

NEWSLETTER

数据合规

2019 第五期 / 总第五期

## 数据合规时事速递

北京市环球律师事务所

2019 年 7 月 19 日

## 目录

|                                      |    |
|--------------------------------------|----|
| 前 言 .....                            | 3  |
| 一、新规速递 .....                         | 4  |
| 1. 多企业签署《用户个人信息收集使用自律公约》 .....       | 4  |
| 二、监管动态 .....                         | 8  |
| 1. 40 款 App 遭督促整改：涉嫌违规收集使用个人信息 ..... | 8  |
| 2. 10 款 App 遭通报：存在无隐私政策等问题 .....     | 9  |
| 三、相关案例 .....                         | 10 |
| 1. 某网站遭简历泄露 .....                    | 10 |
| 2. Facebook 被罚款 50 亿 .....           | 11 |
| 四、环球评论 .....                         | 12 |
| 1. 解读：ICO 对英国航空和万豪国际开出巨额罚单 .....     | 12 |

## 前言

随着《网络安全法》及相关配套法律法规等文件的出台，中国正日益加强对个人信息安全的保护和对网络安全监管。我国对个人信息保护和网络数据安全越来越重视，监管趋势也越来越严。

环球律师事务所数据合规团队收集了国内外最新出台的重要法律法规、市场监管动向以及相关处罚案例，旨在为本期刊的读者提供最实时的法律动态，帮助读者第一时间了解网络治理、信息安全相关信息。据时代的机遇与挑战。



环球律师事务所  
GLOBAL LAW OFFICE

### 团队介绍：

环球律师事务所数据合规团队专注于网络安全与数据合规、个人信息隐私保护等领域。我们在企业数据合规体系建设等方面具备丰富的经验，为多家大型互联网公司、全球企业提供法律服务。

我们为客户提供在网络安全与数据合规、个人信息隐私保护、跨境数据传输、电子商务与广告法领域的法律咨询及相关方案设计，帮助客户迎接数据时代的机遇与挑战。



孟洁

合伙人律师

直线：86-10-6584-6768

总机：86-10-6584-6688

邮箱：mengjie@glo.com.cn

## 一、新规速递

### 1. 多企业签署《用户个人信息收集使用自律公约》<sup>1</sup>

#### 发布背景

7月11日，中国互联网协会在北京举办“互联网个人信息保护论坛”。当日在工信部的指导下，为了更好的治理 App 过度收集和使用用户个人信息的行为，中国互联网协会以及相关业界专家共同制定了《用户个人信息收集使用自律公约》。中国移动、中国联通、中国电信、腾讯、阿里巴巴、百度、京东等 28 家企业现场共同签署了该协议。

当下信息技术正在快速的发展，实践中也出现了越来越多非法收集、滥用、泄露个人信息的安全问题，因此政府部门和社会各界对此十分关注。为了切实保护用户的合法利益，并充分保障网络数据和用户个人信息安全，此次由中国互联网协会以及社会各界专家共同制定的《公约》，能更好地引导各个企业更加规范地收集和使用用户个人信息，打造一个诚信、安全的网络环境。此次《公约》的出台也得到了众多企业的支持和响应。

#### 条约内容

##### 《用户个人信息收集使用自律公约》

第一条 为保障用户个人信息安全，切实保护用户合法权益，引导企业严格遵守国家有关法律、法规、规章，以及政策和标准，促进行业持续健康有序发展，制定本公约。

第二条 互联网从业单位自愿加入本公约，充分尊重并自觉履行本公约的各项

---

<sup>1</sup> 中关村在线消息：《用户个人信息收集使用自律公约》签约仪式举行。

规定。

第三条 本公约所称用户个人信息是指互联网从业单位在提供互联网服务的过程中收集的用户姓名、出生日期、身份证件号码、住址、电话号码、账号和密码等能够单独或者与其他信息结合识别用户的信息，以及用户使用服务的时间、地点等信息。

