附件 1

电信和互联网企业网络数据安全合规性评估要点

（2020 年版）

为进一步指导电信和互联网企业做好网络数据安全合规性评估工作，提升数据安全保护水平，依据《网络安全法》《电信和互联网用户个人信息保护规定》等法律法规，参考《信息安全技术 个人信息安全规范》等标准规范，制定本要点，供各企业在网络数据安全合规性评估中使用。

一、 基础性评估要点

重点围绕机构人员、制度保障、分类分级、合规评估、权限管理、安全审计、合作方管理、应急响应、投诉处理、教育培训等十个方面开展评估。

1.【机构人员】

（1）明确企业数据安全管理责任部门，牵头承担企业数据安全管理工作，包括但不限于制定数据安全管理制度规范，协调强化数据安全技术能力，开展数据安全合规性评估、安全审计管理、安全事件应急处置、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部门的责任分工界面，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。

（3）数据安全管理责任部门应配备数据安全管理责任人员，相关工作执行部门应设置数据安全工作岗位，负责具体落实数据安全管理工作，包括但不限于数据资产梳理、分

类分级、合规性评估、权限管理、安全审计、应急响应、教育培训等工作。

2.【制度保障】

建立企业数据分类分级管理、数据访问权限管理、数据安全合规性评估、数据全生命周期管理、数据合作方管理、数据安全应急响应等制度。

3.【分类分级】

（1）按照数据资产安全管理的目标和原则，定期梳理企业核心数据处理活动有关平台系统1数据情况，形成企业数据资产清单。

（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，结合数据的重要及敏感程度以及一旦泄露、丢失、破坏造成的危害程度等，制定数据分级策略。在数据分类分级基础上，明确重要数据的范围和类型。

（3）针对不同级别的数据，围绕数据全生命周期各环节部署差异化的安全保障措施。对重要数据实施重点保护，按照法律法规及国家有关规定，落实重要数据境内存储、出境安全评估等要求。

4.【合规评估】

（1）将数据安全合规性评估作为企业数据安全管理的重要内容和抓手，按照“谁运营、谁主管、谁负责”的原则，开展企业整体数据安全保护水平评估并形成评估报告。评估内容包括但不限于数据安全制度建设情况、数据分类分级情况、数据安全事件应急响应水平，以及重点业务与系统数据

[1]核心数据处理活动有关平台系统是指：存储和处理用户个人信息的支撑系统。不包含对企业生产经营数据、内部管理数据及企业内部研发测试数据的处理。

合规处理情况、数据安全保障措施配备情况、合作方数据安全保护水平等。

（2）对照企业数据安全制度规范，按年度开展重点业务数据安全合规性评估并形成评估报告。重点评估业务数据处理活动中相关制度规范执行落实情况、数据安全保护措施配备情况等。实现对新上线业务、重点存量业务2的评估全覆盖，业务数据处理模式变化3时应动态跟踪评估。

（3）对照企业数据安全制度规范，按年度开展核心数据处理活动平台系统数据安全合规性评估并形成评估报告。重点评估企业内部管理措施执行落实情况、平台建设运维部门及合作方数据安全保护措施配备情况等。

（4）各项评估报告中应包括评估对象基本情况、评估流程、评估要点对标情况、保障措施配备情况与佐证材料说明、问题分析和改进措施等。

5.【权限管理】

（1）明确企业数据处理活动平台系统的用户账号分配、开通、使用、变更、注销等安全保障要求，及账号操作审批要求和操作流程，形成并定期更新平台系统权限分配表，重点关注离职人员账号回收、账号权限变更、沉默账号安全等问题。

（2）按照业务需求、安全策略及最小授权原则等，合

---

[2]重点存量业务（含移动应用软件）：关注具备收集、使用个人信息功能的业务与平台，包括但不限于网掌微厅、即时通信、在线教育、在线医疗、电子商务、位置服务、营销支撑平台、信息登记平台、大数据平台、用户通讯录管理平台、云业务平台及数据合作类业务。

