编号：CR-MS0502

隐私信息管理体系认证规则

（H/2）

查阅全文请联系北京海德国际认证有限公司
联系电话：010-84905056，010-65817800
邮箱地址：common@hicchina.com.cn

2023-03-01 发布/实施　　2026-05-29 修订

北京海德国际认证有限公司发布

隐私信息管理体系认证规则

1 适用范围

本实施规则用于规范北京海德国际认证有限 HIC（以下简称“HIC”）开展隐私信息管理体系（PIMS）认证活动。

2 认证依据

ISO/IEC 27701:2025《信息安全 网络安全和隐私保护 隐私信息管理体系 要求和指南》

3 术语和定义

3.1 个人可识别信息（PII）

指满足以下条件的信息：a) 可用于建立该信息与所涉及自然人之间的关联；或 b) 直接或间接与某自然人相关联（或可能相关联）。

注释：定义中的“自然人”即“PII 主体”。判断某主体是否可识别，取决于隐私利益相关方（持有数据者）或其他任何方能否合理地建立该组 PII 与自然人之间的关联。

3.2 个人可识别信息主体（PII 主体）

即 PII 所涉及的自然人。

3.3 个人可识别信息控制者（PII 控制者）

指决定 PII 处理目的与方式的隐私利益相关方（或隐私利益相关者），但不包括将数据用于个人目的的自然人。

注释：PII 控制者有时会指示其他方（如 PII 处理者）代其处理 PII，但处理责任仍由控制者承担。

3.4 个人可识别信息处理者（PII 处理者）

指根据 PII 控制者的指示，代其处理 PII 的隐私利益相关方。

3.5 隐私影响评估

指在组织更广泛的风险管理框架内，对 PII 处理过程中潜在隐私影响进行识别、分析、评价、咨询、沟通及处理规划的整体风险评估。

3.6 个人可识别信息的处理

指对 PII 执行的一项或一组操作。

注释：PII 处理操作的示例包括（但不限于）收集、存储、更改、检索、查阅、披露、匿名化、假名化、传播，或通过其他方式提供、删除或销毁 PII。