2021

数据安全治理之
数据安全风险评估白皮书

全知科技（杭州）有限责任公司

版权声明

目录

01

数据安全治理

1 数据安全治理

中国数字经济快速发展。相关数据显示，2020年中国数字经济规模已达到39.2万亿元人民币，占GDP的38.6%，居世界第二位，已成为中国经济增长的重要价值。因此，识别数据安全风险、构建数据安全治理机制的重要性日益凸显。

随着数字经济的快速发展以及传统业务的数字化转型推进，数据价值化加速推进，数据安全已成为数字经济时代最紧迫和最基础的安全问题。如何能系统、全面、有效的建设和提升数据安全防护能力，在数据经济、数据价值和数据安全之间达到平衡，是当下国家、行业以及各企业和组织都非常关注的问题。数据安全治理也成为了近年国际国内的热点，这是一个覆盖了组织架构、数据资产、风险防范、运营监测等多个方面的，从整体策略到具体执行的大命题。

1.1.数据安全治理介绍

数据安全治理，是指依照法律、法规、国家标准、行业标准规范等的规定，建立健全全流程数据安全管理制度，采取相应的技术措施和其他必要措施，保障数据安全。数据安全治理的必要性：

一是法律有规定，数据安全上升到国家层面，国际上欧盟发布《欧洲数据保护监管局战略计划(2020-2024)》，继续加强数据安全保护，保证个人隐私的基本权利美国发布《联邦数据战略与2020年行动计划》，确立了保护数据完整性、确保流通数据真实性、数据存储安全性等基本原则。我国在2021年6月《中华人民共和国数据安全法》正式颁布，2021年9月1日正式实施，第四条 维护数据安全，应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力。

二是数据价值有待释放，数据是企业重要的生产要素，对数据的合理利用能有效打破数据孤岛，推进各地区各部门各组织之间的数据要素流通，能进一步鼓励数据价值的探索和提升。数据价值的释放，对数据的共享开放提出了要求，特别是政务数据在经过了长年累月的积累，形成了海量且权威的数据资源，具备极大的数据价值释放需求和能力。目前各地方也都在积极开展公共数据共享开放的规范制定，数据安全也自然成为了数据共享开放过程中的安全保障基础。

三是现实的需求，数据作为新型生产要素，由于其本身具有流动性、分散性、可复制性等不同于传统生产要素的特性，随着数据价值的升高，个人隐私信息、商业机密甚至国家重要情报均面临着不同程度的敏感数据泄露、数据贩卖、数据篡改、数据跨境流动等数据安全风险。

1.2.数据安全治理主流认知

数据安全相关的法律法规对数据安全职责、数据资产安全、数据处理活动、数据安全风险评估、数据安全监测等均提出了要求，各行业也在陆续开

展有针对性的规范和指导细化。满足法律法规要求，实现数据安全风险管控，是各企业和组织开展数据安全治理的首要目标。

企业和组织需要在实用性和时效性的前提下，识别其当前存在和面临的数据安全风险，特别是需要迫切解决的风险，从而有目标地快速实现数据安全防护能力的提升。数据安全风险评估，是数据安全治理的起点。风险评估能够帮助企业或组织发现业务和自身数据安全问题，明确数据安全治理需求，为建设数据安全管理和数据安全风险处置手段指明方向，给出可落地的实施方案。

目前国家层面密集发布的各种法律法规，结合监管指引的各种要求，企业在落实数据安全治理责任的过程中，广泛遇到的问题，除了合法合规要求的落地执行外，更多的是基于生产经营过程中，如何平衡发展与安全特性的要求，保证数据生产要素发挥更大的价值。数据作为生产资料所体现的新特性，是现阶段治理落地面临的新问题，是企业面临的新难点。以往的数据安全治理往往延续了之前信息系统安全防护的惯性理念，从边界防护出发，试图将数据锁在“笼子”里。但不管从国家出台颁布的相关法律法规也好，还是企业自身经营过程中面临的新发展新问题也好，数据安全治理都是从保证数据流动产生价值的核心出发，在保证价值前提下的安全防护。基于数据流动的特性，数据安全治理工作也面临新的挑战，如何在企业纷繁复杂的生产经营活动中，既能保证数据安全治理工作的顺利进行，又能平衡生产与安全的要求。

基于多年对企业和组织在数据安全治理工作上的实践经验，本白皮书提出了基于数据与数据处理活动的数据安全治理框架（如图1所示），包括数据资产梳理、数据安全风险评估、数据安全风险处置三部分内容。

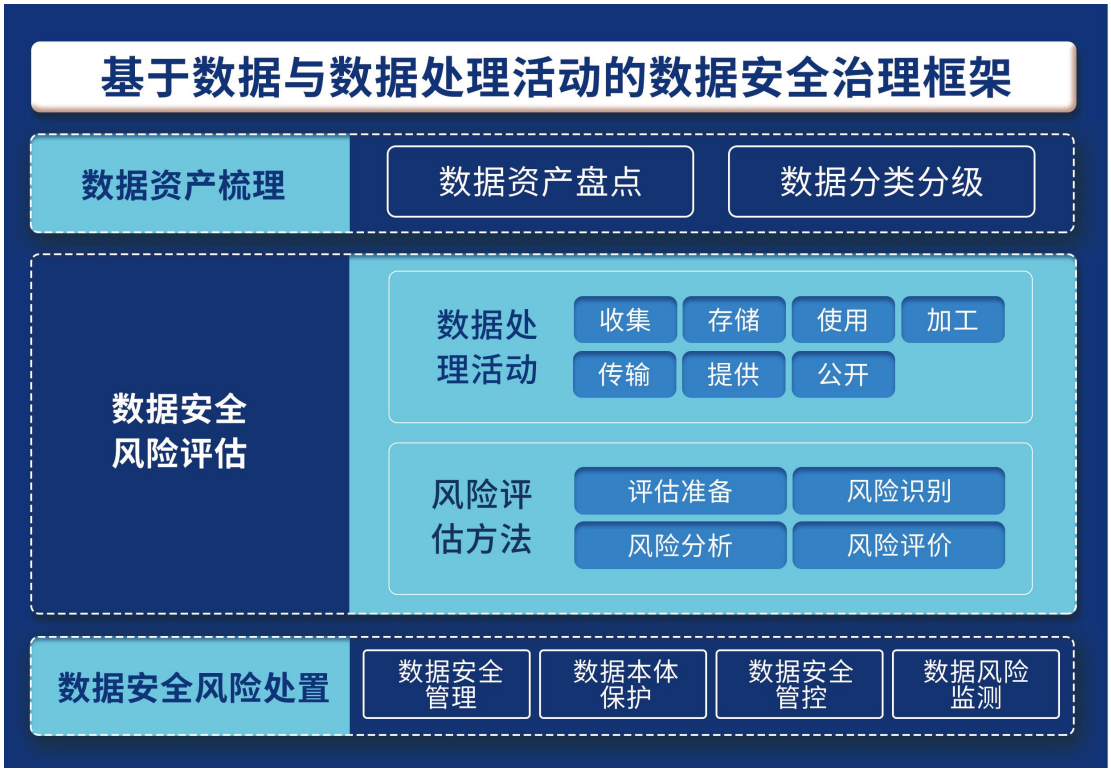

图1 基于数据与数据处理活动的数据安全治理框架

本数据安全治理框架内容，着重于从企业数据资产本身出发，基于企业生产经营活动中所经历的各阶段数据处理活动的不同内容，紧贴法律法规、行业规范等要求，解决企业合法合规经营和生产活动风险安全可控两方面的需求。基于数据与数据处理活动的数据安全治理框架由以下三个方面内容构成：

1) 数据资产梳理，提供了企业数据资产盘点与数据分类分级相关工作的实践指南。
2) 数据安全风险评估，基于企业数据资产梳理工作的内容，提供了企业在不同数据处理活动中，通过数据安全风险评估方法提供实施落地指导，落实数据安全风险评估工作。
3) 数据安全风险处置，基于数据安全风险评估结果，依据不同的发展阶段和生产经营中解决问题的优先级，参照国家法律法规、行业规范等要求，通过数据安全管理、数据本体保护、数据安全管控、数据风险监测等手段，提高企业履行保护管理责任和保障持续安全状态能力。

