YF-S-B01-D0008

上海有孚网络股份有限公司

隐私影响分析（PIA）报告

(V1.0)

-2020.9.25

一、概况

《隐私影响评估标准》(ISO/IEC 29134）是目前欧美流行的隐私评估标准，也得到了 ISO29151、ISO27701、GDPR 等标准的广泛认同。

2020 年 1 月，上海有孚网络股份有限公司（以下简称“公司”）ISO27018 项目团队开始依照 ISO29134 标准开展了个人隐私影响分析（Privacy Impact Analysis）活动，又称为个人信息保护风险评估活动。随后，在疫情基本稳定后，项目团队于 2020 年 5 月份底完成个人信息（PII）资产的收集，并于 6 月上旬完成了全部的个人隐私影响分析（个人信息风险评估）活动，并编制本报告初稿。2020 年 9 月，在风险处置和残留风险评价完成后，本报告定稿并通过公司管理层审批。

二、评估范围

公司 2020 年 PIA 活动按照公司组织机构进行，包括业务单元、行政单元、财务单元、技术单元、基建单元。所涉及个人信息主体，既包括客户、访客，也包括公司内部员工。

三、评估方法

从表面上来看，个人信息也具备保密性（C）、完整性（I）、可用性（A）三大特征，所以可适用传统信息安全风险评估的理念和方法，使用资产、威胁、脆弱性分析的方式进行评估,这些方法已经非常成熟并获得了很高的认可度和广泛的应用,在 2019 年 ISO27018 体系初步建立阶段也是将个人信息视为 ISO27001

数据资产的一种子类型完成了风险评估。但是，除个人信息自身 CIA 安全因素外，个人信息处理行为也会同样带来风险，个人信息处理行为对用户权益产生的影响，比如个人信息的不当处理可能危害个人人身和财产安全（例如账户被盗、遭受诈骗、被勒索恐吓、限制自由等）、损害个人名誉和身心健康（例如被公开不愿为人知的事实、被频繁骚扰、被监视追踪等）、导致歧视性待遇、影响个人自主决定权（例如被强迫执行不愿执行的操作、无法更正错误上传的个人信息、无法选择推送广告的种类、被蓄意推送影响个人价值观判断的资讯）等，这些影响层面和传统信息安全风险评估对资产、组织利益的关注完全不同。因此，个人信息安全风险评估与传统信息安全风险评估方法应当有所不同。

《隐私影响评估标准》（ISO/IEC 29134）既套用了传统风险评估中威胁、脆弱性等概念，又提及合规性评估等方法兼顾个人信息处理行为，是目前欧美流行的隐私评估标准，也得到了 ISO29151、ISO27701、GDPR 等标准的广泛认同。项目团队经过全面分析，发现 ISO29134 标准更倾向于评估个人信息因传统安全问题带来的风险，如保密性、完整性、可用性受到破坏，对个人权益的影响考虑偏少。因此，项目团队进行了借鉴和改进，显著增加了对于个人信息处理的合规性方面的评估内容。具体体现在：

（一）在个人信息资产（PII）梳理和识别时，不仅关注客户方的个人信息，也考虑潜在客户、访客以及公司员工的个人信息，确保资产识别的全面性。

（二）在进行个人信息资产（PII）资产的重要性判定时，考虑到如果个人信息被破坏（例如泄露、篡改、损毁），不仅个人信息主体（自然人）的权益将受到影响和损害，而且组织的权益（例如公司各类信息资产的机密性、完整性和可用性以及品牌声誉）也可能受到影响。因此，对个人信息主体的影响和损害可划分为四个纬度：个人自主决定权、引发差别性待遇、个人名誉受损或遭受精神压力、个人财产受损，根据影响和损害严重程度的不同，划分为五个等级，对应取值范围从“5”到“1”（5 为最高，1 为最低）；而对于对组织权益的损害也考虑四个方面：品牌声誉、机密性、完整性、可用性等。根据损害程度的不同划分为五个等级，对应取值范围从“5”到“1”（5 为最高，1 为最低）。最终，综合

