|  |  |
| --- | --- |
| ICS  | 点击此处添加ICS号 |
| CCS  |

|  |
| --- |
|   |

点击此处添加CCS号 |

团体标准

T/CHNSA XXXX—XXXX

航运大数据 船舶

第2部分：数据安全合规指南

Big data for shipping Vessels

Part 2：Guide of data compliance management

（本草案完成时间：2023-08-04）

XXXX - XX - XX发布

XXXX - XX - XX实施

中国船东协会  发布

目次

[前言 III](#_Toc142056356)

[引言 IV](#_Toc142056357)

[1 范围 1](#_Toc142056358)

[2 规范性引用文件 1](#_Toc142056359)

[3 术语和定义 1](#_Toc142056360)

[4 基本要求 2](#_Toc142056361)

[5 组织管理 2](#_Toc142056362)

[5.1 机构与岗位 2](#_Toc142056363)

[5.2 职责分工 2](#_Toc142056364)

[5.3 人员保障 2](#_Toc142056365)

[5.4 资金保障 2](#_Toc142056366)

[6 数据识别与分类分级 3](#_Toc142056367)

[6.1 航运数据资产盘点 3](#_Toc142056368)

[6.2 航运数据分类分级 3](#_Toc142056369)

[6.3 个人信息识别 3](#_Toc142056370)

[6.4 公共数据识别 3](#_Toc142056371)

[6.5 数据合规风险识别 3](#_Toc142056372)

[7 数据全生命周期合规管理 4](#_Toc142056373)

[7.1 数据收集 4](#_Toc142056374)

[7.2 数据存储 4](#_Toc142056375)

[7.3 数据使用加工 4](#_Toc142056376)

[7.4 数据传输 4](#_Toc142056377)

[7.5 数据提供 4](#_Toc142056378)

[7.6 数据销毁 4](#_Toc142056379)

[7.7 数据出境 5](#_Toc142056380)

[8 管理措施 5](#_Toc142056381)

[8.1 安全制度建设 5](#_Toc142056382)

[8.2 安全同步 5](#_Toc142056383)

[8.3 权限管理 5](#_Toc142056384)

[8.4 密码保护 5](#_Toc142056385)

[8.5 日志留存 5](#_Toc142056386)

[8.6 安全审计 5](#_Toc142056387)

[8.7 信息上级 6](#_Toc142056388)

[8.8 应急管理 6](#_Toc142056389)

[8.9 教育培训 6](#_Toc142056390)

[8.10 安全评估 6](#_Toc142056391)

[8.11 合作方管理 6](#_Toc142056392)

[9 评价与改进 6](#_Toc142056393)

[9.1 自评 6](#_Toc142056394)

[9.2 设计评估 6](#_Toc142056395)

[9.3 执行评估 7](#_Toc142056396)

[9.4 质效评估 8](#_Toc142056397)

[附录A（资料性） 船舶典型场景下的数据合规 9](#_Toc142056398)

[A.1 船舶运输集装箱货物流程及数据合规要点 9](#_Toc142056399)

[附录B（资料性） 航运数据分类分级示例 11](#_Toc142056400)

[表B.1 航运数据分类分级 11](#_Toc142056401)

1. 前言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由××××提出。

本文件由××××归口。

本文件起草单位：

本文件主要起草人：

1. 引言

《中华人民共和国网络安全法》第十五条规定，“国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。”《中华人民共和国数据安全法》第十七条规定，“国家推进……数据安全标准体系建设。国务院标准化行政主管部门和国务院有关部门根据各自的职责，组织制定并适时修订有关数据开发利用技术、产品和数据安全相关标准。国家支持企业、社会团体和教育、科研机构等参与标准制定。”根据上述规定，制定该《指引》，为航运产业数字合规工作提供方向与指导，是法律的要求。

2020年12月7日，中共中央印发《法治社会建设实施纲要（2020－2025年）》，提出要“增强全民法治观念、增强全民法治观念……加强社会治理制度建设，推进社会治理制度化、规范化、程序化。”提出了全民合规的要求。

