瀚一律师事务所
HAN YI LAW OFFICES

网络安全和数据安全合规
— 每一家现代企业都要了解的十个合规事项

在全球推进数字化经济的背景下，数据日渐成为国家新兴的战略资源。各国对数据的开发、利用、流动和交易的需求日渐强烈。与此同时，针对数据的非法交易、过度开发和针对网络的恶意攻击也愈演愈烈。据统计，2020 年全球公开范围报告了 3,932 起安全泄露事件，泄露的记录数量达到 370 亿条，同比增长 145%[1]。2021 年 12 月，阿里云发现阿帕奇(Apache) Log4j2 组件存在严重安全漏洞，波及到我国政务部门和大多数企业。Log4j 是被广泛应用在服务器上的软件，这一漏洞可能导致设备被远程控制，海量信息被盗以及设备服务中断等严重危害。

近年来我国大力推行产业数字化和数字产业化，国家一方面大力建设信息化社会、鼓励发展数字经济，另一方面也将网络安全和数据安全放在国家利益的高度加以保护。在立法方面，《网络安全法》《数据安全法》和《个人信息保护法》三部由全国人大常委会颁布的法律划定了网络安全和数据安全领域的监管框架。在此框架之内，国家互联网信息办公室（“**国家网信办**”）和其他相关部门也密集出台和/或修订了各项配套法律文件（包括曾引发市场震动的《网络安全审查办法》（修订后的办法已于 2022 年 2 月 15 日正式生效；“**《网安审查办法》**”）和《网络数据安全管理条例（征求意见稿）》（“**《数安管理条例（草案）》**”）），以落实和细化上位法律的各项规定。上述法律文件加上《网络安全法》时代已经颁布的各项法规，初步形成了我国网络安全和数据安全保护的法律体系。

据统计，自 2017 年《网络安全法》颁布以来，涉及网络安全和数据安全的法律法规及国家标准约有 140 余篇，其中既有普遍适用于所有数据处理者的法律文件（如《数据出境安全评估办法（征求意见稿）》和《网络安全等级保护条例（征求意见稿）》），也有专门针对特殊数据处理者、特定数据和/或特定行业的法律文件（如《关键信息基础设施安全保护条例》《儿童个人信息网络保护规定》和《汽车数据安全管理若干规定（试行）》）。而随着 2021 年《数据安全法》和《个人信息保护法》的生效，可以预见未来还将会出台大量配套的部门规章和/或专门性规定。

面对如此庞杂细碎的法律法规，普通数据处理者（在本文特指非关键信息基础设施运营者和非互联网平台运营者，下文统称为“**企业**”）在日常运营中需要注意哪些合规要求？

本文将通过对我国现行网络安全和数据安全相关法律文件（包括尚未生效的征求意见稿）的梳理和分析，总结出企业必须注意的八个常规合规点及两个特殊合规点，以供企业参考。篇幅所限，本文不对关键信息基础设施运营者、互联网平台企业展开讨论，也不涵盖任何行业的特殊规定与国家/行业标准。

---

[1] 详见《安全内参》报道：https://www.secrss.com/articles/28972。

一、 关于数据和网络安全的几个基本概念

1. 数据、网络数据、数据安全和网络安全

根据我国法律，**数据**指任何以电子或其他方式对信息的记录；**网络数据**，是指通过网络收集、存储、传输、处理和产生的各种电子数据[2]；**数据安全**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；**网络安全**指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

2. 数据安全和网络安全的关系

从以上定义可以看出，数据安全保护的对象仅包括数据本身；而网络安全保护的对象既包括网络数据本身，又包括我国境内网络运行的安全[3]。因此笼统地说，网络安全包含了数据安全（尽管从字面理解，网络安全保护的信息仅指“网络信息”，比数据安全法定义的范围略小。但考虑到现代企业几乎离不开电子化信息，因此对绝大多数企业而言，两部法律下所保护的信息外延没有实质差别）。相应地，网络安全法规和数据安全法规在条款上也有诸多交叉和关联。因此，企业的网络/数据合规不能仅关注某一类法律文件，需同时留意网络安全和数据安全领域所有相关的法律规定。

