- 银行@sh用户数据正在暗网贱卖
- 数据安全合规基准---如何在全生命周期保障数据安全?

一、通用性评估要点

1.【组织机构】

（1）明确企业数据安全管理责任部门，负责牵头承担企业内部数据安全管理工作，包括但不限于制定数据安全管理整体方针策略，协调建立数据安全技术保障措施，牵头做好数据安全事件应急处置、数据安全合规性评估、教育培训等工作。

（2）明确数据安全管理责任部门与各项工作执行落实部门责任分工界面，建立数据安全管理制度执行落实情况监督检查和考核问责制度。

2.【人员保障】

在数据安全管理责任部门和相关工作执行落实部门配备数据安全管理专职人员，形成企业数据安全岗位人员名单。相关人员负责具体承担落实数据安全管理工作，包括但不限于数据资产梳理、合规性评估、权限管理、安全审计、应急响应等工作。

3.【分类分级】

（1）建立企业内部数据分类分级管理制度，明确分类分级管理适用范围、管控系统类型、数据分类分级原则、分类分级策略标准变更流程和要求等内容。管控系统类型完整覆盖企业相关数据处理活动涉及的平台系统。

（2）综合考虑数据的类别属性、使用目的等，明确数据分类策略。在数据分类的基础上，对每一类数据类型，结合数据重要及敏感程度、安全保护需求以及一旦泄露、丢失、破坏造成的危害程度等，制定数据分级标准。

4. 【资产梳理】

（1）建立数据资产梳理制度，明确数据资产的安全管理目标和原则，定期梳理企业各数据存储平台系统情况，对照数据分类分级策略标准，完成各数据库表等字段映射，形成企业数据资产清单，明确重点保护对象。

（2）明确数据资产梳理周期，对已形成的数据资产清单进行定期更新，对数据资产使用、留存及报废等状态进行登记，形成数据资产表单变更台账。

（3）针对数据资产清单中不同级别的数据，围绕数据全生命周期各环节明确差异化的安全管理要求及技术保障措施企业数据管理相关部门据此做好管理要求落实和技术能力配备。

（4）各数据运维支撑相关部门应具备个人敏感信息发现能力，对相关平台系统数据资产进行定期扫描，能及时发现未按照相关分类分级要求使用数据的情况。

5. 【合规评估】

（1）企业数据安全管理责任部门会同业务管理部门、运维支撑部门等建立数据安全合规性评估制度，明确评估对象、启动条件、评估人员组成、评估流程、评估要点内容、问题整改跟踪及结果报备要求。按照“谁运营、谁主管、谁评估”的原则，建立数据安全合规性评估初评与复核机制，业务管理部门负责主管业务与管理平台数据安全合规性评估初评；运维支撑部门负责所运维系统和平台数据安全合规性评估初评；数据安全管理责任部门负责进行复核。

（2）企业数据安全管理责任部门针对企业整体数据安全保护水平每年至少组织开展一次数据安全合规性评估，评估内容包括但不限于数据安全制度规范完善程度、数据安全风险情况、数据合规使用提供情况、数据安全保障措施配备情况与完善程度、合作方数据安全保护水平。

（6）企业业务和平台系统存在数据出境、数据开放共享等重大操作行为前，涉及新增合作方等情况下，应及时启动数据安全动态评估工作，识别业务涉敏情况、业务与系统平台面临的安全风险、存在的弱点和造成的影响。

6. 【权限管理】

（1）建立企业数据访问权限管理制度，明确企业数据处理活动平台系统的账号分配、开通、安全保障要求，及账号操作的审批要求和操作流程等，形成并定期更新平台系统权限分配表。

（2）按照业务需求和安全策略合理配置系统访问权限，并实施权限控制措施，符合最小授权和角色权限制约等要求，严格控制数据处理活动平台系统超级管理员权限账号数量。

（3）对数据安全管理人员、数据使用人员、安全审计人员的角色进行分离设置，涉及授权特定人员超权限处理数据的，应由数据安全管理责任部门或数据安全责任人进行审批并记录。

（2）建立企业数据安全审计制度，明确审计对象、审计内容、实施周期、结果规范、问题整改跟踪等要求。各数据处理活动平台系统负责部门配备日志安全审计员，加强日志访问和安全审计管理，通过安全审计类设备对高风险数据操作进行配置，监控数据访问和操作行为，发现并处置敏感数据非授权访问、批量操作等异常情况，至少每季度形成一份数据安全审计报告。

（3）建设具有自动化安全审计能力的平台系统

（3）与合作方全量签订服务合同或安全保密协议，根据实际合作项目明确具体条款内容，包括但不限于合作方及参与项目的员工可以接触到的数据处理相关平台系统范围，及其数据使用权限、内容、范围及用途，合作方数据安全保护责任，合作方安全保护措施配备情况，合作结束后数据删除要求，合作方违约责任和处罚条款。其中数据使用权限、内容、范围及用途应符合最小化原则，以有效约束合作方，切实防范数据泄露、滥用等安全风险。

9. 【数据防泄漏】

建立数据防泄露能力，覆盖企业核心数据处理活动平台系统。相关部门通过各类数据防泄漏设备，具备对网络、邮件、FTP、USB 等多种数据导入导出渠道进行实时监控的能力，及时对未授权敏感数据导入导出、大量数据导入导出等异常情况进行预警拦截，防范数据泄露风险。

（3）结合数据安全事件场景和等级制定数据安全事件应急响应预案，明确应急响应工作责任分工、实施环节、应急响应措施。实施环节至少包括事件监测、定位、分级、启动、响应处置、报告、事件评估、结束响应、应急总结、情况跟踪等阶段。