《上海市国民经济和社会发展第十四个五年规划和二〇三五年远景目标纲要》提出，“‘五个中心’功能实现整体提升。……基本建成国际航运中心……现代航运服务体系基本形成。”2021年6月，上海市政府发布《上海国际航运中心建设“十四五”规划》，明确要“基本建成便捷高效、功能完备、开放融合、绿色智慧、保障有力的世界一流国际航运中心”。

2022年1月26日，为进一步促进浦东航运业发展，浦东公布《浦东新区“十四五”期间促进航运业发展财政扶持办法》，明确规定对于落户于浦东的航运企业、航运机构，给予相应的资金扶持。

2022年2月23日，上海市推进上海国际航运中心建设领导小组会议上龚正市长指出，“要拉长板，……深入参与国际航运规则的制定。要锻新板，……以数字化转型赋能航运业蝶变跃升。要固底板，……扎实做好常态化防控和安全生产工作。”

根据上述文件和会议的精神，航运业数据合规能力的建设，是提升航运业整体软实力、建设国际航运中心及现代航运服务体系的重要组成部分。

《中华人民共和国网络安全法》《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》等法律及相关法规出台后，企业普遍面临合规压力，但由于配套的实施细则尚未出台、我国的数据合规法律体系尚在完善当中，只是基础框架，还缺乏实施细则，企业此时普遍面临如何落实法律提出的合规要求的问题，无所适从。

因此，航运企业也迫切需要一份数据合规指南，为航运企业后续数据合规工作提供切实可行的操作手册。

航运大数据 船舶

第2部分：数据安全合规指南

* 1. 范围

本文件给出了船舶大数据安全合规相关的基本要求、组织管理、数据识别与分类分级、数据全生命周期安全管理、管理措施及评价改进等内容。

本文件适用于船舶大数据安全合规的管理。

* 1. 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069 信息安全技术术语

GB/T 29246-2017 信息技术安全技术信息安全管理体系概述和词汇

GB/T 35273-2020 信息安全技术个人信息安全规范

GB/T 37973-2019 信息安全技术大数据安全管理指南

GB/T 41479-2022 信息安全技术网络数据处理安全要求

ISO 37301 合规管理体系要求及使用指南

* 1. 术语和定义

GB/T 25069-2022和GB/T 29246-2017界定的以及下列术语和定义适用于本文件。

安全 security

对某一系统，据以获得保密性、完整性、可用性、可核查性、真实性以及可靠性的性质。

[来源：GB/T 25069-2022，3.1]

数据安全 data security

通过管理和技术措施,确保数据有效保护和合规使用的状态。

保密性 confidentiality

信息对未授权的个人、实体或过程不可用或不泄露的性质。

[来源：GB/T 25069-2022，3.41]

完整性 integrity

准确和完备的性质。

[来源：GB/T 25069-2022，3.612]

可用性 availability

可由经授权实体按需访问和使用的性质。

[来源：GB/T 25069-2022，3.345]

合规 compliance

履行组织的全部合规义务。

[来源：GB/T 35770-2017 / ISO37301，3.26]

数据处理 data processing

对原始数据进行抽取、转换、加载的过程。

1. 数据处理包括开发数据产品或数据分析等。
2. 数据产品包括但不限于能访问原始数据，提供数据计算、数据存储、数据交换、数据分析、数据挖掘、数据展示等应用的软硬件产品。

个人信息 personal information

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。

公共数据 public data

国家机关和依法经授权、受委托履行公共管理和服务职能的组织（以下统称公共管理和服务机构），在依法履行公共管理职责或提供公共服务过程中收集、产生的数据。

1. 公共管理和服务机构，包括各级政务机关、事业单位，其他依法经授权或受委托管理公共事务的组织，以及供水、供电、供气、公共交通、教育、卫生健康、社会福利、环境保护等提供公共服务的组织。
2. 公共数据通常不包括组织专有的知识产权数据和商业秘密。
	1. 基本要求

