

智慧民航建设中航空企业数据风险的预防与合规

于 涵

中国民航大学法学院, 天津

收稿日期: 2024年4月23日; 录用日期: 2024年5月7日; 发布日期: 2024年6月21日

摘 要

民航业数据泄露事件频发, 凸显出智慧民航建设中数据保护工作的重要性。航空数据面临内部人员、外部攻击, 流动性强, 参与主体众多等一系列因素带来的泄露风险时, 航空企业应当承担起数据三法等相关法律法规规定的各项数据义务和社会责任。面对数据保护仍存在内部防护不足, 外部风险加剧, 相关法律法规不够细化, 航空企业合规不足的现状, 航空企业应当完善合规工作, 积极参与行业自律并积极参与完善民航领域的数据的分类分级制度建设, 制定有效的用户隐私协议以减少法律风险对航空企业的影响, 积极预防应对航空数据泄露问题, 保障智慧民航建设的安全发展。

关键词

智慧民航, 航空企业, 数据分类分级, 数据合规

Prevention and Response to Data Risks of Aviation Enterprises in the Construction of Intelligent Civil Aviation

Han Yu

Law School, Civil Aviation University of China, Tianjin

Received: Apr. 23rd, 2024; accepted: May 7th, 2024; published: Jun. 21st, 2024

Abstract

Frequent data leaks in the civil aviation industry highlight the importance of data protection in the construction of smart civil aviation. When aviation data faces the risk of disclosure caused by a se-

文章引用: 于涵. 智慧民航建设中航空企业数据风险的预防与合规[J]. 争议解决, 2024, 10(6): 31-37.

DOI: 10.12677/ds.2024.106300

ries of factors such as internal personnel and external attacks, strong liquidity, and many participants, aviation enterprises should assume the data obligations and social responsibilities stipulated by relevant laws and regulations such as the Three Laws on Data. Faced with the current situation of insufficient internal protection of data protection, intensified external risks, insufficient refinement of relevant laws and regulations, and insufficient compliance of aviation enterprises, aviation enterprises should improve compliance work, actively participate in the self-discipline of the industry and actively participate in the construction of data classification and classification system in the civil aviation field, and formulate effective user privacy agreements to reduce the impact of legal risks on aviation enterprises. They should also actively prevent and respond to aviation data leakage problems, and ensure the safe development of smart civil aviation construction.

Keywords

Intelligent Civil Aviation, Aviation Enterprises, Data Classification and Grading, Data Compliance

Copyright © 2024 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

《“十四五”民用航空发展规划》以智慧民航建设为主线，将数据安全视为民航安全和智慧民航建设的基础保障。在数字经济时代到来的背景下，随着智慧民航工作的不断推进，对于数据安全问题的关注和研究变得更为迫切[1]。积极应对网络数据安全威胁多样化和复杂化新挑战，确保民航关键信息基础设施、重要业务信息系统和关键数据资源安全是航空企业在数据利用中的重要课题。

英国航空的客户信息被黑客盗用和泄露事件在 2018 年被曝光后，原因是英国航空内网系统登录账号被黑客盗用后，其公司客户信息被传输到外部第三方网站，而该事件的发生中英航未尽到数据安全义务。同样受到处罚的还有国泰航空，泄露了乘客的姓名、身份证号码、护照号码等涉及旅客身份的个人数据，以及与民航客机预计飞行和历史飞行记录等民航业独有的数据。可见，出现在民用航空业的数据泄露除常见的个人数据泄露，还包括大规模的航空数据非法搜集窃取。境外的间谍机构还可能会利用信息窃取程序窃取旅客的民航出行历史数据。

民航业作为我国重要的交通出行行业，掌握着我国民航旅客出行信息、地理位置信息和经济生产运行数据。通过这些数据的重要性可见数据安全之于民航领域的关键地位。航空数据是与航班时刻、航权、研发技术等具有同等重要地位的民航业资源。民航数据具有着巨大开发利用的潜力，但这一潜力得到挖掘的同时应当重点关注如何找到数据利用和数据安全之间的平衡。可见对于航空企业来说，应当提前预防与应对数据泄露的风险。

2. 航空企业数据保护问题

随着智慧民航建设的逐步深入，智能化民航和数字化民航不仅促进了民航业的发展，还暴露出了数据泄露等安全风险问题。民航业数据传输链条复杂、储存主体多样再加上航空数据丰富量大的特点都加剧了航空企业数据风险。而航空企业在面对数据存在的风险的对策也不足。不仅如此，还存在着现存的数据保护法律法规已经不能满足民航领域智能化不断提高的现状的问题。