02

数据安全风险评估

2 数据安全风险评估

2.1.风险评估综述

风险评估是对信息资产（即某事件或事物所具有的信息集）所面临的威胁、存在的脆弱性、造成的影响，以及三者综合作用所带来风险的可能性的评估。风险评估方法包括：评估准备、风险识别、风险分析及风险评价。

《中华人民共和国数据安全法》第三十条中，明确规定“重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。”其中风险评估报告中的内容包括“重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等”。

2.2.数据安全风险评估

参照《中华人民共和国数据安全法》中的定义，数据安全风险评估的核心内容，是基于数据资产，在数据处理活动中，识别所面临的风险及其应对措施。其中数据处理活动，指执行数据处理的企业业务活动。数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。本文中所涉及的数据安全风险泛指广义的风险，既包括合法合规性风险，又包括技术安全性风险。

2.2.1.数据安全风险评估要素关系

信息安全风险评估方法，是针对信息系统生命周期不同阶段的实施要点和工作形式的总结，包括：评估准备、风险识别、风险分析、风险评价四部分内容。数据安全风险评估方法在参照原有信息安全风险评估方法基础上，更关注数据资产，以及在相关数据处理活动中所面临的风险情况。参照信息安全风险评估要素及其关系，数据安全风险评估中要素及其关系如图2所示。

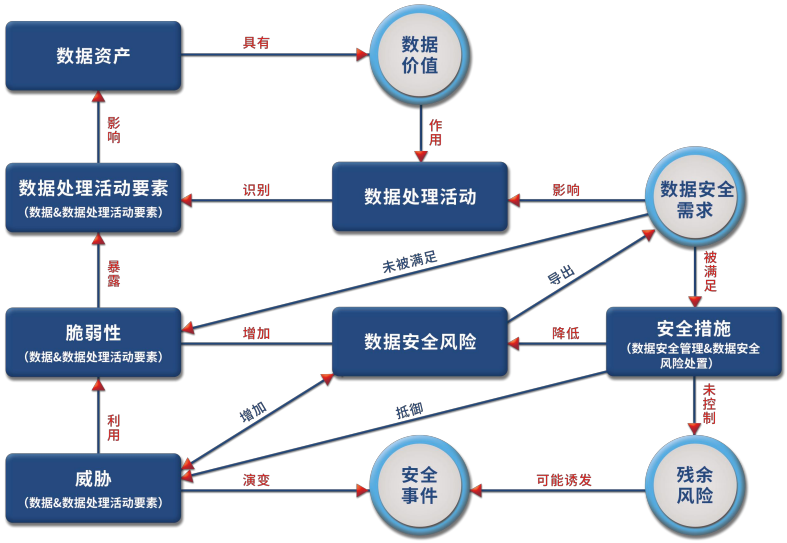

图2 数据安全风险要素及其关系

2.2.2.数据安全风险分析原理

参照信息安全风险分析原理，结合数据安全风险评估中各个要素关联的特性，梳理出数据安全风险分析原理，如图3所示。

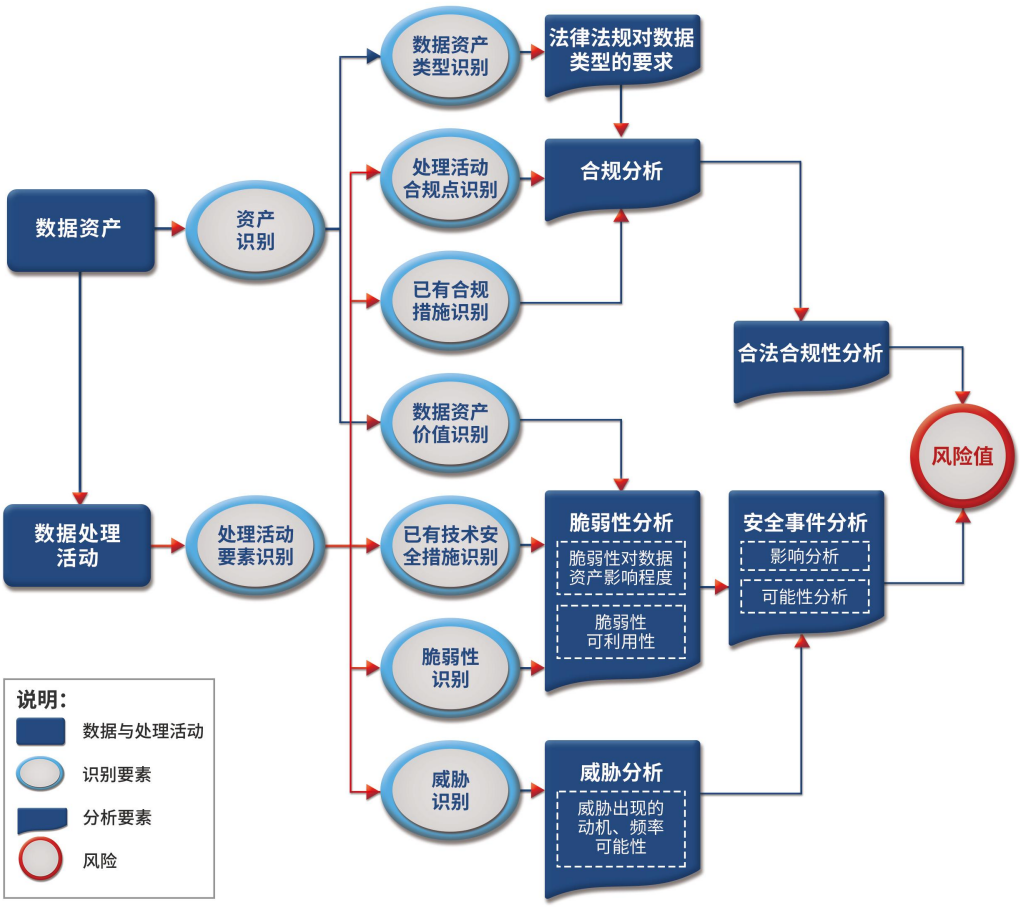

图3 数据安全风险分析原理

通过对数据资产和数据处理活动中要素的梳理，结合已有合规措施，在充分识别法律法规对不同数据类型的要求和处理活动中合规点要求的基础上，完成数据安全合法合规性分析。

通过对数据资产和数据处理活动中要素的梳理，结合已有技术安全措施，参考数据资产价值、处理活动脆弱性和威胁识别等要素，完成技术脆弱性和威胁分析，形成数据安全事件分析。

综合数据安全合法合规分析和数据安全事件分析，最终形成数据安全风险值。

2.2.3.数据安全风险评估方法

信息安全风险评估工作的开展，可参考GB/T 20984-2007《信息安全技术 信息安全风险评估规范》中的内容执行，但数据安全风险评估工作的内容，暂时还没有发布国家层面的可参考标准。不管是国家相关法律法规中的

要求，还是行业标准落地检查中的要求，相关企业都迫切需要可参照、可落地的方法，来指导数据安全风险评估工作的落实。基于以上需求，全知科技联合相关研究院所和机构，共同推出了数据安全风险评估的实施方法，立足于指导相关企业落实数据安全风险评估工作。

参照信息安全风险评估方法，结合多年来在企业数据安全风险评估领域的工作实践，依据法律法规、行业标准规范等要求，以企业的数据资产为评估对象，数据处理活动中所面临的风险为评估内容，提供一套可落地可指导实践的数据安全风险评估方法，如图4所示。核心内容包括：评估准备、风险识别、风险分析和风险评价。

图4 数据安全风险评估方法

评估准备：当前企业与组织实施风险评估工作，更多是从国家法律法规及行业监管、业务需求评估等相关要求出发，从战略层面考量风险评估结果对企业相关的影响。数据安全风险评估准备的内容，主要包括：评估对象、评估范围、评估边界、评估团队组建、评估依据、评估准则、制定评估方案并获得管理层支持。

风险识别：主要包括资产价值识别、数据处理活动要素识别、合法合规性识别、威胁识别、脆弱性识别以及已有安全措施识别。

风险分析：完成了资产价值识别、处理活动要素识别、合法合规性识别、已有安全措施识别、威胁识别和脆弱性识别后，通过采取适当的方法与工具，可得出企业所面临的合法合规性风险、数据安全事件发生的可能性以及数据安全事件发生对组织的影响度，从而得到数据安全风险值。