航运企业宜结合自身业务特点，在对自身数据资产进行全面盘点的基础上，对自身面临的风险点及合规需求进行分析，从组织管理、制度建设、数据生命周期管理等角度出发，建立企业数据合规制度。

* 1. 组织管理
		1. 机构与岗位

处理一般数据的航运企业（或称数据处理者），宜设置数据安全责任管理专职岗位，配备至少一名专职人员。

处理重要数据和核心数据的航运企业（或称数据处理者），宜建立覆盖本单位相关部门的数据安全管理责任工作体系，明确数据安全管理责任负责人和管理机构。本单位法定代表人或者主要负责人是数据安全管理第一责任人，领导团队中分管数据安全管理的成员是直接责任人。

* + 1. 职责分工

航运企业宜明确各部门数据安全管理职责，建立常态化沟通与协作机制。

航运企业应明确数据安全管理责任岗位、部门与各项工作执行落实部门责任分工界面。

航运企业应建立数据安全合规管理制度执行落实情况监督检查和考核问责制度。

处理重要数据和核心数据的航运企业宜明确由数据安全管理机构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合规管理整体方针策略，协调相关部门建立数据安全技术保障措施，牵头做好数据安全应急处置，组织开展数据合规性评估、教育培训等工作。

* + 1. 人员保障

处理重要数据和核心数据的航运企业宜在数据安全管理责任部门和相关部门配备与数据规模相匹配的数据安全管理专职人员，形成企业数据安全管理岗位人员名单。

宜确认数据处理关键岗位及人员，签署数据安全责任书，记录数据处理活动。

相关人员负责具体承担落实数据安全合规管理相关工作，包括但不限于权限管理、安全审计、应急响应、合规性评估、数据安全事件处置、信息安全事件处置和信息报送等工作。

* + 1. 资金保障

航运企业宜就数据合规工作提供专项资金计划，并列入年度预算。

处理重要数据和核心数据的航运企业宜保障专门安全管理机构的运行经费，并依法依规严格规范经费使用和管理，防止资金挤占挪用。

* 1. 数据识别与分类分级
		1. 航运数据资产盘点

航运企业宜对数据资产进行梳理与判断，并在此基础上对数据进行分类分级。

* + 1. 航运数据分类分级

航运企业宜按照数据一旦遭到纂改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，将航运数据从低到高分成一般数据、重要数据、核心数据共三个级别。

对于一般数据，航运企业宜按照数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对个人、组织合法权益造成的危害程度，将一般数据从低到高分为1级、2级、3级、4级共四个级别。

1. 1级数据：数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，不会对个人合法权益、组织合法权益造成危害。1级数据具有公共传播属性，可对外公开发布、转发传播，但也需考虑公开的数据量及类别，避免由于类别较多或者数量过大被用于关联分析；
2. 2级数据：数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对个人合法权益、组织合法权益造成轻微危害。2级数据通常在组织内部、关联方共享和使用，相关方授权后可向组织外部共享；
3. 3级数据：数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对个人合法权益、组织合法权益造成一般危害。3级数据仅能由授权的内部机构或人员访问，如果要将数据共享到外部，需要满足相关条件并获得相关方的授权；
4. 4级数据：数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对个人合法权益、组织合法权益造成严重危害，但不会危害国家安全或公共利益。4级数据按照批准的授权列表严格管理，仅能在受控范围内经过严格审批、评估后才可共享或传播。
	* 1. 个人信息识别

通过分析特定自然人与数据之间的关系，符合下述情形之一的航运数据，可判定为个人信息：

1. 可识别特定自然人：即从数据到个人，依据数据本身的特殊性可识别出特定自然人，包括单独或结合其他信息识别出特定自然人。
2. 与特定自然人关联：即从个人到数据，如已知特定自然人，由该特定自然人在其活动中产生的数据（如个人位置信息、个人通话记录、网页浏览记录等），可识别为个人信息。
	* 1. 公共数据识别

