LINKS Law Offices 通力律师事务所

上海
上海市银城中路 68 号
时代金融中心 19 和 16 楼
邮编：200120
电话：+86 21 3135 8666
传真：+86 21 3135 8600

SHANGHAI
19/F&16/F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

北京
北京市建国门北大街 8 号
华润大厦 4 楼
邮编：100005
电话：+86 10 8519 2266
传真：+86 10 8519 2929

BEIJING
4/F, China Resources Building
8 Jianguomenbei Avenue
Beijing 100005 P.R.China
T: +86 10 8519 2266
F: +86 10 8519 2929

香港
香港中环皇后大道中 5 号
衡怡大厦 27 楼
电话：+852 2969 5300
传真：+852 2997 3385

HONG KONG
27/F, Henley Building
5 Queen's Road Central
Central, Hong Kong
T: +852 2969 5300
F: +852 2997 3385

伦敦
1/F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

LONDON
1/F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

www.llinkslaw.com
master@llinkslaw.com

公司及并购法律评述
2018 年 5 月

浅析 GDPR 对中国企业海外运营的影响及应对

作者：潘永建 | 李天航

欧盟《通用数据保护条例》(General Data Protection Regulation，以下称“GDPR”)已于 2016 年 4 月由欧洲议会和欧盟理事会通过，2018 年 5 月 25 日起正式实施。GDPR 不仅对欧盟的自然人、法人、非法人组织产生重大影响，效力也将覆盖至欧盟以外。这将对中国企业走出去，尤其是向欧洲发展带来重大影响。本文将从中国企业的视角分析 GDPR 对企业的影响，并提出相应对策。

上 GDPR 概述

自欧洲议会和欧盟理事会 1995 年 10 月 24 日颁布《关于涉及个人数据处理的个人保护以及此类数据自由流动的指令》(以下简称“95 指令”)以来，欧盟出台了一系列规章、指令、公约、条约等对个人数据保护的规定。但 95 指令作为保护个人数据的最低标准，仍需欧盟成员国通过国内立法予以实现。同时，随着互联网技术的发展，云计算、大数据、移动互联、智能终端等新形态、新业态的出现，使

如您需要了解我们的出版物，
请与下列人员联系：

郭建良: (86 21) 3135 8756
Publication@llinkslaw.com

通力律师事务所
www.llinkslaw.com

得 95 指令难以应对当前社会对个人数据保护的需求。2012 年 1 月 25 日欧盟委员会通过更新后的数据保护法规的初步建议，启动了 GDPR 的立法程序; 2014 年 3 月 12 日欧洲议会通过了 GDPR 的首次审读; 2015 年 6 月 15 日欧盟理事会通过首次审读的版本。至此, GDPR 进入最后立法阶段，即欧洲议会、部长理事会和欧盟委员会之间的“三方会谈”。经过多轮三方会谈, GDPR 最终于 2016 年 4 月 8 日和 4 月 16 日由欧盟理事会和欧洲议会通过。

GDPR 作为欧盟的条例，将直接约束欧盟境内的自然人、法人、非法人组织，无需通过欧盟成员国的立法予以转化。限于篇幅的原因，本文仅就与自然人、法人、非法人组织的权利义务相关的内容作简要介绍。

一. 宗旨及保护对象

1. 宗旨：个人数据的保护与自由流动的平衡

GDPR 开宗明义，旨在保护自然人的权利和自由，尤其是自然人的个人数据保护权，但又明确不得以保护个人数据为由限制个人数据在欧盟内部的自由流动。由此可见, GDPR 试图在个人数据的保护与在欧盟区域内自由流动之间寻找平衡点。

2. 保护对象：个人数据

GDPR 对个人数据的定义为: 指任何指向一个已识别或可识别的自然人(“数据主体”)的信息。该可识别的自然人能够被直接或间接地识别，尤其是通过参照诸如姓名、身份证号码、定位数据、在线身份识别这类标识，或者是通过参照针对该自然人一个或多个，如物理、生理、遗传、心理、经济、文化或社会身份的要素。