风险评价：企业在执行完数据安全风险分析后，通过风险值计算方法，会得到风险值的分布状况，对风险等级进行划分，一般会划分为：高、中、低三个等级。依据风险评价中风险值的等级，明确风险评估结果内容。

企业通过数据安全风险评估，最终得到企业风险评估结果。依据风险评价等级结合企业面临的生产活动实际情况，制定后续的数据安全风险管控策略，执行数据安全风险处置。本白皮书核心聚焦在风险识别部分的内容，数据安全风险处置相关的内容，敬请关注后续发布的数据安全治理系列白皮书。

2.2.3.1合法合规性识别

中央网信办、工业和信息化部、公安部、市场监管总局四部门联合发布《关于开展App违法违规收集使用个人信息专项治理的公告》，在全国范围组织开展App违法违规收集使用个人信息专项治理，并成立App违法违规收集使用个人信息专项治理工作组。

工信部针对App违规处理用户个人信息、设置障碍、骚扰用户、欺骗误导用户等问题，推进App侵害用户权益整治行动。组织检测上百万App，累计通报数千款款违规App，下架百款款拒不整改的App。其中上百款App因被发现存在“违反必要原则，收集与其提供的服务无关的个人信息”“未经用户同意收集个人信息”等问题。

在数据处理活动中，基于数据资产识别和处理活动要素识别，梳理出企业处理活动要求和合规措施要求。再将具体的要求点与处理活动要素点进行比对，明确后续的合规整改点。比如：企业基于C端业务，需要收集用户个人敏感信息，依据《个人信息保护法》的要求，需要获取用户授权，明示收集目的、类型等情况。在合规分析中，就需要针对收集环节的处理活动，梳理处理目的、处理行为等要素，判断业务合法合规性。

涉嫌违规事由举例说明，参见表1:

表1.涉嫌违规事由示例

事由编号	涉嫌违规事由	法律相关要求
DV-1	违背目的公开合法	履行数据处理目的公开合法
DV-2	违背保护管理责任	履行数据保护管理责任
DV-3	违背最小必要原则	履行数据处理最小必要原则
DV-4	违规跨境	履行数据合法跨境
DV-5	违背主体授权同意原则	履行数据主体知情同意原则
DV-6	违背公开透明原则	履行数据处理公开透明原则

合法合规性识别和分析，对企业业务生产经营的顺利开展，具有决定性影响，企业一定要将合法合规性评估放在风险评估的首位。

2.2.3.2资产价值识别

在信息安全风险评估中，资产识别是风险评估的核心环节，通过将资产按照业务、系统、组件和单元的分层，进行层层递进识别，明确资产的价值等级。

企业数据资产的表现形式，在不同的数据处理活动中，是有所不同，包括但不限于：数据本体、数据载体、数据流等。所以在数据资产价值识别中会依据不同的表现形式和资产类别，来区分识别。资产类别包括但不限于：重要数据、个人信息等。其中重要数据、个人信息等的数据安全风险评估内容，请参见2.3中的内容。相关名词概念如下：

- 数据本体：被记录的信息本身；
- 数据载体：信息以某种记录形式的存在，如：数据库中的库表字段，或以文件形式存储的数据文件等；
- 数据流：数据在处理活动中，从一个处理环节流动到另一个处理环节的流向情况。如：数据从存储服务器流动到应用服务器到客户终端；
- 重要数据：以电子方式存在的，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的数据。（参见《网络数据安全管理条例》（征求意见稿））；
- 个人信息：个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。（参见《中华人民共和国个人信息保护法》，第四条）。

2.2.3.3处理活动要素识别

➢ 数据处理活动要素

企业在进行与数据处理相关的业务活动时，会涉及到的要素有：业务场景、处理主体、处理方式、处理环境、处理类型和量级、处理行为、处理目的、处理结果、处理活动要素管理等。

- 业务场景：一般以数据处理的业务场景来区分，主要包括：收集、存储、使用、加工、传输、提供、公开等场景；
- 处理主体：数据控制者或数据处理者；
- 处理方式：依据不同的数据处理活动，满足不同业务诉求的技术处理要求。内容包括：协议、API、SDK等；
- 处理环境：依据数据本体的相关特征以提供符合要求的处理操作环境。如：终端环境、生产环境等；
- 对象类型和量级：一般指数据本体或载体。依据不同的数据存在形式，结合数据本身的处理特性，提供符合处理要求的量级。内容包括：对象类型：重要数据、业务数据、个人数据等；
- 处理行为：依据不同的数据处理活动，执行符合该活动的数据处理操作行为。内容包括：数据收集、数据加工、数据删除等；
- 处理目的：依据数据处理需求，实现数据处理目标。内容包括：用户画像分析、购物行为分析等；
- 处理结果：通过数据处理活动，获取到符合企业要求的结果数据。在

执行处理活动的过程中，数据相关的流通关系和状态会发生变化；

- 处理活动要素管理：负责对数据处理活动中，各个要素履行保护管理责任。

➢ 数据处理活动要素识别模型

数据在数据处理活动中具有许多变化的特性，包括：数据所属权的变更、数据的流动性、数据量级的影响、数据处理带来的价值提升、数据的关系及状态在持续变化等，这些特性使得数据在数据处理活动中，更难以梳理和精确掌控。

为了在数据处理活动中，能够精确掌控数据变化的特性，更有针对性的执行数据处理活动要素的动态管理工作，特提出了一个基于处理活动要素识别的模型，便于企业基于该模型来精确的掌控数据的变化，完善要素的动态管理工作。

图5 数据处理活动要素识别模型

如图5所示，该模型包括四个部分内容：

1) 被处理对象：主要关注业务场景中，需要处理的对象类型和量级。
2) 处理活动：主要关注在处理活动中，处理主体在处理环境下，通过处理方式，执行的处理行为，以及最终是否达到了处理目的。
3) 处理结果：主要关注在处理结果中，是否获取到符合企业预期的数据。其中包括数据相关的流通关系和状态的变化。
   - 数据流通关系变化，具体内容是指从数据所有者转移至数据控制者；
   - 数据状态变化，内容包括：时间状态、地域状态、物理状态、内容状态、量级状态等。
4) 处理活动要素管理：主要关注数据处理活动中，各个要素的保护管理责任。

分析模型提供了针对数据处理活动中所涉及的处理要素识别的方法。通过“被处理对象-处理活动-处理结果”的方式，将数据处理活动中可能涉及的处理要素变化识别清楚，再结合处理要素管理的内容，便于企业基于该模型来精确的掌控数据的变化。

2.2.3.4威胁识别

数据威胁识别是一种对数据资产在数据处理活动中，可能发生的对保密性、完整性、可用性等造成危害的起因识别，并进一步分析其威胁动机、频率和发生的可能性。数据安全威胁类型可梳理在数据处理活动中面临的各类威胁，威胁建模方法参照微软STRIDE威胁建模方法，参见表2。业内还有传统的威胁识别类型，可参考信息安全风险评估中的威胁识别内容。

表2.威胁类型示例

威胁编号	威胁	威胁说明	安全属性
DT-1	欺骗	伪造他人账户	认证
DT-2	篡改	修改数据	完整性
DT-3	抵赖	不承认做过某行为	审计
DT-4	信息泄露	数据或信息泄漏	保密性
DT-5	拒绝服务	服务不可用	可用性
DT-6	权限提升	未经授权，或提升权限	授权

2.2.3.5脆弱性识别

数据安全风险评估中所涉及的脆弱性识别，主要涉及数据资产本身的脆弱性和数据处理活动中处理要素存在的脆弱性。数据威胁利用数据处理活动中处理要素的脆弱性，对数据资产造成影响。企业一般会通过各种可能的安全措施，来降低数据处理活动中可能存在的脆弱性，以此来缓解数据安全事件发生的可能性。

脆弱性识别需要从管理和技术两个方面进行，管理脆弱性分为数据安全组织流程管理脆弱性和技术管理脆弱性两方面；技术脆弱性涉及数据处理活动中各个要素可能面临的技术安全问题。脆弱性识别的依据可以参考信息安全风险评估中脆弱性识别的内容，也可以参照行业规范、应用实践等相关的安全要求。