符合以下任一情形的航运数据，可识别为公共数据：

1. 各级政务机关在依法履行公共管理和服务职能过程中收集和产生的数据；
2. 具有公共管理和服务职能的企事业单位和社会团体，在依法履行公共管理和服务职能过程中收集和产生的数据；
3. 提供公共服务的组织,在开展公共服务（如供水、供电、供热供气、教育、医疗、公共交通、通信、邮政、养老、环保等）过程中收集和产生的数据；
4. 在为国家机关提供服务，参与公共基础设施、公共服务系统建设运维管理，利用公共资源提供服务过程中收集、产生的数据。
	* 1. 数据合规风险识别

航运企业宜从以下方面考虑自身面临的数据合规风险：

1. 企业的整体业务战略与目标；
2. 企业及其合同相对方必须满足的法律、法规、规章制度和合同要求，及社会文化环境；
3. 企业为支持其运行，针对信息的收集、处理、存储、传输和删除而建立的原则、目标和业务要求。
	1. 数据全生命周期合规管理
		1. 数据收集

数据处理者收集数据宜遵循合法、正当、必要的原则，不得窃取或者以其他非法方式收集数据。

数据处理者宜制定数据收集规则。宜采取配备技术手段、签署安全协议等措施加强对数据收集人员、设备的管理，并对数据收集的时间、类型、数量、频度、流向等进行记录，并定期根据规则在业务系统中执行数据收集合规性审查。

通过间接途径获取数据的，宜要求数据提供方做出数据源合法性的书面承诺，并承担相应的法律责任。

宜保障训练数据可追溯性，记录训练数据获取时间、来源、数据量、存储介质的标识、采样方法，并保证训练数据有完整签名或校验码。明确训练数据不包含标签错误、记录造假等恶意伪造的药饵数据。

* + 1. 数据存储

数据处理者宜依据法律规定或者与用户约定的方式和期限存储数据。宜防止训练数据在传输、存储环节被窃取或篡改，防止数据存储、使用等环节被投放药饵数据。

存储重要数据的，还宜采用校验技术、密码技术等措施进行安全存储，不得直接提供存储系统的公共信息网络访问，并实施数据容灾备份和存储介质安全管理，定期开展数据恢复测试。存储核心数据的，还宜实施异地容灾备份。

* + 1. 数据使用加工

数据处理者未经个人、组织等同意，不得使用数据挖掘、关联分析等技术手段针对特定主体进行精准画像、数据复原等加工处理活动。

利用数据进行自动化决策的，宜保证决策的透明度和结果公平合理。使用、加工重要数据和核心数据的，还宜加强访问控制，建立登记、审批机制并留存记录。

数据处理者宜建立数据资源持有权、数据加工使用权、数据产品经营权等分置的产权运行机制，深度参与对原始数据的使用加工和开发利用，积极开展航运数据流通和交易。数据处理者宜依法依规行使数据应用相关权利，促进数据使用价值复用与充分利用，促进数据使用权交换和市场化流通。宜审慎对待原始数据的流转交易行为。

