JONES DAY

众达法律评论

2018 年 8 月

法国数据保护当局确认涉及数据控制者安全义务的执法趋势

概要

现状：早在《通用数据保护条例》于 5 月 25 日生效之前，通过加重处罚强制执行安全义务的显著趋势即已呈现。

发展动态：法国数据保护当局（国家信息自由委员会，CNIL）就眼镜连锁店 Optical Center 的电子商务网站安全漏洞问题做出罚款处罚。

展望：《通用数据保护条例》现已生效，数据控制者和处理者尤其需要确保采取稳固完善的安全政策和程序。

2018 年 5 月 7 日，CNIL 做出决定，针对眼镜连锁店 Optical Center 的电子商务网站安全漏洞问题，对该公司处以 250,000 欧元的罚款。虽然这项决定的做出时间要早于《通用数据保护条例》的生效日期，即 5 月 25 日，但这项决定确认了通过加重处罚对安全义务从严执法的趋势。当然这一趋势在 CNIL 今年早些时候针对一家家用电器经销商的处罚决定中也已初见端倪。

尽管该眼镜连锁公司在获知消息后迅速做出反应，对异常现象予以纠正，但 CNIL 仍旧认为公司网站并未采取“最基本的安全措施”，进而认定 Optical Center 违反了保护消费者个人数据的安全责任。

CNIL 曾在该公司的电子商务网站上成功访问到存储在客户账户内的文件，包括客户的发票和订购记录。此外，CNIL 能够访问的文件还包括客户所上传处方中的健康信息以及客户的社保号码。该网站并未设置仅限特定用户访问网站文件的认证系统，因此仅通过修改 url 地址即可访问客户账户。

CNIL 指出，Optical Center 与供应商之间关于新网站功能的沟通依旧不正式。这就导致了作为数据控制者的 Optical Center 对供应商在安全措施等方面做出的行为、矫正措施或建议缺乏了解。

根据 CNIL 在处罚决定中的具体论证，Optical Center 应在其网站上采用如下最低限度的安全措施：

实施访问控制功能，以便公司能够在用户访问个人文件之前核验该用户是否属于认证用户；

开展网站安全审计，包括测试访问控制功能；

与供应商之间就网站开发、纠错和建议（包括安全方面）开展正式化的沟通交流；

在推出新功能或更新之前对将要采用的测试程序予以说明，并通过文件（例如正式验收表）证明已在各种情况下实施遵守测试程序。

这种不给予提前正式通知即发布处罚措施的做法是《法国数据保护法》（由 2016 年 10 月 7 日之《数字共和国法》予以修改）第 45 条新授予 CNIL 的处罚权力。该法条规定，如果违法行为不可在获得正式通知过程中予以矫正，则可未经提前正式通知直接对违法行为做出处罚。《通用数据保护条例》也做出了类似规定。

尽管 Optical Center 做出辩驳称，此次安全违规行为并非有意为之，公司未从中获益，也没有证据表明有除 CNIL 调查组之外的人发现数据泄露，而且亦似乎未给相关数据主体造成伤害，但是，CNIL 还是下令认为将处罚决定公之于众这一额外的处罚应在本案中适用。

随着《通用数据保护条例》项下的处罚力度加剧，上述决定再次表明，数据控制者和处理者必须核实确保已有稳固完善的安全政策和程序投入实施，包括对参与设置数据处理工具的供应商的限制政策和程序。按照《通用数据保护条例》， 5 月 25 日之后发生的违反安全义务的行为的罚款金额最高为 1,000 万欧元或违法公司在上一年度全球年营业额的百分之二。

关键要点

鉴于近期的趋势以及《通用数据保护条例》项下的监管力度增加，各公司需确保拥有稳固完善的消费者数据保护方案和程序。违反安全义务会被处以高额罚款。

本文是原版英文众达法律评论的翻译。欲阅读全文，请点击原文。

联系律师

黄敏琪
上海
+86.21.2201.8092
ahuang@jonesday.com

唐承慧
北京
+86.10.5866.1183
jtang@jonesday.com

袁黎明
上海
+86.21.2201.8106
lyuan@jonesday.com