（4）根据数据安全事件应急响应预案制定演练计划并定期组织演练，保存演练记录。每类数据安全事件场景至少一年

开展一次演练。每个数据处理活动涉及的平台系统至少两年开展一次演练。

（5）在发生数据安全事件时及时采取补救措施，并将有关情况向电信主管部门报告。发生大规模用户个人信息泄露、毁损和丢失时，应采取合理、有效的方式通告事件情况。

二、数据生命周期评估要点

（一）基础性评估要点

1.【数据采集】

（1）制定数据采集规则，规范数据采集渠道、数据格式、采集流程和采集方式，并定期根据规则在业务系统中执行数据采集合规性审查。

前面从数据安全组织管理、数据识别梳理、分类分级、权限控制、审计、应急等角度看数据安全合规

（2）在进行个人信息采集前，将采集规则以通俗易懂、简单明了的文字向个人信息主体明示，包括收集、使用个人信息的目的、方式和范围等，并获得个人信息主体的授权同意。

（3）收集个人信息遵循最小必要原则，收集的个人信息类型应与实现产品或服务的业务功能有直接关联。

（4）严格遵守数据采集规则，网站、应用程序涉及采集用户数据的功能设计应同隐私政策保持一致，同步调整。

3. 【数据存储】

（1）明确数据存储安全策略和操作规程，对授权收集到的数据采用技术手段（如加密、授权、数字水印、数字签名等）实施安全存储保护。

（2）按照数据访问权限管理制度和数据存储安全策略，针对不同数据存储平台系统配备对用户或业务（应用程序）的访问控制措施，确保非授权用户或业务（应用程序）不能访问数据。

4. 【数据使用】

（1）遵循目的明确原则，制定数据使用安全策略和操作规程，区分不同目的下数据使用审批流程、数据脱敏处理使用规则，明确数据使用结果发布和应用的安全保护规则。

（2）除为达到用户授权同意的使用目的所必需外，处理个人信息时消除明确身份指向性，避免精确定位到特定个人。特殊情况下（如信用体系评价、被监护人行踪轨迹、执法部门协助等），应告知数据处理场景及可能对用户产生的影响。

（3）因业务需要，确需改变个人信息使用目的或改变个人信息使用规则时，应再次征得用户明示同意；并针对目的变更后的情况，进行个人信息安全风险评估，重新调整安全措施。

5.【数据开放共享】

（1）建立数据开放共享的审核制度，审核共享数据的数据内容，确认属于满足数据共享业务场景的需求范围和应用场景，对数据开放共享进行有效控制，确认没有超出需求和授权范围开放共享数据。

（2）与数据开放共享接口调用方签署合作协议，在合作协议中明确了对数据的使用目的、供应方式、保密约定等。

6.【数据销毁】

（1）结合数据分类分级管理制度和安全需求，建立相应的数据销毁安全策略和操作规程，明确销毁对象、原因（如数据业务下线、用户退出服务、节点失效、过多备份、数据试用结束、超出数据保存期限等）和流程、存储介质销毁处理策略和操作规程。

（2）建立数据销毁审批机制，设置销毁相关监督角色，监督操作过程，并对数据的批量销毁采用多人操作模式。

（3）违反法律法规规定或与个人信息主体的约定收集、使用个人信息，个人信息主体要求删除的，应及时删除个人信息。

（二）重点业务评估要点°

1. IDC（资源协作）

【数据存储】

（1）存储个人信息不应超出采集使用规则中明确的存储期限，在不违反法律法规或者国家有关部门留存要求的前提下，用户注销账号后应及时删除其个人信息或做匿名化处理，经过处理无法关联到特定个人且不能复原的除外。

（3）收集个人信息后，宜立即进行去标识化处理，并采取技术和管理方面的措施，将可用于恢复识别个人的信息与去标识化后的信息分开存储并加强访问和使用的权限管理。

（3）明确数据备份操作规程，包括数据备份周期、备份方式、备份地点、数据恢复性验证机制等内容，保障数据的可用性和完整性。一旦发生数据丢失或破坏，能够利用备份恢复数据。

2. 大数据技术应用与服务

【数据使用】

（1）除为实现个人信息主体授权同意的使用目的所必需外，使用个人信息时应消除明确身份指向性，避免精确定位到特定个人。例如，为准确评价个人信用状况，可使用直接用户画像，而用于推送商业广告目的时，则宜使用间接用户画像。

（2）在向个人信息主体提供业务功能的过程中使用个性化展示的，应显著区分个性化展示的内容和非个性化展示的内容

3. 移动应用商店业务

【安全审查】

在移动应用软件上架前，对移动应用软件实施用户个人信息保护安全审查，包括但不限于软件开发者真实身份信息；用户个人信息收集、传输、存储、使用、销毁的合规性。

【准入机制】

建立移动应用软件准入制度，明确未通过用户个人信息保护评估的移动应用软件不得上架，版本更新后不能满足合规性要求的及时进行下架处理。

4. 即时通信业务

【数据使用】

对用户个人信息使用进行权限控制，遵循权限最小化原则，在授权范围内进行用户个人信息操作，非授权者不能接触用户个人信息。业务系统记录授权者操作行为日志，定期对操作行为日志进行审计，对异常行为及敏感数据访问行为进行预警。

【数据共享】

将用户个人信息提供给第三方使用前，应告知用户并获得授权同意，且明确告知用户第三方数据使用权限，并要求第三方遵守数据存储、传输、使用环节相关管理规定。建立对第三方用户个人信息保护监督管理制度，定期对第三方使用用户个人信息情况进行监督检查。