考虑个人信息被破坏后对个人信息主体及组织的影响值，取最大值后，确定个人信息资产的重要性。

（三）在识别个人信息保护所面临的威胁和脆弱性时，兼顾目前 ISO27005 等风险评估标准采用的资产价值、弱点的严重程度、威胁的可能性等要素，基于公司各部门业务流程和企业运营管理中对个人信息处理的具体场景，从个人信息全生命周期角度对个人信息处理活动进行全面的梳理和识别。其中，个人信息处理活动的识别内容包括个人信息收集、存储、使用、对外提供、废弃环节涉及的目的、处理场景、处理方式，以及个人信息处理过程涉及的资源和相关方（如策略和规程、合同和协议、内部信息系统、个人信息处理者、第三方、交易平台经营者、外部服务供应商、云服务商等）。

四、评估内容

（一）个人信息（PII）资产识别

通过公司个人信息（PII）资产的全面识别、梳理和重要性判定，最终确定个人信息（PII）资产总计 29 项，其中需要进行风险评估的重要个人信息资产为 18 项。如下：

资产识别与评估表 -- 个人信息(PII)资产

序	类别	说明	涉及部门及第三方单位	个人信息主体权益				组织权益				资产价	是否重要资
1	个人生物识别信息	脸部图像、脸部视频、指纹、掌纹、虹膜等	IT部门（考勤/门禁系统）、人力资源部	3	3	3	3	4	4	3	3	4	是
2	个人健康医疗信息	个人健康医疗信息PHI（体检报告等）、个人医疗信息	人力资源部门体检外包单位	3	4	4	3	4	4	3	3	4	是
3	个人金融信息	个人工资奖金收入（薪酬）、个人五险一金数额及缴费记录等	人力资源部、外包人事代理单位	3	3	4	4	4	4	3	3	4	是
5	重要岗位个人普通信息	姓名、性别、工作单位、工种、年龄等	人力资源部、人事代理外包机构等	2	3	3	2	4	3	3	3	4	是
7	普通员工个人敏感信息	个人简历（电话、工作学习经历、家庭住址、家庭成员信息等）；个人通信录、好友联系方式、定位信息和轨迹、电话通讯记录、网站浏览内容、网络行为记录、信用记录、财产信息、住宿信息、婚史等	个人使用、APP服务提供商授权使用（微信、支付宝、导航软件、云备份等）	3	3	4	3	4	4	3	3	4	是
8	重要岗位个人敏感信息	个人简历（电话、工作学习经历、家庭住址、家庭成员信息等）；个人通信录、好友联系方式、定位信息和轨迹、电话通讯记录、网站浏览内容、网络行为记录、信用记录、财产信息、住宿信息、婚史等	个人使用、APP服务提供商授权使用（微信、支付宝、导航软件、云备份等）	3	4	4	3	4	4	3	3	4	是
9	敏感岗位个人敏感信息	个人简历（电话、工作学习经历、家庭住址、家庭成员信息等）；个人通信录、好友联系方式、定位信息和轨迹、电话通讯记录、网站浏览内容、网络行为记录、信用记录、财产信息、住宿信息、婚史等	个人使用、APP服务提供商授权使用（微信、支付宝、导航软件、云备份等）	3	4	4	3	4	4	3	3	4	是
14	潜在客户个人敏感信息	客户的个人电话、公司名称、家庭住址、个人联系地址、QQ或微信号等	销售部门、市场部（营销推广活动）、IT部门（BI）	2	2	3	2	4	4	3	2	4	是

