猎豹移动DPIA系统开源

猎豹安全中心 小豹讲安全 今天

01 背景

近些年来，随着大数据技术的的广泛应用与普及，个人数据滥用、信息泄露等较为安全事件层出不穷，用户个人隐私以及企业资产、国家安全面临着巨大挑战，个人数据安全受到了空前的重视，个人数据的安全发展需要社会的监管与企业的自律完善。目前，针对个人数据保护，各国已经相继出台了大量法规与标准，包括2018年5月正式生效的GDPR，2017年6月1日正式生效的我国《网络安全法》，2018年5月1日正式生效的《GB/T 35273《信息安全技术个人信息安全规范》，以及已经制定的《数据安全管理办法》等

作为一家同时为国内外用户提供服务的企业，毫无疑问隐私安全保护和合规在猎豹公司充为重要。为了快速、有效地响应国内外隐私合规要求，保护所服务用户的合法权益，猎豹移动公司设计并研发了DPIA系统。

02 DPIA系统

DPIA系统为猎豹移动公司内部使用系统，旨在帮助公司落实GDPR、GB/T 35273—2017.信息安全技术个人信息安全规范等合规要求，规避法律风险，降低信息安全风险。

DPIA系统可以应用到服务产品研发、运营等不同阶段。在产品研发阶段，可使用DPIA系统指导产品设计的理念工作，帮助进行个人数据收集合规规划与指引，防止收集非必要或违法律禁止收集的信息，同时指导个人数据安全保护措施的设计与落实；在产品上线阶段，可使用DPIA系统评估个人数据隐私合规情况；运营阶段，如发生个人数据安全事件，可快速对接到产品的隐私负责人，并根据前期的评估工作记录进行追溯，不断迭代流程与产品。

DPIA系统定位为一款灵活且可扩展的工具，在不断且快速的迭代过程中，目前系统已实现的模块包括：

- 产品基本信息
- 个人数据影响度评估
- 个人数据检查 checklis

产品基本信息

产品基本信息包括产品的名称、功能、产品隐私负责人以及产品隐私专员信息。通过产品基本信息的识别，可以快速定位到产品责任人，初步判断产品可能需要收集、使用、存储的个人数据，是数据收集合理性判断以及不合规、信息安全事件处理的基础。

个人数据影响度评估

1）检查理点字段中是否存在禁止收集的个人数据

公司已识别并规定出高风险敏感数据字段，包括禁止收集或禁止处理的数据字段。高风险敏感数据字段默认禁止收集，无特殊情况，收集此信息皆不合规，不能通过合规评审，影响产品上线。

2）检查理点字段中包含的个人数据并进行影响度评估

系统中已识别出可能会涉及到个人数据，可根据产品收集个人数据的情况进行选择。并对每一个选择的个人数据字段分别进行合规评估，评估的内容来源于GDPR、GB/T 35273—2017.信息安全技术个人信息安全规范的合规要求，PS：已识别的个人数据是依据猎豹移动部分产品整理，针对不同的应用产品会进行相应调整。

个人数据检查 checklis

除对收集的每个个人数据进行评估之外，还需对其他安全合规要求进行差距分析，确保个人数据保护工作落实到位。

03 结束语

系统仍在不断迭代与完善，小豹们也在个人数据安全合规的路上不断摸索和创新，希望DPIA系统的简单介绍可以给更多隐私安全建设工作者提供思路，也希望大家提出宝贵的意见，为隐私合规增加一份力量。

代码传送门：https://github.com/cmcmsec/dpia

猎豹安全中心技术分享频道

1. 海量日志分析的预处理
2. OSSEC-Execd功能模块分析
3. 通过流量快速识别域名信息
4. 从android源码看脱壳
5. Ossec-Agentd模块分析