能受到 GDPR 的监管。比如，位于中国的企业开展跨境业务，也面向位于欧盟的顾客，一个在欧盟的个人

登陆了网站，注册了账户，购买了网上的服务或产品，企业在这过程中收集了个人数据，那么就要受到 GDPR 的管辖了。

如果企业在欧盟设立了运营实体，且中国总部还希望或需要拿回位于欧洲的运营实体收集到的欧盟内的个人数据，那就涉及个人数据从欧盟出境的问题，也需要符合 GDPR 里面的相关规定，尤其是上文所述的 GDPR 第五章“个人数据向第三方国家或国际组织转移”里面的规定。考虑到当前中国还没有被纳入“充分性决定”的名单，中国企业只能采取上文所述的“适当的保障措施”或者符合“可以减轻保护程度的特定情形”以满足 GDPR 的要求，避免被处罚。

- **总部不在中国但在中国有运营实体的企业**

对于总部并非在中国的企业，尤其是外资企业，面临的最大挑战就是如何符合中国的《网络安全法》关于数据存储和数据出境的法律要求。如果这家外资企业还被认定为是关键信息基础设施，那么，个人信息和重要数据就必须存放中国境内，如果个人信息和重要数据需要出境（比如传回国外总部），就需要按照法律法规的要求开展数据出境安全评估。

对于上述两类企业，以及暂时没有开展涉外业务的企业，仍然建议尽早关注、筹划、建立数据合规体系，以应对全球共同掀起的数据合规监管浪潮。

作者介绍

蔡军祥　副主任/高级合伙人，昌言（上海）律师事务所

justincai@changyanfirm.com，　www.changyanlawfirm.com

蔡军祥律师获得复旦大学和美国杜克大学法学硕士学位，具有超过 16 年的律师工作经验，曾长期供职于金杜、中伦、美国威嘉（Weil），元达（MWE）等国内外一流的律师事务所，为大量世界 500 强企业提供法律服务。蔡律师业务领域包括网络安全和数据合规、反商业贿赂（含 FCPA）、知识产权保护、跨境投资、成长性企业投融资、房地产并购等。

黄晴　律师（见习期），昌言（上海）律师事务所

黄晴律师毕业于香港中文大学和西南政法大学，分别获得法学硕士和法学学士学位，且在比利时根特大学有近半年交换学习经历。黄晴曾在招商银行担任两年法务，具有比较丰富的合规审查经验。

（实习生蒋晓涵对本文亦有贡献）

---

[1]GDPR Article 3 Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing ofpersonal data of data subjects who are in t he Union by a controller orprocessor not established in the Union, where the processing a ctivities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

[2]GDPR Article 44 General principle for transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

[3]注：GDPR 第 48 条还规定了一种非由欧盟法律核准的数据转移或披露情形，只适用于司法裁判或行政机关的决定要求个人数据转移的情形，本文不展开。

[4]详见 GDPR Article 45 Transfers on the basis of an adequacy decision

1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

……

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).

[5]https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

[6]GDPR Article 46 Transfers subject to appropriate safeguards

1.In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

[7]根据 GDPR 第 51 条第 1 款，监管机构是指欧盟每个成员国负责监管 GDPR 实施的独立的公共主管当局。

GDPR Article 51 Supervisory authority

1.Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union (‘supervisory authority’).

[8]GDPR Article 46 Transfers subject to appropriate safeguards

2. The appropriatesafeguards referred to in paragraph 1 may be provided for, without requ iringany specific authorisation from a supervisory authority, by:

(a) a legally binding and enforceable instrument between public authorities or bodies;

(b) binding corporate rules in accordance with Article 47;

(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);

(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);

(e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

(f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

[9] GDPR Article 46 Transfers subject to appropriate safeguards

3. Subject to the authorisation from thecompetent supervisory authority, the appropriate safeguards referred to inparagraph 1 may also be provided for, in particular, by:

(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or

(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

[10] GDPR Article 49 Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 45(3), or ofappropriate safe guards pursuant to Article 46, including binding corporaterules, a transfer or a set of trans fers of personal data to a third country oran international organisation shall take place onl y on one of the followingconditions:

(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

(d) the transfer is necessary for important reasons of public interest;

(e) the transfer is necessary for the establishment, exercise or defence of legal claims;

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

[11] Article 83 General conditions for imposing administrative fines

5. Infringements ofthe following provisions shall, in accordance with paragraph 2, be subj ect toadministrative fines up to 20,000,000 EUR, or in the case of an undertaking, upto 4 % of the total worldwide annual turnover of the preceding financial year,whichever is hig her: …… (c) thetransfers of personal data to a recipient in a third country or aninternation al organisation pursuant to Articles 44 to 49; ……

[12]https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

[13] https://www.ceelegalblog.com/2019/03/pln-1-million-fine-for-gdpr-violation/

[14]https://iapp.org/news/a/germanys-first-fine-under-the-gdpr-offers-enforcement-insights/