3. 我国网络安全和数据安全的监管架构

我国对网络安全和数据安全采用的是**国家网信办牵头，多部门协同的联合监管模式**。这意味着企业的网络/数据合规涉及多个监管部门，需要根据企业自身所在行业找准所有对口监管部门，并保持与各部门的持续良好沟通，以掌握立法趋势和实践中各部门的执法尺度。下面列出我国联合监管模式下，各部门的协作关系和主要工作内容：

- **国家网信办统筹协调**：主要表现为国家网信办单独或者联合其他相关部门发布各项法规（如《App 违法违规收集使用个人信息行为认定方法》由国家网信办联合工业和信息化部、国家市场监督管理总局以及公安部发文；《汽车数据安全管理若干规定（试行）》由国家网信办联合国家发展与改革委员会、工业和信息化部、交通运输部和公安部发文），以及对数据安全和网络安全进行日常监管（如对拟出境数据的安全评估、对数据处理者可能影响国家安全的数据处理活动进行网络安全审查）。

- **各行业主管部门承担本行业、本领域的监管职责**：主要表现为出台本行业、本领域的核心数据和重要数据目录以及依照相关法律法规执行监管权（如大型互联网平台境外设立总部/运营或研发中心应向国家网信办和行业主

[2] 尚未生效的《网络数据安全管理条例（征求意见稿）》将网络数据定义为“任何以电子方式对信息的记录”。单纯从字面理解，这一定义涵盖了存储在本地的电子化信息，在一定程度上扩大了网安法对网络数据的定义。

[3] 网络运行安全包括网络设施（如电信基站、水电站等）安全、网络信息系统安全以及网络产品和服务（如 APP，软件操作系统等）安全。

管部门报告）。

- **公安部门、国安部门**打击各类网络和数据安全违法犯罪活动，起到震慑违法行为、保障法律实施的作用。

4. 我国的数据保护体系

我国对数据采用**分类分级**的保护体系。分类指数据的类别，分级指保护的级别。分类分级保护即根据数据的类别采取不同等级的保护方式。根据我国目前的法律法规，数据按类别可分为：**国家秘密**、**核心数据**、**重要数据**和**一般数据**。国家秘密因为其特殊性，一般性企业接触到的可能性不大，因此本文不展开讨论。核心数据指关系国家安全、国民经济命脉、重要民生和重大公共利益等的数据。重要数据指一旦遭到篡改、破坏、泄露或非法获取、利用，可能危害国家安全和公共利益的数据（如出口管制物涉及的核心技术、设计方案等数据、需要保护或者控制传播的国家经济运行数据；达到有关部门规定的规模或者精度的基因、地理等数据）。非国家秘密、核心数据或重要数据的数据则属于一般数据。相应地，国家秘密享有最高的保护级别，核心数据为严格保护级别，重要数据为重点保护级别。

另外，法规单列了**个人信息**，并与前述四类信息并列，而依据信息主体和性质的不同，个人信息有可能落入前四类数据中的任何一类。国家明确对个人信息进行重点保护；但我们理解若个人信息落入核心数据或国家秘密的类别，则应相应实行更高级别的保护。

5. 何种活动将受到网络安全和数据安全的监管

网络的所有者、管理者或者网络服务提供者在我国境内建设、运营、维护、使用网络或者通过网络提供产品或服务，需要满足网络安全法的规定。在中国境内收集、存储、使用、加工、提供、传输、公开数据均属于数据处理活动，需要满足数据安全相关法律法规。此外，在中国境外处理中国境内个人和组织数据的活动，若符合特定情形（包括以向境内提供产品或者服务为目的；分析、评估境内个人、组织的行为；涉及境内重要数据处理等），则也需适用数据安全法规的有关规定。

6. 企业如何判断所处理的数据涉及重要数据/核心数据或自身是关键信息基础设施（“CII”）运营者

我国对重要数据/核心数据和 CII 设置了更高的保护级别，并配有专门法规，合规成本更高。因此对企业而言，判断自身及所处理数据的性质非常重要。

- **核心数据/重要数据**：如上文介绍，法律已对核心数据和重要数据做出了定性规定，同时要求各地区、各部门出台适用于本地区、本部门以及相关行业、领域的核心数据/重要数据目录。这项规定意味着核心数据/重要数据的范围将基于地区和行业的不同而有所区别，因此建议企业密切关注本地区和本行业后续的立法，并保持与主管部门的沟通。