数据处理活动脆弱性示例，参加表3内容：

表3. 脆弱性示例

数据处理活动	脆弱性描述	脆弱性类型	缓解手段
收集	数据上传接口存在漏洞；配置错误或操作错误；人员或系统访问权限授权有误或权限管控粒度不足	技术脆弱性	身份认证及访问管理
	内部或合作方员工违规业务数据收集	技术脆弱性 流程管理脆弱性	数据业务风险评审 数据行为监测 数据行为溯源
存储	数据脱敏不完全或伪脱敏	技术脆弱性	数据脱敏校验 模拟攻击审计
	关键岗位员工存在解密权限且有被收买可能性	技术脆弱性	数据加密 数据行为监测 安全意识培训和审计监测
传输	数据以明文传输；数据传输通信道未防护到位	技术脆弱性	数据加密 传输信道加密
使用	办公终端缺乏使用监测能力	技术脆弱性	数据行为溯源 数字水印
	业务接口上线缺乏安全审查	技术脆弱性	多因素认证 接口权限校验 数据传输加密
加工	大数据平台/数据加工技术组件存在漏洞	技术脆弱性	建立安全漏洞监测与预警手段、外部威胁情报采买
	内部员工操作配置错误或操作行为缺乏记录	技术脆弱性	数据行为溯源 数据安全操作管理流程与审计
提供	对第三方合作使用数据机构缺少相关的安全管理条款或约束协议；对第三方合作使用数据缺乏技术监督监测措施	技术脆弱性 技术管理脆弱性	数据提供管理评审 数据匿名 数据加密 数据行为监测

2.2.3.6已有安全措施识别

已有安全措施的识别，是针对企业已采取的安全措施有效性的确认。参照信息安全风险评估中安全措施的分类，数据安全风险评估中，已有安全措施也可以分为：预防性和保护性两种。预防性安全措施可以从事前降低数据安全时间发生的可能性，如：数据安全业务风险评审，可以在业务开展前期就介入预防风险的发生；保护性安全措施可以在事中以及事后，减少组织数据安全事件的影响，如：针对内部员工数据访问行为的审计系统，可以在事中及事后对员工数据泄露行为进行审计和追溯，提升泄漏事件的排查进度，降低泄露事件的影响等级。

已有安全措施的识别，将减少企业在数据安全管理和技术两个方面的脆弱性。依据数据安全风险分析原理，已有安全措施识别将影响脆弱性可利用性与脆弱性对数据资产影响程度。

2.3.企业实施数据安全风险评估思路

企业所拥有的数据资产，依据国家法律法规、行业标准规范等各项要求，可分为三类：重要数据部分、个人信息部分、其他数据部分。依据企业数据资产执行数据安全定级后的不同情况，探讨如何针对不同类型数据执行数据安全风险评估工作。

- 重要数据的风险评估方法

《中华人民共和国数据安全法》中第三十条“重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。”企业在实施落地数据安全风险评估前，需要优先满足合法合规经营的要求，切实落实法律法规、行业规范中对合法合规经营的要求，这是数据安全的底线，也是企业经营的底线。企业在落实重要数据的风险评估工作中，可参照本白皮书之前介绍的数据安全风险评估方法，识别重要数据，对数据处理活动进行定期风险评估工作，并将风险评估报告报送给有关部门。重要数据的识别可参照《信息安全技术 重要数据识别指南》（征求意见稿）中的内容。

- 个人信息的风险评估方法

《中华人民共和国个人信息安全保护法》中第二十八条“敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。”企业在落实个人信息的风险评估工作中，可参考GB/T 39335-2020《信息安全技术 个人信息安全影响评估指南》中的评估方法，也可参照本白皮书之前介绍的数据安全风险评估方法，特别是拥有大量敏感个人信息数据的企业，在数据采集、数据使用（个人数据画像、行为分析等）、数据共享、数据存储等场景下，更要严格落实个人隐私影响评估（PIA）工作，符合国家相关法律法规、行业标准规范中关于敏感个人信息的要求。

➢ 其他数据的风险评估方法

国家网信办发布的《网络数据安全管理条例（征求意见稿）》中规定了关于10万人以上个人信息和100万以上个人信息等相关的数据安全管理要求。企业其他数据的风险评估工作，除了需要遵照法律法规、行业规范的合法合规性要求外，也可参照本白皮书之前介绍的数据安全风险评估方法的思路，灵活实施相关的数据安全风险评估工作。

03

数据安全风险评估案例

3 数据安全风险评估案例

3.1.案例1-电信行业的数据安全风险评估

背景

为更好落实数据安全管理工作，近年工信部、通信管理局等监管单位针对电信企业数据安全提出了合规性安全要求，并组织开展数据安全管理工作专项行动。2020年，工业和信息化部办公厅发布了《关于做好电信和互联网行业网络数据安全管理工作的通知》，全面开展网络数据安全合规性评估，评估要点主要围绕基础性、数据生命周期及技术能力三方面，同时将数据安全合法合规性评估作为基础电信企业省级公司和专业公司网络与信息安全工作考核要点之一。

面临的挑战

电信行业运营商从2018年至2021年，每年都会组织数据安全合规性评估，一方面由于电信行业从业企业属于国家关键基础设施运营者，需要满足《关键信息基础设施安全保护条例》（以下简称《关基条例》）中的合规要求，另一方由于电信行业业务中包含大量关键基础设施数据（重要数据、个人信息），一旦发生数据泄露，可能对国计民生等都会造成重大影响。

《关基条例》第十七条中要求，“运营者应当自行或者委托网络安全服务机构对关键信息基础设施每年至少进行一次网络安全检测和风险评估，对发现的安全问题及时整改，并按照保护工作部门要求报送情况。”对电信行业运营商在风险评估中的落地执行和报送有明确要求。

但在实际落地关基风险评估，以及数据安全风险评估工作的过程中，可参照实施的指导方案和执行工具均处于摸索阶段，造成评估工作执行落地困难，很多地方均需耗费大量资源，投入产出比低效。

数据安全风险评估实施

参照信息安全风险评估方法以及本白皮书提出的数据安全风险评估方法，针对“某运营商某客服系统数据收集、存储、使用”数据应用场景，执行数据安全风险评估工作，评估流程如下：

1. 核心要素分析

- 数据处理角色：
  - 数据主体：运营商自然人用户；
  - 数据控制者：运营商；
  - 数据处理者：运营商内执行数据处理工作的组织或员工。
- 数据处理过程：
  - 数据处理环境：客服系统业务服务提供过程中需要的环境，包括：客服统一门户网站（包括：SDK、API接口等）、直播平台、小程序及相关网络环境等。

- 数据处理方式：
  - 系统数据收集方式主要通过客服远程柜台、支撑平台，收集用户手机号、身份证号、免冠照、手持身份证照、音视频录音录像等信息，未收集外部数据源；
  - 收集数据信息通过网络环境传输至客服系统服务端环境，并存储在业务系统数据库；
  - 数据使用场景一般为运营商内部其它部门向业务责任部门申请清单级数据、日常生产运营统计数据报表等。
- 数据处理操作：
  - 在数据收集环节，门户网站、直播平台及小程序通过让用户明示同意隐私政策的方式，获取用户相关个人信息、业务信息等数据；
  - 收集到的数据通过https方式传输回业务服务的服务器端；
  - 在数据使用环节，业务系统提供API接口（token方式鉴权）、SFTP等服务方式，对企业内部各类数据使用场景进行共享。

➢ 处理范围：
- 数据类型：业务数据包括会话编号、服务日期、服务工号、聊天内容等，用户个人信息包括手机号、身份证号、身份证照片、免冠照、手持身份证照等敏感信息；
- 数据量级：依据业务开展的用户数决定；
- 数据主体范围：中华人民共和国境内用户信息，主要为成人信息。

➢ 处理目的和结果
- 处理目的的实现：通过向用户明示隐私政策协议内容，用户主动勾选授权同意后，提供客户服务，在服务过程中，视频通话将收集用户手机号、设备系统、网络通讯、摄像头、麦克风、扬声器、相册、地理位置等信息，实名认证将收集用户姓名、身份证号、身份证照片、免冠照等；
- 数据流通关系变化：用户业务与个人信息使用权，从用户变动到业务系统责任部门；
- 数据状态发生变化：可能存在时间状态（过期存储）、地域状态（跨境）、内容状态（客户数据值等）等发生变化。

