

猎豹移动DPIA系统开源

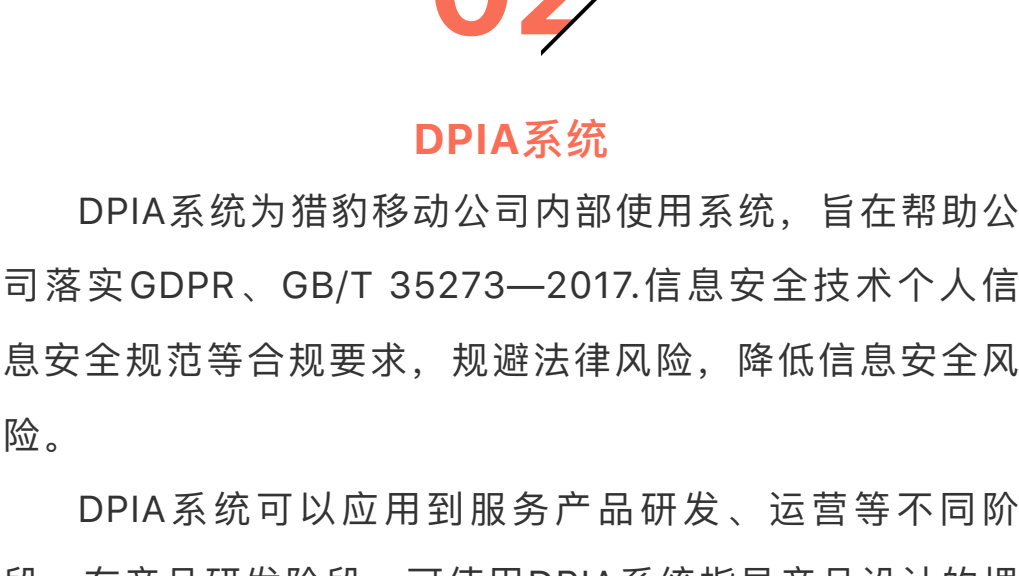
猎豹安全中心 小豹讲安全 今天



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、信息泄露导致的安全事件层出不穷，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尤为重要。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埋点工作，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。

产品基本信息 - [添加产品](#)

产品名称*

产品介绍*

产品隐私负责人（默认一级部门负责人）*

产品隐私专员（默认产品经理）*

个人数据影响度评估

1) 检查埋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。

产品个人数据影响度评估 - [个人数据定义](#)

1. 以下数据不可收集，若收集请选择

☐ 支付密码 ☐ 面部特征数据 ☐ 声音特征数据 ☐ 其它生物特征

2. 以下数据禁止处理，若处理请选择

☐ 种族民族出身 ☐ 政治观点 ☐ 宗教信仰 ☐ 工会会员资格

☐ 生物学数据（基因数据、个人生物识别信息） ☐ 健康数据 ☐ 性取向性生活方式

2) 检查埋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。

3. 以下数据为个人数据，请作出影响度评估

<input type="checkbox"/> 手机的品牌、型号、分辨率、CPU型号、内存大小等	<input type="checkbox"/> Mac address、IMEI、智能硬件的硬件序列号、aid、推送ID（REGID）、	<input type="checkbox"/> 用户应用使用情况（记录）
<input type="checkbox"/> 用户设备中已经安装的应用包名列表	<input type="checkbox"/> 社交功能产品、第三方社交账号：FB、Google、微信、微博等	<input type="checkbox"/> 经纬度、GPS
<input type="checkbox"/> 邮箱	<input type="checkbox"/> 用户名	<input type="checkbox"/> 登录密码
<input type="checkbox"/> 姓名	<input type="checkbox"/> 手机号	<input type="checkbox"/> 电话号码
<input type="checkbox"/> 地址	<input type="checkbox"/> 身份证号	<input type="checkbox"/> 指纹、高风险
<input type="checkbox"/> 面部肖像数据、高风险	<input type="checkbox"/> 安全功能产品、提供保险服务：上险的用户保单信息和保单号	

