一、用户中心

**默认只提供脱敏的数据：**

**访问接口对请求进行认证、鉴权：**

1. **代码中原来接口**只返回脱敏的数据；

2. **代码中原来接口**有AppId和SecureKey校验。

**禁止默认以明文或批量导出数据：**

1. **系统开发负责人**签字确认。

**每次只能获取单条数据：**

**通过白名单方式进行授权：**

**登记并审核业务系统后授予其唯一访问Key：**

1. **代码中新的接口**只能通过参数Uid获取用户敏感信息；

2. **代码中新的接口**参数SecureKey和AppId能够对应到每个业务系统，对应不到的应删除；

3. **代码中新的接口**参数SecureKey只授权给了明确需要明文敏感数据的业务系统。

**获取敏感信息的请求，需记录获取日志，实现审计：**

1. **代码中新的接口**测试获取用户敏感数据时能够记录下审计的日志；

2. **代码中新的接口**日志信息包括：业务系统标识、访问时间、API请求信息、API响应状态。

**日志每周备份一次，留存6个月：**

1. **运维或开发代码**检查日志备份的代码实现，保存6个月不删除。

二、业务系统

**本地未保存获取到的用户敏感信息：**

1. **系统开发负责人**签字确认。

**系统认证和鉴权机制完善：**

**满足用户信息使用最小化：**

**系统的用户可以映射到员工：**

1. **前后端业务系统**认证和鉴权机制完善；

2. **前后端业务系统**页面是否存在滥用用户敏感数据直接展示的行为；

3. **前后端业务系统**不存在公用账户，全部账户能够唯一定位到使用者本人。

**有用户中心授予的API访问Key：**

**系统获取敏感数据日志记录完善、具有日志审计功能：**

1. **代码调用新接口**中AppId和SecureKey是唯一的；

2. **代码调用新接口**测试获取用户敏感数据时能够记录下审计的日志；

3. **代码调用新接口**日志信息包括：业务用户标识、访问时间、API请求信息、API响应状态。

**日志每周备份一次、留存6个月：**

1. **运维或开发代码**检查日志备份的代码实现，保存6个月不删除。

**之前获取的敏感信息已删除：**

**本地存储中不包含用户敏感信息：**

**无法通过API获取到用户敏感数据：**

1. **系统开发负责人**签字确认。