“可识别性”是前述受保护个人数据的首要条件，相较于我国刑法、《网络安全法》以及《信息安全技术 个人信息安全规范》(GB/T 35273-2017)等法律及规范关于个人信息的界定, GDPR 所定义的个人数据范围较为狭窄。在我国，个人信息不仅包括已识别、可识别性个人信息，也包括与个人有关的信息。

二. 适用范围

GDPR 不仅适用于设立在欧盟内的企业，为保护欧盟公民个人数据，在以下三种情况下，也适用于设立在欧盟以外的企业:

(1) 向欧盟内的数据主体提供商品或服务的，无论此项商品或服务是否需要数据主体支付对价;

(2) 对数据主体发生在欧盟内的行为进行监控的;

(3) 对个人数据的处理虽然是由设立在欧盟之外的控制者进行，但欧盟成员国法律通过国际公法适用于该控制者所在地的。

三. 监管体制

GDPR 在监管体制方面作了最大程度的统一，对企业实施一站式监管，结束以往企业接受多头监管的局面。GDPR 规定企业主营业地或者唯一营业机构所在地的监管机构作为最高监管机构，负责监管企业的所有数据处理活动。同时，为了保证对企业在欧盟内数据处理活动监管的统一性，GDPR 规定了最高监管机构与其他监管机构之间的合作、互助机制以及联合行动机制。对于监管机构不遵守合作、互助机制以及联合行动机制的，将由欧洲数据保护委员会进行检查。

四. 个人数据处理

GDPR 规定，对数据的处理是指针对个人数据或个人数据集合的任何一个或一系列操作，诸如收集、记录、组织、建构、存储、自适应或修改、检索、咨询、使用、披露、传播或其他的利用，排列、组合、限制、删除或销毁，无论此操作是否采用自动化的手段。

GDPR 将数据主体的同意作为对个人数据处理的合法前提，但并非唯一前提，除此之外还设定了若干其他合法处理个人数据的情形。

(一) 处理的原则

1. 合法性、公平性和透明性。必须以合法、公正、透明的方式处理与数据主体有关的数据;

2. 目的限制。收集个人数据的目的必须特定、明确、合法，而且数据处理必须符合目的;

3. 数据最小化。充分、相关以及以该个人数据处理目的之必要为限度进行处理;

4. 准确性。使数据保持准确，及时更新、删除不准确的数据;

5. 存储限制。在不超过个人数据处理目的之必要的情形下，允许以数据主体以可识别的形式保存；为达到公共利益、科学或历史研究或统计的目的而处理，个人数据能被长时间存储;

6. 完整性和机密性。确保个人数据以适度安全的方式被处理，包括使用适当的技术或组织措施来对抗未经授权、非法的处理、意外遗失、灭失或损毁;

7. 控制者举证责任。个人数据控制者应当证明处理行为符合上述原则。

(二) 处理的合法要件

1. 同意

数据主体的同意是对个人数据处理的合法要件之一。根据 GDPR 规定，同意是指数据主体依照其意愿自愿作出的任何指定的、具体的、知情的及明确的指示。通过声明或明确肯定的行为作出的这种指示，意味着其同意与他或她有关的个人数据被处理。

基于该前提，数据控制者应当证明其已经获得数据主体的同意或者授权。并注意以下义务:

(1) 如果该同意基于书面声明的方式获得，且书面声明涉及其他事项，那么对同意的请求应以**易于理解且与其他事项显著区别**的形式呈现;

(2) 数据主体有撤回同意的权利:

a) 数据主体有权随时撤回他或她的同意。同意的撤回不应影响在撤回前基于同意作出的合法的数据处理;
b) 在作出同意前，数据主体应被告知上述权利;
c) 撤回同意应与作出同意同样容易。

2. 同意之外的其他合法情形

除了数据主体的同意之外，以下情形也属于处理个人数据的合法情形:

(1) 处理是为履行数据主体参与的合同之必要，或者是因数据主体在签订合同前的请求而采取的措施;

(2) 处理是为履行控制者所服从的法律义务之必要;

