PNR Agreements and related cybersecurity risks

Mrežar, Mihaela

UNIVERSITY OF ZAGREB

FACULTY OF LAW

Mihaela Mrežar

PNR AGREEMENTS AND RELATED CYBERSECURITY RISKS

Graduate thesis

Mentor: Associate professor Iva Savić

Zagreb, September 2023.

Izjava o izvornosti

Ja, Mihaela Mrežar, 0066276635, pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključiva autorica diplomskog rada te da u radu nisu na nedozvoljeni način korišteni dijelovi tuđih radova te da se prilikom izrade rada nisam koristila drugim izvorima do onih navedenih u radu.

Mihaela Mrežar

_____

TABLE OF CONTENTS

SUMMARY

The use of Passenger Name Records (PNR) data for security purposes, started in the USA in 2001, following the 9/11 terrorist attack. Ever since, the USA have been using their influence to enter into agreements with other states that would allow them to exchange passenger data and achieve better results using the PNR system. The first PNR agreement between the EU and USA was signed in 2004, but has since been re-negotiated twice, due to its incompability with existing human rights regulations. The EU interest in PNR and its own counter-terrorism strategy, while at first undoubtedly influenced by the USA, after the terrorist attacks in 2015 and 2016 finally culminated in the adoption of a Directive on PNR. PNR data has more recently been shown to be a target of a growing number of cyberattacks, causing significant financial damage to both airlines and their passengers. Cyberattacks committed with the specific goal of obtaining information are a subject of both aviation security regulation as well as data protection. This paper aims to examine the provisions of PNR agreements concluded by the EU with other states as well as the PNR Directive, and the relevant judicial decisions. An emphasis will be put on the issue of cyberattacks targeting the aviation industry with the goal of obtaining passenger data, their characteristics and the international documents regulating cybersecurity and their applicability to cyberattacks.

Key words: PNR data; civil aviation; cyberattack; cybersecurity; PNR agreement; terrorism

SAŽETAK

Korištenje podataka iz evidencije imena putnika (PNR) u sigurnosne svrhe počelo je u SAD-u 2001. godine, nakon terorističkog napada 11. rujna. Od tada SAD koristi svoj utjecaj za sklapanje sporazuma s drugim državama koji bi im omogućili razmjenu podataka o putnicima i postizanje boljih rezultata korištenjem PNR sustava. Prvi PNR sporazum između EU-a i SAD-a potpisan je 2004. godine, ali je od tada dva puta ponovno pregovaran zbog neusklađenosti s postojećim propisima o ljudskim pravima. Interes EU-a za PNR i vlastitu strategiju za borbu protiv terorizma, iako je isprva bio nedvojbeno pod utjecajem SAD-a, nakon terorističkih napada 2015. i 2016. konačno je kulminirao donošenjem Direktive o PNR-u. Nedavno se pokazalo da su PNR podaci meta sve većeg broja kibernetičkih napada, uzrokujući značajnu financijsku štetu i zrakoplovnim prijevoznicima i njihovim putnicima. Kibernetički napadi počinjeni sa specifičnim ciljem dobivanja informacija predmet su kako propisa o sigurnosti zračnog prometa, tako i zaštite podataka. Ovaj rad ima za cilj ispitati odredbe PNR sporazuma koje je EU sklopila s drugim državama, kao i PNR Direktivu, te relevantne sudske odluke.

Naglasak će biti stavljen na problematiku kibernetičkih napada na zrakoplovnu industriju počinjenih s ciljem krađe podataka o putnicima, karakteristikama kibernetičkih napada te međunarodnim dokumentima koji reguliraju kibernetičku sigurnost i njihovu primjenjivost na kibernetičke napade.

Ključne riječi: PNR podatci; civilno zrakoplovstvo; kibernetički napad; kibernetička sigurnost; PNR sporazum; terorizam

1. INTRODUCTION

PNR (Passenger Name Record) data consists of identifying information which the passengers provide and air carriers collect in the ticket reservation and buying process. The collected data can differ, but usually include names, addresses, payment method and information, e-mails, telephone numbers, frequent flyer information, baggage information, passport information, travel agency, seat number, travel itinerary and travel destinations, health requirements and even meal preferences of the passengers.

The reliance of all sectors of the aviation industry on information and communication technology has resulted in increased global cooperation of states and information sharing. PNR information is necessary for air carriers to operate flight reservations and check-ins, but the issue is what this information, once collected, is used for, and who has access to it. Namely, the use of PNR information for profiling of passengers, carried out by government authorities, was questioned in the context of human right regulations, discrimination as well as the danger of data theft. While states have tried to justify the intrusions into human rights by emphasising the general interest of crime prevention, the question of necessity and proportionality remains.

Therefore, PNR data has been a subject of discussion as it is a great example of conflict between the interests of general security, which are a key consideration in the aviation industry, and individual human rights.

Another issue which has been raised in the more recent years is the growing number of cyberattacks targeting the aviation industry, with the particular goal of collecting this exact data, either in ransomware attacks (where the attackers take over control of a system and refuse to give it back until ransom is paid) or to steal passenger and personnel information for financial gain. While in the past the most significant threat to aviation security were plane hijackings, the development of technology in more modern times and the dependency of the aviation industry on information technology have led to an increase of criminal misuse of technology, which became an issue with possible global consequences. Taking this into consideration, the idea of collecting, keeping, analysing and sharing of numerous categories of private information by air carriers can be questioned.

In this paper I will analyse the utilisation of PNR information in ensuring the security of civil aviation, focusing on the PNR agreements signed by the EU with other states, as well as the issues which appeared in practice. The paper will review a number of judicial decisions on the

compatibility of PNR data agreements with the existing human rights regulations. An emphasis will be put on the issue of cyberattacks targeting the aviation industry, with the particular goal of obtaining PNR data. The paper will further analyse the characteristics of cyberattacks and the international documents regulating cybersecurity and their applicability to cyberattacks, especially regarding data theft.

2. CYBERSECURITY IN CIVIL AVIATION

Safety and security has always been the main priority of civil aviation and the measures taken to ensure it have only improved and increased through the years to provide better protection of passengers on board flights. While security threats that have existed for longer, such as seizure of aircraft, have extensive legal regulatory framework, widely accepted in the international community, cyberattacks have only more recently been recognised as a significant safety threat that requires more direct regulation and address. In the context of PNR, a particular danger is presented by cyberattacks targeting the large databases of passenger information that air carriers collect. The considerations of aviation safety, cybersecurity and data protection, as well as the damage to passengers and air carriers make the issue of PNR data theft both serious and complex.

This Chapter will analyse and compare international and EU legislation regulating cybersecurity and data protection, their deficiencies and possible areas of improvement.

2.1. General characteristics

The risk of cyberattacks has dramatically increased in the last couple of years and for the aviation industry to combat it, comprehensive legal framework is an imperative. The aviation industry relies on the confidence and trust of the public for its success, which can be undermined by hostile actors through cyberattacks and publicising their actions. Even though cyberattacks are becoming more common, they are not a new occurrence in the field of aviation. Namely, the first recorded cyberattack targeting an aviation stakeholder happened in 1997, at an airport in Worcester, Massachusets. A teenager managed to disable numerous airport safety and security services and caused major disruption and flight delays.[1] Luckily this cyberattack had

[1] Bergamasco F., Cassar R., Popova R., Scott B. I., Cybersecurity - Key Legal Considerations for the Aviation and Space Sectors, Wolters Kluwer (2020), p. 3.

fairly minimal effects for aviation safety. Still, both national and international regulators have been working on cybersecurity legislation to prevent such instances, which could possibly endanger the safety of passengers.

Modern aviation consists of planes that are supported by ground equipment and computerised systems and large scale interconnected computer network to enable the success and safety of civil aviation.[2] It is this network interconnectivity that makes aviation increasingly vulnerable to cyber operations, such as seizure of control over the aircraft, interference with aircraft flight control systems, navigation and ATC communications systems. Another possible consequence of this are the cascading effects of a cyberattack, which may not be initially intended by the attacker, but are nevertheless caused by the mutual dependence of the network systems.[3] For example, a hypothetical attacker wanting access to passenger data, by disrupting the availability of passenger databases, could cause severe disruption.

Considering the multiple systems necessary to facilitate aviation operations, cases of cyberattacks in the aviation industry, according to the ICAO Legal Committee, can be sorted into one of these four categories, depending on the infrastructure system targeted in the attack.[4] The first category would consist of acts or threats aimed at Air Traffic Management (ATM) systems, meaning attacks targeting communication, surveillance or navigation systems. The second category could be attacks targeting Aircraft Systems, possibly the aircraft control or cabin operational system. The third category are acts interfering with either airline or airport operations, which even though are not directly aimed at an aircraft, could still endanger it by disrupting aviation security measures (for example, screening of passengers and their baggage, departure control). The fourth category consists of attacks on other relevant aviation systems with the goal of stealing important information assets. In particular, such cyberattacks include the theft of PNR data.[5] In connection with the fourth category, a possible risk of cyber operations is the theft of intellectual property, including data, design method, development technique, and technology used in manufacturing.

[2] Klenka, M., *Aviation cyber security: legal aspects of cyber threats*, Journal of Transportation Security Vol. 14 (3) (2021), p. 177.
[3] International Civil Aviation Organisation Legal Committee– 38th Session: Consideration of the adequacy of existing international air law instruments in adressing cyber threats against civil aviation, Working Paper (22nd to 25t March 2021), p. 13.
[4] *Ibid.*, p. 15.
[5] *Ibid.*, p. 15.

Since there is no universally accepted definition of a cyberattack, they can be defined using a combination of relevant elements. The term has been commonly used to describe activities that produce negative effects, with the potential of rising to the use of force. [6] In this sense, the term cyberattack can be defined as "a range of malicious activities conducted using information and communications technology."[7]

Cyberattacks can be either active or passive, depending on whether they produce disruption or disabling of a service or not. So a cyberattack causing denial of service or restriction of access would be considered as an active one. In contrast, a passive cyberattack is, for example, information theft that does not cause the disruption of a system, and can leave the victim unaware. [8]

The lack of physicality is one of the defining characteristics of a cyberattack.[9] Various methods of cyberattacks also include varied locations of the attacker. While some may be committed by an attacker on board the aircraft, others could be committed from a distant location or a different country. Also, the locating the source of a cyberattack can be challenging in itself. Additionally, there is further debate in determining which act is considered to be the attack, which could interfere with defining the location (in particular, the location from where the attack originated or the location where the consequence occurred). The matter of location is particularly important because the relevant instruments determine jurisdiction of a state based on the location of the offence or by identifying the responsible parties. Identifying the involved attackers can also be a problem when taking into consideration that another advantage cybercrime allows is that of anonymity.

While various types of actors such as individuals, states and hacktivist groups may commit a cyberattack and their motives may differ, a review analysing cyberattack incidents targeting civil aviation in the past 20 years determined that the main threat to the industry comes from Advances Persistent Threat Groups (hereinafter: APT groups), collaborating with a certain state actor. Their goal is to acquire intellectual property and intelligence to advance national capabilities.[10]

---

[6] Bergamasco F., Cassar R., Popova R., Scott B. I., *supra* n. 1, p. 23.
[7] Klenka, M., *supra* n. 2, p. 179.
[8] Bergamasco F., Cassar R., Popova R., Scott B. I., *supra* n. 1, p. 24.
[9] Working Paper, *supra* n. 3, p. 13.
[10] Ukwandu, E., Ben-Farah, M.A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, I., Bellekens, X., *Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends*, Information Vol. 13, 146 (2022), p. 1.

2.2. Legal Framework

2.2.1. International air law instruments

In order to analyse the specific legislation regulating cyberattacks, it is necessary to acknowledge the central role of ICAO in international air transport regulation, on account of both its longevity and the number of Member States.[11]

One of its main tasks is to develop and maintain rules, in the form of Standards and recommended practices (hereinafter: SARPs), which play a key role in harmonising global regulation on aviation safety, security, air navigation facilities, rules of air, aircraft registration marks and so on. SARPs are developed in the so called "*amendment process*" or "*standards-making process*". Currently ICAO manages over 12,000 SARPs contained in the 19 Annexes.[12] Both standards and recommended practices are defined in Annex 2, but while standards are mandatory and require Contracting States to conform with them ("in the event of impossibility of compliance, notification to the Council is compulsory under Article 38"), recommended practices only require States to "endeavour to conform" with them.