2.1. 航空企业数据面临众多泄露风险

数据泄露风险从不同角度可以分为不同种类,对于智慧民航建设中数据安全风险包括来自数据系统外部的不法分子利用黑客攻击非法获取数据,以及来自数据系统内部的数据泄漏等。在民航业存在着现实风险和潜在风险,现实风险包括数据系统技术水平不足、保护数据不受侵害能力不足从而在受到计算机病毒攻击时无计可施等;而潜在风险则为数据库超载而遗失重要数据。

2.1.1. 内部人员风险

内部人员作为最接近数据的第一道防线,其是否具有一定的数据安全知识和数据保护意识对数据泄露风险防范有着重要作用。根据威瑞森发布的 2022 年数据泄露调查报告(DBIR),2022 年 82%的数据泄露是人为因素造成的[2]。同样印证了事故三要素中人这一要素的活跃性,虽然报告中人为因素较去年有所下降,但内部人员造成的错误不能被忽视。越权访问、非法外联、滥用移动介质、随意分享敏感信息都是内部人员会出现的错误,这都体现了其缺乏日常工作应有的数据安全和保密意识培训,企业对于此类培训的不重视体现了其“重发展轻安全、重建设轻防护”的错误数据利用理念,导致了如此重要的航空数据暴露风险增加。

2.1.2. 外部攻击风险

航空数据所在系统还会遭受外部黑客或不法分子攻击。2015 年 6 月 21 日下午,波兰航空公司的地面运营系统突然瘫痪,导致预定航班无法起飞。这提醒了航空工业和世界各地的运营商的黑客技术是基本可以破解民航系统的。不仅是波兰航空,马来西亚航空公司、朝鲜高丽航空公司、美国联合航空公司和美国航空公司网络也都曾遭黑客攻击。不法分子通过对系统的攻击,窃取海量数据,这使得航空企业损失了重要的数据资产,若这些数据被不法利用带来的后果将更为严重。在民航领域,黑客的攻击目的不止于对数据的单纯窃取,还有可能导致空管、机场管理系统或航空公司操作系统崩溃,进而对飞机的正常飞行和旅客人身安全造成严重威胁。

2.1.3. 数据流动频繁导致的泄露风险

智慧民航建设十分重视航空数据的有效利用,通过不同环节和不同主体之间进行数据共享与数据交换的方式进行数据利用。基于民航业信息流动性强的特点和数据更为充分的利用的目标,民航企业运营系统中涉及旅客出行的数据、航班数据和飞行数据等是在各系统中传输流转的,涵盖了航空公司、系统服务商、机场、空管局等民航系统。数据流动的流畅就决定了这些数据更容易在传输利用中泄露。参与流通与传输的系统和主体越多就意味着数据利用的途径越复杂,因此泄露的环节就越多。例如越权访问、账号滥用、访问敏感数据、数据过量访问与下载、跨境储存与传输等安全隐患。而多环节的流动也为事后追查与补救带来了困难,加剧了民航业数据保护的严峻形势。

2.2. 现有规定细化程度有待提高

随着数字化转型不断加快,数据保护的重要性进一步凸显,我国的数据保护框架初步建立完善。除了数据三法外,《促进大数据发展行动纲要》《网络安全审查办法》《关键信息基础设施安全保护条例》也已编写完成。此外,还有多项相关标准正在公开征求意见和编写中。

根据《“十四五”民用航空发展规划》的要求,民航业应积极推进数字化、智能化和智慧化转型发展,并以安全为底线。为了配合这一规划,民航局制定了智慧民航数据治理系列规范。目前已经发布了 7 部行业标准和 1 部信息通告,其中包括框架与管理机制、数据架构、数据质量、数据安全以及数据服务等方面的规定。该系列规范立足于民航业,指导企业如何管数据、用数据。如何进行民航业单位之间

数据和业务的统一管理，实现数据互通和安全共享是一个关键问题。为了达到这个目标，一系列规范指导被提出。这将有利于实现各单位内部和单位间的数据融合与复用，从而降低运营成本，大幅提高数字化转型效率[3]。