第四条 收集、使用用户个人信息前，以特定网页或应用界面等易于用户访问、清晰明确、通俗易懂的方式主动告知用户下列事项：

（一）收集用户个人信息的目的、方式、类型、范围、收集场景等内容；

（二）保存期限以及到期后的处理方式；

（三）是否会向第三方提供以及向第三方提供的用户个人信息的目的、方式、类型、范围，以及第三方类型；

（四）用户查询、更正、删除其个人信息的渠道。

第五条 收集、使用用户个人信息应征得用户同意，涉及用户个人身份、生物识别等个人敏感信息的，采用用户主动勾选、主动点击“同意”等方式征得用户明示同意。

第六条 所提供服务涵盖多项业务功能的，收集、使用用户个人身份、生物识别等个人敏感信息时，不得通过一揽子授权的方式获取用户同意，不以默认、捆绑、停止安装使用等手段强迫用户授权。

第七条 用户拒绝提供个人敏感信息的，明确告知服务使用受限的范围；不得因用户拒绝提供而影响对其他业务功能的使用，除非用户拒绝提供的个人敏感信息为服务所必需。

第八条 明确告知用户撤回同意收集、使用用户个人信息的渠道和方式等，并为用户撤回同意提供便利。

第九条 使用个性化展示新闻信息服务的，应为用户提供简单直观的退出或关闭个性化展示模式的选项或者不基于用户个人信息的新闻推荐选项。

根据用户爱好、消费习惯等特征向其个性化展示商品或服务的搜索结果的，应当同时向用户提供不针对个人特征的选项。基于用户所选择的特定位置进行展示和排序搜索结果的除外。

第十条 严格按照国家有关规定和与用户约定的时限存储用户个人信息，并为用户注销号码或者账号提供便捷的服务，且不设置不合理的注销门槛。

第十一条 超出用户个人信息保存期限、停止运营、用户注销号码或账号的，对用户个人信息进行匿名化等处理，确保处理之后的信息无法识别、确认、关联到特定用户，并对处理方法保密，法律法规另有规定的或双方另有约定的除外。

第十二条 使用个人信息时，不超出与收集个人信息时所声称的目的具有直接或合理关联的范围。因业务需要，确需超出上述范围使用个人信息的，应再次征得用户同意。

第十三条 主动在网站或者应用界面的明显位置为用户提供删除、更正个人信息的途径或方法指引，及时受理用户删除、更正相关个人信息的合理要求，并采取措施予以删除或者更正。

第十四条 向第三方提供用户个人信息，应当征得用户同意，并与个人信息接收方订立安全协议，明确各方个人信息保护责任，要求个人信息接收方依法保护。

第十五条 互联网从业单位收购、兼并、重组、破产涉及向外部第三方承接单位转让用户个人信息的，转让单位应与承接单位明确个人信息承接方案和对方案进行自评估，并通过电话、短信、邮件、公告等方式通知可能受到影响的用户。业务承接单位应继续履行原用户个人信息保护的责任和义务，如变更用户个人信息使用目的，应重新取得用户明示同意。

第十六条 委托他人收集、处理用户个人信息的，对委托行为负责，并与受托方订立协议，约定用户个人信息收集、处理的方式、范围、安全保障措施以及发现受托方违反国家有关规定后的处理措施。

第十七条 中国互联网协会个人信息保护工作委员会是本协议的执行机构，负责组织本协议签署和实施，定期公布签署单位名单，向签署单位宣传国家相关法律、法规和政策。

第十八条 协议执行机构组织签署单位对协议履行情况定期开展自查，任何单位和个人均有权向协议执行机构投诉或举报。

第十九条 结合自查和公众监督举报情况，执行机构在查证核实后，对违反本协议的签署单位进行指导和督促整改，必要时予以警告、通报或公开谴责，发现违法违规线索，交相关部门处理。

第二十条 本协议经从业单位法定代表人或者其委托的代表签字并加盖单位公章后生效。遵循“动态修订、逐步完善”的原则，由协议执行机构或者三分之一以上签署单位提议、三分之二以上签署单位同意，可对本协议进行修改。