The ICAO Assembly, pursuant to Resolution A39-19, established the Secretariat Study Group on Cybersecurity (hereinafter: SSGC), which held its first meeting in 2017.[13] The SSGC consists of four working groups.[14] It reviews the Annexes, reinforces existing SARPs relating to cybersecurity, analyses proposals by its working groups for changes to provisions or for the development of new provisions relating to cybersecurity. This would mean that the focus of its work is on unlawful interference.[15] The biggest contribution made by SSGC was the cybersecurity strategy, which the Council adopted during its 217th session.

[11] The 1944 Chicago Convention founded the International Civil Aviation Organisation, a UN specialised agency with the task of regulating and coordinating international air transport. As of now, ICAO has 193 Contracting States.
[12] How ICAO Develops Standards, https://www.icao.int/about-icao/AirNavigationCommission/Pages/how-icao-develops-standards.aspx (last accessed 18 June 2023).
[13] Bergamasco F., Cassar R., Popova R., Scott B. I., *supra* n. 1, p. 172.
[14] A group for legal research, for airlines, a for air navigation systems, and for cybersecurity.
[15] Abeyratne, R., *Legal Priorities in Air Transport*, (2019), p. 192–193.

Preceding ICAO's cybersecurity documents and achievements, cybersecurity was regulated through the UN Resolution of 2001,[16] which mentions the significance of the work on a draft convention on cybercrime by the Council of Europe.

Aside from ICAO regulation, the Cybercrime Convention of the Council of Europe[17] (hereinafter: the Budapest Convention), which entered into force in July 2004,[18] is the first multilateral agreement addressing cybercrime. State Parties agreed by entering the Convention that cooperation between States and private industry is necessary to successfully combat cybercrime.

The Convention, in Article 2, prescribes that "each State Party shall adopt legislative measures necessary to establish as criminal offences under its domestic law, the intentional access to a computer system without right." Article 7, regulating the offense of Computer-related forgery (in the category of computer-related offences), requires each Party to "adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible." This Article is significant to aviation as it protects certain measures, adopted by the aviation industry, to ensure the authenticity of passports and other travel documents, for example, the Public Key Directory (PKD).[19]

a. ICAO instruments

[16] United Nations Resolution adopted by the General Assembly [on the report of the Third Committee (A/55/593)] Combating the criminal misuse of information technologies, 55/63 (22 January 2001). The UN General Assembly Resolution addresses the measures necessary to combat the criminal misuse of information technology. It's adoption in January of 2001 emphasises just for how long cybersecurity has been an issue of importance. It refers to data pertinent in criminal investigations, which could be applied to PNR data, and prescribes that legal systems should allow the quick access to such information. One of the clauses specifically requests the creation of technologies „designed to help prevent and detect criminal misuse, trace criminals and collect evidence to the extent practicable".[16] The need to develop these solutions while considering „the protection of individual freedoms and privacy" but still allow the Governments to efficiently fight the criminal misuse is stressed.

[17] Council of Europe Convention on Cybercrime, European Treaty Series - No. 185, Budapest (23 October 2001).

[18] Bergamasco F., Cassar R., Popova R., Scott B. I., *supra* n. 1, p. 49.

[19] Abeyratne, R., *Cyber terrorism and aviation—national and international responses*, J Transp Secur Vol. 4 (2011), p. 9.

The most important ICAO instrument, the Chicago Convention, stipulates in its Article 3 that all Contracting States must have "due regard for the safety of navigation of civil aircraft". Cyberattacks targeting civilian flights, could be in breach of this provision as an instance of unlawful interference.[20] Additionally, such a cyberattack would also breach Article 3 *bis* of the Convention, which was added to the Chicago Convention by a Protocol, in May of 1984, after the Korean Airlines Flight 007 was shot down by the Soviet air forces in 1983.[21] It entered into force in 1998 and has currently been ratified by 156 States. It prescribes that "every State must refrain from resorting to the use of weapons against civil aircraft in flight". The scope of this Article has been recognised as wider. In fact, air law experts, namely, Professor Milde and Judge Guillaume, are of the opinion that Article 3 *bis* actually declares the customary law principle of non-use of weapons.[22] Therefore, even though not all Parties to the Chicago Convention are Party to Article 3 *bis*, this interpretation would allow for its broader applicability. The next question arising when considering cybersecurity is whether cyberattacks would be considered as a weapon under this provision, as the Chicago Convention or any of its 19 Annexes define either of the terms. One of the possible interpretations is that since the main concern of this Article is the protection of civil aviation, any means that could cause death, injury or damage would amount to a weapon and fall under this provision.[23]

Additionally, Annex 17 is of particular importance because it contains SARPs on aviation security measures in relation to acts of unlawful interference. Cyberattacks could be considered as an act of unlawful interference, if and when they impact aviation security. A new Recommended Practice referring to cyber threats was proposed and adopted at the 21st Aviation Security Panel Meeting of ICAO in 2010 as an amendment to Annex 17. Chapter 4 of Annex 17, appropriately named "Measures relating to cyber threats", contains a Standard and a Recommended Practice. Standard 4.9.1. prescribes that "each Contracting State should implement measures to protect their critical information and communication technology systems and data, used for civil aviation, from unlawful interference". As previously explained, standards established by ICAO are mandatory. Implementation of this standard by all Contracting states would significantly decrease the risk of cyberattacks having huge negative impacts on aviation security.

[20] Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., Spiegel, J., *The Law of Cyber-Attack*, California Law Review Vol. 100 (4) (August 2012), p. 868.
[21] Working Paper, supra n. 3, p. 7.
[22] *Ibid.*, p. 7.
[23] Bergamasco F., Cassar R., Popova R., Scott B. I., *supra* n. 1, p. 157.

In 2019, ICAO published its Aviation Cybersecurity Strategy, after it's demonstration at the 40th Session of the ICAO Assembly.[24] In it, ICAO covered the growing threat of cyberattacks, while acknowledging the dependence of aviation on the "availability of information and communications technology systems as well as on the integrity and confidentiality of data."

The growing number of incidents of unlawful seizure of aircraft and terrorist attacks targeting aviation in the 1950s, as well as the inadequacy of the Chicago Convention in addressing these issues, resulted in the establishment of international criminal air law. It is imperative to review if these instruments are applicable to cyberattacks to determine if they are adequate to prosecute hypothetical attackers. While doing so, it is necessary to remember that the biggest threat when creating this legislation was the seizure of aircraft by cyber means, and therefore the legislation tries to regulate and criminalise that type of cyberattack, while data breaches are, even now, mostly regulated through data protection regulations. The provisions provided in these documents could still apply to the cases of data breaches since they could also present a danger to the security and safety of aircraft in flight, which is the most important applicability criteria. Understandably, none of the earliest criminal air law instruments, such as the Tokyo Convention [25], the Montreal[26] Protocol, The Hague Convention of 1970[27], the Montreal Convention[28] and the Airport Protocol[29]regulate the issue of cyberattacks. Therefore, they can only be applied to cyberattacks under very specific conditions. For example, a common prerequisite, contained in multiple of these conventions, is that the offense was committed during the flight and that the attacker was on board the aircraft, which knowing that cyberattacks can be committed remotely, renders these documents ineffective in prosecuting an attacker. Furthermore, the court of the state of jurisdiction would have to interpret certain terms such as "use of force" to include cyberattacks as they are not mentioned or defined in any of these

[24] *IATA: Compilation of Cyber Security Regulations, Standards, and Guidence Applicable to Civil Aviation (December 2020), https://www.iata.org/contentassets/4c51b00fb25e4b60b38376a4935e278b/compilation-of-cyber-regulations-standards-and-guidance_3.0.pdf (last accessed June 2, 2023),* p. 7.

[25] Convention on Offences and Certain Other Acts Committed on Board Aircraft, signed at Tokyo on 14 September 1963.

[26] Protocol to Amend the Convention on Offences and Certain Other Acts Committed on Board Aircraft (Montréal, 2014).

[27] Convention for the Suppression of Unlawful Seizure of Aircraft (1970).

[28] The Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, signed at Montreal on 23 September 1971.

[29] Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, signed at Montreal on 24 February 1988.

instruments. This lack of an adequate legal basis, was finally resolved in 2010 when both the Beijing Protocol and the Beijing Convention were signed.

b. The Beijing Protocol

The Beijing Protocol[30] modernised the Hague Convention and broadened the regulatory scope, reflecting the evolution of the technological means that can be used when targeting civil aviation.[31] The Protocol is the first aviation document that explicitly mentions cybersecurity and expresses the clear intent to cover it, by adding the terms "or by any technological means" to the definition of unlawful seizure of aircraft in Article 1.[32] There is also no longer the requirement for the qualification of an act of unlawful seizure that the offender must be on board the aircraft during the act, which makes it even more directly applicable to cyberattacks, considering their remote quality.

The timeframe for which unlawful acts are covered to is broadened in the Beijing Protocol "from the beginning of the pre-flight preparation of the aircraft until twenty-four hours after any landing".[33] This could be relevant in cases of acts committed before the flight, during preparations, and also cyberattacks after the flight, during maintenance activities. While the Beijing Protocol directly covers cyberattacks, it remains required to prove that the cyberattack resulted in the "seizing" or "exercising" control of an aircraft, which somewhat limits its scope. These limitations can still be considered negligible when noting the huge improvement this instrument presents from its predecessors in regulating cybercrime. In the future, the international community will probably try to regulate this issue in a more direct manner, better adjusted to the constant development of technology, but the Beijing Protocol is a sufficient start.

c. The Beijing Convention

While the Beijing Convention[34] is a separate instrument, it attempts to consolidate and modernise the Montreal Convention and the Airport Protocol.[35] It came into force in 2018, but

[30] Beijing Supplementary Protocol to the 1970 Hague Convention for the Suppression of Unlawful Seizure of Aircraft (2010).
[31] IATA Compilation, *supra* n. 24, p. 6.
[32] *Ibid.*, p. 6.
[33] Working Paper, *supra* n. 3, p. 12.
[34] Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation, done at Beijing on 10 September 2010 (Doc 9960).
[35] IATA Compilation, *supra* n. 24, p. 6.

currently only 26 states have ratified it.[36] This Convention, by prohibiting offenses targeting air navigation facilities, expanded the scope of application to include cyberattacks. Air navigation facilities are defined as "signals, data, information, or systems necessary for aircraft navigation."[37] Article 1 explicitly states that "Any person commits an offence if that person unlawfully and intentionally: destroys or damages air navigation facilities or interferes with their operation, if any such act is likely to endanger the safety of aircraft in flight." This makes the Convention more applicable to cyberattacks than any of the earlier documents, except for the Beijing Protocol.

Article 1 in paragraph 3 establishes the so-called ancillary offenses,[38] by making it an offence to "make a credible threat to commit any offense against civil aviation" (covering also the new ones prescribed) or to "unlawfully and intentionally cause any person to receive such a credible threat". The application of this provision will depend on national courts, who will have to determine if a person's behaviour constitutes a credible threat. This could once again cause inconsistency in the way the Convention is applied, depending on national interpretation. Additionally, Article 1 paragraph 5 broadens the scope of liability even more to include attempts, organisation, participation and assistance to avoid prosecution. The criminalisation of the acts of a person who "organises or directs others to commit an offence". It is not required in this case for the primary offence to be completed. Furthermore, agreeing to commit an offense as well as contributing in any way is an offense on its own regardless of whether an offense was committed.[39]

The UN created a draft treaty suggesting the creation of an International Criminal Court or Tribunal for Cyberspace, which is an interesting approach to regulating international cybersecurity.[40] Such a judicial body would present a unified law enforcement mechanism for cybercrime and guarantee the proper application of the existing instruments.

In conclusion, the scopes of both the Beijing Convention and the Beijing Protocol are adequate in providing a legal ground for prosecution of individuals conducting cyberattacks

[36] As of 12 December 2018. The Beijing Convention: The Convention on the Suppression of Unlawful Acts, https://unitingaviation.com/news/security-facilitation/the-beijing-convention-the-convention-on-the-suppression-of-unlawful-acts/ (last accessed 31 August 2023).
[37] The Beijing Convention, Article 2 (c).
[38] Piera, A., Gill, M., *Will the New ICAO–Beijing Instruments Build a Chinese Wall for International Aviation Security?*, Vanderbilt Journal of Transnational law Vol. 47:145 (2014), p. 180.
[39] *Ibid.*, p. 181.
[40] Draft United Nations Treaty on an International Criminal Court or Tribunal for Cyberspace, from June of 2015.

against civil aviation, therefore a wider ratification of these instruments is needed to successfully prosecute cyberattacks on a unified, international level. The reasons for why these documents have so few signatories should be studied and discussed, especially now that cyberattacks are becoming much more common than plane hijackings and these two documents are the only ones regulating them. A country not party to the Beijing Protocol or Convention, in the case of a cyberattack, would have to apply one of the aforementioned older instruments, which could result in case dismissals due to the interpretation and the specific circumstances of the attack. In conclusion, a wider ratification of the Beijing instruments is not only necessary, but in everyone's best interest.

