**迎检要求**

1. 迎检备查清单
2. 数据安全管理制度：各单位是否建立了完善的数据安全管理制度，并是否进行了定期的自查和修订。
3. 落实数据安全相关管理制度的记录，包括但不限于数据安全分类分级管理规范及数据资产清单、重要数据目录。
4. 数据安全资产清单，包括不限于全量业务（标注新上线业务）和平台系统清单、企业数据处理活动平台系统的用户账号安全管理记录、数据处理账号操作审批记录、平台系统权限分配表。
5. 全量业务或系统数据分类分级清单，全量合作方业务清单；所有涉及数据共享的业务和系统清单。
6. 数据安全岗位人员名单；重要数据处理岗位登记表、重要数据处理登记、审批记录及审计报告等。
7. 安全审计和监测：是否建立了数据安全审计和监测机制，及时发现并应对异常行为。
8. 数据生命周期管理执行落实文件、记录等。
9. 企业内部数据安全事件应急响应机制和预案、应急演练记录，数据安全处置和报告记录,能够迅速应对数据安全事件。
10. 迎检人员
11. 企业需要指定明确的检查接口人。
12. 检查需各业务系统数据操作相关人员协助（包括业务操作员、审计人员、运维人员等）；请提前准备数据安全风险评估过程中所涉及的各个系统环境等。

三、检查要求

1. 各相关单位需积极配合检查人员的工作，提供相关文件和数据。
2. 检查期间，如发现数据安全问题，需立即采取措施加以整改。
3. 针对检查中发现的数据安全隐患和问题，各单位需制定整改计划，确保问题得到彻底解决。
4. 检查结束后，各单位需提交书面整改报告，详细描述问题的整改情况和措施。