科技发展研究

第 7 期

（总第 546 期）

上海科技发展研究中心　　2019 年 3 月 18 日

编者按:2018年5月,作为欧盟主要数据保护法律框架的《通用数据保护条例》(简称“GDPR”)正式实施。GDPR 堪称史上最严格的数据保护条例，其实施将全面影响涉欧盟业务的中国企业。基于同济大学项目组[1]的研究成果，我们将分两期对 GDPR 的主要内容、做法及影响进行分析。本期重点介绍 GDPR 的立法背景、主要内容及影响，供参考。

寻找数据自由流通与个人信息保护的“平衡点”

——欧盟《通用数据保护条例》的主要做法与启示（上）

当前，云计算、移动互联网、社交网络以及各种智能终端迅速普及，大数据总量指数级增长，随之而来的大数据安全问题成为了全球性新挑战。为了应对挑战，欧盟委员会经过数年的研究讨论，在 1995 年通过的《数据保护指令》(简称《指令》)的基础上，制定出台了《通用数据保护条例》，以欧盟法规的形式确定了个人数据保护原则和监管方式，给欧盟公民的个人数据保护带来革命性的变化。

1 上海市软科学研究计划项目《大数据垄断对上海科创产业竞争力影响及其规制研究》（项目编号：18692103500）。

一、立法背景：积极应对快速变化下的新挑战

一方面，欧盟个人数据保护的内在风险阻碍了数据流通和经济发展。1995 年制定的《指令》在实施过程中所存在的碎片化问题无法得到改善，在保护个人数据，尤其是与线上行为痕迹有关的数据方面存在很大的风险。由于各成员国在适用《指令》时可以基于本国法律做适当的调整，导致《指令》在适用过程中存在法律不确定性。成员国在保护个人权利和自由方面，尤其是在数据处理方面的保护程度不一，阻碍了在欧盟法律框架下的成员国间数据流通。

另一方面，技术飞速发展和数据膨胀带来了全新的挑战。随着欧盟各成员国间经济和社会一体化程度的提高，个人数据在成员国之间的跨境流动逐渐增多。公共部门和私有主体间的数据交换也不断增多，不仅包括自然人数据，还包括社团和组织数据。各成员国政府部门也希望在欧盟法律框架下相互合作和交换数据。个人数据收集和数据共享范围及规模不断扩张，给个人数据保护带来了前所未有的挑战。因此，有必要进一步促进欧盟境内的个人数据自由流动，同时确保将个人数据保护提高到一个新的高度。

二、主要内容：寻找数据流通与信息保护的平衡

一是扩大数据保护范围，保护个人信息安全。GDPR 将个人数据保护范围扩展到涉欧数据。**“个人数据”界定方面**，与 1995 年的《指令》仅将个人信息定义为姓名、地址、照片等直接信息不同，GDPR 的规定中不仅包括直接信息（姓名、住址、电话号码等），还包括网络信息（IP 地址、cookies 等）和间接信息（包括所有可追溯至特定个人的生理、心理、基因、文化等数据）。**适用主体方面**，GDPR 从《指令》的“所有欧盟境内运营的企业和所有使用位于欧盟内的设备

处理数据的企业”，扩大为“所有处理欧盟成员国公民个人信息的企业，无论该公民的现居住地是否在欧盟境内”，由此具有了一定的域外效力。

二是赋权数据提供者，为自由流通提供保障。GDPR 对个人数据处理采用了“数据最小化”的原则，规定只有获得数据主体同意才合法。同时赋予数据主体六项基本权利:**（1）访问权，**即有权从数据控制者处确认关于本人数据是否正在被处理，并有权以确认数据的准确性和安全性为目的访问个人数据和相关信息;**（2）更正权，**即有权要求数据控制者及时纠正不准确数据，保持个人数据完整性;**（3）被遗忘权，**即有权要求数据控制者在没有使用必要或数据被非法处理等情况下及时删除个人数据;**（4）限制处理权，**即数据主体在对个人数据的准确性、数据控制者的使用权限提出争议等情况下，有权限制数据控制者对数据的处理权;**（5）可携带权，**即有权接收自己提供给数据控制者的个人数据，并可直接将个人数据从一个数据控制者迁移到另一个控制者;**（6）拒绝权和自主决定权，**即在任何时间和场景下都有权拒绝数据控制者处理本人数据，数据控制者在没有获得强制性合法理由时不得继续处理个人数据。