2.2.2. EU regulations

One of the issues with regulating cybersecurity on an international level lies in the fact that states are not obligated to ratify the treaties, and only do so according to their national interests, which then results in varying degrees of ratification and protection. This is particularly troublesome considering the international character of cybersecurity and the importance of State cooperation and information sharing which is highlighted in almost every Preamble of the previously mentioned documents. That is why regulating cybersecurity on the EU level could be more effective for its Member States. Specifically, the position of the EU as a supranational organisation means that states, by agreeing to the membership, transfer certain powers to the EU. This also means that the regulations EU creates are fully and automatically binding to the Member states, ensuring harmonisation and uniformity of legal framework regulating a certain subject, such as cybersecurity or data protection. While directives need to be transposed into national laws to be applied, it is still obligatory for states to achieve those goals prescribed in directives.

The EU started tackling the cybersecurity issues with the release of the first Cybersecurity Strategy[41] in May of 2013. This Strategy detailed the guiding principles that the EU cybersecurity policy and law should adopt and presented the five strategic priorities (establishing the relevancy of ENISA and the NIS Directive).[42] It's importance is amplified by the mentioning of UN in the fifth strategic priority (establishing an international cybersecurity

[41] European Parliament Resolution of 12 September 2013 on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013/2606/RSP).
[42] Bergamasco F., Cassar R., Popova R., Scott B. I., *supra* n. 1, p. 69.

policy in cooperation with entities like UN, NATO and OECD), since that would include ICAO.[43]

The European Union Agency for Cybersecurity (hereinafter: ENISA) is an agency tasked with advancing the standard of network and information cybersecurity in Europe. It was first established in 2004 with a mandate that was meant to expire in 2020, but by stepping into force of the Cybersecurity Act, it was given a new and strengthened role.[44] It assists in the development and advancement of the EU cyber policy, creates cybersecurity certification to enhance the trustworthiness of information and communication technology services and products, and improves cooperation among EU Member States.[45]

Directive (EU) 2016/1148[46], better known as the NIS Directive, is the first EU legislation regulating cybersecurity.[47] The Directive came into force in August 2016 and the deadline for Member States to implement it into their national laws was in May of 2018. The main objective of the NIS Directive, as established in Article 1, was "to achieve a high common level of security of network and information systems within the Union". But since not all States have implemented the Directive, cybersecurity measures are still not uniform across all EU States.

The Directive is applicable for two kinds of subjects: "Operators of essential services" and "Digital service providers", with aviation stakeholders falling into the first category. This is confirmed in Article 5, paragraph 2 that prescribes "the criteria for the identification of the operators of essential services". The criteria laid down is: "(a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities; (b) the provision of that service depends on network and information systems; and (c) an incident would have significant disruptive effects on the provision of that service." Therefore, the obligations and rights provided in this Directive apply to aviation stakeholders.[48]

In December 2020, the EU released its 2nd Cybersecurity Strategy (EUCSS), aiming to guarantee strong safeguards in events of cybersecurity risks, and with the biggest announcement being the upgrade of the NIS Directive. In January 2023, the NIS Directive was replaced by

[43] *Ibid.*, p. 72.
[44] *Ibid.*, p. 93.
[45] ENISA Official website, About ENISA, https://www.enisa.europa.eu/about-enisa (last accessed 18 June 2023).
[46] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
[47] Bergamasco F., Cassar R., Popova R., Scott B. I., *supra* n. 1, p. 78.
[48] *Ibid.*, p. 80.

the Directive (EU) 2022/2555 (known as NIS2)[49]. NIS2 improves the existing standard of cybersecurity in the EU, achieved by the application of the aforementioned Directive, by creating a crisis management system specifically for cyber threats and achieving harmonisation between the EU States concerning reporting obligations and cybersecurity requirements. It also assigns certain obligations to ENISA, such as providing support to the organisation of peer reviews, publicising of the annual report on cybersecurity in the EU, as well as creating the registry for private entities that provide cross-border services in the EU. Member States have been required to implement the Directive by 17 October 2024.[50]

Of a more specific relevance for aviation is Regulation (EU) 376/2014[51], which, with the goal of ensuring aviation safety, requires that the relevant information is collected, reported, and then appropriately analysed. It supports the increase of exchange of information concerning safety between Member States, while also protecting the continuous availability of such information. Based on this regulation, Member States should, together with EASA and with other organisations, establish an occurrence reporting system.[52]

Furthermore, Regulation (EU) 2019/1583[53] establishes detailed rules for implementing common standards on aviation cybersecurity. Namely, the goal of this Regulation is to aid Member States in interpreting and ensuring adherence to the new implemented standards 3.1.4. and 4.1.9. of Annex 17 to the Chicago Convention. Another one of its objectives is to establish mechanisms for monitoring compliance with these standards. Additionally, the European Commission issued the Transport Cybersecurity Toolkit with tips and advice for upgrading cybersecurity awareness in the transport industry in general, including aviation.[54]

Since access to personal information can be the goal of a cyberattack, cybersecurity is closely connected with data protection, as was seen in described cases of cyberattacks. The right to the protection of personal data is ensured by Article 8 of the Charter, however, the EU went even further in guaranteeing this right through secondary sources of law. Specifically, Regulation

[49] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).
[50] Official website, https://www.nis-2-directive.com/ (last accessed 18 June 2023).
[51] Regulation (EU) No 376/2014 of the European Parliament and of the Council of 3 April 2014 on the reporting, analysis, and follow-up of occurrences in civil aviation.
[52] IATA Compilation, *supra* n. 24, p. 10.
[53] Commission Implementing Regulation (EU) 2019/1583 of 25 September 2019 amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures.
[54] IATA Compilation, *supra* n. 24, p. 11.

2016/679,[55] often referred to as the GDPR (General Data Protection Regulation), addresses the privacy and protection of data, both within the EU and the EAA, including outside those areas. It came into force in May of 2016, while Member States had two years to implement it into national laws.[56] Article 4 of the GDPR states that it applies to both "controllers" and "processors", meaning the person, body or entity that "determines the purpose and the means of processing personal data", but also the person, entity or body that processes this data. GDPR prescribes obligations that organisations must adhere to in order to legally collect and further process personal data. As a sanction in cases of non-compliance with these obligations, GDPR in Article 83 prescribes administrative fines. These fines can range "up to 20 000 000 EUR, ... or 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher" for the most severe infringements (for example, provisions regulating the basic principles of data processing and data subject's rights).

To conclude, the EU has been constantly developing its cybersecurity strategy and amending the existing legislation regulating this area. The framework adequately addresses data protection and exchange, the roles of EU agencies in promoting and regulating cybersecurity, as well as provides obligations for Member States to adapt their national laws to the newest standards of protection, which leads to a higher level of uniformity and harmonisation of legal systems.

3. PNR AGREEMENTS

While cyberattacks understandably present a prominent threat to aviation safety and security, cyberattacks with the goal of passenger data theft can also cause significant financial loss for air carriers. Namely, oftentimes air carriers either need to pay ransom to the attackers, can be found responsible and are required to pay fines to official authorities for non-compliance with prescribed security measures and might even be sued by the passengers themselves. The collection of PNR data is necessary for airlines to enable the booking of flights, however, the time period for which it is retained and the exchange of this data is regulated by government authorities through bilateral agreements. Why this data is so crucial to governments and law

[55] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
[56] Bergamasco F., Cassar R., Popova R., Scott B. I., *supra* n. 1, p. 87.

enforcement, as well as the measures taken to protect the privacy of passengers and their personal information in PNR agreements will be the topic of the following Chapters.

3.1. History of PNR systems

The development of air traffic safety systems in the USA was influenced by over 50 cases of airplane hijacking in the USA, in the 1960s.[57] In 1973, the screening of passengers and hand luggage with metal detectors was introduced by the Federal Aviation Administration (hereinafter: the FAA) to increase security.[58] Additionally, some air carriers introduced proactive methods that sought to screen out suspicious persons in advance, for example if they used the same phone numbers or credit cards as previous perpetrators. Initially, state bodies were not involved in the safety and security development, and the passenger profiling was an independent activity carried out by air carriers, using the collected PNR data. This activity was over time proven both beneficial and controversial.

The biggest contribution to passenger profiling with the goal of improving aviation security was made by the US carrier Northwest by trying to create profiles of plane hijackers. The success of passenger profiling led to the introduction of a computerised passenger prescreening system called CAPPS (Computer-Assisted Passenger Prescreening System).[59] This system was based on the predicted behavior of potential terrorists and looked at, for example, age, method of payment, flight directions and related data. After the New York City attacks on September 11 of 2001, the Transportation Security Administration (hereinafter: TSA) took over the processing and analysing of PNR data and proposed for profiling in an upgraded and expanded system of CAPPS II for all US flights.[60] Interestingly enough, several of the hijackers who committed the 9/11 attacks were selected by CAPPS.[61] This kind of usage of predictive tools that find certain patterns between what appear to be unrelated facts and establish correlation is called preventive security, and PNR is based on this exact logic.[62]

---

[57] Pejaković-Dipić, S., Karas, Ž., *Neki problemi kod prikupljanja i razmjene podataka o putnicima u zračnom prometu*, Visoka policijska škola, Zagreb (2018), p. 437.
[58] Lindsey, R., *Airports Start Thorough Screening of All Passengers*, The New York Times, January 6, 1973.
[59] Pejaković-Dipić, S., Karas, Ž., *supra* n. 57, p. 437.
[60] *Ibid.*, p. 437.
[61] The Aviation Security System and the 9/11 Attacks, Staff Statement No. 3, p. 6.
[62] Bigo, D., Salomon, S., *Passengers Name Records and Security*, Verfassungsblog on Matters Constitutional (2023), https://verfassungsblog.de/pnr-security/ (last accessed June 18, 2023).

The goal of the CAPPS II system was to cross-reference PNR data with numerous other government records and private entity databases, in particular, criminal records, phone call databases, credit card usage and other related information, so far as to subscription to certain magazines. The result of this software was the grouping of passengers into three groups depending on the calculated risk score: red, orange and green.

Passengers in high risk category (red) were banned from boarding the plane and with possible deferral to law enforcement, such as to questioning or arrest. The second category (orange or yellow) contained names of passengers of a possible threat which required thorough checks and additional screening. The third category (green) meant that the program did not find data that would make it necessary to consider the person a threat. Exact information on how the systems calculated this risk score was never released.[63]

After multiple recommendations from the US Government Accountability Office, the TSA finally cancelled the use of CAPPS II in the August of 2005, due to system deficiencies such as accuracy of data, abuse prevention, unauthorised access prevention and privacy concerns.[64] Such a decision is significant, taking into account that about 100 million US dollars had been spent on the development of this system up until then.

3.2. PNR agreements

To achieve its full purpose in the security and counter-terrorism strategy, it was necessary for PNR data to be shared between different states, making the conclusion of PNR agreements the next obvious step. Certain obstacles started presenting themselves in the conclusion of PNR agreements with the EU due to the high level of privacy protection guaranteed to individuals within EU legislation. In fact, during the negotiations for the conclusion of PNR agreements, information was leaked stating that each record includes almost sixty points of data relating to a certain passenger.[65] Such a substantial amount of information on passengers being collected and kept really puts into perspective the alleged interference into

[63] Pejaković-Dipić, S., Karas, Ž., *supra* n. 57, p. 437.
[64] US Government Accounting Office, Highlights of the Report to Congressional Committees, Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges, February 2004.
[65] Hailbronner, K., Papakonstantinou, V., Kau, M., *The Agreement on Passenger-Data Transfer (PNR) and the EU-US Cooperation in Data Communication*, International Migration Vol. 46 (2) (2008), p. 188.

the right to privacy, as well as the possible outcomes in the cases of data theft. Additionally, multiple experts, such Kaunert[66] and Bigo[67], expressed the opinion that, without the strong influence of the USA, EU would not have entered into PNR agreements or developed its own PNR system. While both the USA and the EU recognised the significant benefits of using PNR data as a security tool, it is unlikely that the EU would have entered into its first PNR agreement as early as 2004, considering the unpreparedness and incompatibility of its legislation with the requirements and obligations of a PNR agreement.

By now, the EU has signed agreements allowing the exchange of PNR with Canada (in 2006), the US (in 2004, 2007 and 2012) and Australia (in 2011).[68] [69] In the meantime, in 2010, the European Commission determined the elements of the EU's foreign policy concerning the PNR policy.[70] The announcement established a number of general criteria, such as data protection principles, that must be met when signing PNR agreements. These general criteria set the basis for the negotiations and conclusion of PNR agreements with Canada, the USA and Australia. The EU has since also undertaken negotiations on PNR data transmission with Mexico in 2015[71] and Japan in 2020[72].