但不论是基础性地位的数据三法，还是上述具有针对性的民航业数据治理规范与标准都存在着基础性规定，但细化程度不足难以具体实施的问题。数据安全保护制度中最为基础核心的要属《数据安全法》第 21 条提出的数据分级分类保护制度，但是《数据安全法》中对这一制度的规定十分概括，具体而言，《数据安全法》中仅对“重要数据”进行了概念上的界定，即《数据安全管理办法》规定重要数据是指一旦泄露可能直接影响国家安全、经济安全、社会稳定、公共健康和安全的的数据。但并未规定具体的识别标准。而《智慧民航数据治理规范数据安全》这一标准中对于重要数据的识别也未有规定，仅作如下表述“重要数据的安全等级不应低于 5 级，重要数据识别和认定应依据国家及行业主管部门有关规定执行。”。如何分类、定级标准等涉及具体实施的部分仍不明确，难以据此规定开展数据分类分级工作，同样无法进行后续执法监督、与刑法行政法领域的参与和衔接也无法实现。

2.3. 航空企业数据合规有效性不足

目前，我国航空企业的数据合规活动难以达到有效预防航空数据泄露的有效程度。在个人信息收集集中，大多航空公司与机场等企业的合规活动最关键的是会向接受其提供航空服务的旅客或用户进行《个人信息保护及隐私政策》这类提示文件，以征得其同意航空企业对个人信息收集、保存、使用、共享。但现实中这种提示方法收效甚微，难以对重要条款起到足够的提示作用。一是阅读航空企业的长篇用户协议会占用旅客较长时间导致旅客不进行实质阅读；二是电子协议的格式条款的突出提醒方式不能达到纸质同样的效果。但若旅客不点击同意就无法获得航空企业的服务，所以用户的同意难以达到实质同意的程度，经常忽视条款内容或者干脆选择妥协，同意航空企业的隐私条款。为了解决这个问题，我们可以考虑改变条款的呈现方式，使关键内容更加突出，提高用户的阅读意愿。

3. 航空企业数据保护的对策建议

基于上述问题的分析，航空企业在数据保护方面还存在着问题与不足。只有积极进行应对上述问题，针对性地做出解决，才能更好地在发挥数据利用价值的同时也能兼顾数据安全这一价值。一方面企业应当制定更加合理的隐私政策完善企业的数据合规制度，另一方面民航相关部门也应当积极完善数据分类分级制度的制定，积极推动民航业协会自律，形成更加良好的民航业数据处理环境，助力智慧民航的建设与发展。

3.1. 设立数据安全负责人或管理机构

为确保数据保护义务得到有效执行，航空企业应设立数据安全负责人职位，以具体负责企业的数据安全工作。根据《个人信息保护法》的明确规定，当数据处理企业处理的个人信息量达到法定标准时，必须指定个人信息保护负责人，负责监督个人信息处理活动及所采取的保护措施。此外，企业还需向公众公开个人信息保护负责人的联系方式，并向负责个人信息保护的相关部门报告负责人的姓名和联系方式。

考虑到航空企业内部职能分工对数据安全工作的影响，规模较大的航空企业可进一步设立专门的数据安全管理机构，以统筹协调相关事务。同时，航空企业也可聘请外部专业律师作为数据安全顾问，提供协作监督。无论是数据安全负责人还是管理机构，其核心目标均在于提升航空企业的数据安全管理能力，构建、制定并执行覆盖数据处理全生命周期的数据安全保护机制。

3.2. 完善民航业数据分类分级制度

从分类角度看,民航行业的数据分类体现于《机场数据规范与交互技术指南》将机场数据按业务分类。对标《四型机场建设导则》在智慧机场的“业务管理层”中,按照业务流程细分,设置103种二级类别数据来补充一级类别,以更好地管理业务[4]。对比其他行业,金融领域在《证券期货业数据分类分级指引》的发布及《金融数据安全数据安全分级指南》的推出中率先行动,通过业务与管理数据作为分类标准,将数据划分为不同类别。在当前的行业数据分类中,业务线条仍然是主要依据。除上述数据划分方式外,还应当对面临不同风险的数据按照可能遭遇的风险进行分类,再根据遭遇风险后产生的影响程度相同的数据进行归类,这样可以兼顾数据管理类别清晰和安全保障的有效性。