(3) 处理是为了保护数据主体或另一个自然人的切身利益之必要;

(4) 处理是为了执行公共利益领域的任务或行使控制者既定的公务职权之必要;

(5) 处理是控制者或者第三方为了追求合法利益的之必要，但此利益被要求保护个人数据的数据主体的利益或基本权利以及自由覆盖的除外，尤其是数据主体为儿童的情形下。该情形不适用于政府当局在履行其职责时进行的处理。

3. 敏感数据处理的限制

对揭示种族或民族出身，政治观点、宗教或哲学信仰，工会成员的个人数据，以及以识别特定自然人为目的的基因数据、生物特征数据，健康、自然人的性生活或性取向的数据的处理应当被禁止。但在以下情形可以依照欧盟或者成员国法律进行相应的处理:

(1) 数据主体明确同意或者被明显公开;

(2) 在社会保障范畴内履行义务、行使权利;

(3) 为了保护数据主体或他人的切身利益之必要，但数据主体物理上或法律上无法给予同意;

(4) 由政治、哲学、宗教、工会性质的协会、组织或其他非营利组织处理内部事务;

(5) 合法行使诉讼权利;

(6) 为了实质的公共利益，数据处理是必要的;

(7) 在公共卫生健康医疗领域或者数据主体的医疗健康;

(8) 为了公共利益、科学或历史研究的目的，或者统计的目的。

五. 处罚与调查

1. 处罚

GDPR 对各类违规行为设定了两档处罚，具体如下:

(1) 针对以下违规行为，可以处以 1000 万欧元，或者企业年度全球营业额的 2%的罚款，二者取额度高者:

a) 违反关于数据控制者和处理者的规定的;
b) 违反关于认证和认证主体的规定的;
c) 违反 GDPR 第 41(4)条关于监管机构的规定。

(2) 针对以下违规行为，可以处以 2000 万欧元，或者企业年度全球营业额的 4%的罚款，二者取额度高者:

a) 违反数据处理的基本原则，包括有关数据主体同意情形的;
b) 违反有关数据主体的权利保障的;
c) 违反有关将个人数据转移到第三国或国际组织的规定的;
d) 违反 GDPR 第九章规定的欧盟成员国法律认可的责任;
e) 不遵守监管机构根据第 58(2)条作出的针对数据处理或暂停数据流动的命令、临时性或决定性限制。

2. 调查程序和调查者权利

对于违反 GDPR 行为，需要进行处罚的，监管机构可以采取以下措施:

a) 告知数据控制者、处理者相关违反行为;

b) 要求违法者提供相关信息，或者向监管机构提供访问此类信息的接口;

c) 现场调查、审计;

d) 命令修改、删除或者销毁个人数据;

e) 可以采取临时性的或者限定性的数据处理禁令。

中 数据主体与数据控制者之权利与义务

六. 数据主体的权利

数据主体在其个人数据被处理中享有以下权利:

1. 知情权

控制者应当以一种简单透明、明晰且容易获取的方式，通过清楚明确的语言，采取合适措施提供个人数据的处理情况，向数据主体提供以下信息:

(1) 控制者的身份和详细联系方式，适当时还要提供代表人的身份和详细联系方式、数据保护部门的详细联系方式、接收方的信息;

(2) 个人信息处理的目的以及处理的法律基础;

(3) 控制者或者第三方追求的立法利益;

(4) 控制者意图将个人数据向第三国或者国家组织进行传输的情况以及采取的保护个人信息的合理安全措施以及获取复印件的方式;

(5) 如果涉及自动化的数据处理，包括数据画像活动，则需要提供基本的算法逻辑以及针对个人的运算结果;

(6) 个人数据的保留周期以及采取该周期的理由;

(7) 依据法律，数据主体享有的权利、投诉权以及相关的监管机构。

2. 访问权

数据主体有权从管理者处确认关于该主体的个人数据是否正在被处理，以及有权在该种情况下访问个人数据以及处理的目的、有关个人数据的类别、存储周期等相关情况。

控制者应提供正在处理的个人数据的副本。对于数据主体要求的任何进一步的文本，控制者可以根据管理成本收取合理的费用。如果数据主体通过电子方式提出请求，除非数据主体另有要求，信息应当以常用的电子形式提供。

