企业数据合规工作指引

法惠企航

青岛市政府购买法律服务督促
惠企政策落实工作联席会议办公室

2022 年

前　言

伴随大数据、云计算、人工智能等新兴技术在数字经济中的广泛运用，数据要素已成为引领中国高质量发展的新引擎。但随之而来的是，数据活动场景复杂性增大，新的信息安全与数据保护风险不断产生。

目前，我国的数据安全也迈入强监管时代。《网络安全法》《数据安全法》《个人信息保护法》等法律陆续出台，健全了我国数据安全法律法规体系，构建了网络空间治理和数据保护的基本法，对企业的数据收集以及使用等各环节，做出了明确规范和要求。

在此背景下，特编制山东省首部《企业数据合规工作指引》，涵盖数据风险评估处置、数据全生命周期保护及企业数据合规体系建设等内容，供参考使用。

组织单位：青岛市司法局

编写单位：山东文康律师事务所

编写人员：马清泉 王译萱

目　录

企业数据合规工作指引

第一章 总则

一、制定目的

为引导企业加强数据合规管理，保护个人信息，保障数据安全，规范数据处理活动，根据《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》等法律法规，制定本指引。

二、适用范围

各类所有制企业进行数据处理活动均可参照本指引开展数据合规管理工作，特别是适用于互联网公司，或具有大量数据处理需求的企业。本指引不具有强制性，法律法规对数据合规另有专门规定的，从其规定。

第二章 数据处理规则

一、禁止从事的数据活动

企业及其员工开展数据处理活动应当遵守法律、行政法规，尊重社会公德和伦理，不得从事以下活动:（一）危害国家安全、荣誉和利益，泄露国家秘密和工作秘密;（二）侵害他人人格权、知识产权和其他合法权益等;（三）通过窃取或者以其他非法方式获取数据;（四）非法出售或者非法向他人提供数据;（五）制作、发布、复制、传播违法信息;（六）法律、行政法规禁止的其他行为。任何个人和组织知道或者应当知道他人从事前款活

动的，不得为其提供技术支持、工具、程序和广告推广、支付结算等服务。

二、个人信息处理的规则

数据处理者在个人信息处理活动中，应当保障《个人信息保护法》规定的个人对其个人信息处理活动享有的知情权、决定权、查阅权、复制权、更正、补充权、删除权等权利。

数据处理者处理个人信息，应当依据《个人信息保护法》的规定遵守以下规则：（一）按照服务类型分别向个人申请处理个人信息的同意，不得使用概括性条款取得同意；（二）处理个人生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感个人信息应当取得个人单独同意；（三）处理不满十四周岁未成年人的个人信息，应当取得其监护人同意；（四）不得以改善服务质量、提升用户体验、研发新产品等为由，强迫个人同意处理其个人信息；（五）不得通过误导、欺诈、胁迫等方式获得个人的同意；（六）不得通过捆绑不同类型服务、批量申请同意等方式诱导、强迫个人进行批量个人信息同意；（七）不得超出个人授权同意的范围处理个人信息；（八）不得在个人明确表示不同意后，频繁征求同意、干扰正常使用服务。

个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，数据处理者应当重新取得个人同意，并同步修改个人信息处理规则。依法无需取得个人同意的除外。

三、向第三方提供数据的规则

数据处理者向第三方提供个人信息，或者共享、交易、委托处理重要数据的，应当遵守以下规则:

（一）向个人告知提供个人信息的目的、类型、方式、范围、存储期限、存储地点，并取得个人单独同意，符合法律、行政法规规定的不需要取得个人同意的情形或者经过匿名化处理的除外；

（二）与数据接收方约定处理数据的目的、范围、处理方式，数据安全保护措施等，通过合同等形式明确双方的数据安全责任义务，并对数据接收方的数据处理活动进行监督；

（三）留存个人同意记录及提供个人信息的日志记录，共享、交易、委托处理重要数据的审批记录、日志记录至少五年。

数据处理者为订立、履行个人作为一方当事人的合同所必需向第三方提供个人信息的，在采取适当的数据保护措施后无需取得个人单独同意。

四、接收方处理数据的规则

数据接收方应当履行约定的义务，不得超出约定的目的、范围、处理方式处理个人信息和重要数据，且不得从事数据法规禁止的行为。

五、跨境提供个人信息等数据的规则

数据处理者因业务等需要，确需向中华人民共和国境外提供数据的，应当符合法律法规关于跨境提供数据的规定，事先开展数据出境风险自评估。

数据处理者跨境提供个人信息的，应当向个人等告知境外数据接收方的名称、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外数据接收方行使个人信息权利的方式等事项，并取得个人的单独同意。