2. 数据处理活动合法合规评估

➢ 运营商客服门户网站、小程序数据收集、存储及使用场景下的合法合规评估
- 合法合规评估：
  - 《中华人民共和国个人信息保护法》要求，数据处理活动中，需要明示数据采集目的、采集数据类型、存储位置、获取用户授权等情况；
  - 通过小程序客户端所提供的服务，执行隐私政策确认工作，不允许替用户默认勾选。这个过程中，涉及合规性风险里，违规采集风险；
  - 记录用户的确认授权收集操作，保存确认记录以备查阅；收集到的用户数据需要境内存储，收集数据需遵循最小化原则；

- 提供的隐私政策协议，需要包含：收集目的、用途、数据类型等相关信息。涉及合法合规性风险有：明示采集目的、最小采集权限、不允许跨境传输、传输保护等；
- 门户网站、小程序提供的查询服务，展示的数据，需保证是经过用户授权的数据；这些数据需要保证是通过合法合规的渠道收集的；
- 业务系统数据需采取定期数据备份恢复机制，确保数据可用可恢复；涉及合法合规性风险有：数据保护管理责任明确落实。

3. 数据处理活动安全性评估

- 运营商客服门户网站、小程序数据收集、存储和使用场景下的安全性风险评估
  - 处理方式安全评估
    - 使用权限安全风险：处理方式提权、处理范围提权、使用类型提权等；
    - 数据传输安全风险：数据窃取和监听、数据明文传输等；
    - 数据存储安全风险：数据明文存储、数据有效性未校验等；
    - 数据使用安全风险：服务接口被DDos攻击、数据非授权访问、数据越权访问等；
    - API数据接口安全风险：接口非授权数据访问、接口非授权数据爬取等。
  - 处理操作安全评估
    - 操作越权安全风险：数据使用未授权、数据使用范围未授权；
    - 操作抵赖安全风险：数据操作行为冒充；
    - 操作滥用安全风险：数据被滥用、数据操作冒充他人等；

    操作泄漏安全风险：数据使用过程中恶意留存、恶意篡改数据等。

4. 解决方案：

在运营商客服系统数据收集、存储及使用场景下，依据上面评估识别的数据安全风险情况，具体的解决方案分为合法合规解决方案和安全性解决方案。

- 合法合规解决方案

针对《中国人民共和国个人信息保护法》、《关基条例》等相关要求，在数据收集环节，需对数据采集目的、采集类型、存储位置等信息，可通过隐私政策明示授权的方式获得用户的许可，且不可默认替用户勾选。针对用户数据中涉及操作和存储合法性风险，需保证中华人民共和国境内数据存储，数据收集最小化，并保存隐私协议授权记录、采集记录和相关操作记录，以备后续检查机构核查。针对门户网站、小程序等展示用户数据，需符合隐私政策要求，保证数据收集渠道的合法性；针对数据存储环节，制定数据备份与恢复操作规程，定期开展数据备份及数据恢复性测试工作，保存测试记录。

- 安全性解决方案

针对运营商客服系统数据收集、存储及使用场景下的安全性风险，主要包括：处理环境、处理方式、处理操作等安全性风险。以上风险需要与已有安全防护措施相结合，需要考虑的数据安全技术、管理手段包括但不限于：

- 采用数据证书实现抗抵赖；
- 采用数字水印实现溯源；
- 数据网络传输加密；
- 敏感数据本体传输加密；
- 敏感数据加密存储；
- 网络安全域配置访问控制策略；
- 数据处理权限最小配置；
- 数据处理操作权限定期审计；
- 数据分类分级及差异化保护措施；
- 数据传输接口鉴权；
- 数据使用去标识化处理；
- 做好自身服务的网络安全防控；
- 预防业务被攻击不可用的风险；
- 与系统运维支撑人员签订数据安全保密协议；
- 数据使用、导出审批机制；
- 数据安全事件应急响应、处置机制；
- 第三方合作方数据安全管理评估。

实践总结

电信行业运营商面临着新老系统并存等问题，同时也面临国家、行业等一系列针对安全生产，特别是数据安全保护责任落实等新的问题。在执行风险评估工作，特别是数据安全风险评估的过程中，缺乏有效便捷的工具支撑，造成严重的人力物力的浪费。在具体的实践落地过程中，电信运营商企业急切需要可实施落地的数据安全风险评估服务。（具体的风险评估工具，可参照附录A中的内容）

3.2.案例2-金融行业的数据安全风险评估

背景

随着金融行业信息化技术的不断发展，金融服务和业务往来均已运行在信息化基础设施上了。在不同的基础设施生产运行的过程中，业务的扩大发展，会产生多种的数据资产。随着大数据、云计算、区块链等新技术的深入应用，金融数据也逐渐地从信息化资产转变为了金融生产要素。数据泄露、滥用等安全威胁的影响也从金融机构内部逐渐扩大到行业间，甚至影响了国家、社会安全与公众利益。如何在符合金融业务发展的基本需求上，保证数据安全的能力，切实防范金融风险，保障金融数据价值，是所有金融企业面临的重要问题。

由于金融数据的重要性，国家、行业等相关机构与监管部门，提供了一系列可参照的规范标准《金融数据安全 数据分类分级指南》、《金融数据

安全 数据生命周期规范》等；另一方面，相关机构也在探索如何科学有效的指导从业企业，防控数据安全事件风险，通过体系化的方式提供有效保障。

面临的挑战

某股份制商业银行，在满足《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、行业标准规范等法律法规以及上级监管机构对数据安全的要求下，还需要提高整体的数据安全保障能力，建立健全数据处理活动下的数据安全管理制度，采取相应的技术措施和其他必要措施，全面保障数据安全。受困于落实数据安全保障工作困难重重，数据在多个业务多个环节中复杂流转，缺乏一套统一的数据安全治理落地方案指导后续的工作。

某股份制商业银行，前期利用已有实践经验，完成了部分数据安全管理的工作，但在面对大量涉及个人信息数据的合法合规经营与业务开展的问题下，缺乏有效的实践落地指导依据。

数据安全风险评估实施

参照同业实践经验与本白皮书提供的数据安全风险评估方法，针对“商业银行手机客户端App数据收集和数据使用”数据处理活动场景，进行个人信息风险评估工作，评估流程如下：

1.核心要素分析

- 数据处理角色：
  - 数据主体：商业银行自然人客户；
  - 数据控制者：商业银行；
  - 数据处理者：商业银行内执行数据处理工作的组织或员工。
- 数据处理过程：
  - 数据处理环境：商业银行手机客户端业务服务提供过程中需要的环境，包括：App（包括：SDK、API接口等）、移动终端操作系统、网络环境等；提供商业银行手机业务服务的服务端环境。
  - 数据处理方式：
    - 在商业银行客户通过手机客户端，使用手机业务服务的过程中，通过终端环境和服务端环境，收集用户的个人信息、业务信息等；
    - 收集到的信息通过网络环境传输至商业银行手机业务服务的服务端环境；
    - 客户通过商业银行手机客户端进行业务查询的过程中，客户相关数据从商业银行服务端环境，通过网络环境传输至客户手机端App内部执行展示。
  - 数据处理操作：
    - 在数据收集环节，App通过让客户同意数据收集授权协议的方式，获取用户相关个人信息、业务信息等数据；
    - 收集到的数据通过加密网络传输回业务服务的服务器端；
    - 在数据使用环节，App提供服务的SDK或API接口等服务组件，向客户提供了数据查询和展示的功能。
- 处理范围：

- 数据类型：个人信息、业务信息；
- 数据量级：依据业务开展的用户数量决定；
- 数据主体范围：中华人民共和国境内用户信息；成人信息或者未成年人信息。

➢ 处理目的和结果

- 处理目的的实现：商业银行业务部门，通过手机客户端App向商业银行客户提供业务服务，在业务服务的过程中，依据数据收集授权协议，收集用户个人信息、业务信息等数据，并提供相关数据查询和展示功能；
- 数据流通关系变化：客户数据使用权，从客户变动到了商业银行；
- 数据状态发生变化：可能存在时间状态（过期存储）、地域状态（跨境）、内容状态（客户数据值等）等发生变化。