- **关键信息基础设施（“CII”）**：为便于理解，我们可将“关键信息基础设施”这一概念拆成“关键”和“信息基础设施”两部分。“关键”指一旦遭到破坏、丧失功能或数据泄露，可能严重危害国家安全、国计民生、公共利益；“信息

基础设施”指网络设施和信息系统，如基站、光缆、微波、卫星等网络基础设施以及重要的信息系统。这些关键基础设施既是国家和军队信息化建设的基础支撑，也是保证社会生产和人民生活基本设施的重要组成部分。2017年《网安法》首次从法律层面引入 CII 的概念，并规定其具体范围和安全保护办法由国务院制定。2021 年，国务院颁布的《关键信息基础设施安全保护条例》中规定了 CII 运营者的各项责任和义务，包括设置专门的安全管理机构，对其负责人和关键岗位人员进行安全背景审查、每年对 CII 运营者至少一次网络安全检测和风险评估等等。根据该条例，CII 的名单将由电信主管部门和行业主管部门认定，且主管部门应将认定结果通知 CII 运营者。

二、 企业日常数据/网络安全合规需关注的 8 个基本合规事项

企业在日常运营中，离不开对数据的处理和对网络的使用。根据我国法律法规，企业在日常数据/网络安全保护方面应做到以下几点：

1. 建立内部制度

企业内部应根据法律法规并结合自身实际，建立数据安全管理制度和技术保护机制（如企业内部的数据分类、存储、加密和备份规则、数据访问控制、发生数据安全事件的应急处理措施等）。

2. 定期开展员工数据安全培训

培训的主题可包括关于网络安全和数据安全基本法律法规、数据分类分级保护的必要性、本企业内部数据安全合规的制度要求、如何识别和防范恶意软件、发生数据安全事件后的应对措施以及个人如何防止数据泄露等，以加强本企业员工对网络安全和数据安全合规的意识。

3. 满足网络安全等级保护的要求

我国对网络实行分等级保护和监管，按网络的重要性分为 5 个安全等级。如果企业利用互联网等信息网络开展数据处理活动，应满足网络安全等级保护制度的要求，具体为：

- **企业应先对自身的网络安全等级进行自评：**如自评为 2 级以上，应组织专家评审并报行业主管部门核准。

- **等保 2 级以上网络的公安部门备案：**企业网络安全等级确定后，如在第 2 级以上的，需及时向当地公安部门备案，并取得公安部核发的网络安全等级保护的备案证明。

- **等保 3 级以上网络的测评要求：**企业新建 3 级网络上线运行前，应当委托网络测评机构进行等级测评，通过后方可运行。以后每年进行一次安全等级测评并向备案的公安机关报告测评结果。

- **每年自查并向公安部门报告：**企业每年应对自身的网络安全状况及落实网络安全等级保护制度的情况做一次自查，发现安全隐患及时整改，并向备案的公安机关报告。

4. 日常风险监测

企业日常数据处理活动应当加强风险监测。如发现数据安全缺陷、漏洞等风险时，要立即补救。

5. 安全事件告知义务

- **告知相关利害关系人**：如果发生数据安全事件，要按照企业内部的应急处置机制及时补救、消除隐患，防止危害扩大。如果安全事件对个人/组织造成危害，需在 3 个工作日内告知利害关系人。涉嫌犯罪的向公安机关报案。

- **告知主管部门**：如果安全事件涉及到**重要数据**或 **10 万人以上的个人信息**，企业还应在发生安全事件的 8 小时内向市级网信部门和有关主管部门报告事件基本信息。事件处理完毕后 5 个工作日内向原报告部门报送调查评估报告，报告内容要包括该起安全事件的原因、后果、责任处理、改进措施等。

  阿里云被处罚事件即是由于阿里云作为网络产品和服务提供者（同时还作为网络产品安全漏洞收集平台），发现其提供的云服务因使用 Log4j2 组件而存在严重安全漏洞后，仅向境外阿帕奇及基金会（即该产品的提供方）报告，**未向电信主管部门报告，未有效支撑工信部开展网络安全威胁和漏洞管理**，违反了《网络安全法》和《网络产品安全漏洞管理规定》等规定而遭到处罚。