第三章 数据风险评估与处置

一、数据风险分级评估

企业在识别数据风险内容的基础上，可根据自身经营规模、组织体系、业务内容以及市场环境，分析和评估数据风险的来源、发生的可能性、后果的严重性等，并对数据风险进行分级，建立数据分类分级制度。

数据合规部门负责人应当根据风险评估结果对不同职级、不同工作范围的管理层与员工进行风险提示，降低管理层和员工的违法犯罪风险。

二、立即停止违法行为

经评估发现可能已经发生数据违法行为，或者数据监管部门已立案并启动调查程序的，企业应当立即停止违法行为并与执法机构合作。

企业积极配合调查或者主动消除、减轻违法行为危害后果的，可能会获得数据监管部门从轻或者减轻处罚。

三、及时采取补救措施

企业应建立健全数据安全事件应急预案与风险处置机制，对识别和评估的各类数据风险设置恰当的控制和应对措施来降低风险。

发生个人信息等数据泄露、篡改、丢失等事件的，数据处理者应当立即采取补救措施，并通知所在地区的数据监管部门。

四、积极应对监管调查

当企业受到数据监管部门调查时，应通知管理层、法务负责人、数据合规负责人和相关业务工作负责人等，按照企业内部受调查操作流程妥善应对，进行内部初步调查，分析相关法律法规并评估数据违法行为成立的可能性与法律后果。

企业应积极配合数据监管机构调查。不得拒绝提供有关材料、信息，或者提供虚假材料、信息，或者隐匿、销毁、转移证据，或者有其他拒绝、阻碍调查的行为。安全事件涉嫌犯罪的，应当及时向公安机关报案。

第四章 数据全生命周期合规要求

一、数据全生命周期

数据全生命周期，是指数据从产生，经过数据收集、数据传输、数据存储、数据使用（包括计算、分析、可视化等）、数据交换，直至数据销毁等各种生存形态的演变过程。

二、数据收集合规要求

数据收集是收集者获得数据控制权的行为，包括由数据主体主动提供、通过与数据主体交互或记录数据主体的行为等自动收集行为，以及通过共享、购买、收集公开信息等间接方式收集数据等行为。

（一）数据收集的主要方式

1.收集者通过与数据主体交互或记录数据主体行为而直接、主动地收集数据，此种方式常见于企业通过App采集和web端采集收集个人用户的数据，包括个人身份信息、交易信息、财产信息、地理位置信息、健康信息、行踪信息等。

2.数据收集者从公开或半公开的互联网平台收集数据，使用该种方式收集数据主要是通过爬虫技术或API等方式从公开或半公开的互联网平台收集数据。

3.数据收集者通过与第三方共享、购买的方式收集数据。应当审查第三方对数据是否具有所有权，以及审查第三方收集数据的方式是否合法、合规。

（二）数据收集的基本原则

企业在数据收集时，应符合合法、知情同意、必要、安全、禁止泄漏等基本原则。

1.合法：企业收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据;

2.知情同意：企业应当向数据主体公开收集数据的规则，明示收集数据的目的、用途、方式、范围、采集源、采集渠道等内容，且应获得数据主体的同意和授权；

3.必要：企业不应收集与提供产品、服务无关的数据，不应当超范围收集数据；

4.安全：企业应保障所收集数据的安全，并落实相应数据安全等级保护要求；

5.禁止泄露：数据收集者应对所收集的数据严格保密，不得泄露、篡改、损毁，不得擅自出售或者非法向他人提供。

三、数据传输合规要求

（一）加密传输

做好传输接口管控和监测，并对涉敏数据进行加密传输。

（二）制度流程

建立数据传输安全管理规范，明确数据传输安全要求，确定需要对数据传输加密的场景。由于加密技术的实现都依赖密钥，所以需要建立密钥管理安全规范，明确密钥生成、分发、存取、更新、备份和销毁的流程和要求。

四、数据存储合规要求

（一）重要数据境内存储

涉及符合关键信息基础设施的企业在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业

务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估。

（二）存储期限

1.根据相关法律法规规定，企业应当保留网络日志至少6个月。

2.企业对于从用户、第三方、公开渠道获得的与用户相关的个人信息、数据进行处理的，应当在事前进行风险评估，并对处理情况进行记录，风险评估报告和处理情况记录应当至少保存三年。

（三）存储合规要求

1.建立数据存储的安全策略;

2.建立企业内部数据存储安全管理制度;

3.建立加密系统;

4.数据丢失预防，建立备份和恢复制度;