[3]业务数据处理模式变化：新增数据出境、数据开放共享等重大操作行为，数据采集、传输、存储、使用、开放共享、销毁方式变化，业务模式、运行环境变化（系统改建、升级或报废），新增合作方、跨业务目的使用和交换数据等情况。

理配置系统访问权限，避免非授权用户或业务访问数据。严格控制超级管理员权限账号数量。

（3）对数据安全管理、数据使用、安全审计等人员角色进行分离设置。涉及授权特定人员超权限处理数据的，由数据安全管理责任部门进行审批并记录；涉及数据重大操作的（如数据批量复制、传输、处理、开放共享和销毁等），采取多人审批授权或操作监督，并实施日志审计。

6.【安全审计】

（1）对数据授权访问、批量复制、开放共享、销毁、数据接口调用等重点环节实施日志留存管理，日志记录至少包括执行时间、操作账号、处理方式、授权情况、IP 地址、登录信息等，能够对识别和追溯数据操作和访问行为提供支撑。定期对日志进行备份，防止数据安全事件导致的日志被删除。

（2）加强企业数据安全审计管理，明确审计对象、审计内容、实施周期、结果规范、问题改进跟踪等要求。企业数据安全管理责任部门或核心数据处理活动相关平台系统负责部门应配备日志安全审计员，加强日志访问和安全审计管理，至少每半年形成一份数据安全审计报告。

7.【合作方管理】

（1）加强数据合作方[4]安全管理，明确合作方数据安全监督管理部门和执行配合部门，明确企业对外合作中数据安全保护方式和合作方责任落实要求。

[4]合作方：受托代理市场销售和提供业务合作、技术支撑、数据服务等可能接触到组织机构数据的外部机构。其中，业务合作主要包括数据业务合作推广、渠道接入等形式；技术支撑主要包括系统开发集成、系统维护、技术支撑等形式；数据服务主要包括数据建模、数据挖掘、数据分析等数据服务能力提供形式。

（2）合作方监督管理部门建立合作方台账管理机制，牵头梳理形成并定期更新合作方清单（含合作方企业名称、合作业务或系统、合作形式、合作期限、合作方联系人等），加强对合作方数据使用情况的监督管理。

（3）与合作方签订服务合同和安全保密协议中，应根据实际合作项目明确具体条款，包含但不限于下述内容：合作方及项目参与员工可接触到的数据处理相关平台系统范围，及数据使用权限、内容、范围及用途（应符合最小化原则），合作方数据安全责任、保障措施配备情况（保障措施不得低于本企业），合作结束后数据删除要求，合作方违约责任和处罚等。

8.【应急响应】

（1）强化企业数据泄露（丢失）、滥用、被篡改、被损毁、违规使用等安全事件应急响应能力。

（2）参照《公共互联网网络安全突发事件应急预案》及数据安全事件对企业和个人信息主体合法权益影响等因素划分事件等级。结合事件场景和等级制定应急预案并开展演练，典型场景至少每年开展一次演练；每个核心数据处理活动有关平台系统至少两年开展一次演练。

（3）发生数据安全事件时及时采取补救措施，并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，采取合理、有效方式告知用户。及时总结数据安全事件情况，分析原因、查找问题，调整企业数据安全策略，形成事件调查记录和总结报告，避免再次发生类似情况。

9.【举报投诉处理】

完善数据安全用户举报与受理机制，建立用户数据安全举报投诉渠道，如电子邮件、电话、传真、在线客服、在线表格等。明确举报投诉处理部门和人员、处理流程、处理要求等。针对有效举报线索，及时核查处理并在接到投诉之日起十五日内答复投诉人。

10.【教育培训】

（1）制定数据安全管理相关岗位人员培训计划，培训内容应包括数据安全制度要求和实操规范，如法律法规、政策标准、合规性评估、技术防护、应急响应、知识技能、安全意识等。