* + 1. 数据传输

数据处理者宜根据传输的数据类型、级别和应用场景，制定安全策略并采取保护措施。

传输重要数据和核心数据的，宜采取校验技术、密码技术、安全传输通道或者安全传输协议等措施。

涉及跨组织机构或者使用公共信息网络进行数据传输的，宜建立登记、审批机制。

跨不同数据处理主体传输核心数据的，宜通过国家数据安全工作协调机制审批。

* + 1. 数据提供

数据处理者提供数据，宜明确提供的范围、类别、条件、程序等，并与数据获取方签订数据安全协议。

提供重要数据和核心数据的，宜对数据获取方数据安全保护能力进行评估或核实，采取必要的安全保护措施。

* + 1. 数据销毁

数据处理者宜建立数据销毁策略和管理制度，明确销毁对象、规则、流程和技术等要求，对销毁活动进行记录和留存。

个人、组织依据法律规定、合同约定等请求销毁的，工业和信息化领域数据处理者宜销毁相应数据。

销毁重要数据和核心数据的，宜及时向行业监管部门更新备案，不得以任何理由、任何方式对销毁数据进行恢复。

* + 1. 数据出境

数据处理者开展数据出境活动，宜符合相关法律法规的要求。

在中华人民共和国境内收集和产生的重要数据，宜依照法律、行政法规要求在境内存储，确需向境外提供的，宜依法依规进行数据出境安全评估。

* 1. 管理措施
		1. 安全制度建设

数据处理者开展数据处理活动宜依照法律、法规的规定，建立数据全生命周期安全管理制度，针对不同级别数据，制定数据收集、存储、使用、加工、传输、提供、公开等环节的具体分级防护要求和操作规程。

* + 1. 安全同步

数据处理者宜确保数据安全管理和技术保护手段与产品研发、生产运营、业务发展同步规划、同步建设、同步运行。

* + 1. 权限管理

数据处理者宜制定数据访问权限管理制度，严格实施人员权限管理。宜明确各部门和相关人员权限管理要求，包含但不限于账号权限分配原则、流程等，建立并定期更新企业数据处理活动平台系统权限分配表。满足以下要求：

1. 宜建立合理的账号权限开通审批流程，并记录审批流程和结果；
2. 宜按照业务需求和安全策略为用户配置合理的权限，如符合最小授权和角色权限制约等要求。宜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. 对所有接入数据处理活动平台系统的用户或业务进行身份接入认证和权限控制，包括基于IP的鉴权和基于账号、口令等的鉴权。
	* 1. 密码保护

数据处理者宜使用商用密码进行数据保护，可自行或者委托商用密码检测机构每年至少开展一次商用密码应用安全性评。

* + 1. 日志留存

数据处理者宜对数据授权访问、批量复制、开放共享、销毁，及数据接口调用等重点环节实施日志留存管理。满足以下要求：

1. 记录信息宜包括执行时间、操作账号、处理方式、授权情况、登录信息等，并确保组织机构内部数据操作相关日志字段记录规则统一，记录完整、准确、不可修改；
2. 宜定期对日志进行本地备份，防止数据安全事件导致的日志被删除。保存时间宜满足国家相关法律法规要求，不少于6个月；
3. 宜对日志操作进行权限控制，配备日志审计员加强日志访问和处理管理。
	* 1. 安全审计

数据处理者宜建立数据安全审计制度，明确数据安全审计工作牵头部门和相关执行部门，审计目的、审计对象、审计内容（异常操作的定义）、审计操作规程、审计频度、审计结果规范、审计问题整改跟踪等内容。审计对象宜完整覆盖企业相关数据处理活动涉及的平台系统。

数据处理者宜定期进行安全审计，并形成审计报告，涉及重要数据和核心数据的，宜至少每半年进行一次。

数据安全审计的内容宜包括企业内部权限控制、企业内部数据流向跟踪情况、数据安全保障措施有效性等，能够发现和处置数据非授权访问、批量导出等异常情况。

* + 1. 信息上级

数据处理者宜制定数据安全事件信息上报机制，发生数据安全事件的，及时将自身数据安全风险情况向行业监管部门、网信部门报告。

* + 1. 应急管理

数据处理者宜制定数据安全事件应急响应预案，充分考虑企业涉及的各类数据安全事件业务场景，包括但不限于数据泄露（丢失）、数据滥用、数据被篡改、数据被损毁、数据违规使用等。

宜结合数据安全事件业务场景和等级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。

数据处理者宜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。数据处理者宜针对应急演练发现的突出问题和漏洞隐患，及时整改加固，完善保护措施。