3. 反对权

数据主体有权在以下两种情形下随时拒绝对其数据的处理:

(1) 数据主体有权随时以其自身原因拒绝对其处理的任何处理，包括数据画像，除非数据控制者基于自身合法利益或者执行公共利益领域的任务或行使控制者既定的公务职权之必要;

(2) 数据控制者基于直接营销的目的，包括与直接营销相关的数据画像。

4. 可携权

对于数据主体提供给控制者的个人数据，可以要求数据控制者将其转移至另外一个数据控制者，数据控制者无权对此加以干涉，而且必须配合提供相应的数据文本或者复制件。

5. 纠正权

数据主体应当有权要求控制者无不当延误地纠正不准确个人数据。考虑到处理的目的，数据主体应当有权使不完整的个人数据完整，包括通过提供补充声明的方式。

6. 删除权/被遗忘权

被遗忘权的行使以数据控制者的删除义务为基础，即数据控制者必须应数据主体要求删除其个人数据:

(1) 数据主体撤回同意、个人数据被非法利用或者数据控制者不再具有合法理由的情形下;

(2) 如果控制者已将个人数据公开，并且有义务删除这些个人数据，控制者在考虑现有技术及实施成本后，应当采取合理步骤，包括技术措施，通知正在处理个人数据的控制者，数据主体已经要求这些控制者删除该个人数据的任何链接、副本或复制件。

7. 限制处理权

(1) 数据主体根据其合法需求在下列情况下，有权限制控制者处理数据:

a) 数据主体对个人数据的准确性提出争议，且允许控制者在一定期间内核实个人数据的准确性;

b) 对于个人数据的处理是非法的，并且数据主体反对删除该个人数据，要求限制使用该个人数据的;

c) 控制者基于处理目的不再需要该个人数据，但数据主体为设立、行使或捍卫合法权利而需要该个人数据;

d) 数据主体在核实控制者的法律依据是否优先于数据主体的法律依据之前已行使拒绝权的。

(2) 对于限制处理的，除储存之外，这些个人数据只能在数据主体同意的情况下，或为设立、行使或捍卫合法权利，或为保护其他自然人或法人的权利，或为了欧盟或成员国的重要公共利益的原因被处理。

(3) 控制者应当在解除上述信息处理限制之前通知行使限制处理权的数据主体。

8. 免受数据画像影响

数据画像是指自主化的个人决策，包括为评估与自然人相关的某些个人情况，对个人数据进行任何自动化处理、利用的方式，特别是针对与自然人的工作表现、经济状况、健康状况、个人偏好、兴趣、信度、习性、位置或行踪相关的分析和预测。

GDPR 规定数据主体有权不受仅基于自动化处理而做出的、对其产生法律效力或其他类似效力的决定(包括数据画像)的限制除非自动化处理的决定是基于以下情形之一:

a) 对于数据主体和数据控制者之间合同的建立和履行是必要的;

b) 控制者是数据主体，以及确立保护数据主体权利、自由和正当化利益的适当措施是联盟或成员国的法律所规定的;

c) 数据主体的明确同意。

GDPR 禁止对于敏感信息的画像，除非基于数据主体的同意，或者维护数据主体工作、社会保障的需要，以及确立适当的措施维护数据主体的权利、自由和正当化利益。

七. 数据控制者与数据处理者的义务

数据控制者(Data Controller)指能单独或联合决定个人数据的处理目的和方式的自然人、法人、公共机构、行政机关或其他非法人组织。其中个人数据处理的目的和方式，以及控制者或控制者资格的具体标准由欧盟或其成员国的法律予以规定。