第二十一条 本协议由中国互联网协会个人信息保护工作委员会负责解释。

## 二、监管动态

### 1. 40 款 App 遭督促整改：涉嫌违规收集使用个人信息<sup>2</sup>

#### 违规 App

近日，App 专项治理工作组发布了《关于督促 40 款存在收集使用个人信息问题的 App 运营者尽快整改的通知》（以下简称“《通知》”），该《通知》称，针对网民举报的在收集和使用个人信息出现问题的各类 App，App 专项治理工作组对其进行了调查与核实，并进行了相应评估，发现包括某社交软件，某学习类软件和某直播类软件等共 40 款 App 存在相应问题，并且没有提供联系相应负责人的渠道。

#### 整改要求

该《通知》要求，被点名的 40 款 App 应当在《通知》发布起 10 日内联系工作组，领取相应的整改通知。并且，在《通知》发布之日起 30 日内完成相应的整改并提交整改报告。如果逾期没有领取整改通知或没有完成整改的，工作组将建议相关部门对其予以处置。

---

<sup>2</sup> App 治理工作组：《关于督促 40 款存在收集使用个人信息问题的 App 运营者尽快整改的通知》。



## 2. 10 款 App 遭通报：存在无隐私政策等问题<sup>3</sup>

### 违规 App

近日，App 专项治理工作组发布了《关于 10 款 App 存在无隐私政策等问题的通报》（以下简称“《通报》”），该《通报》指出 10 款没有隐私政策的 App 和 20 款要求用户一次性同意开启多个权限且不同意则无法安装使用的 20 款 App。

### 整改要求

该《通报》要求，被点名的 App 运营者应当在《通报》发布起 30 日内完成整改。逾期未完成整改的，工作组将建议相关部门对其予以处置。

---

<sup>3</sup> App 治理工作组：《关于 10 款 App 存在无隐私政策等问题的通报》。

## 三、相关案例

### 1. 某网站遭简历泄露<sup>4</sup>

#### 案情简介

2019年7月5日，北京市朝阳区人民法院审理了一起某网站员工参与的倒卖个人信息案。该案涉及的公民个人信息达16万余份，一份信息售价5元左右。该案件在北京市朝阳区法院第二次开庭审理。

此案最早是由该网站于2018年6月在日常巡查中发现的，据悉，淘宝网络上有售卖简历的行为。该网站在发现后于第一时间报案，积极协助公安机关进行调查。2018年8月，该网站上海分公司销售人员卢某和王某被公安机关带走。

根据法院开庭情况，卢某和王某时任该网站销售，无业人员郑某与二人勾结，违反公司制度，骗取企业会员账号获取简历，在网络上非法销售牟利。截至7月5日，此案尚未宣判。

#### 专家视角

目前由于我国的《个人信息保护法》尚在起草当中，相关现行法律在保护个人信息方面尚存在不完善之处，这给一些不法分子提供了可乘之机。该网站对个人信息管理也存在漏洞，第三方售卖平台也有一定连带责任，应受到相关法律的惩罚。

---

<sup>4</sup> 澎湃新闻：《每条1元，某网站员工倒卖求职简历受审》。

## 2. Facebook 被罚款 50 亿<sup>5</sup>

### 案情简介

2018 年，一款测试应用窃取了 8700 万 Facebook 用户的个人数据，并将这些数据与政治咨询公司 Cambridge Analytica 分享。丑闻被曝出之后，FTC 开始针对 Facebook 展开调查。此前据预测，Facebook 将为此事承担 30 亿至 50 亿美元的罚金。

当地时间 2019 年 7 月 12 日，美国联邦贸易委员会（FTC）与 Facebook 达成了一项和解协议，由 FTC 对 Facebook 开出 50 亿美元的罚单，来结束有关针对 Facebook 隐私问题的调查。50 亿美元的天文数字，创下了新的罚款纪录。如果 50 亿美元的罚金得到确认，这将相当于 Facebook 年收入的 9%，甚至远高于欧洲《通用数据保护条例》所规定的罚款金额不超过企业全球收入 4% 的上限。

对于违反隐私保护规定的科技公司，这是有史以来 FTC 开出的最高罚单，也意味着 FTC 可能将结束针对 Facebook 不当处理用户个人信息开展的调查。一位知情人士表示，此事已经被移交至美国司法部的民事部门，现在尚不清楚最终结案需要多长时间。据悉，美国司法部的审查是 FTC 流程的一部分，但通常不会改变委员会的决定。