数据处理者在数据安全事件发生后，宜按照应急预案，及时开展应急处置。

* + 1. 教育培训

数据处理者宜建立数据安全合规教育培训制度，针对数据安全合规管理相关岗位制定相应培训计划，并对培训计划定期审核和更新。需满足以下要求：

1. 每年宜至少开展一次数据安全合规管理培训；
2. 培训人员宜覆盖企业数据安全岗位人员名单全体人员；
3. 数据安全培训内容宜完整覆盖数据安全制度要求和实操规范等内容，如数据安全法律法规、刑事违法案例、标准制度、管理方法、合规性评估、技术防护、应急演练和相关知识技能；
4. 培训结束后，宜对培训效果进行评定、记录和归档。
	* 1. 安全评估

数据处理者宜制定数据安全评估制度，依据数据安全评估规范，开展数据安全评估及整改。

* + 1. 合作方管理

数据处理者宜建立合作方数据安全管理制度，加强保密管理，明确不同合作类型的数据安全保护方式和责任落实要求，并对义务与责任履行情况进行监督。

* 1. 评价与改进
		1. 自评

航运企业宜建立数据合规定期自评估体系，定期审核评估数据安全和算法合规的落地实施，定期评估工作应由数据合规管理机构负责牵头实施。自评估内容主要包括对数据安全合规体系的设计评估、执行评估及质效评估，以确保数据安全合规目标的实现。

* + 1. 设计评估

数据安全合规体系设计的有效性评估和审查标准主要有：

1. 数据安全合规风险的识别和评估：
	1. 是否定期组织数据安全管理机构对可能面临的数据安全合规风险进行全面评估，重点识别机器学习算法在数据收集、存储、使用、加工、传输、提供、公开、删除等数据全生命周期的风险；
	2. 是否根据风险识别和评估规范确定的合规管理重点问题，发现可能面临的数据安全合规风险，配置相匹配的风险控制和处理能力；
	3. 是否定期更新风险识别监测预警机制及安全评估制度，及时识别和评估原有风险的新变化及新产生的风险。
2. 政策和程序安排：
	1. 是否根据数据处理者的合规风险、业务范围、规模等，制定数据安全合规管理相关制度，对各个环节进行规范化管理；
	2. 是否明确相关制度的执行标准，明确责任主体和责任内容；
	3. 是否针对数据全生命周期各环节建立数据安全合规管理机制，防控可能产生的风险。
3. 培训和沟通安排：
	1. 是否建立合规培训制度，定期组织开展有针对性的数据安全合规学习培训，确保员工充分认识到数据安全合规重要性，通过培训提升各层级的数据安全合规意识；
	2. 是否建立数据安全合规管理的内部及外部沟通渠道，并将数据安全合规文化、合规目标及合规业务纳入沟通内容，确保及时收集和反馈相关信息。
4. 举报和调查机制：
	1. 是否建立数据安全合规举报及调查管理办法，是否对重点风险岗位人员建立专门检查制度；
	2. 是否以公开方式设置举报途径，是否确保所有人员了解举报程序并能够流畅使用相关举报程序；
	3. 是否建立不合规调查程序，确保及时、彻底地调查不合规行为及其原因。
5. 执行和保障机构：
	1. 是否设立数据安全合规管理部门及合规人员，作为企业合规管理牵头部门，组织、协调和监督管理工作；
	2. 是否明确审计、监察、内控、质量、安全及各业务部门在各自职权范围内配合落实数据安全合规管理的日常工作；
	3. 是否在确定数据安全合规相关人员时，要求具备相应的专业资质、良好的业务素质及职业操守。
6. 第三方监督机制：
	1. 是否定期对数据安全合规体系进行合规监督并形成合规评估报告，重点评价数据安全合规体系运行的有效性，以确保数据安全合规目标的实现；
	2. 是否在必要时聘请第三方机构，对企业数据安全合规体系及合规风险管理有效性进行评估，并出具评估报告。
		1. 执行评估