（2）培训可采取线下集中授课或线上培训等形式，数据安全管理责任人员年度培训时长不少于 10 学时，并开展培训人员考核评定。

二、数据生命周期评估要点

重点围绕数据采集、传输、存储、使用、开放共享、销毁等六个环节开展评估。

1.【数据采集】

（1）规范数据采集渠道、数据格式、采集流程和采集方式，定期开展数据采集合规性审查。利用外部数据源采集数据的，应对数据源的合法性进行确认，涉及个人信息的，应要求提供方说明个人信息来源与个人信息主体授权同意的范围。

（2）在进行个人信息采集前，以通俗易懂、简单明了

的方式向个人信息主体明示采集规则，如收集、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。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。

2.【数据传输】

（1）根据业务流程、职责界面、网络部署、安全风险等情况，合理划分企业网络系统安全域，区分域内、域间等不同数据传输场景，明确数据传输安全策略和操作规程。

（2）梳理企业存在数据出境情况的业务，对涉及个人信息和重要数据出境的场景、类别、数量级、频率、接收方情况等进行梳理汇总。

3.【数据存储】

（1）明确企业核心数据处理活动有关平台系统、存储介质等数据存储安全要求。与系统支撑运维人员签订保密协议，有效约束操作行为。

（2）加强对数据存储平台系统接入移动存储介质的管控，对将数据下载到本地终端的行为进行严格审核和日志记录。

（3）根据数据级别明确数据备份操作规程，保障数据的可用性和完整性。

4.【数据使用】

（1）区分不同目的下数据使用审批流程、数据脱敏处理规则，鼓励在保障安全的情况下，开展数据利用。

（2）除为达到用户授权同意的使用目的外，使用个人

信息时消除明确身份指向性，避免精确定位到特定个人。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。

5.【数据开放共享】

（1）对数据对外开放共享实施审核，确认没有超出需求和授权范围，采取必要措施提升共享场景下的数据溯源能力。

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

（3）共享个人信息时，应事先向个人信息主体告知共享个人信息的目的、接收方情况等，并征得个人信息主体授权同意，经过处理无法识别特定个人且不能复原的除外。

（4）法律法规或中央政策对数据对外提供使用另有规定的，从其规定。

6.【数据销毁】

（1）明确销毁与删除的对象、原因（如数据业务下线、用户退出服务、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，数据批量销毁采用多人操作模式。

（3）因违反法律法规规定或双方约定收集、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。法律、行政法规另有规定的，从其规定。

三、技术能力评估要点

重点围绕数据识别、安全审计、防泄露、接口安全管理、个人信息保护等五个方面开展评估。

1.【数据识别】

配备技术能力，定期对相关平台系统数据资产进行扫描，能够发现识别个人敏感信息。定期对数据脱敏效果进行验证，确保各类数据处理场景中数据脱敏的有效性和合规性。

2.【操作审计】

规划建设具有自动化操作审计能力的平台系统，具备数据操作权限配置、异常操作告警与处置等核心功能，分批次将数据处理活动平台系统接入安全系统，数据操作审计内容和企业平台系统权限分配表作为系统策略进行配置。

3.【数据防泄露】

涉及存储、处理个人敏感信息和重要数据平台系统配备数据防泄露能力，优先从网络侧和终端侧等进行部署，逐步扩大能力覆盖范围。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，及时对异常数据操作行为进行预警拦截，防范数据泄露风险。

4.【接口安全管理】

面向互联网及合作方开放的数据接口具备接口认证鉴权与安全监控能力，能够限制违规设备接入，对接口调用进行必要的自动监控和处理。对涉及个人信息和重要数据的传输接口实施调用审批，定期开展接口日志审计。

5.【个人信息保护】

对授权收集到的个人敏感信息，采取去标识化、关键字段加密安全存储措施；在跨安全域或通过互联网传输个人敏感信息时，采用加密传输措施（如可确保安全的加密算法或传输通道）；在用户端显示个人敏感信息时，采取措施防止未授权人员获取个人敏感信息。