数据处理者是指为控制者处理个人数据的自然人、法人、公共机构、行政机关或其他非法人组织。

1. Data Protection Officer(以下简称“DPO”)的设置

(1) 数据控制者、处理者在以下情形必须设立 DPO:

a) 系政府部门及公共机构的;

b) 对数据主体的数据监控和使用是系统性和常规化的，且规模较大;

c) 涉及收集和处理一些敏感数据的，例如犯罪数据、医疗数据、生理数据等等；或者数据处理活动与刑事指控、定罪相关的。

(2) DPO 必须具备数据保护专业知识和技能，有能力且能独立地履行职责。

(3) 企业集团可以指定一位独立的 DPO 负责整个企业集团的事务，但前提是 DPO 能够便捷地介入所属公司或者其他运营地，处理具体事务。

2. 文档化管理

数据控制者及其代理人必须全面记载其对数据的处理活动，包括数据控制者的信息、处理的目的、种类、数据公开或者跨境传输的情况、数据保存的时间、采取的安全措施等等。

3. 数据保护影响评估

(1) 对于高风险的处理方式，应当统筹考虑处理过程的性质、范围、内容和目的，在进行数据处理之前，控制者应当对就个人数据保护所设想的处理操作方式的影响进行评估。以下情形应当予以评估:

a) 对自然人个人情况评估所进行的系统和广义上的自动分析;
b) 对敏感数据大范围的数据处理或者对于刑事定罪和罪行相关的个人信息进行处理;
c) 一个大规模的公共可访问区域的系统性监测。

(2) 评估可以寻求数据保护当局的帮助。

4. 事先咨询机制

(1) 对于高风险的处理方式，经过数据保护影响评估后确定如果控制者没有采取措施减少风险处理过程将会是高风险的，控制者应当在处理之前向监督机构进行咨询。

(2) 监督机构应当至迟在 8 周以内向控制者提出书面建议，根据预期处理的复杂性可以延长 6 周。

5. 数据泄露报告机制

个人数据外泄是指个人数据在传输、存储或进行其他处理时的安全问题引发的个人数据被意外或非法破坏、损失、变更、未经授权披露或访问。

(1) 对于发生个人数据泄露的，控制者至少应当在知道之时起 72 小时以内向监管机构报告。如果迟于 72 小时的，应当对迟延原因进行解释。处理者发生个人数据泄露事件的，应当立即通知控制者。

(2) 向监管机构的报告应当至少包含以下内容:

a) 关于数据泄露事故的描述，涉及的数据主体的总量、类型以及数据记录的总量;
b) 数据保护当局或者企业 DPO 的姓名和联系方式;

c) 泄露可能造成的结果;

d) 企业已经采取的止损措施。

在不造成延误的情况下，前述内容可以分阶段报告。

(3) 数据控制者应当将所有的数据泄露事故记载形成文档，以便监管机构能够检查其合规工作。

6. 安全保障措施

GDPR 要求对控制者、处理者应当执行合适的技术措施和有组织性的措施来保证合理应对风险的安全水平，尤其要酌定考虑以下因素:

a) 个人数据的匿名化和加密;

b) 数据系统保持持续的保密性、完整性、可用性以及弹性的能力;

c) 在发生自然事故或者技术事故发的情况下，存储有用信息以及及时获取个人信息的能力;

d) 定期对测试、访问、评估技术性措施以及组织性措施的有效性进行处理，力求确保处理过程的安全性。

7. 数据跨境流动遵守的规则

根据 GDPR 规定, “跨境处理”是指以下情形之一:

a) 个人数据处理发生在一个欧盟内的设立在多个成员国的控制者或处理者在多个成员国的营业机构的活动中;

b) 个人数据的处理发生在一个欧盟内的控制者或处理者的唯一营业机构的活动中，但是这种处理严重影响或可能会严重影响多个成员国的数据主体。

发生在欧盟内的数据跨境流动是被允许的，但是对于向第三国或者国际组织进行数据转移须符合以下情形之一。

(1) 充分性决定

向欧盟委员会认定具有充分保护水平的第三国或国际组织转移个人数据时，无需获得任何

特别授权，评估具有充分保护水平基于以下三个方面:

a) 法律、对人权和基本自由的尊重、相关立法等;
b) 第三国或者国际组织独立监管机构的存在和有效运作，包括确保和强制执行数据保护规则、帮助和建议数据主体落实权利以及与成员国监管部门合作的适当的执法权力;
c) 第三国以及国际组织加入的个人数据保护的国际承诺、具有法律约束力的公约或者参与的多边和区域体系。