三是加强对数据控制和处理者的约束。GDPR 对数据控制者和处理者设置了严格的法定义务，个人数据处理必须是出于履行合同、执行公务或保护数据主体利益之必要才为合法，同时必须承担四方面义务:**（1）告知义务，**在数据获取、处理和传输阶段，均需要通过各种途径告知数据主体;**（2）采取必要措施确保数据主体基本权利不被侵害，**应采用适当的技术或组织措施以确保数据处理符合 GDPR 规定;**（3）确保数据处理过程的安全性，**应采取将个人数据匿名化和加密、保持数据处理系统和服务的保密性、定期评估测试保护措施的有效性

等技术和组织措施，确保数据处理的安全性；**（4）记录数据处理活动。**应保持处理活动的记录，包括各类数据控制者的联系信息、数据主体和数据的类别、数据处理目的、接收数据传输的第三方以及数据传输安全记录、数据的保存期限、所采取的安全措施等。此外，由于儿童对于个人隐私泄漏的风险更不敏感，GDPR 规定 16 岁及以下儿童的个人信息处理须经过其监护人同意。

四是完善各项监督管理机制。监管机制方面，GDPR 规定欧盟成员国每国设一位监督人员并建立相应的执行机制，需要处理大量敏感数据的企业亦需聘用一位数据保护官（DPO），监督企业操作的合规性。若企业发生数据泄漏，并可能危害用户的个人权利和自由时，企业必须在发现数据泄漏 72 小时内通知监督人员。**处罚机制方面，**若企业有违规记录用户个人数据、违规后未及时通知监管人员、存在数据安全问题、违反隐私影响评估等行为，最高可处 1000 万欧元或其全球年营业额 2%的罚款；若企业违规内容涉及未经用户同意使用数据、侵犯用户人权或非法跨境流通数据，最高可处以 2000 万欧元或其全球年营业额 4%的罚款（两者取较高值）。

三、主要影响：对我国企业运营合规性的挑战

一方面，企业的运营与合规成本大幅提高。GDPR 目标非常明确：一方面，通过统一立法来保护欧盟个人数据的基本权利和促进欧盟境内的数据自由流通；另一方面，通过对网络平台巨头在数据收集、存储、处理和使用全过程的监管，力求为欧盟境内的数字经济发展谋取缓冲期。GDPR 最直接的效应就是提高企业（尤其是跨国公司）的运营与合规成本。普华永道调查显示，近 60%的美国公司表示将花费至少 100 万到 1 千万美元以满足 GDPR 的要求，近 9%的企业合规成本

将超过1千万美元，近52%的公司将因不合规而遭到罚款。腾讯公司则宣布，2018年5月20日起在欧盟境内暂时停止QQ国际版的旧版服务。因此，我国企业必须早做准备，尽快采取必要的数据保护措施，尽可能降低合规成本。

另一方面，采取必要的合规措施以应对法律风险。为避免随时面临在欧盟境内被起诉或罚款的法律风险，我国企业应建立相关制度，在数据传输、存储、加工等各环节采取必要措施，确保所有业务活动符合数据保护要求并保留相关合规文档。其中，当务之急是任命数据保护官进行法律风险评估，建立数据保护计划，并实时评估和更新数据保护计划以应对《条例》要求。值得注意的是，除了来自政府的监管调查和处罚外，GDPR还允许个人提起集体诉讼，企业对此也要建立预警和应对机制。

执　笔：曾彩霞、尤建新

整　理：龚　晨、汤天波

责任编辑：汤天波　　编　辑：刘　琰　　联系电话：24197936　　传真：64315005

地　　址：中山西路1525号1115室　　邮政编码：200031　　电子邮件：fzzx@stcsm.gov.cn