合规管理体系执行的有效性评估和审查标准主要有：

1. 资源配置：
	1. 数据处理者是否为数据安全合规管理配套相关基础设施，将遵守数据安全合规制度及要求作为人员的雇佣条件，配置相应人员；
	2. 是否设立数据安全经常性预算科目，包括用于数据安全培训、管理体系运行、维护及更新等费用，保障数据安全合规管理工作正常进行。
2. 职责权限：
	1. 是否明确数据安全管理机构、数据安全合规管理责任人等相关部门和人员的岗位职责；
	2. 是否明确法定代表人、主要负责人及领导团队中分管数据安全的成员等应当履行的必要合规管理职责；
	3. 是否明确各部门配合落实数据安全合规管理的日常工作的职责及沟通程序。
3. 合规意识：
	1. 管理层及责任人员是否具有数据安全合规意识，是否熟悉数据安全领域的法律法规，是否将数据安全合规工作列入公司管理、考核重点专项工作；
	2. 员工是否具备数据安全合规基本意识，是否了解并遵守数据安全合规制度及要求。
4. 合规管理能力：
	1. 数据安全合规管理相关制度是否能够有效运行，数据安全合规重点环节的合规管理运行机制根是否运行流畅；
	2. 是否统筹衔接法律风险防范、审计监察、内控及风险管理等工作，确保数据安全合规管理闭环；
	3. 是否加强对第三方合作企业的数据安全合规风险监督管理，明确不同合作类型的数据安全保护方式和责任落实要求，包括评估合作方数据安全保护能力、定期组织合作方动态合规性评估等。
5. 奖惩机制：
	1. 是否建立科学的数据安全合规绩效考评指标，围绕合规风险特征相关指标对员工进行考核；
	2. 是否建立并实施相关激励流程，调动员工数据安全合规管理的积极性；
	3. 是否对违反数据安全合规义务、目标、制度和要求的相关人员进行必要的处分。
6. 文件化信息管理：是否将数据安全合规管理过程中的各项要素创建为文件化信息，并有效维护和及时更新。
	* 1. 质效评估

合规管理体系效果的有效性评估和审查标准主要有：

1. 合规文化：
	1. 是否将经营活动各环节相关的数据安全合规管理要求通过流程、制度、合同以及培训、会议等沟通方式向企业员工进行宣传、推广，将数据安全合规管理理念及企业合规价值观根植于经营活动中，营造数据安全合规文化；
	2. 是否构建有利于调动员工积极性的激励机制，树立尊重和保护数据安全的企业形象。
2. 合规目标：
	1. 企业所有的经营活动是否满足合规目标、符合合规要求；
	2. 实现企业合规目标的资源配置是否完善，是否有明确的时间安排及细化流程；
	3. 是否定期监督、检查、记录、评估数据安全合规目标的进度并进行及时更新调整。
3. 可持续发展能力：
	1. 是否根据数据安全相关法律规范的调整，及时调整企业的数据安全合规管理体系，确保其保持最新状态，适应数据安全合规目标；
	2. 是否定期开展数据安全合规内部监察，针对发现的合规风险，及时提出具体解决方案并积极落实整改。
4. 违规事件及其处理：
	1. 发现违规事件时，数据处理者是否及时采取措施控制并纠正，分析违规事件产生的原因；
	2. 是否针对违规事件反映的管理问题及时进行改进和弥补管理漏洞，包括改进业务流程、重新培训员工、加强预警机制等；
	3. 是否向内部和外部通报违规事件相关情况，保留文件化信息。
5.
6. （资料性）
船舶典型场景下的数据合规
	1. 船舶运输集装箱货物流程及数据合规要点
		1. 主要业务流程