欧盟委员会将至少 4 年一次对前述充分保护水平决定进行检查，以确定该第三国、第三国的特定区域或者国际组织是否不再具有充分决定保护水平。

(2) 有约束力的公司规则

有约束的公司规则(Binding Corporate Rules, BCR)由监管部门根据一致性机制予以批准，以事业群或从事联合经济活动的集团企业在集团内部实现数据的跨境转移。该机制最早由欧盟第 29 条工作组发展而来，是欧盟委员会提出的标准化格式合同的一个替代选择。

对关于批准后的有约束力的公司规程，欧盟委员会应当详细说明在数据控制者、处理者、监管部门之前交换信息的形式和流程。

(3) 标准合同条款

标准合同条款是指欧盟委员会或者监管部门根据 GDPR 程序批准的数据保护条款。在 GDPR 生效前，欧盟委员会已通过的 3 个标准合同条款(Standard Contractual Clauses)仍然有效。此外, GDPR 增加了，由成员国数据监管机构、欧盟委员会通过一致性机制指定标准合同条款的机制。

(4) 其他

如果不符合前述三种情形的，则只能在符合下列情形之一时，向第三国或者国际组织转移个人信息:

a) 数据主体被告知可能的风险后明确表示同意;
b) 执行数据主体与数据控制者之间的合同的必要，或者根据数据主体的要求执行合同前

事务;

c) 执行数据控制者与其他自然人和法人之间的合同的必要，该合同旨在维护数据主体的利益;

d) 为了公共利益;

e) 为了建立、行使、抗辩法律索赔;

f) 转移是为了保护数据主体或其他人的实际利益，同时数据主体在物理上或者法律上无法给出同意的意思表示;

g) 转移是由根据欧盟或成员国法律向公众提供信息的机构实施的，该机构向一般公众和利害关系人开放咨询。但是仅适用于欧盟或成员国法律规定的情形。

如果仍然不符合上述条件的，则向第三国或者国际组织转移个人信息只能在同时满足以下条件时发生:

a) 数据转移不是重复发生的，涉及有限数据主体，且目的是实现控制者的合法利益，这些利益不会侵害数据主体的利益、权利和自由;

b) 数据控制者已经评估了数据转移过程中面临的所有环境，并且基于这一评估提供了恰当的个人数据保护措施。

在此情况下，数据控制者应当向监管机构通报，并通知数据主体。

下 影响及应对

随着中国企业走出去的步伐逐步加快，欧洲/欧盟国家已经成为中国企业对外投资经营的重要区域，越来越多中国企业将选择在欧洲设立分支机构或者向欧洲开拓业务。即使没有在欧州境内实际经营，基于互联网无国界的特性，欧盟公民主动登录中国企业网站或者与中国企业发生关联的情况也时有发生。因此，GDPR 将对中国企业在欧洲的运营或与欧盟公民发生的数据行为产生重要影响。综合来看，GDPR 对中国企业既有有利的方面，也有提出更高要求的方面。

八. 法律及监管的有利变化

1. 统一的法律要求

在 GDPR 的规定中，除了个别条款赋予欧盟成员进行细化的空间外，其他条款都将直接规制欧

盟成员国及欧盟境内的自然人、法人、非法人组织，统一了欧盟范围内个人数据保护的法律要求。这对中国企业走向欧洲来说是极为有利的，中国企业无需考虑欧盟各个成员国法律规定的差异，只需按照 GDPR 的规定履行义务、行使权利即可。

2. 一站式的监管

GDPR 明确了一站式监管的机制，只要企业选定了一个符合 GDPR 规定的监管机构作为主要监管机构，将无需再与其他欧盟成员国监管机构或者欧盟监管机构进行交涉，避免多头监管带来的不利影响。