### 专家视角

互联网分析师杨世界分析说，这笔 50 亿美元的罚款只是一种形式，Facebook 隐私泄露的案例非常具有典型性，一方面，监管机构想要将其作为一个具有代表性的案例，另一方面，从更深的角度来看，这一次处罚也可能是为大选作一个铺垫。因为之前 Facebook 就发生过疑似数据门事件被怀疑影响总统大选。Facebook 作为一个影响力极大的社交平台需要承担相应的数据保护和监管的责任。

---

<sup>5</sup> 第一财经：《Facebook 被罚 50 亿美元还不够，国会听证会继续拷问》。

## 四、环球评论

### 1. 解读：ICO对英国航空和万豪国际开出巨额罚单<sup>6</sup>

#### 案件背景

2018年5月25日,《欧盟数据保护通用条例》(General Data Protection Regulation, 简称“GDPR”)正式生效。但条例生效后的1年多,欧洲各国监管机构尚未对违规企业作出巨额罚款。终于,在2019年7月8日与9日,英国信息监管局(Information Commissioner’s Office, 以下简称“ICO”)先后对英国航空和万豪国际开出1.83亿英镑和9920万英镑的巨额罚单,拉开GDPR强硬执法的序幕。

#### 案件解读

##### (一) 英国航空数据泄露事件

ICO对英国航空作出的1.83亿英镑的罚款是ICO至今所作出的最大一笔罚款,也是GDPR生效后在欧盟境内首笔大额的罚款,达到英国航空2018年全年营业额的1.5%。

该罚款针对的是2018年9月英国航空网站发生的数据泄露事件。在该事件中,用户被移转到虚假网站,攻击者通过这个虚假网站收集了客户详细信息,包括客户个人信息和银行卡信息,如姓名、地址、邮箱,以及信用卡的号码、有效期和背面的验证码(CVV)等。英国航空最初表示只有38万份客户资料外泄。在经过ICO详细调查后,确定信息泄露人数扩大到50万。

就此事件以及做出的处罚,ICO负责人Elizabeth Denham表示,“公民个人信息数据是极其私密的。当受委托的组织未能保护其客户数据免受损失、损坏或者被盗时,客户的潜在损失已经远远超过了给他们带来的不便。”

##### (二) 万豪国际数据泄露事件

ICO对万豪国际作出的9920万英镑的罚款是有关数据泄露的第二笔巨额罚单,

---

<sup>6</sup> 作者: 孟洁、张淑仪。

占万豪国际 2018 全年营业额的 3%。

该罚款针对的是万豪国际因其旗下喜达屋酒店的客房预订数据库被黑客攻击，泄露了全球约 3.83 亿条住户记录，其中包括 3000 万欧洲经济区（EEA）居民，700 万英国居民。

据 ICO 调查，喜达屋酒店客房预订系统因黑客攻击导致的数据漏洞自 2014 年便存在。万豪国际在 2016 年收购了喜达屋酒店，但在 2018 年才发现此漏洞。ICO 认为万豪国际在收购喜达屋酒店时未作充分的尽职调查，并且在保证酒店系统安全方面，万豪国际也未采取更多的保护措施。

就此事件以及做出的处罚，ICO 负责人 Elizabeth Denham 表示“GDPR 明确规定，组织应对其持有的个人数据负责。组织在收购时应当进行足够的尽职调查，不应采取适当的措施评估已取得的个人数据，还应当评估如何保护这些数据。”

Denham 还表示，“个人数据具有真正的价值，因此组织有法律义务确保其安全，就像处理任何其他资产一样。如果组织没有这样做，ICO 则会毫不犹豫地采取强有力的行动，以保护公众的权利。”

目前 ICO 对英国航空和万豪国际的处罚并非终局性处罚，两公司均表示会对 ICO 做出的处罚进行上诉。

## 对我国司法部门的建议

英国航空事件涉及约 50 万人的极度私密信息，万豪国际事件更是关系到全球 3.83 亿人的数据安全，其他大型数据泄露事件也屡见不鲜。安全情报提供商 Risk Based Security 的报告显示，2018 年全球公开披露数据泄露事件超过 6500 起，有 12 起数据泄露事件涉及人数超过 1 亿。