This chapter will examine specific provisions of PNR agreements between the EU and Canada and the EU and USA, the motivations of the EU for entering into these agreements and following their eventual annulment and re-negotiation.

3.2.1. EU-Canada PNR Agreement

[66] Kaunert, C., Leonard, S., Mackenzie, A., *The social construction of an EU interest in counter-terrorism: US influence and internal struggles in the cases of PNR and SWIFT*, European security, 2012, Vol. 21, No. 4, p. 474-496.
[67] Bigo, D., Salomon, S., *supra* n. 62.
[68] Orrù, E., *The European PNR Directive as an instance of pre-emptive, risk-based algorithmic security and its implications for the regulatory framework*, Information Policy Vol. 27 (2022), p. 133.
[69] Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, L 186/4, Official Journal of the European Union, 14.7.2012.
[70] Pejaković-Dipić, S., Karas, Ž., *supra* n. 57, p. 451.
[71] Joint statement: Beginning of negotiations between Mexico and the European Union on PNR data transmission,14 July 2015, Joint_statement__Beginning_of_negotiations_between_Mexico_and_the_European_Union_on_PNR_data_transmission%20.pdf (last accessed June 18, 2023).
[72] EU-Japan PNR agreement: Council authorises opening of negotiations, 18 February 2020, https://www.consilium.europa.eu/en/press/press-releases/2020/02/18/eu-japan-pnr-agreement-council-authorises-opening-of-negotiations/(last accessed June 18, 2023).

The EU concluded an agreement on PNR transfer and use with Canada in 2006[73], which never entered into force.[74] The reason for its immediate annulment was the opinion given by the Court of Justice of the European Union (hereinafter: CJEU). Namely, in November 2013, the European Parliament sought the opinion on the compatibility of the PNR Agreement with the Charter of Fundamental Rights of the European Union (hereinafter: The Charter) from the CJEU.[75] Since it had recognised that the EU-Canada PNR agreement contained very serious intrusions into human rights protected by Article 7, concerning the respect for private and family life, and Article 8, concerning the protection of personal data of The Charter.[76] This doubt was confirmed by the European Data Protection Supervisor[77], because the EU regulating data protection does not permit the transferring of sensitive, personal data, to non-member countries if they do not guarantee a degree of protection of fundamental human rights essentially equivalent to the level guaranteed in the EU. This was confirmed in Max Schrems v. The Data Protection Commissioner in 2015.[78] However, this approach in data protection matters, also referred to as "gunboat diplomacy"[79] has been criticized as problematic, as it basically forces every other (non-EU) state to implement similar, if not the same, legislation as its own.[80] Nevertheless, this approach failed in negotiations with strong opponents such as Canada and the USA, in both cases resulting in agreements not in line with EU law.

In July 2017, the CJEU issued Opinion 1/15 regarding the PNR Agreement.[81] The Court stated that the Agreement was, in fact, not in conformity with Article 7, Article 8 and Article 52, para. 1 of the Charter,[82] because "the transfer and processing of PNR data, including

[73] Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data.
[74] Orrù, E., *supra* n. 68, p. 133.
[75] Pejaković-Dipić, S., Karas, Ž., *supra* n. 57, p. 452.
[76] *Ibid.*, p. 452.
[77] Opinion on the Proposal for a Council Decision on the conclusion of an agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information (API) / Passenger Name Record (PNR) data, OJ C 218, 6.9.2005, p. 6
[78] Maximillian Schrems v Data Protection Commissioner, Judgment of the Court (Grand Chamber) of 6 October 2015, Case C-362/14.
[79] Hailbronner, K., Papakonstantinou, V., Kau, M., *supra* n. 65, p. 194
[80] *Ibid.*, p. 194.
[81] Opinion 1/15 Of the Court of Justice of the European Union (Grand Chamber) on the Draft Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, 26 July 2017., Avis 1/15.
[82] *Ibid.*

information on identified individuals, would interfere with the fundamental rights to respect for private life the protection of personal data". [83]

While the Court believed that international exchange of personal information could be justified by the objective of common interest of the EU, namely to ensure public security and fighting terrorism and transnational crime, it nevertheless decided that multiple provisions of the agreement failed the test on necessity and proportionality, applied to intrusions into fundamental rights.[84] It stated that specific categories of PNR information were too sensitive to transfer and other categories that could be transferred were not defined specifically enough.[85] The CJEU further required Canada to conduct either a judicial or administrative review before using the PNR data for extended purposes and to „impose additional controls on onward disclosure to third countries, and identify an internal oversight authority with greater independence".[86, 87]

3.2.2. EU-US PNR Agreement

After the terrorist attack of 9/11, the US Bureau of Border and Customs Protection (hereinafter: CBP) started requiring access to PNR from international airlines, as obliged by the recently adopted US Aviation and Transportation Security Act.[88] Based on this, airline companies needed to submit passenger data to the US competent authorities prior or immediately after the airplane takes off. In the event of non-compliance with this requirement, the airlines could be fined as much as 5,000 US dollars per passenger whose information have not been suitably transmitted.[89]

For European airlines this meant the inability to fly to the US if they refused to abide by CBP, and if they did, they would likely break their domestic law, since the USA notoriously fails the aforementioned level of adequate data protection provided in the Schrems case. To resolve this

[83] Mendez, M., *Opinion 1/15: The Court of Justice Meets PNR Data (Again!)*, European Papers Vol. 2 (3) (2017), p. 808.
[84] *Ibid.*, p. 808.
[85] Opinion 1/15, *supra* n. 81, para. 24.
[86] *Ibid.*, para. 208, 215, 232.
[87] Propp, K., *Avoiding the Next Transatlantic Security Crisis: The Looming Clash over Passenger Name Record Data*, Atlantic Council (2021), p. 7.
[88] Hailbronner, K., Papakonstantinou, V., Kau, M., *supra* n. 65, p. 189.
[89] Guild, E., Brouwer, E., *The Political Life of Data: The ECJ Decision on the PNR Agreement between the EU and the US,* CEPS Policy Brief n. 109 (July 2006), p. 1.

issue, the European Commission started negotiations with the USA, which lasted for most of 2003, in order to establish an EU PNR policy and regulate the PNR matter for all Member States in the same manner.

a. The 2004 PNR Agreement

The first EU-USA PNR Agreement entered into force on May 28th, 2004.[90] Only a couple of months after, in July 2004, the European Parliament filed two actions before the CJEU claiming that the PNR agreement was *ultra vires*, that it relied on the wrong legal ground, and that fundamental rights had been infringed.[91] The European Data Protection Supervisor expressed his support of the Parliament in both actions.[92]

In its decision from 30 May 2006, the Court found that since the Agreement did not refer to commercial but to security matters, the legal basis of it could not be the EU Data Protection Directive (it being the only data protection law at the time).[93] Therefore, the first EU-US PNR Agreement needed to be annulled and re-negotiated. The Court further set a deadline for a new PNR Agreement to be entered by 30 September 2006. Negotiations for the second PNR Agreement started in July 2006.

b. The 2007 PNR Agreement

The second, 2007 PNR Agreement, was concluded allowing the processing and exchange of PNR data of passengers traveling on flights departing or landing in the USA, and does not substantially differ from the previous one. [94]

In practice, this meant that all carriers flying to, through or from the USA, upon request by DHS, must submit the PNR information. Before the plane's departure from the EU, DHS would collect PNR data by directly collecting the information from the air carriers' database or by requesting and receiving information from the air carrier.[95]

There is a basic principle of reciprocity in international law, in accordance with which the EU had the right to demand the same data from US airlines flying to Europe. However, since a comparable counter-terrorism system did not exist in the EU at the time, there was no ground

[90] Hailbronner, K., Papakonstantinou, V., Kau, M., *supra* n. 65, p. 189.
[91] *Ibid.*, p. 190.
[92] *Ibid.*, p. 190.
[93] *Ibid.*, p. 191.
[94] Tanaka, H., Belanova, R., Ginsburg S., De Hart, P., *Transantlantic Policy Sharing: At a Crossroads, Migration Policy Institute* (January 2021), p. 16.
[95] *Ibid.*, p. 16.

for EU to demand the same obligation from the USA. To compare, at the time when the USA was adopting a regulation requiring all air carriers flying to, from or through the USA to report information on passengers aboard those flights to American authorities before departure (US Aviation and Transportation Security Act), regulation was in force in the EU forbidding such data exchanges.[96] Only in 2004 did the EU adopt a much milder version of the passenger data exchange system, the API Directive[97], according to which carriers are obliged to deliver passenger information to competent authorities of Member States. However, this agreement pertained exclusively to biographical and travel data, which was deleted 24 hours after the/their receipt. In contrast, DHS required passenger data from as many as 19 categories, keeping it for 15 years from the moment of collection.[98] It was agreed that in the event of the EU or one of the Member States adopting the PNR system, DHS will promote the actively cooperation of the air carriers.

A big problem arose concerning the right of DHS to dispose of data by making it available to other US protection agencies. The matter of reciprocity was an obstacle on the US side as well. Namely, while the US required data on passengers arriving to the US, there was no requirement of registration for citizens or residents like most EU countries.[99] Meaning, this more liberal approach toward regulating personal records was in opposition to the equal reciprocity of data exchange.

c. The 2012 PNR Agreement

After the Lisbon Treaty entered into force in 2009, PNR Agreements required the approval of the European Parliament and needed to include a specific provision on the protection of personal data.[100] This was reasonable considering that the previous PNR agreement was annulled for, among other reasons, not providing EU citizens with adequate data protection. Instead of giving its approval, the European Parliament requested from the Commission to renegotiate the agreement concerning data protection. The new and final agreement was adopted on 13 December 2011.[101] Despite the improved negotiating position of the EU, the

[96] Radionov, N., Marin, J. (ur.), Europsko prometno pravo, Zračni promet, Pravni fakultet Sveučilišta u Zagrebu (2011), p. 190.
[97] Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, Official Journal of the European Union, L 261/24.
[98] Radionov, N., Marin, J., *supra* n. 96, p. 190.
[99] Hailbronner, K., Papakonstantinou, V., Kau, M., *supra* n. 65, p. 196.
[100] Tanaka, H., Belanova, R., Ginsburg S., De Hart, P., *supra* n. 94, p. 6.
[101] Agreement between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security, 2012 O.J. L 215.

emphasis on EU interests, and the oversight by the European Parliament, a lot of the doubts from the previous agreement remained.

Concerning the previously addressed issue of the inconsistency of the Agreement with fundamental rights, particularly the right to privacy and data protection, the Preamble of the Agreement now recognises the need to adhere to principles of necessity and proportionality in the application and analysis of PNR data. This request, while expected and seemingly logical, can be considered futile in the context of PNR, since the system analyses everyone's data regardless of whether or not they are suspected in a criminal investigation. Therefore, necessity as well as proportionality of implementing the PNR system are already presumed in order for it to fulfil its counter-terrorism purpose. Furthermore, data security is expressly regulated in Article 5 of the Agreement, making it an obligation of DHS to ensure appropriate technical means to protect PNR data "against accidental, unlawful or unauthorised destruction, loss, disclosure, alteration, access, processing or use."

The already extensive purposes for the application of PNR data prescribed in the previous agreements were once again broadened in the latest agreement. Namely, Article 4 in paragraph 1 lists conduct that would be considered a terrorist offense or a related crime, as well se other transnational crimes „punishable by a sentence of imprisonment of three or more years".[102] The following two paragraphs name other reasons for which the use of PNR data is permitted, such as "on a case-by-case basis where necessary in view of a serious threat and for the protection of vital interests of any individual or if ordered by a court."[103] As there are no definite requirements prescribed, this would allow the application of PNR on any objective ordered by a court. [104] Allowing personal information provided by people for a very specific purpose, as is buying a plane ticket, to be analysed and further exchanged by government authorities in such a wide variety of situations could still arguably be infringing on the right to privacy - but the Agreement remains in force.

A controversial provision of the EU-US Agreement is Article 16 which concerns domestic sharing of PNR data by the DHS, linked to the purposes named in Article 4.[105] Therefore, since

[102] *Ibid.*, Article 4, paragraph 1 (b).
[103] *Ibid.*, Article 4, paragraph 2.
[104] Hornung, G., Boehm, F., *Comparative Study on the 2011 draft Agreement between the Unites States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security*, Greens/EFA Group in the European Parliament (March 2012), p. 9.
[105] The PNR Agreement, Article 16, paragraph 1 (a).