3. 促进数据的流动，尤其是跨境流动

虽然 GDPR 通篇以保护个人数据、对数据控制者、处理者进行监管为主要内容，但 GDPR 的宗旨是为了更好的促进个人数据的自由流动。个人数据的自由流动将能够极大的促进大数据技术的发展与运用，因此，企业只要能够遵守 GDPR 的规定，将尽可能多地获得个人数据，存进企业的发展。

九. 主要风险提示

1. 同意与隐私政策、协议

目前，隐私政策、协议是获得数据主体同意的主要方式，而国内企业绝大多数隐私政策、会员协议以及其他协议，有关个人数据收集、使用等内容晦涩冗长，且混杂于其他内容之中，难以达到清晰、明确和易于理解的要求。此外，在隐私政策、会员协议中通过一揽子打钩或者推定的形式获得同意，也将违反 GDPR 的要求。鉴于此，建议采取以下措施:

a) 将有关个人数据收集、使用的内容独立，用清晰、明确、易于理解的方式表述;
b) 通过技术手段将前述内容作为进行下一步动作的必经环节，如果没有获得同意的，则不能进入下一步动作，或者后续服务会受到相关限制;
c) 如果在对个人数据的后续运用中超出前述同意范围的，尤其是对于敏感个人数据或者个人画像等方面，应当单独重新获得个人数据主体的同意;
d) 必须要告知个人数据主体撤回同意的途径和方式，该途径和方式必须与作出同意同样容易。

2. 数据处理行为界定更严

我国法律对于数据处理行为采取概括式的描述，即使作为国家标准的《信息安全技术 个人信息安全规范》，也仅仅明确了收集、用户画像、删除、公开披露、转让、共享、匿名化与去标识化等行为。而 GDPR 通过概括加列举的形式，对所有围绕数据实施的处理行为都明确列入数据处理的范畴，使 GDPR 在对数据处理的约束与规范上做到无死角。因此，我国企业在对欧盟公民数据进行处理时应当特别注意，不要忽视我国法律和国家标准对数据处理界定范围以外的处理行为也将受到 GDPR 的约束。

3. 拒绝权、撤回同意权与营销

目前，我国企业对个人数据的主要应用之一是直接营销。为了实施精准营销，绝大多数企业对个人数据进行自动化分析，即个体或者群体画像。从应用的顺序上看，企业一般先进行自动化分析，再开展直接营销。并且，告知拒绝权往往仅针对营销环节。因此，即使数据主体行使拒绝权，拒绝的效力没有覆盖企业自动化分析的环节。更有甚者数据主体撤回同意的，企业仍然保留其个人数据并使用。实施前述行为，将实质违反 GDPR 关于先告知数据主体，后开展自动分析和直接营销的规定。将来一旦有欧盟公民针对企业的前述行为提出质疑并向欧盟监管机构申诉，企业将面临被制裁的风险。因此，企业应当严格按照 GDPR 的要求使用个人数据进行直接营销。

4. 对数据主体权利的保护

在实践中，中国企业设置专门的数据保护人员(DPO)的情形较少。但 DPO 的设置是 GDPR 的明确要求，如果中国企业在欧盟范围内设置分支机构或者投资企业的，应当遵守前述规定，并由 DPO 依照职责检查、督促企业履行对数据主体权利保护的义务，诸如知情权、访问权、反对权、拒绝权、撤回同意权、限制处理权等，避免因对数据主体权利保障不及时，被投诉，遭受制裁。

5. 数据控制者与数据处理者的权利与风险划分

虽然 GDPR 分别规定了数据控制者和数据处理者的义务，但在实践中数据处理者与数据控制者多数情况存在委托关系，数据控制者将承担处理者对个人数据处理造成的法律风险。为此，数据控制者与处理者之间应当签订合同，明确控制者与处理者的权利义务以及风险划分，尤其是关于增加处理者、采取安全措施、突发事件应对、保密协议、数据返还等方面，避免因合同约定