资产识别与评估表 -- 个人信息(PII)资产

序号	类别	说明	涉及部门及第三方单位	个人信息主体权益				组织权益				资产价值	是否重要资产
16	普通客户个人敏感信息	客户购买的产品或服务的名称、类别、数量、价格等；客户个人的QQ或微信号等	销售部门、市场部（营销推广活动）、IT部门（BI）	2	2	3	2	4	4	3	2	4	是
17	重要客户个人敏感信息	客户购买的产品或服务的名称、类别、数量、价格等；客户个人的QQ或微信号等	销售部门、市场部（营销推广活动）、IT部门（BI）	2	2	4	3	4	4	3	2	4	是
18	默认收集数据	用户访问公司网站或使用业务服务时驻留客户端的Cookie等小型数据文件；用户访问公司网站或使用业务服务时默认后台收集的客户端的IP/MAC等标识信息	IT部门	4	3	2	3	4	3	3	3	4	是
19	业务开通数据-告知	业务开通时，向客户展示的因提供服务必须收集个人信息的告知文字条款或其他形式的说明（最新版本及历史版本），例如《用户开通协议》或服务协议	业务部门、IT部门	4	4	3	3	3	1	4	3	4	是
20	业务开通数据-征求同意	向客户展示的“征求同意”的文字条款或其他形式（最新版本和历史版本）	业务部门	4	4	3	3	3	1	4	3	4	是
21	业务开通数据-同意证据	客户“明示同意”或“默认同意”产生的相应证据和后台日志等记录	业务部门、IT部门	4	4	3	3	3	1	4	3	4	是
24	业务变更数据-同意证据	客户对业务变更时出示的征求同意，“明示同意”、“默认同意”或“拒绝”而产生的相应证据和后台日志等记录	IT部门	4	3	2	2	4	3	3	2	4	是
27	业务关闭数据-同意证据	客户“明示同意”、“默认同意”或“拒绝”而产生的相应证据和后台日志等记录	IT部门	4	3	2	2	4	3	3	2	4	是
28	个人权益服务数据	用户提出个人信息变更权、删除权等相关权益时，公司各部门的处理记录	IT部门、业务部门、数据加工处理部门	4	3	3	2	4	3	3	3	4	是
29	客户投诉申诉信息	客户围绕产品或服务中侵犯个人信息时提出的申述或投诉、提出的赔偿/补偿要求等，以及对应的投诉处理记录	客户服务部门、IT部门	2	2	3	3	4	3	3	3	4	是

此外，在 ISO27001 标准中，公司信息资产划分为六大类，包括：物理资产、数据资产、文档资产、软件资产、服务资产、人员资产。以上识别的全部个人信息（PII）资产均归属为数据资产，以电子形式或纸质形式存在与公司的业务系统及文档资料。

（二）风险评价

通过对 18 项重要个人信息资产开展风险评价，总计识别风险 35 项，其中“很高风险”0 项，“高”风险 0 项，“中”风险 3 项，“低”风险 32 项。

中风险项（编号 RDF-1、RDF-5 和 RDF-9）的具体内容如下

风险评价表(个人信息PII)

返回目录

风险编号	资产名称	威胁名称	弱点名称	风险描述	风险Owner	风险因素			风险值
						资产价值	威胁值	弱点值	
RDF-1	个人生物识别信息	非授权访问/使用	10V01 缺乏有效的操作管理程序	公司考勤系统采集了指纹等员工个人信息，IT部门在维护考勤系统时可能对这些个人信息非授权访问或私自拷贝，导致个人生物识别信息的泄露。	IT负责人	4	3	3	36
RDF-5	普通员工个人敏感信息	数据泄露	08V11 缺乏信息安全意识	员工个人安全意识不足，使用手机APP服务时泄露住宿、网络行为记录等个人敏感信息，导致个人名誉严重受损和巨大精神压力，严重影响个人权益。	员工个人	4	3	4	48
RDF-9	隐私报告相关材料	未及时发布	05V04 隐私报告等材料内容不完整	截止2020年5月底，公司尚未按照隐私保护相关标准的要求及时发布或更新《隐私报告》、《PIA报告》等材料，或报告内容缺失以致违反了国家相关法规、政策和标准的要求，则会导致公司存在个人隐私保护不合规的风险。	标准化中心负责人	4	3	4	48

（三）风险处置

风险处置表(个人信息PII)