6. 企业组织形式变更的报告义务

根据《网络数据安全管理条例（征求意见稿）》，如果企业发生合并、重组或者分立情况且涉及重要数据或者 100 万人以上个人信息的，应向市级主管部门报告；发生解散、被宣告破产情况的，应该向市级主管部门报告，并按照主管部门的要求移交或删除数据，主管部门不明确的，向市级网信部门报告。

7. 禁止非法爬取

企业在使用自动化工具访问收集数据时，不得干扰网络服务的正常功能。如企业涉嫌侵入计算机信息系统，获取该计算机信息系统中存储、处理或者传输的数据，情节严重的，还可能构成刑法下的非法获取计算机信息系统数据罪。

8. 建立投诉举报渠道

企业应当公布接受投诉举报的联系方式、责任人信息，每年公开披露受理和收到的个人信息安全投诉的数量、处理情况等。

如企业不履行上述 8 个方面的合规要求，有可能被监管机关处 200 万元以下罚款，直接负责的主管人员可处二十万元以下罚款；如造成大量数据泄露等严重后果，除罚款外，还可能被责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照等严重后果。

三、 特殊情形触发的 2 个合规要求

除上述所列 8 种日常合规注意点外，以下两种特殊情形下的合规要求也值得企业特别注意：

1. 网络安全审查

根据 2022 年 2 月正式生效的《网安审查办法》：CII 运营者采购网络产品和服务以及“网络平台运营者”的数据处理活动“**影响或者可能影响国家安全**”的，均需进行网络安全审查。

- **与数据安全审查的关系**：《数据安全法》规定了数据安全审查制度，对“**影响或可能影响国家安全的数据处理活动**”进行国家安全审查。《网安审查办法》明确规定国家对数据安全审查另有规定的，应该在符合网络安全审查规定的同时，符合数据安全审查的规定。因此我们认为网络安全审查和数据安全审查为两类不同的审查，相关企业需同时符合。

- **审查机关**：国家网信办网络安全审查办公室。

- **审查报送的材料**：根据《网安审查办法》，申报材料包括申报书、关于影响或可能影响国家安全的分析报告、拟提交的 IPO 材料或采购文件/协议/合同及国家网信办要求的其他材料。

- **审查的关注点**：网络安全审查关注的是“国家安全”。相应地，审查考量因素聚焦在因上市存在的核心数据/重要数据/大量个人信息被外国政府影响、控制、恶意利用的风险以及网络信息安全风险，或核心数据/重要数据/大量个人信息被窃取、泄露、毁损或非法出境的风险；以及 CII 是否会被非法控制、遭到干扰、破坏以及 CII 采购的产品/服务的安全性、稳定性等方面的风险。

- **主动申报网络安全审查**：企业采购及提供网络产品和服务时，要先进行自我预判。如果认为可能影响国家安全，应该申报安全审查。就预判标准而言，CII 保护工作部门会制定本行业和本领域的预判指南，但相关立法尚未要求监管部门对一般数据处理者制定预判指南。因此建议企业密切关注本行业、本部门监管机构的立法/执法动态，同时在日常运营中与监管机构保持良好和正常的沟通。

- **强制网络安全审查**：对于非 CII 运营者或非互联网平台运营者的企业而言，最可能触发强制网络安全审查的情形有 2 种，即：(i)**处理 100 万人以上个人信息的网络平台运营者赴国外上市**；和(ii)**数据处理者赴香港上市，影响或者可能影响国家安全的**。

首次提出因上市而触发强制网络安全审查要求的是 2021 年 7 月颁布的《网络安全审查办法（草案）》。该草案要求“掌握超过 100 万用户个人信息的数据处理者赴国外上市”必须进行网络安全审查。这一规定曾引发市场对其适用范围的广泛关注，同年 11 月出台的《数安管理条例（草案）》在一定程度上对此做出了澄清，将“赴国外上市”和“赴香港上市”做了区分，并规定赴国外上市的，“处理