2.数据处理活动合法合规评估

- 《中华人民共和国个人信息保护法》要求，数据处理活动中，需要明示数据采集目的、采集数据类型、存储位置、获取用户授权等情况；
- 商业银行客户，需要通过商业银行手机客户端所提供的确认服务，执行确认隐私协议工作，且不允许替用户默认勾选。这个过程中，涉及合规性风险里，违规采集风险；
- 商业银行，需要记录客户的确认授权采集操作，保存确认记录以备查阅；采集到的客户数据需要境内存储；采集客户数据需遵循最小化原则；提供的隐私告知协议，需要包含：采集目的等相关信息。涉及合规性风险里，采集目的、最小授权、跨境存储、传输保护；
- 商业银行提供的查询服务，在客户端App内展示的数据，需保证是经过客户授权的数据。这些数据需要保证是通过合法合规的渠道收集。

3.数据处理活动安全性评估

➢ 商业银行手机客户端App数据收集和数据使用场景下的安全性风险评估：

- 处理方式安全评估
  - 使用权限安全风险：处理方式提权、处理范围提权、使用类型提权等；
  - 数据使用安全风险：服务接口被DDos攻击、数据非授权访问、数据越权访问等；
  - API数据接口安全风险：接口非授权数据访问、接口非授权数据爬取等。
- 处理操作安全评估
  - 操作越权安全风险：数据使用未授权、数据使用范围未授权；
  - 操作抵赖安全风险：数据操作行为冒充；
  - 操作滥用安全风险：数据被滥用、数据操作冒充他人等；

- 操作泄漏安全风险：数据使用过程中恶意留存、恶意篡改数据等。

4.解决方案：

在商业银行手机客户端App数据收集和数据使用场景下，依据上面评估识别的数据安全风险情况，具体的解决方案分为合法合规解决方案和安全性解决方案。

➢ 合法合规解决方案

针对《中华人民共和国个人信息保护法》、行业相关标准规范等要求，在数据收集环节，对数据采集目的、采集类型、存储位置等信息，需要对用户明示，可通过隐私授权协议的方式获得用户的许可，且不可默认替用户勾选。针对客户数据中涉及操作和存储合法性风险，需保证中华人民共和国境内数据存储，数据采集最小化，并保存授权协议、采集记录和相关操作记录，以备后续检查机构核查。针对客户端内展示用户数据，需符合隐私协议和采集协议的要求，保证数据采集渠道的合法性。

➢ 安全性解决方案

针对商业银行手机客户端App数据收集和数据使用场景下的安全性风险，主要包括：处理环境、处理方式、处理操作等安全性风险。以上风险需要与已有安全防护措施相结合，需要考虑的数据安全技术手段包括但不限于：

- 终端需要App加固、反破解反爬虫；
- 网络传输需要加密；
- 敏感数据需要本体加密；
- 数据处理权限需要审计；
- 数据操作情况需要监测和审计；
- 数据分类分级；
- 数据使用鉴权；
- 数据服务接口鉴权；
- 数据脱敏/加密后在App展示；
- 做好自身服务的网络安全防控；
- 预防服务被攻击不可用的风险；

实践总结

金融行业相关企业面临的数据安全风险并不一致。特别是由于金融行业的特殊性，不管是业务数据还是客户数据，均存在极高的商业价值。近些年屡屡发生数据安全事件问题（如大量客户数据泄露），给相关机构带来了巨大的行业影响和声誉影响。

在具体的评估实践过程中，由于数据管理工作的特殊性，不仅仅是跨部门甚至涉及跨区域部门共同协作。尤其落实数据安全管理工作，更是对责任与业务部门都提出了更高要求。大多数机构内部安全管理，均倾向于通过发现客观实际存在的风险，推动业务相关部门整改需求的方式，并提高整体的数据安全风险防控水位。这也意味着，数据安全风险评估工作需要评估方法与评估工具的融合，通过使用工具发现风险问题客观存在的角度，推动业务整改执行。

3.3.案例3-IT互联网行业的数据安全风险评估

背景

IT互联网行业由于自身业务发展的需要，会收集、存储、加工和使用大量个人数据。面对国家法律法规和监管机构相关的要求，个人数据在数据处理活动过程中合法合规的满足情况，是IT互联网企业当前面临的重要问题。特别是《网络数据安全管理条例（征求意见稿）》中对互联网平台运营者义务的要求，是IT互联网企业在数据安全管理工作中的重点。

互联网企业信息化程度高，新技术运用充分，其中大量使用个人数据来处理相关业务。大型互联网平台在发展的过程中，对于个人数据的使用和处理，已经融入用户的日常生活中。

面临的挑战

伴随着IT信息化建设和互联网企业的高速发展，互联网企业利用海量个人数据，进行业务分析与业务运营的工作已经成为了互联网行业高速发展的推进剂。但其中也不乏，前期法律法规不完善与行业高速发展过程中，遇到的违规问题，造成大量损害互联网用户的行为，如：大数据杀熟、用户数据滥用等行为。《网络数据安全管理条例（征求意见稿）》中第五十四条，“互联网平台运营者利用人工智能、虚拟现实、深度合成等新技术开展数据处理活动的，应当按照国家有关规定进行安全评估。”

数据安全风险评估实施

参照大型互联网企业数据安全管理实践经验与本白皮书提供的数据安全风险评估方法，针对“互联网企业数据使用”数据处理活动场景实施数据安全风险评估工作。

1. 核心要素分析

- 数据处理角色：
  - 数据主体：互联网企业C端自然人用户；
  - 数据控制者：互联网企业；
  - 数据处理者：互联网企业内执行数据处理工作的组织或员工。
- 数据处理过程：
  - 数据处理环境：互联网企业内部使用数据的环境，包括：数据查询平台、数据提取平台、客户端App用户数据展示等。
  - 数据处理方式：
    - 通过数据服务API接口执行相关数据操作；
    - 通过内部数据提取流程获取用户相关数据。
  - 数据处理操作：
    - 互联网企业内部员工通过数据查询API接口，执行用户数据查询操作，获取用户数据，开展业务活动；
    - 互联网企业内部员工通过数据提取流程，提交用户数据获取申请，审批后通过数据提取平台获取用户数据，执行业务活动；

- 客户端App软件，通过数据服务API接口，获取用户数据，展示在App显示页面上，供互联网企业C端用户使用数据。

➢ 处理范围：

- 数据类型：个人信息、业务信息；
- 数据量级：依据业务开展的用户数决定；
- 数据主体范围：中华人民共和国境内用户信息；成人信息或者未成年人信息；

➢ 处理目的和结果

- 处理目的的实现：
  - 互联网企业内部员工通过数据服务API接口，执行数据相关操作，使用相关数据开展业务活动；
  - 互联网企业内部员工，通过数据提取流程，获取到数据后，在本地终端中执行相关数据分析和存储后，使用相关数据执行业务活动；
  - 互联网企业C端客户，通过客户端软件，执行个人数据查询操作，获取存储在互联网企业内的用户个人数据。
- 数据状态发生变化：可能存在使用范围状态（超范围使用）、使用目的状态（超目的使用）、时间状态（过期使用）、地域状态（跨境使用）、内容状态（脱敏或加密到明文）、物理状态（服务器存储-终端存储）等发生变化。

2. 数据处理活动合法合规评估

- 互联网企业数据管理部门，需要记录企业内部员工获取数据的操作请求等，需要对数据使用目的进行合法合规性校验，需要对数据使用种类、数量、范围等进行最小原则校验，需要对数据是否需要跨境使用执行审计，需要对数据使用场景是否与用户同意使用场景相符合，执行检查操作等；
- 互联网企业内部员工，需要依法依规依据业务需求最小原则，使用数据。使用数据过程中，不允许出境使用，不允许擅自变更用户同意使用场景，不允许将获取的用户数据转作其他目的使用；
- 互联网企业C端客户，向互联网企业申请使用个人数据时，需提供具有可鉴别身份和目的的数据主体相关信息。数据使用过程中，须符合国家法律法规的要求。

3. 数据处理活动安全性评估

- 处理方式安全评估：
  - 使用权限安全风险：使用方式提权、使用范围提权、使用类型提权等；
  - 使用角色安全风险：角色冒用等；
  - 使用服务可用性安全风险：查询服务被拒绝服务攻击等；
  - 数据传输安全风险：数据窃取和监听、数据明文传输等；
  - API数据服务接口安全风险：接口未鉴权、接口存在水平越权等；
- 处理操作安全评估：
  - 操作越权安全风险：数据使用未授权、数据使用范围未授权；