5.关注企业网络安全性。

五、数据使用合规要求

（一）数据访问控制措施

1.对被授权访问数据的人员，严格遵循数据处理最小化、必要原则，明确数据的处理和使用规范。对数据进行操作时，应做好去标识化处理，明确数据脱敏的业务场景和统一使用适合的脱敏技术。

2.对数据的重要操作设置内部审批流程，特别是进行批量修改、拷贝、下载等重要操作。

（二）个人信息展示

涉及通过界面展示个人信息的（如显示屏幕、纸面），个人信息控制者宜对需展示的个人信息采取去标识化处理等措施，降低个人信息在展示环节的泄露风险。例如，在个人信息展示时，防止内部非授权人员及个人信息主体之外的其他人员未经授权获取个人信息。

（三）用户画像

1. 对个人信息主体的特征描述不应：

（1）包含淫秽、色情、赌博、迷信、恐怖、暴力的内容；

（2）表达对民族、种族、宗教、残疾、疾病歧视的内容。

2.在业务运营或对外业务合作中使用不应：

（1）侵害公民、法人和其他组织的合法权益；

（2）危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序。

3.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。

六、数据共享合规要求

（一）建立数据共享规范，共享前应进行严格的审批并存档，同时开展个人信息安全影响评估。

（二）共享前开展风险评估（记录留存 3 年），与共享的接口调用方签订合作协议。

（三）开展共享监测和审计，数据导入导出应进行严格的审批和监控，建立数据交换、共享审核流程和监管平台，以确保数据对于数据共享的所有操作和行为进行日志记录，并对高危行为进行风险识别和管控。

七、数据删除和销毁合规要求

（一）数据删除合规要求

1.企业应当删除存在如下两种情形的个人信息:

（1）企业违反法律、行政法规的规定处理个人信息的;

（2）企业违反与自然人之间的约定处理个人信息的。

2.符合以下情形，个人信息主体要求删除的，企业也应及时删除个人信息:

（1）企业违反法律法规规定，收集、使用个人信息的;

（2）企业违反与个人信息主体的约定，收集、使用个人信息的;

（3）企业违反法律法规规定或违反与个人信息主体的约定向第三方共享、转让个人信息，且个人信息主体要求删除的，企业应立即停止共享、转让的行为，并通知第三方及时删除;

（4）企业违反法律法规规定或违反与个人信息主体的约定，公开披露个人信息，且个人信息主体要求删除的，企业应立即停止公开披露的行为，并发布通知要求相关接收方删除相应的信息。

（二）数据或介质销毁合规要求

应建立数据销毁机制，明确存储介质删除方法，数据销毁需由企业领导审批，同时采用可靠的技术手段，确保被删除和销毁的用户个人数据不能被再次还原。针对不同的存储介质和设备有其不可逆的销毁技术及流程，建立销毁监察机制，严防数据销毁阶段可能出现的数据泄露问题。

数据销毁包含物理层面和逻辑层面的销毁，按照处理成本、复杂性和安全性由低到高的顺序，将数据销毁方式分为数据覆盖、消磁，以及物理破坏数据及其存储介质等三个级别。

第五章 企业数据合规体系

一、合规组织

（一）合规责任人

企业的最高管理者是数据合规的第一责任人。最高管理者应当承担以下职责：1.分配足够和适当的资源来建立、发展、实施、评估、维护和改进数据合规管理体系；2.确保建立举报数据违规的有效机制；3.确保战略和运营目标与履行数据合规义务之间的一致性与平衡性；4.建立和维护问责机制，包括纪律处分和后果；5.确保将数据合规落实情况和效果纳入企业内部人员绩效考核体系。

（二）数据合规管理部门

鼓励各类企业设置专门的数据合规管理部门，或者将数据合规管理职能融入现有的企业合规管理体系。企业应当向数据合规管理部门负责人提供足够的授权、人力、财力以支持数据合规管理体系的运行。

（三）数据合规管理部门管理职责

数据合规管理部门应履行以下职责：1.制定数据合规管理整体方针策略，协调建立数据合规技术保障措施，牵头做好数据风险识别、风险评估、风险处置等工作；2.制定、完善数据合规计划，并推动其有效实施；3.审核评估企业的经营管理和业务行为，确保企业与供应商、代理商、经销商、关联企业、分支机构的业务活动，以及处理个人信息等活动符合数据法规的要求，并制定数据风险应对措施；4.组织或协助管理部门、业务部门等开展数据合规教育培训，并向管理层和各部门员工提供数据合规咨询；5.建立数据合规举报记录台账，对数据合规举报制定调查方案并开展调查；6.推动将数据合规责任纳入企业岗位职责和员工绩效考核评价体系。