数据处理过程	数据处理内容	数据处理要求	评估结果
获取关注点	数据收集必要性，是否是业务所需要	如业务所需，可收集，并隐私政策中说明及征得用户同意	符合
	获取来源		Nothing selected
使用关注点	使用该数据的显示方式	不登录也可见	符合
	是否进行用户数据画像		
	该字段所关联的操作系统日志是否保留6个月,主要是指该字段自主生成的相关日志。例如用户登录、删除、下线的记录	处理日志保留6个月	符合
传输关注点	该字段是否向第三方进行传输，传输方式是否加密	不可向第三方传输	符合
	该字段是否向内部传输，传输方式是否加密	加密传输	符合
存储关注点	用户数据在服务器内的呈现形式	用户授权，系统自动生成	符合
	该数据是否存储在公司服务器，还是通过系统接口调用	可服务器端存储	符合
	存储的数据的是否采用加密算法，是否明文，还是不存储	可明文存储（无法推导自然人）	符合
	关联该字段的服务器的日志记录，主要是指公司后台对于该字段的运维操作日志。例如后台运维人员检查该用户一些账户行为所产生的记录	N/A	符合
删除关注点	字段删除（一般关联账户一体化删除）	完全删除，不可恢复，并通知第三方删除。	符合
埋点字段	<input type="text" value="半角分号(;)分隔"/>		
备注信息	<input type="text" value="不超过250字"/>		

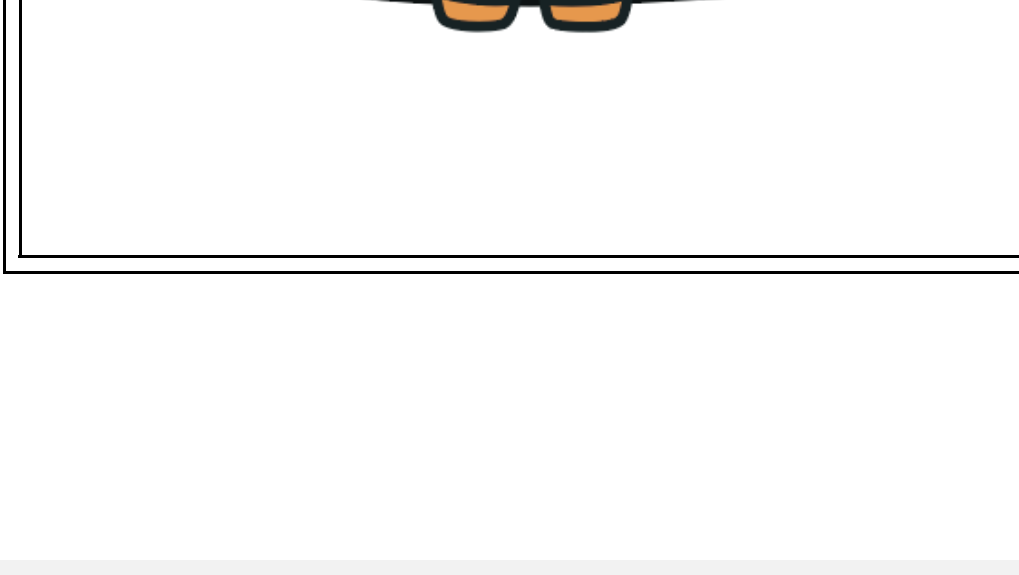
个人数据检查 checklis

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。

产品个人数据检查checklist - [完成第二部分产品个人数据影响度评估](#)

猎豹移动个人数据字段评估

数据传输*	检查是否使用HTTPS进行传输	符合
后台数据库管理*	最后访问数据库敏感字段加密	符合
用户同意*	收集敏感个人信息，用户详细功能是否在记录用户同意过程	符合
隐私策略*	产品隐私策略是否更新在最新产品中，内容是否包含产品功能和数据进行了更新	符合
投诉反馈机制*	用户投诉处理流程是否建立，相关管户人员是否接受了培训	符合
第三方使用个人数据*	是否有第三方使用本产品的个人数据	未使用
checker备注信息	为遗漏的问题在此处填写说明信息	
数据跨境*		Nothing selected
用户所在国家*		Nothing selected
数据保存位置（国家）*		Nothing selected



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/cmcsec/dpia>

猎豹安全中心技术分享频道

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

长按下方二维码关注我们