从分级角度,《数据安全法》要求各地区和部门确定该领域的重要数据目录从而进行不同程度的保护。因此,民用航空数据管理部门需要制定适用于民用航空业的重要数据目录。航空重要数据目录需要长期不断进行调整,航空主管部门、航空行业协会和航空企业三方在收集重要数据的实践的第一线,因此他们在实践中遇到的问题及经验都应当是确定标准和定期更新的重要参考,在制定成目录基础上进行灵活运用。同时还能助力实现民航业单位之间数据和业务管理的统一,推动民航业数据安全互通和共享。第21条将数据分为一般数据、重要数据和核心数据,核心数据实行更加严格的管理制度。企业对关键数据和重要数据的掌握使他们有机会获取更多数据带来的机会,但同时也面对着数据伦理和职业道德的风险责任加重这一挑战。

在具体的分类分级操作中,需要首先判断航空数据的重要程度。判断时应关注安全问题,《数据安全法》提出从是否危及国家安全、影响经济运行、不利于社会稳定和危害公共健康等社会公共领域涉及的常见安全问题确定数据的重要程度。其次,要明确航空数据的分级分类旨在平衡数据流通和数据安全,那么随着数据的重要程度提升,监管的强度也应加大,呈现出一般数据鼓励流动开发,重要数据能够流动但更重视安全以及核心数据以安全为底线的监管局面。

最后,航空数据的定级应是动态发展的。在实际业务场景中,航空线路位置的变动将导致航行位置历史数据可能变为一般数据。一般航空数据为泄露不会使国家和经济运行受损,但对社会、组织和个人可能产生危害。例如航空人员数量、航班人数、旅客的数量。在合法收集后仅需正常使用保护,无需进行额外保护。重要航空数据泄露会危害经济运行、社会稳定和公共利益,如运营数据、行程轨迹、航空偏好、个人数据等可识别的航空数据[5]。这类数据使用目的和告知范围都需特定,若不进行严格的技术处理是不属于合法使用的。最重要的核心航空数据一旦被泄露则可能会危及国家安全、损害经济运行秩序、不利于社会稳定,其收集事由必须要有完全的正当性,数据出境需要获得我国政府的许可,包括空管数据、航空位置数据等。

3.3. 制定有效的用户隐私协议

在数据分级的基础上,航空企业还需要制定有效的用户隐私协议,由于个人航空数据同样适用《个人信息保护法》,那么对于敏感信息的规定也应适用于航空数据,旅客的个人信息应当按照其标准划分为一般与敏感航空数据,进而采用不同的保护方式。在香港国泰航空公司的信息泄露事件中,被泄露的数据一半以上是为旅客个人航空信息,旅客姓名及国籍、身份证号、护照信息、机票出行信息、乘机航行历史等,也就是个人信息在航空领域形成的个人数据。这样的数据本质上还应当属于个人信息,因为其仍然具有《个人信息保护法》所提出的可识别到个人这一特性,但由于在航空领域被收集处理产生痕迹,所以在航空企业数据保护的范围内。因此,旅客基于公务旅行医疗等目的选择民航这一出行方式产生的可以识别到个人和具有敏感性的航空数据,不仅要在分级分类标准下进行管理还要确保《个人信息

保护法》规定的“知情同意原则”得到实质遵循。

《个人信息保护法》对于知情同意模式有严格要求，实践中企业大多采用用户隐私协议的方式对被收集信息的旅客进行告知、提示。将重大利害关系条款文本加粗或下划线，从而将其突出显示。实践中的数据协议不乏令非专业人士困惑的专业词汇和难以分辨的免责条款，旅客或者迷失于协议的模糊内容中或为了乘坐飞机而不得不同意企业提供的数据协议。而这种有争议的“知情同意”也使得航空企业陷入旅客维权的漩涡。在司法实践中，法官认为相关隐私政策提供方未履行提示义务的情形主要包括：第一，在使用 App 时无需点击或者勾选隐私政策，这种情况在企业合规活动后较为少见；第二，未以明显方式提示“已阅读并同意隐私政策”模块，仍有许多购票时隐私政策部分为浅色小字排列在页面底部；第三，系统默认勾选“我已经阅读并同意隐私政策”。

另外，航空企业履行提示义务的时机也需要进行统一规定，司法实践中因为信息收集一方仅在用户首次接受服务时提示用户阅读隐私政策，后续处理信息时未予以一定程度的提示，仍会使得用户难以对信息处理的实际效果产生清醒的认识，减弱知情同意的效果，难以达到企业合规的目的。在旅客要求航空企业对隐私协议条款进行解释时，航空公司作为数据收集者的说明义务产生。航空企业通过在隐私政策中设置专门的电子邮箱或电话收集用户的对该协议的疑问并及时进行相关回复，以达到《个人信息保护法》规定的对数据收集企业隐私政策的说明义务要求。

