GIDE
基德律師事務所

资讯快递

欧洲/法国 | 电信、媒体和科技 | 2018 年 06 月

客户通报/遵守欧盟最新数据保护框架（GDPR）

您是否在处理欧盟居民的个人数据，以及决定处理该等数据的用途和方式？如果您在欧盟开展业务活动，或者因为向欧盟居民提供商品和服务或对其进行监控而直接实施个人数据处理，则您属于个人数据控制者。因此，您可能需要遵守《欧盟通用数据保护条例》，从而必须履行多项新义务。

您在欧盟是否有企业客户？您是否会代表这些企业客户（通过呼叫中心、咨询台、外包服务或业务流程外包等业务活动）处理欧盟居民的个人数据？无论您的设立地在何处，您都属于个人数据分包者（即数据处理者），且很有可能需要遵守《欧盟通用数据保护条例》。

由于区域范围涵盖较广，《欧盟通用数据保护条例》可能适用于那些并非在欧盟设立的公司。因此，在欧盟进行投资或处理源自欧盟的数据的中国公司可能将直接受到《欧盟通用数据保护条例》的影响。

《欧盟通用数据保护条例》（GDPR）于 2016 年 4 月 27 日通过，2018 年 5 月 25 日实施。

尽早达到《欧盟通用数据保护条例》的合规要求至关重要。本通报旨在向您介绍您作为个人数据控制者或分包者需遵守的一些主要义务。

个人数据控制者的主要义务有哪些？

1. **分析您使用个人数据的法律依据。**确保您有正当理由处理个人数据（如：个人同意、合法利益、合同约定、法律义务）。
2. **修改您的隐私和公告通知：**
   - 您应当向数据主体提供**清晰、明白易懂和易于获取的信息**；及
   - 如果处理需取得同意，**必须告知用户，由用户同意对其数据进行处理**。数据控制者具有用户同意举证责任，必须有清楚明确的同意。

3. **执行尊重数据主体权利的程序。**当数据主体行使其权利时（包括访问权、修改权、反对权、携带权、撤销同意权），您必须处理其权利主张和请求。

4. **接受“通过设计保护隐私”和“通过默认设置保护隐私”。**您必须实施保护个人数据所必要的一切技术和组织措施，包括通过产品或服务设计保护隐私和通过默认设置保护隐私。具体而言，您必须注意**从一开始就将处理的数据量降至最低**，以便仅收集和处理**实现您目的严格必需的数据**。

5. 根据责任原则，**始终实施适当的数据保护措施和政策并证明您符合相关规定**。您尤其需要落实以下合规手段：

   - **记录**您实施的数据处理。员工少于 250 人的公司不适用此项义务，除非实施的数据处理可能对相关个人的权利构成风险，或数据处理不具偶然性，或涉及特殊类型的数据或与刑事检控有关的数据。由于具有偶然性的处理极少，因此保存记录的义务鲜有例外情况；
   - 实施明确的政策，以确保您可以在 72 小时内向有关机构**报告安全违规情况**，以及在该等违规可能对数据主体的权利和自由造成高度风险的情况下，向其告知该等违规情况；
   - **个人数据处理认证，如适用**；
   - **遵守行为准则，如适用**；

6. 在某些情况下，**指定一名数据保护官**，尤其是您的业务活动涉及需要对数据主体进行定期和系统的大规模监控的处理操作时；

7. 在某些情况下，开展**隐私影响评估**，尤其是有关具有风险的个人数据处理的评估，包括敏感数据的处理和在系统全面评估自然人个人信息基础上的数据处理；

8. 在某些情况下，**指定一名欧盟代表**，由其负责与相关监管机构和数据主体进行沟通。

9. 如果您有分包商，**证明您的分包商知晓其最新的义务和责任**。尤其是，确保在合同中规定分包商有关所处理的个人数据的安全、保密和保护义务。

个人数据分包者的主要义务有哪些？

1. 根据《欧盟通用数据保护条例》第 28 条的规定，**与您的客户签订合同**（或补充协议），规定每一方有关个人数据的义务，包括仅根据客户的书面指示处理数据以及协助客户履行其作为处理责任主体的义务。

2. **记录**您的客户信息，描述您代表客户实施的数据处理并记载其所有指示。员工少于 250 人的公司不适用此项义务，除非实施的数据处理可能对数据主体的权利构成风险，或数据处理不具偶然性，或涉及特殊类型的数据或与刑事检控有关的数据。由于具有偶然性的处理极少，因此保存记录的义务鲜有例外情况。