Article 4 is drafted so broadly, the same can be said about the situations in which domestic sharing is allowed. Another issue is that of the absence of indication of the authorities authorised to receive PNR data. This would mean that DHS is permitted to share the relevant passenger information with other US competent authorities, who are not specified in the agreement, in an extensive amount of cases, once again putting into question the right to privacy of passengers who are not aware that their information is being exchanged and to whom. Therefore, as the amount of cases in which DHS is allowed to require PNR data from air carriers and share it with other, not-specified, competent authorities are pretty broad, DHS should be able to justify each occasion of information exchange if necessary. Finally, while the Agreement permits domestic sharing of information for DHS, there is no provision expressing the same concession to EU competent authorities.

Regarding the method of transfer of PNR data, the Agreement, in Article 15, now requires the application of the "push" method[106], but allows exceptional use of the „pull" method "to respond to a specific, urgent, and serious threat".[107] Since the agreement does not further define "an urgent and serious threat", the decision is likely on DHS to determine the appropriate situation and access the relevant database.

Another heavily criticised provision was Article 8, prescribing the data retention period, mainly because of its extension in comparison to the previous agreements as well as it's proportionality to the purpose.[108] According to the current Agreement, the PNR data is retained "in an active database for up to five years." However, „after the initial six months of this period, PNR shall be depersonalised and masked".[109] Depersonalisation is achieved through hiding identifiable information such as names, contact information and API information.[110] Whether this measure is enough to erase all concerns regarding the longer period of data retention is yet to be determined. In the context of data theft, it remains possible to steal and use the information despite it being depersonalised. For example, credit card information is not listed in the Agreement as information that will be masked after the six-month period, but can be considered a significant piece of information to be targeted in a cyberattack and that passengers would

[106] The PNR Agreement, Article 15, paragraph 1.
[107] The PNR Agreement, Article 15, paragraph 5.
[108] In the first EU-US PNR Agreement, the data retention period was 3.5 years, while in the second it was already extended to 7 years, in comparison with other PNR agreements, in which the periods are much shorter. Namely, in the Agreement with Canada, 3,5 years and with Australia 5,5 years. (Hornung, G., Boehm, F., *supra* n. 104, p. 7.)
[109] The PNR Agreement, Article 8, paragraph 1.
[110] The PNR Agreement, Article 8, paragraph 2.

want to be deleted or more protected. After the five-year period, data is "transferred to a dormant database for a period of up to ten years".[111] This data can only be repersonalised "in connection with law enforcement operations and then only in connection with an identifiable case, threat or risk."[112]

Data subject's rights

Of particular significance are the provisions concerning data subject's rights. The US agreed to handle PNR data in compliance with the EU rules on privacy and protection of data. In particular, individuals now have the rights to access to their PNR data, to correction and rectification of erroneous data, and the right to judicial redress. According to Article 11 "any individual, regardless of nationality, country of origin, or place of residence is entitled to request his or her PNR from DHS". The Article points individuals to the Freedom of Information Act (hereinafter: FOIA), which guarantees this right. However, paragraph 2 expresses that the disclosure of the requested information can be restricted to "safeguard privacy-protected, national security, and law enforcement sensitive information."[113] These limitations could possibly be overused and hinder individuals in accessing their information, but as there is not yet extensive public practice on the exercise of this right, it is to be seen whether the authorities will provide the requested information or which basis for rejection will be used.

Concerning the individual's right to access, the first US instance involving a PNR request made by a citizen is the Hasbrouck v. U.S. CBP.[114] Hasbrouck made multiple requests to access information on his personal data, collected by the CBP, between 2007 and 2009. The basis for the requests was the FOIA and the Privacy act, but Hasbrouck only received the incomplete information three years later after filing appeals. The CBP was unable to provide the information on data transfer to other authorities due to PNR being exempted from the Privacy Act.[115] This decision contradicts EU law on data protection, according to which, individuals have the right to request and access information about the further transfer of their personal data.[116] Moreover, this case puts into question the practical enforceability of both the right to access, as well as the rights to correction and redress. The fact that a US citizen was only able

[111] The PNR Agreement, Article 8, paragraph 3.
[112] The PNR Agreement, Article 8, paragraph 3.
[113] The PNR Agreement, Article 11, paragraph 2.
[114] Case No.: C 10-03793 RS, Edward Hasbrouck, Plaintiff, v. U.S. Customs and Border Protection, Defendant (September 21, 2011).
[115] Hornung, G., Boehm, F., *supra* n. 104, p. 17.
[116] GDPR, Article 67.

to receive limited information, and only after a three-year delay, makes it seem unlikely that EU citizens will not face similar or worse difficulties in enforcing their rights.

Article 12 stipulates that any individual "may seek correction or rectification including the possibility of erasure or blocking, of his or her PNR by DHS". The Article does not elaborate on the legal basis for this request, nor does it provide the obligation to correct the incorrect data. DHS is only required to make a decision and inform the individual on it, so the exercise of this right seems more formalistic.

Possibly the most important right for individuals is the right to judicial and administrative redress in case "personal information has been processed and used in a manner inconsistent with this Agreement".[117]

Finally, US and EU governments published the joint evaluation of compliance with the agreement in January of 2021.[118] The review is overwhelmingly positive, highlighting operational effectiveness and the critical role PNR databases have had in the fight against terrorism. However, the EU team noted that several aspects of the PNR Agreement are not completely in line with Opinion 1/15, which does not surprise as the EU-US Agreement was concluded before the CJEU issued the Opinion. Some of the inconsistencies include the retention period of PNR data, the sensitive data processing, the requirement of a prior independent review of the use of PNR data, domestic sharing rules, oversight and the sole use of PNR to terrorism and serious transnational crime.[119]

4. THE APPLICATION OF PNR AGREEMENTS

This chapter will first elaborate on the implementation and provisions of the PNR Directive and the decision of the CJEU on the validity of the Directive. The goal of this chapter is to examine some of the benefits of the utilisation of PNR data as a security tool and to try to determine if they outweigh the issues of human rights infringement, discrimination and possible data theft.

[117] *Ibid.*, Article 13.
[118] Report from the Commission to the European Parliament and the Council on the joint evaluation of the Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, Brussels, 12.1.2021.
[119] *Ibid.*, p. 4.

4.1. The PNR Directive

As previously mentioned, when describing the lack of legal ground for the 2004 EU-US PNR Agreement, there was no appropriate legislation in the EU that would allow transferring and processing of data to third countries. The only relevant regulation was the API Directive[120], however, according to it, air carriers were only obliged to hand over the passenger information if requested by the border control authorities.[121] Therefore, there was no systematic obligation for Member States to submit passenger data. This is explained by the main goal of the API Directive being control of borders and prevention of illegal migration. This absence of legal framework was finally addressed, when in April of 2016, the European Parliament and Council adopted Directive 2016/681 on the use of data from passenger data records (PNR) for the prevention, detection, investigation and prosecution of terrorist offenses and serious crimes.[122]

The terrorist attacks in Paris in November 2015 and Brussels in 2016 urged European law makers to immediately create a counter-terrorism policy in the EU, resulting in the PNR Directive being voted so soon in the aftermath of these events. However, the EU counter-terrorism legislation faced certain challenges, namely, the freedom of movement of EU citizens and the EU democratic rule of law. Currently, as of June 2023, Denmark is the only Member State that has not transposed the Directive.[123]

The PNR Directive prescribes that "*the processing of these data is limited to the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime*"[124]. While the collecting of PNR data and its processing is only obligatory for flights departing from or landing in third countries (extra-EU flights), in Article 2, Member States were given the option of applying it to intra-EU flights. Almost every Member State that has implemented the Directive has applied this option.[125]

In accordance with the Directive, EU Member States must require air carriers who are operating flights outside the EU, to transmit the collected PNR data to a Passenger Information Unit

[120] Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, Official Journal of the European Union, L 261, p. 24.
[121] API Directive, Article 3, paragraph 1.
[122] Directive (EU) 2016/681 of the European Parliament and the Council on the use of PNR data of air passengers of flights operated between the European Union and third countries (27 April 2016). OJ (2016) L119, p. 132-149.
[123] Orrù, E., *supra* n. 68, p. 134.
[124] PNR Directive, Article 1.
[125] Orrù, E., *supra* n. 68, p. 134., (EU Commission, 2020a, p. 10).

(hereinafter: PIU) of the Member State from the territory of which the flight is departing or in which it is landing. Article 4 of the Directive establishes the obligation that each Member State creates its own PIU, which is the authority in charge of receiving PNR data from airlines, and further storing, processing and transferring this data. PIUs can also transfer the results of their processing to competent authorities and exchange the data with departments of other Member States for the purposes of "preventing, detecting, investigating or prosecuting terrorist offences or serious crime."[126] Each Member State is required to adopt a list of authorities who are entitled to request and receive PNR data and the processing results from the PIU.

National PIUs are responsible for assessing the transmitted information against European, but also international databases, for example, the Schengen Information System (SIS).[127] The PIUs themselves establish certain risk criteria, based on which they analyse the received data in order to determine potentially dangerous persons before their planned arrival in, or departure from, a Member State. Passengers identified as high-risk are selected, in accordance with national law, for further examination after an individual, non-automatic confirmation of their data processing results. [128]

According to Article 10 of the Directive, another agency allowed to request and receive the PNR data by the PIU, as well as the results of its processing is Europol, "within the limits of its competences and for the performance of its tasks".[129] To understand what those competences and tasks are, it is important to note that Europol is law enforcement agency in the EU, founded in 1998. It assists Member States national law enforcement in the areas of its competency, of particular importance for this subject, in cybercrime.[130] Interestingly, Europol was the first European agency to conclude an agreement concerning law enforcement and promoting cooperation and data exchange with the US in 2001.[131]

To guarantee effective data protection, the state should arrange independent monitoring of the data processing by a supervisory authority in addition to the data protection officer. To ensure this, "every PIU needs to appoint a data protection officer."[132] Furthermore, Article 13 prescribes that "every passenger shall have the same right to protection of their personal data,

[126] The PNR Directive, Article 7, paragraph 4.
[127] Pejaković-Dipić, S., Karas, Ž., *supra* n. 57, p. 446.
[128] The PNR Directive, Article 6, paragraph 5.
[129] The PNR Directive, Article 10.
[130]Bergamasco F., Cassar R., Popova R., Scott B. I., *supra* n. 1, p. 97.
[131] Agreement between the USA and The European Police Office signed on 6 December 2001.
[132] The PNR Directive, Article 5.

rights of access, rectification, erasure and restriction and rights to compensation and judicial redress." This Article also prescribes the obligation of Member States to ensure that in the case of a data breach, likely to cause the endangerment of an individual's personal data, the PIU is required to notify this individual without undue delay. The mentioning of the possibility of a data breach targeting this particular information, as well as the obligation to notify the individuals to whom the data is related is of particular significance in the context of cyberattacks, as there are recent examples of passenger information being stolen in a cyberattack and the airline not notifying the passengers until months after the event (see more *infra* in Chapter 4.3.3.). Therefore, this is a very positive development in the regulation of PNR data collection and recognises the direct responsibility of the air carrier to both protect sensitive data and in the case of a cyberattack make sure the passengers are aware and able to take appropriate measures, such as change their passwords or possibly seek judicial redress.

The Directive establishes two methods of data transfer: firstly, the "*pull*" method by which authorities are able to access the airline's PNR system and extract a copy of the requested data; and secondly, the "*push*" method by which air carriers themselves transfer the requested data from their PNR system to the authority that requires them, meaning that air carriers retain control over the transferred data.[133] Article 8 of the Directive states that airlines transfer data from the PNR using the method of entry into the database of the PIU, not mentioning the push-pull method. Since both possible methods of data transfer are listed in the Preamble, it remains unclear whether this provision should be understood as mandatory or optional, or whether it is the intention of the European legislator that in the future all data transfers are performed exclusively by the input method. Since the "*push*" method is better to ensure data protection, it should be obligatory.

The PNR data retention period should be restricted to the time strictly necessary for the analysis and use in investigations. Following that, the data is depersonalised. Therefore, in Article 12, the period of retention of data is limited to five years, after which it must be permanently deleted, notwithstanding cases where the data has been transferred to a competent authority for use in investigations. Paragraph 2 further prescribes, similarly to the EU-US PNR Agreement, that 6 months after the data transfer, all data has to be depersonalised through masking of the enumerated elements which could be used to identify the particular passenger (e.g. names, addresses and contact information, data on payment methods and loyalty programs, general

[133] Pejaković-Dipić, S., Karas, Ž., *supra* n. 57, p. 449.

notes and all collected API data). Re-access to full PNR data, after the 6-month period, is permitted under strict and limited conditions. Regardless of the prescribed deadlines, if certain data are transferred to a domestic competent authority for the use in criminal investigations or prosecutions, their retention is governed by national law.