一百万人以上个人信息”即触发强制网络安全审查；而赴香港上市的，则在“影响或可能影响国家安全”的情况下触发强制网络安全审查。值得一提的是，因2022年正式生效的《网安审查办法》将其适用对象从“数据处理者”统一修改为“网络平台运营者”，相应地，强制网络安全审查的对象也因此从“数据处理者”变为“网络平台运营者”。遗憾的是该办法本身并未对“网络平台运营者”给出具体定义，但这一修改看似是立法者对网络安全审查适用对象的限缩。鉴于《数安管理条例（草案）》中关于强制网络安全审查条款仍采用“数据处理者”的提法，在《网安审查办法》已修改适用对象的情况下，正式版的《数安管理条例》有可能也将对该条做出相应调整。另外，因为《数安管理条款（草案）》中已存在“互联网平台运营者”这一定义，并对该等对象的网络数据安全合规做了专章规定，如该草案正式稿采用“网络平台运营者”这一概念，则更有必要对其具体涵义做出规定（或澄清其与互联网平台运营者的区别），否则很可能引起法律适用上的混淆。

至于何种情况会构成“影响或可能影响国家安全”，草案并未进一步说明。在相关立法尚未完善的情况下，企业可以《网安审查办法》第10条规定的网络安全审查时的考虑因素作为参照依据之一。

2. 数据出境安全评估

企业因业务等原因需要可依法向境外提供数据，但须满足《数安管理条例（草稿）》和《数据出境安全评估办法（征求意见稿）》的有关条件。

- **数据出境的条件**：根据《数安管理条例（草稿）》，如企业拟**向境外提供数据**，需满足以下条件之一：(i)通过国家网信部门组织的数据出境安全评估；(ii)提供方和接收方均通过中国网信部门认定的专业机构的保护认证；(iii)双方按照国家网信办的标准合同模板订立合同；或(iv)法律、行政法规、国家网信办规定的其他条件。但本条不适用于：为了保护个人生命健康和财产安全必须向境外提供个人信息；或者企业为了履行个人作为一方当事人的合同必须向境外提供个人信息的情况。

- **评估监管原则**：事前评估和持续监督，风险自评估和强制评估相结合。

- **强制安全评估**：如果存在以下情形之一，则触发强制数据出境安全评估，企业不能再依赖其他数据合法出境的基础：(i)如出境的数据中**包括重要数据**；(ii)如提供方是**CII运营者**或处理**100万人以上个人信息的**数据处理者**且向境外提供个人信息**；或者(iii)国家网信部门规定的其他情形。

  值得注意的是，《数安管理条例（草案）》中规定的强制数据出境安全评估情形**删除了**《数据出境安全评估办法（征求意见稿）》中要求“累计向境外提供超过10万人以上个人信息或一万人以上敏感个人信息”触发强制数据出境安全评估的要求。鉴于《数安管理条例（草案）》比《数据出境安全评估办法（征求意见稿）》晚一个月发布，这一变化可能是监管机关有意减少强制评估的信号。鉴于两份法规目前均为征求意见稿，最终生效的规定如何还有待监管机关明确。

- **审查机关**：国家网信办。

- **报送材料**：申报书、数据出境风险自评报告、数据出境提供方和接收方拟

订立的合同等。

- **年度报告义务：**向境外提供个人信息和重要数据的企业，应编制年度数据出境安全报告，并向市级网信部门报告。

- **向境外执法/司法机构提供数据需事前审批：**除非经主管机关批准，任何境内的个人、组织不得向外国执法/司法机构提供境内数据。

* * *

本文主要是基于我国现行网络安全和数据安全相关法律文件和部分尚未生效的征求意见稿对企业在网络安全和数据安全方面的合规要点进行的提炼和小结，供感兴趣的企业参考。鉴于我国网络安全和数据安全方面的立法和实践仍在不断的发展和完善以应对快速变化的网络数字时代，文中提及的部分法律概念的解读和合规实践的具体执行还有待主管部门的进一步明确，如企业对某项具体数据或数据处理行为的分级/性质认定存在疑问，建议企业就具体事项进一步咨询专业顾问和安全评估机构的意见或与主管部门进行个案沟通。