- 操作抵赖安全风险：数据操作行为冒充；
- 操作滥用安全风险：数据被滥用、数据操作冒充他人等；
- 操作泄漏安全风险：数据使用过程中恶意留存、恶意篡改数据等。

4. 解决方案：

在互联网企业数据使用场景下，依据上面评估识别的数据安全风险情况，具体的解决方案分为合法合规解决方案和安全性解决方案。

➢ 合法合规解决方案

针对内部数据使用场景的合法性风险，需要采取一系列审批、监控、审计等手段，对使用数据的内部员工的处理行为进行监测。包括：数据获取请求审批、数据使用合法性审批、数据跨境使用审批、数据超范围使用审批等。针对使用过程中，需要执行全程监测和事后审计，包括：使用范围、使用场景、使用目的、是否存在出境访问等。针对使用服务的C端客户，需校验客户身份的有效性，保证不出现非授权访问的情况。

➢ 安全性解决方案

针对互联网企业数据使用场景下的安全性风险，主要包括：处理环境、处理方式、处理操作等安全性风险。以上风险需要与已有安全防护措施相结合，需要考虑的数据安全技术手段包括但不限于：

- 传统终端安全与Web网络安全；
- 文件交换安全；
- 数据使用身份鉴权；
- 数据分类分级；
- 数据服务接口鉴权；
- 数据脱敏/加密后应用（消除个人身份特征）；
- 数据传输加密；
- 数据使用操作监控和审计，并保存相关操作记录；
- 做好自身服务的网络安全防控，预防服务被攻击不可用的风险；
- 终端需要App加固、反破解反爬虫。

实践总结

互联网企业在利用新技术、大数据分析等高新技术方面，促进了互联网业务的极大发展，但也不可忽视高速发展过程中，对于数据安全管理的要求，特别是在内部数据使用和第三方数据共享与使用过程中，需要密切关注国家、行业等监管合规机构的要求，在切实提升用户服务质量的同时，减少对用户的影响，特别是用户个人数据滥用以及违法违规业务经营上的问题。

⊕ 3.4.案例4-医疗行业的数据安全风险评估

背景

随着医疗行业数字信息化的大力发展，为医患提供便捷的医疗服务，进而会产生大量的医疗数据。特别是借助互联网的应用、提供的小程序，导致

大量医疗数据的流转，如电子挂号、电子病历、电子诊断信息的传输，加大了数据泄露的风险，关乎国家和人民的利益。

由于医疗机构本身不具备强大的信息化能力，大量的信息化建设均第三方外部机构承建和运维。更多的关注在医疗水平的提升上，忽视了关于医疗信息化过程中，医疗数据特别是医患数据的共享与管理问题。

面临的挑战

从《中华人民共和国个人信息保护法》中关于敏感个人信息数据中医疗健康数据的要求，个人信息处理者需要做好充分的数据安全风险评估工作和个人敏感数据影响评估工作。高速信息化发展的阶段，不管是国家监管层面，还是社会个人层面，都对医疗数据的安全管理，提出了更高的要求。

数据安全风险评估实施

参照大型医院在医疗数据安全管理上的经验以及本白皮书提供的数据安全风险评估的方法，针对“数字医疗行业中个人医疗数据公开”数据应用场景进行数据安全风险评估，具体流程如下：

1. 核心要素分析

- 数据处理角色：
  - 数据主体：医疗机构患者；
  - 数据控制者：医疗机构；
  - 数据处理者：医疗机构员工、内部运维人员。
- 数据处理过程：
  - 数据处理环境：医疗机构内部公开数据的环境，包括：病例查询平台、患者端App用户病例查询展示等。
  - 数据处理方式：
    - 通过数据服务API接口执行相关数据操作。
  - 数据处理操作：
    - 医疗结构相关展示设备通过数据查询API接口，执行患者医疗数据查询操作，获取患者医疗数据，提供业务服务；
    - 患者端App软件，通过数据服务API接口，获取患者医疗数据，展示在App显示页面上，供医疗机构患者查询自己的医疗数据。
- 处理范围：
  - 数据类型：敏感个人信息、医患相关信息；
  - 数据量级：医疗患者数量决定；
  - 数据主体范围：中华人民共和国境内用户信息；成人信息或者未成年人信息。
- 处理目的和结果
  - 处理目的的实现：
    - 医疗机构相关展示设备通过数据服务API接口，执行患者医疗数据查询操作，获取患者医疗数据，提供医疗病例公开查询等服务；
    - 患者端App客户，通过客户端软件，获取患者医疗数据，展示在App显示页面上，供医疗机构患者查询自己的医疗数据。

- 数据状态发生变化：可能存在使用范围状态（超范围使用）、使用目的状态（超目的使用）、时间状态（过期使用）、地域状态（跨境使用）、内容状态（脱敏或加密到明文）、物理状态（服务器存储-终端存储）、等发生变化。

2. 医疗机构数据公开的合法合规评估

- 医疗机构内部，需要记录内部员工或第三方信息化运维机构人员获取数据的操作请求等，需要对数据使用目的进行合法合规性校验，需要对数据使用种类、数量、范围等进行最小原则校验，需要对数据是否需要跨境使用执行审计，需要对数据使用场景是否与用户同意使用场景相符合，执行检查操作等。特别是对第三方信息化服务提供机构的合法合规性评估，需要明确在信息化建设过程中，依据国家法律法规的要求，对医患数据做了合法合规的处理操作；
- 患者端App客户，向医疗机构申请获取个人医疗数据时，需提供具有可鉴别身份和目的的数据主体相关信息。数据使用过程中，须符合国家法律法规的要求。

3. 医疗数据公开的安全性风险评估

- 处理方式安全评估
  - 使用权限安全风险：使用方式提权、使用范围提权、使用类型提权等；
  - 使用角色安全风险：角色冒用等；
  - 使用服务可用性安全风险：查询服务被拒绝服务攻击等；
  - API数据服务接口安全风险:接口未鉴权、接口存在水平越权等；
- 处理操作安全评估
  - 操作越权安全风险：数据使用未授权、数据使用范围未授权；
  - 操作抵赖安全风险：数据操作行为被抵赖；
  - 操作滥用安全风险：数据被滥用、数据操作冒充他人等。

4. 解决方案：

在医疗机构数据公开场景下，依据上面评估得到的数据安全风险情况，具体的解决方案分为合法合规解决方案和安全性解决方案。

➢ 合法性解决方案

针对内部数据公开场景和第三方运维场景的合法合规，需要采取一系列审批、监控、审计等手段，对使用数据的内部员工和外部第三方运维人员的处理行为进行监测。包括：数据使用合法性审批、数据跨境行为审计、数据超范围使用审批等。针对使用过程中，需要执行全程监测和事后审计，包括：使用范围、使用场景、使用目的、是否存在跨境访问等。针对使用服务的C端患者，需校验患者身份的有效性，保证不出现非授权访问的情况。

➢ 安全性解决方案

针对医疗结构数据公开场景下的安全性风险，主要包括：处理环境、处理方式、处理操作等安全性风险。以上风险需要与已有安全防护措施相结合，需要考虑的数据安全技术手段包括但不限于：

- 传统终端安全与Web网络安全；

- API数据安全身份鉴权、接口鉴权、使用监控和审计，并保存相关操作记录；
- 文件交换安全；
- 数据分类分级；
- 数据脱敏/加密后应用（消除个人身份特征）；
- 数据传输加密；
- 数据使用操作监控和审计，并保存相关操作记录；
- 做好自身服务的网络安全防控，预防服务被攻击不可用的风险；
- 终端需要App加固、反破解反爬虫。

实践总结

2021网络安全周上曝光医患数据泄露的安全问题。主要是由于医院在信息化过程中，对于医患数据的安全管理问题，没有足够的重视。委托第三方进行建设和运维的过程中，对于第三方管理上存在疏漏，导致医疗数据服务和管理风险并存的局面。