不明，致使在发生纠纷或者责任承担时，难以确定责任主体。

十. 应对策略

1. 完善企业内控机制

企业因不当处理导致个人数据泄露的，即便因为员工的疏忽或者个人行为导致，也将面临严重的处罚。因此，企业应当完善内部对个人数据处理的内控机制，根据岗位设置处理数据的权限，保证每个岗位处理数据的权限符合最少、够用的原则，并通过技术措施确保落地执行，定期开展对个人数据处理的审计。

2. 建立完善数据泄露报告制度及应急预案

对于个人数据的泄露，GDPR 规定了向监管机构报告，并根据可能造成的风险程度向数据主体进行通报，否则将受到严厉的惩处。如果企业采取了合理的技术性、组织性的风险控制措施，则可适当地降低前述报告和通报义务，因此，建议企业健全完善相关应急预案，加强演练，确保将泄露事件造成的影响降到最低限度。

3. 谨慎实施数据画像

对个人数据的画像是国内企业在数据运用中的常见手段，并将个体画像作为直接营销的基础。但 GDPR 对数据的画像作了严格限制，除非基于数据主体的明确同意，或者履行合同的必要措施，或者基于欧盟法律的规定，特别是禁止对敏感数据的画像。因此，国内企业对于个人数据进行画像并开展直接营销的模式需要改变，应当在获得个人数据主体的明确同意后再开展相关画像行为。

4. 配合监管机构

GDPR 规定了极为严厉的处罚措施，并明确了监管机构调查的程序和调查措施。倘若国内企业在欧盟范围内受到调查，应当“入乡随俗”按照当地法律和执法实践，积极配合监管机构开展调查，而不能沿用国内经营中“怠慢轻视”法律的思维，以避免因配合调查的义务履行不当，遭受更加严厉的处罚。

参考资料

1. GDPR Timeline of Events，公布于 https: //www.eugdpr.org/gdpr-timeline.html，最后访问于 2018 年 4 月 2 日 10 点 51 分。

2. 欧盟《一般数据保护条例》的出台背景及影响。《信息安全与通信保密》2010 年 10 月，何治乐、黄道丽。

3. 欧盟《通用数据保护条例》详解。《中国征信杂志》,2016 年第 7 期，王融，中国信息通信研究院互联网法律中心副主任，高级工程师。

4. 欧盟《通用数据保护条例》最新发展及启示，张继红，《金融新发展的法治之维》，法律出版社 2017 年版。

浅析 GDPR 对中国企业海外运营的影响及应对

如需进一步信息，请联系:

作　者	
潘永建 电话:+86 21 3135 8701 david.pan@llinkslaw.com	

上　海	
俞卫锋 电话: +86 21 3135 8686 david.yu@llinkslaw.com	**刘贇春** 电话: +86 21 3135 8678 bernie.liu@llinkslaw.com
佘　铭 电话: +86 21 3135 8770 selena.she@llinkslaw.com	**娄斐弘** 电话: +86 21 3135 8783 nicholas.lou@llinkslaw.com
钱大立 电话: +86 21 3135 8676 dali.qian@llinkslaw.com	**孔焕志** 电话: +86 21 3135 8777 kenneth.kong@llinkslaw.com
吴　炜 电话: +86 21 6043 3711 david.wu@llinkslaw.com	**潘永建** 电话: +86 21 3135 8701 david.pan@llinkslaw.com
姜　琳 电话: +86 21 6043 3710 elyn.jiang@llinkslaw.com	
北　京	
俞卫锋 电话: +86 10 8519 2266 david.yu@llinkslaw.com	**刘贇春** 电话: +86 10 8519 2266 bernie.liu@llinkslaw.com
杨玉华 电话: +86 10 8519 1606 yuhua.yang@llinkslaw.com	
香　港(与张慧雯律师事务所有限法律责任合伙联营)	
俞卫锋 电话: +86 21 3135 8686 david.yu@llinkslaw.com	**吕　红** 电话: +86 21 3135 8776 sandra.lu@llinkslaw.com
伦　敦	
杨玉华 电话: +44 (0)20 3283 4337 yuhua.yang@llinkslaw.com	