After entry and application of the Directive, Member States were supposed to provide the European Commission with yearly statistics.[134] This statistical information was examined by the European Commission and used to create a review report about the application and efficiency of the PNR Directive, as is prescribed in Article 19. In this report, the Commission confirms that PNR data is only a piece of evidence, like any other, and as such should not be isolated or specifically credited with the results of an investigation.[135]

4.1.1. Comparison of the EU-US PNR agreement and the PNR Directive

Since the PNR Directive was created and entered into force years after the 2012 EU-US PNR agreement, it was able to better address some of the inadequacies, including data protection, wide purposes for the PNR data analysis and a long retention period. Looking into some of the differences between the latest EU-US PNR agreement and the PNR Directive will help determine which act provides more appropriate data protection safeguards.

Firstly, the two documents provide different external oversight. While Article 5 of the PNR Directive prescribes that the bodies responsible for the monitoring of data processing will be the national data protection officers, the oversight according to the Agreement is under exclusive control of the US bodies. Secondly, according to the PNR Directive, air carriers transfer the data to national PIUs, who process the data, whereas an equivalent body does not exist in the Agreement. Namely, DHS and CBP are the so-called competent authorities in charge of processing PNR data, which can then be exchanged with other domestic agencies. Finally, the PNR Directive requires the data to be encrypted as soon as it is collected, as well as prescribes the implementation of the "push" method, which is, as previously established, better for data protection. The data is only encrypted when stored in the database, according to the Agreement.[136]

[134] The PNR Directive, Article 19, paragraph 1.
[135] Report from the Commission to the European Parliament and the Council On the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (2020), p. 9–10.
[136] Blasi Casagran, C., *The Future EU PNR System: Will Passenger Data be Protected?*, European Journal of crime, criminal law and criminal justice Vol. 23 (2015) 241-257, p. 249.

In conclusion, the PNR Directive provides overall better data protection than the latest PNR agreement, which makes sense considering it was made independently of outside sources and influences, and prioritising EU law. Despite the existing differences between the PNR agreement and the Directive, there is, as of August of 2023, no suggestion of re-negotiation of the Agreement. Due to the legal nature of directives, as acts that only requires Member States to achieve certain goals, agreements concluded between EU and third countries take priority. Meaning in this case, that for any PNR data transfer from any EU country to the USA, the 2012 EU-US PNR agreement would be the primary source of law. Furthermore, the PNR Directive regulates the transfer of PNR data from air carriers to national competent authorities, meaning the two documents can coexist despite the aforementioned differences since their scopes differ.

4.1.2. The CJEU Decision

In July 2017, a Belgian non-profit organisation *Ligue des droits humains*, filed an action for annulment with the Belgian Constitutional Court, against a national law from December 2016 which transposed into domestic law, among others, the PNR Directive.[137] During these proceedings, in October 2019, the Belgian Court requested a preliminary ruling by the CJEU, questioning the validity of the PNR Directive and its compatibility with Article 7, Article 8, Article 21 and Article 52 paragraph 1 of the Charter. The CJEU rendered its judgment on 21 June 2022.[138]

In its judgement, the CJEU concluded that "the interpretation of Directive 2016/681 in the light of Articles 7, 8 and 21 as well as Article 52(1) of the Charter of Fundamental Rights of the European Union ensures that that directive is consistent with those articles of the Charter of Fundamental Rights, the examination of Questions 2 to 4 and Question 6 referred for a preliminary ruling has revealed nothing capable of affecting the validity of the said directive."[139]

When contemplating the PNR Directive's validity, the CJEU further explained that "an EU act must be interpreted, as far as possible, in such a way as not to affect its validity and in

[137] *Ibid.*, p. 1.
[138] Press Release No 105/22 Luxembourg, 21 June 2022, Judgment of the Court in Case C-817/19 | Ligue des droits humains, p. 1.
[139] Judgement of the Court of Justice of the European on the Validity of the Union Directive (EU) 2016/681 – Use of PNR data of air passengers of flights operated between the European Union and third countries, Case C-817/19 (21 June 2022), Ruling, point 2.

conformity with primary law as a whole and, in particular, with the provisions of the Charter"[140].

While the CJEU confirmed the notion of the *Ligue des droits humains*, that the PNR Directive does in fact interfere with the fundamental rights guaranteed in Article 7 and Article 8 of the Charter,[141] it noted that the Directive's objective „to ensure the internal security of the EU and to combat terrorist offences and serious crime" are able to justify the breaches into the rights in question.[142] The Court further acknowledged that the debated rights are protected in the Directive, by the provisions defining "the exercise of those rights, the purposes for processing PNR data and rules governing those processing operations."[143]

The application of the system established by the PNR Directive must be limited to terrorism and serious crime that has an objective link with the air travel of passengers. The reasoning for this was that "although […] the objective of combating serious crime is capable of justifying the serious interference with Articles 7 and 8 CFR, the same is not true of the objective of combating criminality in general."[144] Such reasoning raises the question of whether the wide purposes for PNR data exchange and analysis in the EU-US PNR agreement are in line with the expressed limitation and if they will need to be later addressed. The CJEU obliges Member States to ensure that national transposition of the PNR Directive is strictly limited to the purposes of combatting terrorism and serious crime.[145] Meaning that PNR data may not be processed for purposes not expressly mentioned in the Directive, such as, to combat ordinary crime or used by intelligence and security services for monitoring purposes.

Finally, the CJEU severely decreased the scope of Article 2 of the Directive, which enables Member States to extend the PNR regime to intra-EU flights. Firstly, the Court states "that the possible extension of the application of the PNR Directive to selected or all intra-EU flights, should be limited to what is strictly necessary and must be open to effective review, either by a court or by an independent administrative body whose decision is binding." Secondly, it can only be extended to all intra-EU flights indiscriminately in exceptional situations of "a terrorist threat which is shown to be genuine and present or foreseeable". [146] This decision will have

[140] *Ibid.*, para. 86.
[141] *Ibid.*, para. 94-97.
[142] *Ibid.*, para. 121-122
[143] *Ibid.*, para. 119
[144] *Ibid.*, para 148.
[145] *Ibid.*, para. 157.
[146] *Ibid.*, para. 171.

interesting effects considering the aforementioned fact that almost every Member State that transposed the Directive, applied the extended scope and will now have to cease this practice. However, this decision certainly confirms the intention of protection of the right to privacy of EU citizens.

4.2. Effectives in crime prevention

The previously discussed issues surrounding PNR agreements and their compliance with both existing human right legislation and the Directive created to enable their use in the EU would probably be considered too much of an obstacle if PNR data was not proven to be beneficial in crime prevention. Even though there is no publicly accessible systematic information on the success of PNR data in the prevention of terrorist offenses and organised crime, DHS and governments have disclosed a couple of instances in which both PNR databases and agreements have helped in crime prevention by providing necessary information on suspects and evidence in investigations.

One of such cases was of Faisal Shahzad, who attempted to set off a bomb in a car in Times Square in 2010.[147] To avoid revealing his identity, he purchased a car in cash and did not register it. However, his identity was exposed to the authorities because the phone number he gave to the seller ended up being a match to a number found in a PNR database from a flight he had taken years earlier.[148] Managing to escape FBI surveillance, after the attempted bombing, Shahzad booked a flight to the UAE from the John F. Kennedy Airport. After the PNR data was transferred to DHS, it immediately set off an alarm and he was removed from the plane.[149]

Another case was that of David Headley, who was planning a terrorist attack in Europe.[150] A security service that only had his name and general travel information, notified CBP, who then managed to give the FBI his full information that led to Headley's arrest in only a couple of hours.[151] Following the arrest, it was discovered that he was involved in the Mumbai terrorist

[147] Faisal Shahzad Indicted for Attempted Car Bombing in Times Square, US Department of Justice, Office of Public Affairs, June 17, 2010. https://www.justice.gov/opa/pr/faisal-shahzad-indicted-attempted-car-bombing-times-square (last accessed 31 August 2023).
[148] Propp, K., *supra* n. 87, p. 2.
[149] *Ibid.*, p. 2.
[150] *Ibid.*, p. 2.
[151] *Ibid.*, p. 2.

attack, in November 2008, killing 166 people and was planning another attack in Europe. He was finally sentenced to 35 years in prison for his crimes.[152]

The third case in which PNR data was used to arrest potential attackers was of Najibullah Zazi, who planned to set off bombs in the subway in New York, in 2009. [153] CBP records showed that, in 2008, Zazi and several of his associates flew from Newark to Peshawar, Pakistan, where they received training from al-Qaeda. PNR data was used to connect Zazi and his associates Adis Medunjanin and Zarein Ahmedzay. Finally, all of them were arrested in 2009. [154]

All of these situations prove that PNR data is invaluable to law enforcement operations, because of both the significant amount of information it contains and the ability to exchange information between multiple states and government agencies. This makes it particularly effective in contributing the necessary data in a timely manner, which is essential in high-risk events such as terrorist attacks.

While counter-terrorism is the main purpose for the application of the PNR system, it's effectiveness has also been demonstrated in border control. Another example of successful PNR application was the so called Project Semaphore implemented in the UK, that compares PNR and API information against government records in order to assist law enforcement as well as for border control purposes. The statistical data on the success of this project stated that "since 2005 made 4,650 arrests for murder, rape and assault, sexual offenses, kidnap, and document fraud, and has seized false documents, tobacco, and drugs."[155]

In conclusion, the fact that PNR data has been confirmed to be an extremely effective tool in both identifying potential attackers and preventing terrorist attacks, makes it easy to understand why governments are willing to go to such extents and renegotiate PNR agreements in order to enable its sharing. After discussing the examples of successful application of PNR data in law enforcement investigations and its effectiveness in counter-terrorism, it is important

---

[152] US Department of Justice, "David Coleman Headley Sentenced to 35 Years in Prison for Role in India and Denmark Terror Plots," Press release, January 24, 2013. https://www.justice.gov/opa/pr/david-coleman-headley-sentenced-35-years-prison-role-india-and-denmark-terror-plots (last accessed 19 June 2023).
[153] Propp, K., *supra* n. 87, p. 3.
[154] *Ibid.*, p. 3.
[155] House of Lords European Union Committee, The Passenger Name Record (PNR) Framework Decision: Report with Evidence, 15th Report of Session 2007-08 (London, United Kingdom: The Stationary Office Limited, 2008), http://www.statewatch.org/news/2008/jun/eu-pnr-uk-hol-report.pdf. (last accessed 19 June 2023).

to note a number of issues that appeared with this practical use of PNR, to understand why it remains a topic of debate.

4.3. Issues with the collection and analysis of PNR data

While the matter of compatibility of analysis of PNR data with the fundamental right to privacy - guaranteed in numerous international human rights documents and EU legislation - has been previously discussed as one of the grounds for the annulment of the first EU-US PNR agreement, specific cases confirm that this issue has significant consequences for individuals. This issue, as well as the issue of discrimination of passengers, due to the automatic processing of PNR data, have both been recognised ever since the conclusion of the first PNR agreement between the US and EU in 2004. Possible solutions have been offered for their regulation in relevant Court decisions and resulted in the amendments and renegotiations of these agreements. However, a more recent danger of an increasing number of cyberattacks, targeting specifically airlines with the goal of obtaining passenger information, particularly credit card and travel document information for ransom, needs to be further examined and addressed. This is of particular importance in the context of PNR data, as passengers when making a flight reservation or booking a ticket, do not have the option of requesting their information to be immediately deleted, as is now common in other online service areas.

4.3.1. Discrimination

One of the problems that occurred in the analysis of PNR data, due to both the nature of this information and its utilization for profiling of potential criminals, is discrimination. As explained earlier, the way PNR systems function is that they cross-reference PNR data with other relevant databases in order to generate a risk-assessment of a passenger based on the existing information. This automated response takes certain predetermined characteristics of a person and determines their similarity with the characteristics or behavioural patterns of previous criminals. Numerous situations since the very beginning of PNR use have shown that being a certain race, or of a particular ethnic origin, is more likely to make one passenger automatically selected as a possible security threat. Since this could result in the restriction of the individual's right to travel, based on a discriminatory characteristic, it can undoubtedly be considered discrimination. This resulted in discrimination soon being recognised and then

addressed by the creators of the PNR Directive (which highlights the principle of non-discrimination in multiple provisions).