现阶段大部分医疗单位和服务机构都已经开始重视医患数据的管理，国家层面也制定了相关的法律法规和行业规范。但落地评估和检查，缺乏一套行之有效的检测方案和落地工具。

04

数据安全治理未来展望

4 数据安全治理未来展望

实践推动规则的细化

数据安全治理不能成为空中楼阁，不能仅仅停留在策略的规划和设计，需要通过数据安全风险评估的方式，在实践中形成匹配数据治理成果、数据安全管理要求需求变化、数据安全技术发展的持续能力提升。通过实践才有可能形成行业、地区、甚至整体数据安全治理的良好实践直至最佳实践的总结，为数据安全治理更全面更有效地覆盖到数据生产要素价值发挥的每一个细节中，确保数据价值持续地提升。

面对层出不穷的数据安全风险，数据安全治理需要在规则上不断精细化，将国家、地方、行业的整体安全规划把控有效分解到具体的执行和操作层面，帮助各企业和组织能更简单更有针对性地开展数据安全治理活动，更精确地发现风险，提升数据安全防护能力。

新技术新应用的数据安全治理

在数据安全治理工作的不断开展和进步中，平衡数据价值和数据安全的各类新技术不断出现，差分隐私、多方计算、联邦学习等，都是伴随着数据安全治理的需要而出现，并逐渐扩展了适用的场景和领域。新的业务场景，如物联网、车联网等的发展，也在持续为数据安全治理提出了新的需求。与时俱进，迎接新挑战，拥抱新技术，也是数据安全治理未来发展和变化的重要方向。

数据安全风险管理来推动安全治理

基于数据与数据处理活动的数据安全治理框架，提供了一种全新的依托数据资产识别和数据处理活动要素相结合的风险分析方法。通过对数据处理活动典型场景的风险评估，协助企业更好的从合规性和安全性两个维度处理数据安全治理工作。依托企业后续全面建设的数据安全风险管控能力，数据安全风险治理工作必将快速落地。

5 致谢

技术指导单位：CCIA数据安全工作委员会。
指导专家：何延哲、陈妍、陈世翔（以上专家排名不分先后）。

6 附录A 风险评估工具

风险评估工作的顺利开展与进行，对企业来说，通常意味着很大的成本，原因在于大部分的风险评估工作的开展，需要专家的专业性和经验的传承与应用。在企业明确了具体的风险评估方法后，需要借鉴或参照行业经验或国家相关法律法规相关规定，执行具体的风险评估操作，其中大部分工作，都需要手动评估执行。

参考 GB/T 20984-2007《信息安全技术 信息安全风险评估规范》中附录 B 中的分类和内容，明确数据安全风险评估方法的落地实施操作，可评估过程中，可以沉专家经验，甚至是自动化执行相关评估操作使用的工具，进行分类，包括：数据处理活动识别工具、数据处理活动合法合规判别工具、数据处理活动安全探测工具。

➢ 数据处理活动识别工具

此类工具的主要作用为：帮助风险评估实施人员识别待评估系统内进行的重要数据处理活动，并对数据处理活动要素进行拆分梳理。此类工具侧重流程梳理，利用专家的经验进行数据处理活动识别。此类工具可通过问卷、模型等方式呈现。

- 问卷工具：此种工具将提供多种的数据处理活动探测角度，从多种维度对待评估系统进行分析，帮助评估人员进行数据处理活动梳理，同时收集数据处理活动要素，为安全风险分析提供帮助。
- 模型工具：此种工具提供多种常见重要数据处理活动集合，使用者可将模型库内容与待评估系统进行对照分析，识别梳理数据处理活动。

➢ 数据处理活动合法合规判别工具

此类工具的主要作用为：对数据处理活动中存在的合法合规性进行识别。此类工具将协助评估人员对数据处理活动合法合规评估要点进行识别与提取，同时提供合法合规要求参考库，帮助评估人员进行判断。此类工具主要有：

- 隐私政策解析：此类工具将对待评估系统隐私政策进行解析，对隐私政策中声明的敏感数据收集、使用、共享等情况进行自动化解析梳理，辅助业务合规性判定。
- 数据映射：此类工具将协助评估人员对待评估数据资产进行数据-业务关系梳理，识别数据流上下游链路。
- 法律合规库：此类工具将对数据安全领域的法律、标准、条例等进行梳理，汇总合规要求条目并进行要点分析，评估者可参照合规集合进行安全评估。

➢ 数据处理活动安全探测工具

此类工具的主要作用为：探测收集数据处理活动中各活动要素的安全现状，评估数据处理活动安全性风险。此类工具主要建立在自动化探测基础上，结合专家经验全面探测数据处理活动安全情况。随着评估工作的经验累积，此种类评估工具可不断丰富、优化检测规则。

- 安全漏洞扫描：此种工具内置多种漏洞探测规则，主要对操作系统、数据库系统、网络协议等进行安全脆弱性检测，帮助评估人员快速进行安全漏洞发掘探测。

- 数据资产识别：此种工具可自动扫描探测待评估系统多种类型数据资产，包括结构化数据、非结构化数据及半结构化数据，自动识别敏感数据类型，检测数据保护能力，如数据加密、数据脱敏等情况。
- 账号权限探测：此种工具可对操作系统、应用、数据库等账号进行权限探测及梳理，检测违规的权限开放、特权账号等。
- 数据暴露检测：此种工具可自动梳理待评估系统数据接口，识别数据接口的返回内容，检测敏感数据暴露面。
- 数据流向探测：此种工具可自动识别敏感数据流向、敏感数据访问情况，包括数据库出入库、应用系统间的数据调用、跨区域数据传输等情况。

➢ 相关概念：

- 数据暴露：指数据在具体的应用过程中，通过某种技术手段对外提供服务。例如：API 数据接口服务方式。
- 数据流向：与数据流相同，指数据在处理过程中，从一个处理环节流动到另一个处理环节的流向。例如：数据从存储服务器流动到应用服务器；数据从国内服务器流动到境外服务器等。

风险评估工具的使用价值，最大化的减轻了企业在数据安全风险评估中的实施工作量。基于数据资产识别工具和数据处理活动识别工具，识别和分析企业数据的重要程度和影响面，再借助合法合规判别工具中及时更新的法律法规要点解读，配合各种安全探测工具，从合法合规角度和技术风险角度，全方位保证了风险评估的全面覆盖。

同时由于工具化的专家经验沉淀，以及在大数据处理能力上的工具化操作，都最大程度的为企业风险评估工作的实施落地，提供了宝贵的经验沉淀和成本的降低。特别是针对大型集团类企业的多地多设备的数据风险评估工作，可便携式测评工具，是更好的选择，即解决了多中心测评部署问题，也解决了测评自动化问题，可谓是一举多得的事情。

7 参考文献

编号	名称	类型
1	《中华人民共和国网络安全法》	法律
2	《中华人民共和国数据安全法》	法律
3	《中华人民共和国个人信息保护法》	法律
4	《关键信息基础设施安全保护条例》	行政法规
5	《网络数据安全管理条例(征求意见稿)》	部门规章
6	GB/T 20984-2007《信息安全技术 信息安全风险评估规范》	国家标准
7	GB/T 35273-2020 《信息安全技术 个人信息安全规范》	国家标准
8	GB/T 39335-2020 《信息安全技术 个人信息安全影响评估指南》	国家标准
9	GB/T 37988-2019 《信息安全技术 数据安全能力成熟度模型》	国家标准
10	GB/T 37973-2019《信息安全技术 大数据安全管理指南》	国家标准
11	JR/T 0197-2020 《金融数据安全 数据安全分级指南》	行业标准
12	JR/T 0171-2020 《个人金融信息保护技术规范》	行业标准
13	《电信网和互联网数据安全风险评估实施方法》	行业标准
14	《网络安全态势感知技术标准化白皮书》	其他
15	《数据安全治理白皮书》	其他
16	《银行业数据安全体系建设指南》	其他

数据风险全知道

KNOW YOUR DATA, MANAGE YOUR RISK

杭州：杭州市余杭区文一西路1338号海创大厦A座10楼1001室
北京：北京市海淀区中关村南大街2号数码大厦A座910室
上海：上海市长宁区天山西路568号统一企业广场A座8A0607室
深圳：深圳市宝安区富源商贸中心C座1702室
广州：广州市番禺区市莲路傍江西村段18号新安商务中心452室

电话：400-100-9516
官网：www.data-sec.com
合作：marketing@mail.qzkeji.cn
支持：support@mail.qzkeji.cn