二、合规机制

（一）咨询机制

企业可建立数据合规咨询机制，管理层和各部门员工在工作中可以向数据合规管理部门咨询数据合规问题。数据合规管理部

门应当不断学习、提升合规管理水平，也可以同外部机构和专业人士开展数据合规咨询合作。

（二）发现机制

发现机制是数据合规管理部门通过日常监测和定期评估发现数据不合规行为的机制，可以通过设置日常的流程监控、内部审核、重点核查以及定期评等方式发现企业及员工的违规行为，并及时按照合规计划采取相应的处置措施。

数据合规管理部门应定期向合规负责人汇报数据合规管理情况。当发生可能给企业带来重大数据合规风险的违规行为时，应当及时向合规负责人汇报，并提出相应的解决方案。

（三）举报机制

举报机制是员工根据合规计划举报企业内部违规行为的机制，应当允许员工实名或者匿名通过内部举报系统举报数据违规行为，并严格保护实名举报者和匿名举报者不受打击和报复，尤其是保护匿名举报者的个人信息安全。

（四）考核机制

企业应当结合自身情况建立数据合规考核机制，数据合规考核结果作为企业绩效考核的重要依据，与员工的评优评先、职务任免、职务晋升以及薪酬待遇等挂钩。

对于严格遵守数据合规的管理层和员工，制定适当的激励措施使合规计划得到一致遵守和执行。

对于不严格执行甚至违反合规计划的管理层和员工，采取适当的纪律措施进行惩戒，并根据违规程度采取不同的风险处置措施。

（五）培训机制

数据合规管理部门应当建立培训机制，定期为管理层、员工培训数据合规，使其充分了解数据法规、数据合规计划、岗位角色与职责等。

鼓励企业管理层和其他员工作出并履行明确、公开的数据合规承诺，内容主要是知悉、愿意遵守数据合规计划，愿意承担违反数据合规承诺的后果。

第六章 企业数据安全技术建设

一、自动化工具

数据处理者在采用网络爬虫等自动化工具访问、收集数据时，应当评估对网络服务的性能、功能带来的影响，不得干扰网络服务的正常功能。

二、软件开发工具包

企业在应用程序开发和运营过程中使用第三方软件开发工具包时，应当通过合同等形式明确第三方的数据安全责任义务，并督促第三方采取必要的数据安全保护措施，加强数据合规管理。

三、数据安全技术体系

（一）数据梳理，即对企业重要数据、敏感数据进行全面排查梳理，并根据业务需要对不同角色接触、处理数据的权限进行梳理。

（二）入侵防御，即建立、检查数据库防火墙，以便对外部攻击进行有效防护，同时也对内部数据库漏洞进行有效防护，防止漏洞被违规利用。

（三）权限管控，即针对不同访问需求，规范数据访问权限，并严格记录访问情况，实现内部数据操作行为的有效控制与监管。

（四）脱敏流转，即在数据使用流转过程，遵循数据最小使用原则，去标识，去隐私，实现数据的安全高效利用，在安全的前提下提升数据的使用价值。

（五）密文存储，即落实重要数据识别和分类分级保护要求，对重要的核心数据加密存储，守护数据安全。

（六）监管稽核，即建立有效的内部数据安全合规监管体系，从数据产生，到场景化使用，进行流向监控、精准分析，实现有效监管。

（七）应急处置机制，即一旦发生安全事件，确保企业有完善的应急预案和应对处理机制，防止事态进一步扩大。

第七章 数据合规风险的法律责任

数据处理者违反数据法规规定处理个人信息等数据的，被侵权者可以要求数据处理者承担民事责任；数据监管部门可以追究数据处理者的行政责任。

数据处理者违反《刑法》规定，可能被追究以下刑事责任：侵犯公民个人信息罪、破坏计算机信息系统罪、非法侵入计算机信息系统罪、非法获取计算机信息系统数据、非法控制计算机信息系统罪、提供侵入、非法控制计算机信息系统程序、工具罪、拒不履行信息网络安全管理义务罪、非法利用信息网络罪、帮助信息网络犯罪活动罪、侵犯商业秘密罪等。

附件 1：
基本概念介绍

1.数据，是指任何以电子或者其他方式对信息的记录。

2.数据合规，是指企业及其员工的经营管理行为符合个人信息保护、网络安全、数据安全等数据法规的要求，既包括形式上使用数据合规，也包括数据内容本身的实质合规。

3.数据合规管理，是指以预防和降低涉数据违法犯罪为目的，以企业及其员工经营管理行为为对象，开展包括合规管理体系、风险识别、风险评估与处置、合规运行与保障等有组织、有计划的管理活动。