Namely, Article 6 paragraph 4 of PNR Directive prescribes that any evaluation of passengers "shall be carried out in a non-discriminatory manner." The criteria applied in the assessment must be direct, proportional and determined and must not in any case be based on the race, ethnicity, political opinions or religion of a person. Every positive automated match must be individually verified to decide if is necessary to take further measures. Paragraph 6 of Article 7 again prohibits any kind of discrimination, stating that "competent authorities may not make any decision that would produce an adverse legal effect on a person... such decisions may not be based on a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, state of health, sex life or sexual orientation". This is even further expanded by Article 13, according to which "Member States prohibit the processing of data from PNR that reveal a person's race or ethnic origin, his political views, religion or philosophical beliefs, trade union membership, state of health or sex life or sexual orientation". While these provisions provide a solid basis both for individuals working in PIUs and analysing PNR data and passengers for any future complaints, they seem more theoretical than practical – except for the rule to manually check the automatic risk assessment. This issue being addressed and regulated in multiple provisions in the PNR Directive, despite the principle of non-discrimination being a general rule of international law and already contained in numerous human rights conventions, shows that the European law-makers were aware of the serious consequences and damage individuals could suffer from being wrongfully identified as a possible threat.

The severity of consequences of transmitting incorrect PNR data can best be illustrated by the case of Canadian-Syrian citizen Maher Arar. Mahrer Arar was suspected of involvement in the terrorist attacks in September 2002, and for this reason, detained in New York.[156] From there, he was returned to Syria where he was imprisoned and tortured for over a year. After his return to Canada in October 2003, a federal investigation was finally conducted. The results of this investigation were released 3 years later, in September 2006, and cleared Mahrer of any suspicion of is involvement in the attacks. The wrongful basis on which Mahrer was suspected was determined to be the fact that there were serious deficiencies in the transmission of the correct information from the Canadian to the USA authorities.[157] On January 26, 2007, the

[156] Pejaković-Dipić, S., Karas, Ž., *supra* n. 57, p. 441.
[157] *Ibid.*, p. 441.

Canadian Prime Minister offered an official apology and 10.5 million dollars in compensation.[158]

The Directive does not go into detail on how exactly the relevant data will be analysed and which specific characteristics the system takes into consideration during the pre-screening, therefore it is hard to say whether the aforementioned case is just an exception or is bound to reoccur. The measure of individuals manually checking the positive generated automatic assessments of passengers should be enough if applied diligently and carefully by the responsible authorities. However, if mistakes do happen, the right to judicial and administrative redress guaranteed in both the Agreement and the Directive should be effective in ensuring rightful compensation.

4.3.2. The right to privacy

The right to privacy has already been mentioned in addressing the Opinion 1/15 and the CJEU decision C-817/19 (see *supra*, Chapter 4.1.2.). Both of these decisions have expressed that while certain interferences into human rights can be justified to ensure public safety, these interferences need to be necessary and proportional to the objective, as is prescribed in Article 52 the Charter.

The collection of numerous data points, not at all related to air traffic, as an activity that can have a large impact on the citizens' rights, has been debated ever since the introduction of PNR in the American system. The extent of the information included in this database, that does not exist in any other area of social activity or industry, makes PNR both an advantageous, but also possibly harmful tool. One of the objections has been that the system does not distinguish between suspects and innocents, collecting information on everyone.[159] That kind of approach to security regulation was common in the early stages of counter-terrorism in the US and was justified by the so called 1% doctrine that dictates "if it was necessary to surveil and detain 99 innocent persons in order to identify one terrorist, the measures were considered justified."[160] This means that every passenger is placed under monitoring, despite not being suspected in an

[158] *Ibid.*, p. 441.
[159] Vavoula, N., *I Travel, therefore I Am a Suspect: an overview of the EU PNR Directive*, Queen Mary University of London, https://eumigrationlawblog.eu/i-travel-therefore-i-am-a-suspect-an-overview-of-the-eu-pnr-directive/?print=print (last accessed August 16, 2023).
[160] Bigo, D., Salomon, S., *supra* n. 62.

active investigation. The analysis of PNR data does not differentiate between certain potential risk passengers and others, but rather considers everyone a possible security risk until their information confirms or rebuts this presumption. This approach can be justified in the event of temporary assessments in immediate high risk situations, but is questionable when there is no knowledge of present and foreseeable threat.[161]

Since the analytical processing of PNR can result in the restriction of freedom of movement or the right to travel, this raises the question of justification for these restrictions, as well as the choice of the body that makes such a decision. The legal means a person can use if they consider that there are grounds for contestation also need to be defined. Limitations and infringements of human rights can normally only be decided by a judicial body after a judicial procedure and not by individual airport security authorities.

The main right endangered by the processing of PNR information for security purposes is the freedom of movement. The "right to travel" was recognised by the US Federal Supreme Court in the case Sáenz v. Roe, 526 U.S. 489 (1999) as a fundamental human right, despite it not being specifically declared as such in constitutional sources.[162] It consists of the right to enter another country and to not be considered undesirable, both of which would be denied in the case of someone being identified as a threat by PNR analysis. While this system serves its security purpose in many cases, it is not infallible, proven by the fact that multiple times innocent passengers have been restricted in their right to travel and put by the US government on the so called "No Fly Lists", just because of the faulty functioning of the system and the agents in charge of manual checks.

The crucial court decision Gordon v. FBI, 388 F. Supp. 2d 1028 (N.D. Cal. 2005) established for the first time that public authorities must disclose the No Fly Lists to citizens.[163] The dismissal of human rights is made apparent in the case of Malaysian architecture professor Rahinah Ibrahim, who was a guest at Stanford University in California. She was, for no reason, placed on the List of prohibited travelers on her way back to Malaysia. The court proceedings established that this was a result of a mistake made by an agent who carelessly filled out a form.[164] This case once again confirms that even though the automatically generated risk

[161] Pejaković-Dipić, S., Karas, Ž., *supra* n. 57, p. 442.
[162] *Ibid.*, p. 442.
[163] *Ibid.*, p. 443.
[164] Rahinah Ibrahim v. U.S. Dept. Of Homeland Security, No. 14-16161 9th Cir. 2017.

assessments can be a great asset, it absolutely needs to be carefully verified by PIU agents, especially taking into account the possible consequences of errors.

4.3.3. Cyberattacks

Finally, while the characteristics and regulatory framework of cyberattacks have previously been elaborated (see *supra* Chapter 1), statistical information and examples of cyberattacks might better demonstrate just how significant the issue has become. The main objective of cyberattacks targeting the aviation industry to gain access to passenger data is for ransom purposes or other types of financial gain.

In July 2021, Eurocontrol published a report titled "Airlines under attack: Faced with a rising tide of cybercrime, is our industry resilient enough to cope?" using the data collected by EATM-CERT (European Air Traffic Management Computer Emergency Response Team), the agency's service.[165] This data revealed that the number of cyberattacks is growing, "with a 530% yearly rise from 2019 to 2020 in reported incidents across the aviation industry"[166], and "airlines being targeted in 61% of all 2020 aviation cyber-attacks"[167]. The report also indicates that "aviation experiences a ransomware attack every week"[168] (a type of cyberattack in which a hacker acquires control over a computer system and withholds it until the victim pays a ransom). These attacks often have serious financial impacts, because of the cost of buying back of data, or the one required to gain back control of the systems.

Other data points that stand out in this report include the fact that "61% of all cyber-attacks in 2020 targeted airlines (16% for manufacturers and 15% for airports), 95% of which were financially motivated".[169] This means that political or ideological attacks present only a very small minority and that the target of the attack is more commonly data (possibly PNR data) which can be used for financial gain. The report confirms this, stating that data theft is a major

[165] EUROCONTROL EATM-CERT Services Think Paper, *Aviation under attack: Faced with a rising tide of cybercrime, is our industry resilient enough to cope?*, (5 July 2021) https://www.eurocontrol.int/sites/default/files/2021-07/eurocontrol-think-paper-12-aviation-under-cyber-attack.pdf (last accessed 19 June 2023).
[166] *Ibid.*, p. 1.
[167] *Ibid.*, p. 1.
[168] *Ibid.*, p. 1.
[169] *Ibid.*, p. 2.

problem, it being the case in 36% of all reported incidents and proven by the data hacks of multiple globally significant airlines.[170]

To better understand this statistical information, we will look into a couple of the most relevant and recent cyberattacks, the considerable consequences they had for both the airlines and their passengers as well as the steps certain airlines have taken to prevent them from happening in the future.

On March 26th, 2022, an unknown group (allegedly the "Anonymous") executed a cyberattack targeting the Russian Federal Air Transport Agency. Documents, aircraft registration data, mails from the servers, totalling approximately 65 terabytes of data, were erased from the Agency's servers in the attack. The consequences of the attack forced the Agency to send hard copies of notices through the post, until it was able to locate the back-up copies of the files.[171]

Another cyberattack with significant consequences happened in March 2021 on SITA (Société Internationale de Télécommunications Aéronautiques), involving passenger data. SITA is a company which provides technology and communication services and operates passenger processing systems for airlines.[172] SITA provides IT services to 90% of the airlines in the world. It disclosed that some of the airlines affected in this cyberattack included Air India, Finnair, Japan Airlines, Jeju Air, Lufthansa, Malaysia Airlines, Singapore Airlines and Cathay Pacific. Just Singapore Airlines announced that information on 580,000 costumers was stolen, while Air India evaluated that personal information belonging to 4.5 million passengers was exposed in the attack.[173]

Shortly beforehand, easyJet was the target of a cyberattack in January of 2020, in which hackers acquired the email address and travel details of approximately 9 million customers were accessed, including 2,208 customers' credit-card information. [174] The carrier only published the official statement notifying the passengers about the attack on May 19th, 2020, over 4 months after the event. As a consequence, today more than 10,000 passengers are pursuing around £18 billion in damages. The action was taken under Article 82 of GDPR, which gives customers the

[170] *Ibid.*, p. 2.
[171] Aviation is facing a rising wave of cyber-attacks in the wake of COVID (8 August 2022). https://www.shlegal.com/insights/aviation-is-facing-a-rising-wave-of-cyber-attacks-in-the-wake-of-covid (last accessed 19 June 2023).
[172] SITA Official website, About us, https://www.sita.aero/about-us/ (last accessed 19 June 2023).
[173] SITA Statement on the Security Incident, https://www.sita.aero/pressroom/news-releases/sita-statement-about-security-incident/ (last accessed 19 June 2023).
[174] Aviation is facing a rising wave of cyber-attacks in the wake of COVID, op. cit. (n. 94).

right to compensation for inconvenience, distress, annoyance and loss of control of their personal data.[175]

One of the most significant cyberattacks, in regard to both the amount of stolen information and the financial loss for the attacked airline, occurred in August of 2018 when the system of British Airways was infected with a computer virus. This resulted in the stealing of personal information belonging to 429,612 customers and staff members from the company's servers. The airline said the personal data of at least 380,000 customers had been compromised in the incident, with payment card information, customer names, email addresses, and home addresses affected but not travel or passport details.[176] An investigation conducted by the Information Commissioner's Office (hereinafter: ICO) found that "BA failed to process the personal data of its customers in a manner that ensured appropriate security of the data, including: protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures, as required by Article 5(1)(f) and by Article 32 GDPR". This resulted in British Airways receiving a fine of £20 million for failing to protect the information of its customers, still considerably smaller than the £183m that the ICO originally said it intended to issue back in 2019, but taking into account "the economic impact of Covid-19".[177]

In another case of a data breach, the hacking of Air Canada's mobile application in August of 2018, caused the leak of extremely sensitive personal data including the customers' passport information. The company stated that around 20,000 user profiles have been accessed.[178]

Cathay Pacific was also a victim of a cyberattack in 2018, affecting approximately 9.4 million customers. The breach included a variety of types of data, namely: passenger names, nationalities, dates of birth, phone numbers, email addresses, postal addresses, passport and identity card numbers, frequent flyer membership numbers, customer service remarks and historical travel information. An investigation conducted by the ICO revealed that Cathay

[175] easyJet Notice of cyber security incident (19 May 2020), http://otp.investis.com/clients/uk/easyjet1/rns/regulatory-story.aspx?cid=2&newsid=1391756 (last accessed 19 June 2023).
[176] Aviation is facing a rising wave of cyber-attacks in the wake of COVID (n. 94).
[177] Information Commissioner's Office Penalty Notice, Section 155, Data Protection Act 2018, Case ref: COM0783542 British Airways, https://ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf (last accessed 19 June 2023).
[178] Aviation is facing a rising wave of cyber-attacks in the wake of COVID (n. 94).