返回目录

风险编号	风险描述	风险Owner	风险因素			风险值	处理策略	控制项
			资产价值	威胁值	弱点值			建议控制措施
RDF-1	公司考勤系统采集了指纹等员工个人信息，IT部门在维护考勤系统时可能对这些个人信息非授权访问或私自拷贝，导致个人生物识别信息的泄露。	IT负责人	4	3	3	36	接受风险	公司已建立ISO27001\ISO27018等管理体系，保持现有控制措施即可。该风险可接受。
RDF-5	员工个人安全意识不足，使用手机APP服务时泄露住宿、网络行为记录等个人敏感信息，导致个人名誉严重受损和巨大精神压力，严重影响个人权益。	员工个人	4	3	4	48	消减风险	在开展ISO27001员工信息安全意识培训时，增加有关个人敏感信息保护的介绍，谨慎、妥善使用手机APP应用。 责任人：李慧 ，完成时间：2020年9月30日
RDF-9	截止2020年5月底，公司尚未按照隐私保护相关标准的要求及时发布或更新《隐私报告》、《PIA报告》等材料，或报告内容缺失以致违反了国家相关法规、政策和标准的要求，则会导致公司存在个人隐私保护不合规的风险。	标准化中心负责人	4	3	4	48	消减风险	在完成PIA隐私影响分析活动后，编制《PIA报告（2020年度）》、《隐私报告（2020年度）》并在7月底之前完成发布。 责任人：李慧 ，完成时间：2020年9月30日

（四）残留风险评价

残留风险评估表(个人信息PII)

风险编号	风险描述	风险Owner	风险值	处理策略	控制项	控制之后的风险因素		控制之后的风险值	残余风险说明
					建议控制措施	可能性	严重性		
RDF-1	公司考勤系统采集了指纹等员工个人信息，IT部门在维护考勤系统时可能对这些个人信息非授权访问或私自拷贝，导致个人生物识别信息的泄露。	IT负责人	36	接受风险	公司已建立ISO27001\ISO27018等管理体系，保持现有控制措施即可。该风险可接受。				
RDF-5	员工个人安全意识不足，使用手机APP服务时泄露住宿、网络行为记录等个人敏感信息，导致个人名誉严重受损和巨大精神压力，严重影响个人权益。	员工个人	48	消减风险	在开展ISO27001员工信息安全意识培训时，增加有关个人敏感信息保护的介绍，谨慎、妥善使用手机APP应用。 责任人：李慧 ，完成时间：2020年9月30日	2	4	32	2020年9月25日，标准化中心对个人信息风险处置后的残留风险进行了评价，确认李慧已完成培训并保留培训记录。该项风险已降为低风险，残留风险可接受。
RDF-9	截止2020年5月底，公司尚未按照隐私保护相关标准的要求及时发布或更新《隐私报告》、《PIA报告》等材料，或报告内容缺失以致违反了国家相关法规、政策和标准的要求，则会导致公司存在个人隐私保护不合规的风险。	标准化中心负责人	48	消减风险	在完成PIA隐私影响分析活动后，编制《PIA报告（2020年度）》、《隐私报告（2020年度）》并在9月底之前完成发布。 责任人：李慧 ，完成时间：2020年9月30日	3	2	24	2020年9月25日，标准化中心对个人信息风险处置后的残留风险进行了评价，确认《PIA报告》《隐私报告》已发布。该项风险已降为低风险，残留风险可接受。

有孚网络隐私报告（V1.0 版）

-（20200630 发布）

一、《隐私策略》的发布

随着社会的进步和科技的发展，用户个人信息安全问题日渐凸显。过度收集个人信息、对个人信息进行二次开发利用以及个人信息交易等严重侵犯用户隐私的现象时有发生，诉诸法律诉讼的案件和官司缠身的网络公司不胜枚举。2016 年国家《网络安全法》的颁布，不仅对网络运营者及其他主体保护用户个人信息的责任做出了更具体严格的规定，也赋予了网络用户更广泛的的个人信息权，对我国加强网络个人信息的保护具有重要的意义

