广州市商务委员会

穗商务公平函〔2018〕6号

广州市商务委关于通报欧盟通用数据保护条例相关工作的通知

各区商务主管部门、各有关企业:

欧盟《通用数据保护条例》已于2018年5月25日正式实施，该条例规定无论处理数据的公司是否总部位于欧盟，只要该公司处理和持有欧盟的个人数据，就需要遵守此条例，违反条例将处以高额的罚款。条例对个人信息保护范围之广、实施标准之高、监管力度之大前所未有，被称为“史上最严”的数据保护法案。我国相关产业，特别是处于快速发展上升期的信息通讯及互联网产业将面临严峻挑战。

现通报该条例的相关内容，请各区商务主管部门根据辖区企业情况，通知可能涉及的重点企业主动收集该条例的实施信息，认真研究受到的影响。如有对该条例的评论意见和有关诉求，请以书面材料报送我委（公平贸易处），由我委统一上报。

附件：欧盟通用数据保护条例介绍

（此页无正文）

广州市商务委

2018 年 6 月 19 日

（联系人：庄彦青、潘毅华 电话：81097465、88906195）

附件

欧盟通用数据保护条例介绍

欧盟个人数据保护新规《通用数据保护条例》（以下简称条例）于5月25日正式实施，现就条例的出台背景、详细内容和执行现状等整理如下：

一、条例简介

通用数据保护条例(General Data Protection Regulation)，简称GDPR，是欧盟秉着“顾客优先”的态度出台的个人数据保护新规。该规定于2016年4月14日出台，定于2018年5月25日正式投入实施，面向所有收集、处理、储存、管理欧盟公民个人数据的企业，限制了这些企业收集与处理用户个人信息的权限，旨在将个人信息的最终控制权交还给用户本人。

二、出台背景

早在1980年，由20个欧洲经济共同体成员国、美国和加拿大等国构成的的经济合作与发展组织(OECD)便提出了一份关于“保护隐私和个人数据跨境流动”的指导方针，对企业使用、收集和保存用户数据的目的、步骤，和数据的跨境流动做出了基本限制。虽然如此，由于该法案对于其成员国没有约束力，成员国间的隐私保护条例并未得到实际统一。

1995 年 10 月，欧洲议会通过了“资料保护指令”(Directive

95/46/EC)。该指令提出企业对个人数据的处理须遵守透明、目的合理、数据完整准确等标准，并规定个人数据若要流向欧盟以外的第三方国家，必须满足该国家有同等个人隐私保护条例的前提。但不同于指导方针，“资料保护指令”对于欧盟成员国具有约束力，并规定成员国须于 1998 年年底前将该指令转化为法律在各国内实施。

2012 年 1 月，欧盟委员会宣布即将通过一个全新的“通用数据保护条例”取代之前各欧盟成员国根据“资料保护指令”的相关立法，并称为欧盟各国间的唯一、统一的数据保护条例。其主要目的还包括优化数据流向欧盟外国家的管理办法，以及增强用户对于其个人信息的控制。经过四年酝酿，欧盟通用数据保护条例(GDPR)最终于 2016 年被通过，并设置两年缓冲期，于 2018 年 5 月 25 日正式投入实施。

三、条例内容与执行现状

（一）详细内容

相比“资料保护指令”，数据保护条例在条例适用范围、个人数据处理方式以及监督管理上有九大主要特点：

1.重新定义“个人信息”

资料保护指令（1995）仅将个人信息定义为姓名、地址、照片等直接信息；而 GDPR（2016）对个人信息的定义不仅包括直接信息（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（包括所有可追溯至某一特定个人的生理、

心理、基因、文化等特征）。

2.适用范围增大

资料保护指令（1995）的适用范围为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；而 GDPR（2016）的适用范围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。

3.优化数据处理体系

GDPR 规定企业必须将保护个人信息和数据融入到对于产品的最初设计和公司日常的运营中去，推荐方法包括拟定假名或加密个人数据。

4.责任共担

过去，收集和使用数据的数据拥有者需要对数据保护负责。如今，史无前例的，数据处理者(如提供数据处理服务的云服务提供商等)也将需要直接承担合规风险和义务。在数据保护上，数据供应链自上而下的各方都会被问责。网络公司必须与合作伙伴们明确各自的责任和义务。