船舶运输业务方面代表性业务为集装箱货物的出运，其主要流程如下：

1. 航运公司根据自有船舶运力情况、已获审批的航线情况等，发布船期表，向社会公布特定港口之间的航运运输计划；
2. 货方根据自身的需求，结合航运公司公布的船期表，联系货运代理企业或者全程物流公司，要求其在特定时间、特定地点安排将集装箱送至货方；
3. 货方将货物装入相应集装箱；
4. 物流公司联系船公司，根据货方要求，要求船公司安排将相应集装箱在特定日期装上特定航线船舶；
5. 船公司根据物流公司提供的货物信息，包括货物重量、卸货港、货物危险性等，安排集装箱在船上的具体装载位置，即箱位；
6. 货方通过物流公司将集装箱送到指定码头，船公司提前将装箱计划及箱位提供给码头；
7. 码头根据船公司提供的装船计划，将重箱装上船舶指定位置，并将需要卸下的集装箱卸下；
8. 船运运输集装箱至目的港后，将集装箱卸下；
9. 船公司通知物流公司集装箱运抵情况，物流公司向货方反馈，货方自行或安排第三方至卸货港码头提取集装箱；
10. 集装箱到达收货人指定处所后，收货人取出货物，并将集装箱归还给物流公司。
	* 1. 涉及的主要数据

船舶运输集装箱的过程中涉及的数据包括以下方面：

1. 发货人信息，包括名称、地址、联系方式；
2. 收货人信息，包括名称、地址、联系方式等；
3. 货物信息，包括名称、数量、重量、体积、危险性等；
4. 货物运输信息，包括装货港、卸货港、装船日期等。
	* 1. 数据合规要点

就船舶运输集装箱业务，宜从以下方面考虑数据合规要点：

1. 信息收集：宜根据最小必要原则进行收集，不额外采集数据，比如货物原产地信息、价格信息。货物价格信息可能涉及到货方的商业秘密，除非有必要，否则船公司原则上不宜采集；
2. 信息查询：船公司宜向公众提供货物运转情况信息，以促进物流也的智能化发展。另一方面，船公司不宜向公众提供过于细节的信息，宜隐去货物的具体名称、收发货人、价格等具体信息，仅提供集装箱概位信息即可，无需提供精确位置信息。船公司提供的集装箱动态信息对于一般用户而言极为重要，船公司宜确保信息的准确性、完整性；
3. 传输安全：宜采用校验技术或密码技术保证数据在传输过程中的保密性、完整性，加密方法的选择宜考虑应用场景、传输方式、数据规模、效率要求等。设备宜默认开启数据加密功能。对于非经加密技术传输的信息，船公司宜与相关方做进一步核实，确保信息的准确性，避免信息泄露或者被篡改；
4. 存储安全：提供并使用管理、物理和技术保护措施来保护数据免责免遭受未经授权的泄露或访问；定期备份数据；限制移动存储设备（例如光盘、U盘的）使用。船公司掌握的集装箱动态信息事关国际供应链的健康有序运转，且与相关方实时交互，宜采用多活措施确保信息的完整性、可用性。
5. （资料性）
航运数据分类分级示例

航运数据分类分级示例如表B.1所示。

* 1. 航运数据分类分级

| 一层子类 | 二层子类 | 三层子类 | 建议级别 |
| --- | --- | --- | --- |
| 属性层 | 登记信息 | 船型信息 | 1级 |
| 建造信息 | 1级 |
| 经营信息 | 1级 |
| 动力信息 | 1级 |
| 其它登记信息 |  |
| 其它属性层数据 |  |  |
| 行为层 | 船舶调度 | AIS航行轨迹 | 3级 |
| 航线上的海洋气象数据 | 1级 |
| 挂靠港口 | 2级 |
| 其它船舶调度数据 |  |
| 船舶事故 | 海事仲裁 | 2级 |
| 其它船舶事故数据 |  |
| 其它行为层数据 |  |  |
| 协作层 | 货物运输 | 配载数据 | 1级 |
| 积载数据 | 1级 |
| 海事仲裁 | 2级 |
| 其它货物运输数据 |  |
| 船舶检验 | 定期、年度检验 | 1级 |
| 其它船舶检验数据 |  |
| 船港协同 | 货物装卸 | 1级 |
| 船期 | 2级 |
| 预抵港 | 2级 |
| 其它船港协同数据 |  |
| 其它协作层数据 |  |  |
| 感知层 |  |  |  |
| 监管层 |  |  |  |
| 交易层 |  |  |  |