我国虽在 2019 年 3 月全国人大的发布会上表示将制定数据安全法，但截止目前尚未明晰有关数据泄露的《数据安全法》的草案或者细节。我国《网络安全法》第 42 条第 2 款虽然规定了数据泄露的通知，但仅限于个人信息泄露，且缺乏必要的程序实施细则与处罚要求。这些均需要《数据安全法》进行补充加强，从而尽量降低泄露带来的损失。

参考 GDPR 以及欧盟数据保护委员会（European Data Protection Supervisor, 以下简称“EDPS”）发布的《个人数据泄露报告指引》，数据泄露通知制度应当包括或明确以下内容：

数据泄露通知的主体。在 GDPR 规定下，数据控制者承担通知义务。我国现行的《网络安全法》适用对象分类为“网络所有者、管理者和网络服务提供者”。这种分类过于宽泛，且在实践中可能出现互相推诿责任的情形。故新的《数据安全法》应当明确通知的主体。

引发数据泄露通知的条件。在中国境内发生的泄露事件是一种情况，如果在中国境外发生泄露，也可能会对我国公民的个人信息产生实质性的影响，相关主体也应当负有通知义务。

数据泄露通知的程序。在数据泄露发生后，负有通知义务的主体应当向相关监管机构、受影响的主体及时发出通知，告知事件的性质、范围、数据类型、被影响的数据主体的数量以及损害程度、严重性与持续时间，并应当采取适当的补救措施。

## 对我国企业的启示

### （一）欧盟各国数据保护机构对 GDPR 的执法力度增强。

在欧盟对英国航空开出 1.83 亿英镑罚款之前，ICO 对外数据安全漏洞做出的罚款最高额仅为 50 万英镑（GDPR 体系前的法定最高额）。对英国航空和万豪国际拟处的罚款标志着 GDPR 体系下对于安全漏洞事故的处罚金标准。

组织在处理数据安全问题时，除了要考虑 GDPR 第 32-34 条规定的个人数据安全以及数据泄露对应的处罚金额外（最高额 1000 万欧元或全球年度营业额 2%），还必须考虑 GDPR 第 5 条个人数据处理基本原则中(1)(f)项规定的数据完整性与保密性原则。如果发生未经授权或非法处理数据事项，监管机构可以科处最高额 2000 万欧元或全球年营业额 4%的罚款（以较高者为准）。

目前尚不确定 ICO 计算罚款的标准，例如在英国航空案中是其全年营业额的 1.5%，万豪国际案是其全年营业额的 3%，但 ICO 在其发布的《监管行动政策》中对罚款金额的考虑要素共有三个方面，包括：（i）组织违规行为的性质、严重程度以及持续时间；（ii）受影响的个人信息的类型；（iii）处以罚金的有效性、程度相称性和劝阻性。

ICO 称，对外公布处罚的目的是确保有关组织遵守法律，并对于组织的侵权行为起到有效的震慑作用。通过对英国航空和万豪酒店的执法行动，并对比 GDPR 体系前的处罚金额，可以看出 ICO 试图重新定义处罚金与违约行为之间“程度相称”的标准，以达到 GDPR 所要求的对数据的高水平保护。



（二）GDPR 执法机构对于设立在欧盟境外组织亦积极执法，中国企业应敲响合规警钟

根据 GDPR 第 3 条的规定以及 EDPS 发布的《关于 GDPR 地域管辖的指引》，只要该组织向欧盟境内的个人提供商品或服务（不管是否付费），均要受到 GDPR 的规制。例如，在万豪国际事件中，虽然万豪国际设立在美国，其泄露的 3.83 亿人数数据也并不全是欧盟人，但只要其向欧盟境内的个人提供了商品或服务，则万豪国际就要受到 GDPR 的管辖。

这一要求为中国在全球范围内提供服务的企业敲响了警钟，特别是我国某些已经在欧洲积累了较大的用户的企业，例如国内极为火热的手游国际版在欧洲、北美地区上线后，注册用户已经超过两亿，每日活跃用户高达 8000 万。如此大规模的用户除了带来可观的收入之外，也为企业数据合规带来极大风险。