3. 当您需要分包时，**请获取您客户的书面授权**。

4. 在某些情况下，**指定一名欧盟代表**，由其负责与相关监管机构和数据主体进行沟通。

5. 在某些情况下，**指定一名数据保护官**，尤其是您的业务活动涉及需要对数据主体进行定期和系统的大规模监控的处理操作时。

6. 您必须**保证所处理数据的安全**。具体而言，这意味着：

   - 您必须采取适当的技术和组织措施，以确保达到与风险相对应的安全级别；
   - 处理个人数据的员工必须受**保密义务**的约束；及
   - 您必须尽快**将任何数据违规情况通知您的客户**。

7. 您必须在处理数据的框架内尽到提醒、协助和建议义务：

   - 如果您认为**客户的指示违反相关规定**，需立即给予其提醒；
   - 协助您的客户对**任何个人行使其“传统”权利**（访问权、修改权、反对权和消除权）和 GDPR 赋予的新权利（携带权）的情况进行跟踪；及
   - 向您的客户建议和提供**实施隐私影响评估**或开展审计**所需的所有信息**。

8. 您必须向您的客户作出所有**必要保证**，以使您向客户提供的工具、产品、应用或服务遵守数据保护原则

可否将个人数据向欧盟境外转移？

无论您是个人数据控制者或分包者，**在向不提供充分保护的非欧盟国家转移个人数据时**都必须**使用提供充分且适当保护的工具**。尤其需指出，欧盟未将中国视为提供充分保护的国家。向欧盟境外转移的数据，不仅是转移本身，其任何进一步的处理和再转移仍受欧盟法律的约束。因此，您必须采取以下保障措施：

- 具有约束力的公司规则；
- 欧盟委员会批准的标准合同条款；
- 有关部门通过且欧盟委员会批准的合同条款。经主管机构通过和欧盟委员会批准的标准合同条款；和
- 经主管机构（就法国而言，指法国国家信息和自由委员会（CNIL））授权的特别合同条款。

若无法进行适当保障，《欧盟通用数据保护条例》就符合以下任一条件的数据转移规定了特别情形下的例外条款

- 数据主体作出明确同意；
- 数据主体与数据控制者之间存在协议；
- 合同有利于数据主体；
- 符合公共利益；
- 法庭上的权利辩护；
- 保护数据主体的切身利益；和
- 数据控制者的压倒性合法利益高于数据主体的利益或权利及自由。数据转移本质上不具有重复性，且仅影响有限的数据主体。

因此，遵守《欧盟通用数据保护条例》规定的新义务以及在这方面建立充分的标准，是您在业务活动中实施必要数据转移的条件。

不合规的风险有哪些？

自 2018 年 5 月 25 日起，若违反《欧盟通用数据保护条例》，即使您不是数据处理主体，也仍有可能被认定承担因未遵守相关义务**给数据主体造成损害的责任**。

您还有可能被处以**巨额行政罚款**，罚款金额视违规的类别而定，最严重的可达：

- 1000 万至 2000 万欧元；或
- 上一年全球年营业额的 2%或 4%。

基德团队将随时协助您履行 GDPR 设置的新义务。

联系人

北京
DAVID BOITOUT
boitout@gide.com
郭敏
guo@gide.com

上海
DAVID BOITOUT
boitout@gide.com
范建年
fan@gide.com

巴黎
THIERRY DOR
dor@gide.com
STÉPHANE VERNAY
vernay@gide.com
GUILLAUME ROUGIER-BRIERRE
rougier@gide.com
ANTOINE DE LA GATINAIS
gatinais@gide.com
THOMAS URLACHER
urlacher@gide.com

基德律师事务所 | GIDE LOYRETTE NOUEL
北京代表处 | 北京市朝阳区东大桥路 9 号侨福芳草地大厦 B 座 15 层 01-02 单元邮编：100020 | 电话：+86 10 6597 4511 | beijing@gide.com
上海代表处 | 上海市淮海中路 333 号瑞安广场 2008 室邮编：200021 | 电话：+86 215306 8899 | shanghai@gide.com
巴黎 | 22 cours Albert Ier - 75008 Paris - France | 电话：+33 (0)1 40 75 60 00 | info@gide.com