4.个人信息，是指对以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等，其中不包含匿名化处理后的个人信息。个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

5.数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

6.重要数据，重要数据是指一旦遭到篡改、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。

7.数据处理，包括数据的收集、传输、存储、加工、使用、提供、公开等。

附件 2：
编制依据与参考

法律

《中华人民共和国民法典》

《中华人民共和国网络安全法》

《中华人民共和国个人信息保护法》

《中华人民共和国数据安全法》

《中华人民共和国反不正当竞争法》

《中华人民共和国反垄断法》

司法解释

《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》

行政法规

《关键信息基础设施安全保护条例》

部门规章及规范性文件

《车联网网络安全和数据安全标准体系建设指南》

《移动互联网应用程序信息服务管理规定》

《互联网用户账号信息管理规定》

《个人信息出境标准合同规定（征求意见稿）》

《证券期货业网络安全管理办法（征求意见稿）》

《移动互联网应用程序信息服务管理规定（征求意见稿）》

国家标准

《TC260-001 汽车采集数据处理安全指南》

《GB/T40645-2021 信息安全技术互联网信息服务安全通用要求》

《GB/T40660-2021 信息安全技术生物特征识别信息保护基本要求》

《TC260-PG-20211A 网络安全标准实践指南-人工智能伦理安全风险防范指引》

《GB/T 35273-2020 信息安全技术 个人信息安全规范》

附件 3：
APP 侵害用户权益专项整治行动高频违规项自查清单

类型	违规行为	是/否
违规收集个人信息	APP 首次启动时没有隐私政策弹窗	
	隐私政策弹窗没有设置明确的同意、不同意按钮	
	隐私政策弹窗按钮为“好的”“我知道了”等模糊字样	
	用户点击同意隐私政策前 APP 即申请权限	
	APP 申请打开敏感权限时未同步告知用户为何需要此项权限	
	用户浏览完隐私政策并点击同意按钮前，APP 和 SDK 有收集行为或者关联动作，例如和服务器之间发送或者接收信息的行为	
	隐私政策中未逐一列出 APP 接入的所有的 SDK 收集使用个人信息的目的、方式、范围	
	用户点击同意隐私政策前 SDK 就开始收集个人信息或打开可收集个人信息的权限	
	APP 在征求用户同意环节，设置为登录即同意	
	默认勾选用户同意隐私政策	
	APP 或 SDK 收集 IMEI/MAC 地址/软件安装列表/设备名称/操作系统版本/SIM 卡 IMSI	

	信息但隐私政策未写明	
超范围收集个人信息	存在静默状态下或后台运行时按照一定频次读取 IMEI、IMSI 信息、MAC 地址等行为（每隔几秒或几分钟），未在隐私政策中写明收集主体、对应的业务场景及必要性	
	APP、SDK 收集的个人信息与实现相应的功能明显不相关	
违规使用个人信息	向隐私政策未列明的 SDK 发送用户个人信息	
强制用户使用定向推送功能	根据用户的标签、浏览记录、订单记录等偏好特征推送消息或提供个性化展示，但未提供退出或关闭个性化展示模式的选项	
	隐私政策中存在有关根据用户的偏好特征推送个性化消息或提供个性化展示的表述，但未提供推出或关闭个性化展示模式的选项	
	用户已于 APP 中关闭个性化推送/个性化展示选项，但仍针对用户作个性化推送/展示（关闭/退出按钮形同虚设）	
APP 强制、频繁、过度索取权限	用户注册、登录时，APP 索取相册、定位等权限，用户拒绝后无法正常登录或注册或直接退出使用	
	用户注册、登录时，APP 索取相册、定位等权限，用户拒绝后仍显示不必要弹窗	
	APP 没有对应的服务或场景时，即申请对应权限（如未用到定位功能即申请定位权限）	
	APP 申请权限时，用户拒绝，非用户主动触发功能且非实现对应业务功能所必须，APP	

	反复弹出申请权限窗口	
	单个场景在用户拒绝权限后，48 小时内弹窗提示用户打开系统权限的次数超过 1 次	
	每次重新打开 APP 或使用某一业务功能时，都会向用户索要或提示用户缺少相关系统权限	
	APP 首次打开或运行中，未见使用权限对应的相关功能或服务时，提前向用户弹窗申请开启通讯录、定位、短信、录音、相机、日历等权限。	
声明：本清单系依据专项整治行动部分被要求整改实例撰写，建议您对照此清单自查并整改高频违规项。但因本清单所依据的样本有限，尚无法覆盖所有违规项，故本清单仅供您参考。		

感谢阅读，如需更多法律服务请扫描下方二维码：

青岛市督促惠企政策落实法律服务平台