有孚网络高度重视个人信息(PII)保护工作，面对〝如何保护用户信息、采用何种方式保护〞的难题，公司积极遵循国家法规政策的要求，及时在公司网站首页发布了《隐私策略》。该隐私策略覆盖了策略范围、收集个人信息的业务功能列表、用户个人信息的更正/删除权利等内容。

随着国标《个人信息安全规范》(GB/T35273-2018）的颁布实施，有孚网络于 2019 年进行了《隐私策略》版本的修订更新，细化了交互式功能设计、用户投诉/申述渠道 (例如隐私服务热线电话、服务邮箱）等内容，使公司个人信息保护工作始终符合国家各项法规政策的最新要求。

二、ISO27018:2014 体系建设和认证活动

有孚网络早在 2015 年就已经通过 ISO27001:2013 信息安全管理体系认证，对客户及员工个人信息提供安全保护。随着社会和科技的进步，公司依照《ISO27018:2014 公有云个人信息处理者个人信息保护》国际标准的要求于 2019 年 3 月正式启动了个人信息保护体系的建设工作，使个人信息保护工作更加标准化、体系化。

在组织建设方面，有孚网络将个人信息保护职责落实到公司现有的信息安全组织架构中，清晰定义了信息安全和个人信息（PII）

保护的“决策领导、管理审计、执行”三层组织架构，明确了执行委员会、管理小组和各部门的职责，使得个人信息保护工作的开展落实了人员和职责。同时，围绕 ISO27018 的落地要求，对本公司的信息安全方针和安全目标、策略等根据进行调整，增加了个人信息(PII)保护方面的指标。

在制度文件方面，有孚网络分为两个阶段推进。第二阶段是在 2019 年 4 月份至 5 月底，标准化中心主导开展了 ISO27001&ISO27018 体系文件制度的修订编写工作，在现有 ISO27001 体系文件基础上，主要是按照 ISO27018 标准的新增要求，修订了个人信息保护方面的目标、策略、SOA 等体系一级文件，新增了《个人信息(PII)保护管理程序》等二级文件；第二阶段是在 6 月中旬至 9 月底，结合风险处置计划和公司其他项目的推进（CSA-STAR、等保三级测评等），结合 ISO27018 标准、网络安全等级保护 V2.0 等国家最新法律法规和标准的要求，更新了隐私策略、采购合同、服务级别协议 SLA、信息安全事件管理程序、业务连续性管理程序等关键文件，并更新了相应的表单模板，最终将个人信息保护具体要求全部纳入公司的日常工作内容中并落实在公司现有的体系制度和流程中，于 2019 年 7 月 1 日正式批量发布了 ISO27001&ISO27018 体系文件制度 V2 版本，有效地避免 ISO27018 成为孤立运行的一套体系。

在活动开展方面，有孚网络于 2019 年 9 月初实施了 ISO27018 体系内部审核活动，以验证公司体系文件实施后的信息安全活动的符合性和有效性，并重点针对高风险制定的控制措施进行了验证。内审活动总计发现 3 个轻微不符合项，0 个严重不符合项和 0 个观察项， 表明体系建设运行整体平稳。随后，2019 年 10 月初进行了体系有效性全面测量活动，对体系的有效性进行了全面的测量、分析和评估，表明通过前期的体系文件编写和宣贯、风险评估和处置、内审及其纠正预防整改工作，公司信息安全和个人信息保护的隐患风险已经基本得到有效控制。最终，10 月中旬召开了管理评审会议

公司管理层对于 ISO27001&ISO27018&ISO20000 体系建设各项活动的组织和工作成绩表示认可，包括信息资产梳理情况、风险评估的最新情况、风险处置进展情况和当前残留风险、体系框架设计和管理制度文件发布后的修订更新情况、文件制度培训活动、内部审核活动及整改进展等等。从整体来看，虽然还存在需要 PDCA 不断改进的方面，但我公司的信息安全和个人信息（PII）保护管理体系、信息技术服务管理体系基本上是适宜的、完备的和有效的。