由于这些数据在未及时进行清理的情况下还会被重复进行利用，航空企业应当定制专门的个人航空数据收集协议模板。在该强制性的格式模板中将数据收集范围、使用目的和交易共享等问题通过简洁通俗的语言进行明确规定，以此减少数据处理权在“知情同意”模式下不明确和随意扩大的问题。企业为了应对逐步完善的数据保护法律法规提出的数据合规要求，应当颁布更新的隐私政策和内部合规指引。可以参考以下隐私政策制定建议：

1) 进一步进行收集目的的规范。《个人信息保护法》规定数据收集应遵循“满足特定目的”且在该目的下尽可能少的收集数据，尽可能缩短保存的时间。但是随着技术的发展导致大量用户数据被推断出来，匿名化这一处理形式不再能达到保护个人不被识别，简单删除客户数据的主要索引远远不够。要求明确和专门说明收集数据的目的。但现实中企业往往难以遵守原始目的规范，许多企业考虑到原始说明的收集目的难以达到大数据发展的用途，将数据利用于原始协议之外的目的，用于许多大数据创新用途[6]。

2) 加强使用安全的保障。这主要是规制数据使用方使用过程中是否遵守协议用途。在未经过该数据所有人授权的情况下，航空企业不得与第三方共享数据，也不得以任何方式随意更改数据的用途。处理个人数据的组织为确保所收集的个人信息的安全，应当做好数据安全保障机制的制定工作，并保障该机制有效运行。

3) 对个人的主体地位进行保证。个人应当对自身被收集数据的处理过程有着主体地位，比如用户个人有删除、更正其数据的权利，对于用户提出的删除和更正，企业应当全力配合，尽管有些情况技术上难以完全抹除数据。

不论数据保护立法多完善，都应当要求数据收集企业进行数据收集和存储的组织对自身数据使用行为负责。因为如果不将法规落实到企业的数据合规实践中，对于国家、企业和个人来说都将遭受不同方面的数据损失甚至更严重。

3.4. 民航行业协会发挥积极作用

民航业协会应发挥积极的引导作用。民航业协会在航空企业与监管部门之间担任着连通这一重要角色。首先，可以收集汇总企业在合规建设中遇到的难题统一反映给有关部门，对于航空企业在数据合规

中的痛点难点，行业协会可以将其整合传达给监管部门，也可以将有关部门最新的监管新规传递给各航空企业。另外对于企业的合规任务也能帮忙推进和监督，分担一部分监管部门承担的职责，对企业和员工进行教育培训、政策宣讲。在企业数据合规制度的构建中，民航业协会的参与与努力是不可缺少的一部分。

4. 结语

民航业的数据资源覆盖了运行、安全、服务等全生命周期。数据安全关系民航安全，也关乎国家安全，但这既是挑战也是机遇，注重数据安全的保护才能更好提升我国民航的国际竞争力、影响力。随着数据安全领域的一系列法律法规日益全面且细化，从事航空数据处理业务的企业也应当主动担当起作为数据收集处理者的法律责任和义务。不仅如此，民航业还要不断探索适用于航空领域的数据安全标准，对实践中出现的特有的数据安全困境也有积极处理和反思的责任。民航企业加强数据合规工作，有效预防数据泄露的发生，才能在不断发掘民航数据利用潜力的同时守好数据安全底线，助力智慧民航规划进一步完成。

基金项目

本文为中国民航大学研究生科研创新资助项目。

参考文献

- [1] 中华人民共和国中央人民政府. “十四五”民用航空发展规划[EB/OL]. https://www.gov.cn/zhengce/zhengceku/2022-01/07/content_5667003.htm, 2023-11-05.
- [2] 2022 Data Breach Investigation Report (DBIR). <https://www.verizon.com/business/resources/reports/2022/dbir/2022-dbir-data-breach-investigations-report.pdf>
- [3] 蒋与文. 数字经济时代民航业数据安全研究工作[J]. 民航管理, 2022(10): 42-45.
- [4] 王欣, 刘一. 以数据标准驱动引领智慧机场建设——《机场数据规范与交互技术指南》解读[J]. 民航管理, 2022(3): 35-38.
- [5] 王瑞亨. 航空数据的分类分级与流动刍议[J]. 民航管理, 2022(12): 84-88.
- [6] 胡玲, 马忠法. 论我国企业数据合规体系的构建及其法律障碍[J]. 科技与法律(中英文), 2023(2): 42-51.