5.取得用户批准

GDPR 规定企业必须获得数据提供者关于某明确合法用途的授权，并可出示数据获取方法的证明。在企业申请用户授权时需阐明：用户数据使用方的身份与联系方式、取得数据的目的与使用方式、数据是否会被跨境传输、数据存贮时长等。

6.保护消费者权益

用户可随时查看、修改、移动、删除数据，并要求企业开具数据备份及数据使用方式。用户也拥有随时取消授权和抗议的权利。当获取数据时所述的目的不再适用或用户不再允许企业使用该数据，GDPR 规定企业必须删除用户信息，同时将用户的数据清除请求告知第三方处理机构。

7.对于儿童的特殊保护

由于儿童相较于成人对于个人隐私泄漏的风险更不敏感，GDPR 规定对于 16 岁及以下的儿童的个人信息处理须经过其监护人同意。

8.发现违规后及时通知监管人员

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(Data Protection Officer)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。但由于该法案刚刚投入实施，具体的监管体系还有待完善。

9.处罚力度增强

GDPR 建立了严格的处罚机制。若企业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相关条例，最高可获 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，最高可获 2000 万欧元或其全球年

营业额4%的罚款（两者取较高值）。

（二）执行现状

虽然GDPR的效力层级在欧盟是“条例”，编号为EU-DSGVO，其效力仅次于宪法，但部分企业与欧盟成员国仍未做好准备。目前，在欧盟28个成员国中，有12个国家已经正式更新了其国内法，将GDPR嵌入其中，同时还有8个国家告知欧盟委员会它们将在近期尽快完成其立法程序，但仍有8个欧盟国家在5月25日后在GDPR同其国内法融合方面毫无作为。欧盟方面表示，已经对上述国家做出了警告，请它们尽快更新法律系统，否则将把它们告上欧洲法院。

四、对中国企业的主要影响

（一）欧盟GDPR具有域外效力

GDPR赋予了欧盟在个人信息安全方面的域外管辖权。根据GDPR的规定，中国企业作为数据控制者或者数据处理者，如果在企业经营的过程中备份或者通过自动化手段处理了全部或部分的个人数据，就应该遵守欧盟关于个人信息安全的法律规定。具体情形包括:

如果企业设立在欧盟，那么无论对个人信息的处理行为是否发生在欧盟;

如果企业非设立在欧盟，但其向位于欧盟内数据主体提供商品和服务的过程中处理了欧盟内数据主体的个人数据，或对数据主体在欧盟内的活动进行监测;

如果企业非设立在欧盟，但根据国际公法，其所在地适用欧盟成员国的法律。

简言之，GDPR 不仅适用于位于欧盟内部的组织机构，也适用于位于欧盟以外的组织机构，无论其所在地位于哪里，只要其向欧盟数据主体提供产品、服务或监控相关行为，或处理和持有居住在欧盟的数据主体的个人数据。

值得注意的是，GDPR 适用于数据控制者和数据处理者。“数据控制者”是确定处理个人数据的目的、条件和手段的实体，“而数据处理者”是代表控制者处理个人数据的实体。这意味着“云”也将毫不例外地被划归至 GDPR 的管辖范围。

（二）企业违反 GDPR 将面临调查和重罚

如果违反 GDPR，企业将面临欧盟相关监管机关的调查，包括：被通知相关违反行为；被要求提供相关信息，或者向监管机构提供访问此类信息的接口；被现场调查、审计；被命令修改、删除或者销毁个人数据；被采取临时性的或者有限的数据处理禁令等。

GDPR 对违规企业采取根据情况分级处理的方法。如果公司未按要求做好相关记录，或者未将其违规行为通知监管机关和数据主体，或者未进行影响评估，则可能被处以其全球年营业额 2% 的罚款。如果发生了最为严重的侵犯个人信息安全的行为，譬如，没有充分获得客户同意就处理数据，或者核心理念违反“隐私设计”要求，相关企业就可能面临高达其全球年营业额的 4% 或 2000

万欧元（以较大者为准）的巨额行政罚款。

除此之外，欧盟各成员国还可以针对数据保护违规行为，制定本国有效、适当和有威慑力的罚则。

公开方式：主动公开