2019 年 10 月底，公司顺利通过国际权威认证机构 DNV 的现场审核,并获得了 ISO27018 证书，充分表明公司现有体系文件和活动开展已经达到 ISO27018:2014 标准的要求,各项管理制度和流程符合本公司实际情况，具有可操作性。

三、个人信息影响分析（PIA）活动

通过 ISO27018 认证之后，通过 ISO27018 认证之后，有孚网络并未止步不前。随着对于个人信息其他标准（例如 ISO27701:2019、ISO29134、ISO29100、ISO29151、欧盟 GDPR、GB/T35273 个人信息安全评估）视野的拓展和实践中的深入，有孚网络进一步加大了个人信息保护工作的力度，有孚网络从个人信息保护的基础性工作-〝个人信息风险评估〞着手，参照 ISO29134 标准，进行了隐私影响评估活动（PIA，Privacy Impact Analysis）的策划。

从表面上来看，个人信息也具备保密性（C）、完整性（I）、可用性（A）三大特征，所以可适用传统信息安全风险评估的理念和方法，使用资产、威胁、脆弱性分析的方式进行评估,这些方法已经非常成熟并获得了很高的认可度和广泛的应用,在 2019 年 ISO27018 体系初步建立阶段也是将个人信息视为 ISO27001 数据资产的一种子类型完成了风险评估。但是，除个人信息自身 CIA 安全因素外，个人信息处理行为也会同样带来风险，个人信息处理行为对用户权益产生的影响，比如个人信息的不当处理可能危害个人人身和财产安全（例如账户被盗、遭受诈骗、被勒索恐吓、限制自由等）、损害

个人名誉和身心健康（例如被公开不愿为人知的事实、被频繁骚扰、被监视追踪等）、导致歧视性待遇、影响个人自主决定权（例如被强迫执行不愿执行的操作、无法更正错误上传的个人信息、无法选择推送广告的种类、被蓄意推送影响个人价值观判断的资讯）等，这些影响层面和传统信息安全风险评估对资产、组织利益的关注完全不同。因此，个人信息安全风险评估与传统信息安全风险评估方法应当有所不同。

《隐私影响评估标准》(ISO/IEC 29134）既套用了传统风险评估中威胁、脆弱性等概念，又提及合规性评估等方法兼顾个人信息处理行为，是目前欧美流行的隐私评估标准，也得到了 ISO29151、ISO27701、GDPR 等标准的广泛认同。有孚网络经过全面分析，发现 ISO29134 标准更倾向于评估个人信息因传统安全问题带来的风险，如保密性、完整性、可用性受到破坏，对个人权益的影响考虑偏少。因此，有孚网络进行了借鉴和改进，显著增加了对于个人信息处理的合规性方面的评估内容。

2020 年 1 月，有孚网络启动了 PIA 活动，开始进行个人信息资产的全面梳理和个人信息保护范围的界定。随后，在疫情基本稳定后，2020 年 6 月有孚网络完成完成了个人隐私影响分析（个人信息风险评估）活动，并编制了相应的《个人隐私影响分析（PIA）报告》，明确了评估范围、评估方法、评估的发现（扼要介绍）、评估结论、风险处置计划概述、对个人信息保护主体应采取措施的建议等内容。

通过开展基于 ISO/IEC29134 隐私影响评估标准的 PIA 活动，有孚网络进一步明确了业务流程中个人信息处理过程的合规性，更加关注对客户及员工个人信息主体的名誉、身心健康、人身和财产安全、歧视性待遇等个人主体的权利保障，从而保障了业务发展与个人信息保护工作的〝同步规划、同步实施、同步发展〞。

四、强化云安全建设活动，开展 ISO27017:2015 云安全国际标准认证

2020 年下半年，有孚网络继续依托国际标准和最佳实践，强化公司云计算平台的安全建设，为个人敏感信息的保护和客户数据的安全提供保障。