然而，与前述中国企业全球服务趋势相矛盾的是，我国企业对于用户数据保护的自觉意识仍十分缺乏，整体合规程度低。南都大数据研究院对企业隐私政策的测评更显示样本中 50% 的 APP 存在越限获取用户信息的情形，整体上不合规企业所占比例高达 80%。这样的情况下，如果欧盟各国 GDPR 监管机构对有出海业务的国内企业进行严格检查，可能导致严重的结果。

（三）企业在日常经营活动需重视对数据的保护

在英国航空事件中是因网站系统不安全而招致的数据隐患，同样在万豪国际事件中的酒店预订系统数据自 2014 年便存在。如果企业在日常经营活动中便重视并做定期的合规性检查，不仅可以降低企业不履行法律义务和违反法律的可能性，且相较事件爆发后收到执法机构的处罚，提前发现问题通常解决起来更简单，所消耗的金钱成本更低。

目前国内发布的《信息安全技术、个人信息去标识化指南（征求意见稿）》、《信息安全技术数据出境安全评估指南（征求意见稿）》、《信息安全技术个人信息安全规范（征求意见稿）》、《信息安全技术个人信息安全影响评估指南（征求意见稿）》等国家标准为企业合规提供了相对具体的指引。其中与企业日常数据合规最为相关的是《信息安全技术个人信息安全影响评估指南（征求意见稿）》（简称“PIA 指南”）。该指南编制说明，该指南不仅适用于“各类组织自行开展个人信息安全影响评估工作”，也适用于“为国家主管部门、第三方测评机构等开展个人信息安全监管、检查、评估等工作提供的指导和依据”。

通过定期个人信息安全影响评估不仅帮助检查组织内部的合规性，还可以帮助组织在持续合规性审计或调查中证明其遵守了相关个人信息与数据保护法律法

规和相关国家标准要求。一旦发生个人信息安全风险或违规事件，个人信息安全影响评估报告作为证据证明组织已经采取适当措施试图阻止上述情况发生，这有助于减轻、甚至免除相关责任和名誉损失。

此外，通过个人信息安全影响评估，组织还可以对员工进行个人信息保护教育，使之警惕可能给组织带来损失的个人信息安全问题。

#### （四）须重视资本市场投并购项目中的数据合规尽职调查

在万豪国际事件中，ICO 认定万豪国际在收购喜达屋酒店时未作充分的尽职调查发现系统漏洞，并且在保证酒店系统安全方面，万豪国际也未采取更多的保护措施。这一巨额处罚本可以在 16 年收购时的尽职调查过程中予以避免，但因为当时对数据调查未施以过多的重视，没有进行得足够深入，16 年埋下的隐患于 18 年爆发。这一教训也提醒了在资本市场的投资、并购项目中，数据合规以及尽职调查的重要性。只要标的公司的业务涉及数据，则应当把数据合规尽职调查放到与公司其他资产尽职调查同等重要的地位，从而避免此类数据漏洞日后给企业带来的巨额损失。



北京市朝阳区建国路81号华贸中心  
1号写字楼15层&20层 邮编: 100025  
15 & 20/F Tower 1, China Central Place,  
No. 81 Jianguo Road Chaoyang District,  
Beijing 100025, China  
电话/T. (86 10) 6584 6688  
传真/F. (86 10) 6584 6666

上海市黄浦区湖滨路150号企业天地  
5号楼26层 邮编: 200021  
26F, 5 Corporate Avenue,  
No. 150 Hubin Road, Huangpu District,  
Shanghai 200021, China  
电话/T. (86 21) 2310 8288  
传真/F. (86 21) 2310 8299

深圳市南山区铜鼓路39号大冲国际中心  
5号楼26层B/C单元 邮编: 518055  
Units B/C, 26F, Tower 5,  
Dachong International Center, No. 39 Tonggu Road,  
Nanshan District, Shenzhen 518055, China  
电话/T. (86 755) 8388 5988  
传真/F. (86 755) 8388 5987