Pacific did not implement any password protection for backup files. Cathay Pacific was issued with a £500,000 fine by the ICO .[179]

These are just some of the countless examples of cyberattacks targeting data from recent years. The fact that the aviation industry seems to be of particular interest to attackers is notable, especially considering the amount of information contained in PNR databases and the disastrous consequences of their theft. This only further confirms that cyberattacks are an issue that has to be discussed in a more detailed manner suitable to its importance. Additionally, the fact that large and influential air transport companies are struggling to find an efficient solution that would resolve this issue despite implementing appropriate cyber security measures, raises the question for smaller, less developed air carriers and their ability to face this threat. This also notifies the level of sophistication of attackers, as they are able to breach the security measures, especially in such significant numbers.

5. CONCLUSION

The role of PNR data in fighting terrorism has been confirmed to be irreplaceable due to it containing information that is not available in any other database. It provides law enforcement both with the information on suspects necessary to plan and conduct an intervention, to identify suspects who were previously unknown, as well as the evidence required in a trial, such as the travel history of a defendant which can be essential in confirming their location at the time of an attack.

The general interests of combatting terrorism and serious crime can be used to justify the application of PNR data for security purposes if the data protection and human rights are appropriately ensured in a practical and effective way and not just proclaimed in the agreements. This mainly means the providing of opportunities for redress and compensation for individuals in cases of unlawful processing of their data. The appropriate address and guarantee of these rights is even more important, considering the increased interest of more states (as aforementioned, Mexico and Japan) in entering into PNR agreements. The existing provisions in both the EU-USA PNR agreement and the PNR Directive, need to be amended and applied in accordance with the latest CJEU decision. In fact, data protection is more adequately

[179] Information Commissioner's Office Penalty Notice To: Cathay Pacific Airways Limited https://ico.org.uk/media/action-weve-taken/mpns/2617314/cathay-pacific-mpn-20200210.pdf

addressed in the GDPR by prescribing more precise obligations for the entities collecting and processing the data, including the sanctions in cases of non-compliance, but these standards are not obligatory for US authorities.

The issue of cyberattacks and the consequence of PNR data theft puts into question the necessity of collection and retention of such sensitive data for a wide group of subjects, not suspected or on trial for serious crime. Furthermore, while international civil aviation instruments address cyberattacks that jeopardise the security of civil aviation, types of cyberattacks with the objective of obtaining passenger information and which may not cause direct security risks, are not covered in these instruments.

The accelerated growth of information technology and the world's, as well as the aviation's, dependency on it, has generated new opportunities for criminals to exploit the vulnerabilities in the existing systems and attack critical cyber infrastructure. This requires the development of cybersecurity measures adequate to protect the information systems against the criminal activity. To achieve this, states have already increased the level of international cooperation, as the need to prevent future cyberattacks is of global importance. Another necessary means of fighting against cyber threats is establishing international legal framework regulating cyberattacks and that would be widely accepted and ratified by the majority of the international community.

The existing legal framework, while partially applicable to cover cyberattacks, presents certain inadequacies, mainly due to the fragmentation caused by the states not ratifying of treaties and the potential differences in the interpretation of some terms, as well as the instruments being antiquated and finally, the instruments not dealing with the more common issue of data breaches.

6. REFERENCES

Books

1. Bergamasco Federico, Cassar Roberto, Popova Rada, Scott Benjamyn I., Cybersecurity - Key Legal Considerations for the Aviation and Space Sectors, Wolters Kluwer (2020)
2. Radionov, Nikoleta, Marin, Jasenko (ur.), Europsko prometno pravo, Pravni fakultet Sveučilišta u Zagrebu (2011)

Articles

1. Abeyratne, Ruwantissa, *Cyber terrorism and aviation—national and international responses*, J Transp Secur Vol. 4 (2011), p. 337–349
2. Abeyratne, Ruwantissa, *Legal Priorities in Air Transport*, (2019), p. 192–193
3. Bigo, Didier, Salomon, Stefan, *Passengers Name Records and Security*, Verfassungsblog on Matters Constitutional (2023), https://verfassungsblog.de/pnr-security/ (last accessed June 2, 2023)
4. Blasi Casagran, C., *The Future EU PNR System: Will Passenger Data be Protected?*, European Journal of crime, criminal law and criminal justice Vol. 23 (2015), p. 241-257
5. Guild, Elspeth, Brouwer, Evelien, *The Political Life of Data: The ECJ Decision on the PNR Agreement between the EU and the US*, CEPS Policy Brief n. 109 (July 2006)
6. Hailbronner, Kay, Papakonstantinou, Vagelis, Kau, Marcel, *The Agreement on Passenger-Data Transfer (PNR) and the EU-US Cooperation in Data Communication*, International Migration Vol. 46 (2) (2008), p. 188-197
7. Hathaway, Oona A., Crootof, Rebecca, Levitz, Philip, Nix, Haley, Nowlan, Aileen, Perdue, William, Spiegel, Julia, *The Law of Cyber-Attack*, California Law Review Vol. 100 (4) (August 2012), p. 817-885
8. Hornung, Gerrit, Boehm, Franziska, Comparative Study on the 2011 draft Agreement between the Unites States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security, Greens/EFA Group in the European Parliament (March 2012)
9. Kaunert, C., Leonard, S., Mackenzie, A., The social construction of an EU interest in counter-terrorism: US influence and internal struggles in the cases of PNR and SWIFT, European security, 2012, Vol. 21, No. 4, p. 474-496.
10. Klenka, M., *Aviation cyber security: legal aspects of cyber threats*, Journal of Transportation Security Vol. 14 (3) (2021)
11. Lindsey, R., Airports Start Thorough Screening of All Passengers, The New York Times, January 6, 1973.
12. Mendez, Mario, *Opinion 1/15: The Court of Justice Meets PNR Data (Again!)*, European Papers Vol. 2 (3) (2017), p. 803-818
13. Orrù, Elisa, *The European PNR Directive as an instance of pre-emptive, risk-based algorithmic security and its implications for the regulatory framework*, Information Policy Vol. 27 (2022), p. 131–146

14. Pejaković-Dipić, Silvija, Karas, Željko, *Neki problemi kod prikupljanja i razmjene podataka o putnicima u zračnom prometu*, Visoka policijska škola, Zagreb (2018)
15. Piera, Alejandro, Gill, Michael, *Will the New ICAO–Beijing Instruments Build a Chinese Wall for International Aviation Security?*, Vanderbilt Journal of Transnational law Vol. 47:145 (2014), p. 147-234
16. Propp, Kenneth, *Avoiding the Next Transatlantic Security Crisis: The Looming Clash over Passenger Name Record Data*, Atlantic Council (2021)
17. Tanaka, Hiroyuki, Belanova, Rocco, Ginsburg Susan, De Hart, Paul, *Transantlantic Policy Sharing: At a Crossroads, Migration Policy Institute* (January 2021), https://www.migrationpolicy.org/sites/default/files/publications/infosharing-Jan2010.pdf (last accessed June 2, 2023)
18. Ukwandu, Elochukwu, Ben-Farah, Mohamed Amine, Hindy, Hanan, Bures, Miroslav, Atkinson, Robert, Tachtatzis, Christos, Andonovic, Ivan, Bellekens, Xavier, *Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends*, Information Vol. 13, 146 (2022), https://doi.org/10.3390/info13030146
19. Vavoula, Niovi, *I Travel, therefore I Am a Suspect: an overview of the EU PNR Directive*, Queen Mary University of London, https://eumigrationlawblog.eu/i-travel-therefore-i-am-a-suspect-an-overview-of-the-eu-pnr-directive/?print=print (last accessed August 16, 2023)

International Conventions

1. Convention on International Civil Aviation (adopted 7 December 1944, entered into force 4 April 1947) 15 UNTS 295 (Chicago Convention)
2. Convention on Offences and Certain Other Acts Committed on Board Aircraft, signed at Tokyo on 14 September 1963
3. Convention for the Suppression of Unlawful Seizure of Aircraft (1970).
4. The Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, signed at Montreal on 23 September 1971
5. Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, signed at Montreal on 24 February 1988
6. United Nations Resolution adopted by the General Assembly [on the report of the Third Committee (A/55/593)] Combating the criminal misuse of information technologies, 55/63 (22 January 2001).
7. Council of Europe Convention on Cybercrime, European Treaty Series - No. 185, Budapest (23 October 2001)
8. Agreement between the European Community and the United States of America on the Processing and Transfer of PNR Data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs, 2004 O.J. L 183, May 20, 2004 (no longer in force)
9. Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security – the PNR Agreement, Council Document 13216/06 (no longer in force)
10. Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data.

11. Agreement between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security, 2012 O.J. L 215
12. Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, L 186/4, Official Journal of the European Union, 14.7.2012.
13. Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft (adopted in Beijing on 10 September 2010) (Doc 9959) (Beijing Protocol)
14. Protocol to Amend the Convention on Offences and Certain Other Acts Committed on Board Aircraft, signed at Montréal, 2014
15. Draft United Nations Treaty on an International Criminal Court or Tribunal for Cyberspace, from June of 2015
16. Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (adopted in Beijing, China on 10 September 2010, entered into force 1 July 2018) (Beijing Convention)

European Union regulation

1. Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, Official Journal of the European Union, L 261/24
2. Regulation (EU) No 376/2014 of the European Parliament and of the Council of 3 April 2014 on the reporting, analysis, and follow-up of occurrences in civil aviation.
3. Directive (EU) 2016/681 of the European Parliament and the Council on the use of PNR data of air passengers of flights operated between the European Union and third countries (27 April 2016)
4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data
5. Commission Implementing Regulation (EU) 2019/1583 of 25 September 2019 amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures
6. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

Case law

1. Opinion on the Proposal for a Council Decision on the conclusion of an agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information (API) / Passenger Name Record (PNR) data, OJ C 218, 6.9.2005
2. Maximillian Schrems v Data Protection Commissioner, Judgment of the Court (Grand Chamber) of 6 October 2015, Case C-362/14

3. Opinion 1/15 Of the Court of Justice of the European Union (Grand Chamber) on the Draft Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, 26 July 2017., Avis 1/15**.**
4. Rahinah Ibrahim v. U.S. Dept. Of Homeland Security, No. 14-16161 9th Cir. 2017
5. Judgement of the Court of Justice of the European on the Validity of the Union Directive (EU) 2016/681 – Use of PNR data of air passengers of flights operated between the European Union and third countries, Case C-817/19 (21 June 2022)

Documents of international organisations and associations

1. Information Commissioner's Office Penalty Notice, Section 155, Data Protection Act 2018, Case ref: COM0783542 British Airways, https://ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf (last accessed 19 June 2023)
2. Information Commissioner's Office Penalty Notice To: Cathay Pacific Airways Limited https://ico.org.uk/media/action-weve-taken/mpns/2617314/cathay-pacific-mpn-20200210.pdf
3. Compilation of Cyber Security Regulations, Standards, and Guidence Applicable to Civil Aviation (December 2020), https://www.iata.org/contentassets/4c51b00fb25e4b60b38376a4935e278b/compilation-of-cyber-regulations-standards-and-guidance_3.0.pdf (last accessed June 2, 2023)
4. Report from the Commission to the European Parliament and the Council On the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (2020)
5. Report from the Commission to the European Parliament and the Council on the joint evaluation of the Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, Brussels (12.1.2021)
6. International Civil Aviation Organisation Legal Committee– 38th Session: Consideration of the adequacy of existing international air law instruments in adressing cyber threats against civil aviation, Working Paper (22nd to 25t March 2021)
7. EUROCONTROL EATM-CERT Services Think Paper, *Aviation under attack: Faced with a rising tide of cybercrime, is our industry resilient enough to cope?*, (5 July 2021) https://www.eurocontrol.int/sites/default/files/2021-07/eurocontrol-think-paper-12-aviation-under-cyber-attack.pdf (last accessed 19 June 2023)

Other sources

1. US Government Accounting Office, Highlights of the Report to Congressional Committees, Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges, February 2004
2. House of Lords European Union Committee, The Passenger Name Record (PNR) Framework Decision: Report with Evidence, 15th Report of Session 2007-08 (London, United Kingdom: The Stationary Office Limited, 2008)http://www.statewatch.org/news/2008/jun/eu-pnr-uk-hol-report.pdf. (last accessed 19 June 2023)

3. Faisal Shahzad Indicted for Attempted Car Bombing in Times Square," US Department of Justice, Office of Public Affairs, June 17, 2010.
4. US Department of Justice, "David Coleman Headley Sentenced to 35 Years in Prison for Role in India and Denmark Terror Plots," Press release, January 24, 2013. https://www.justice.gov/opa/pr/david-coleman-headley-sentenced-35-years-prison-role-india-and-denmark-terror-plots (last accessed 19 June 2023)
5. Joint statement: Beginning of negotiations between Mexico and the European Union on PNR data transmission,14 July 2015, Joint_statement__Beginning_of_negotiations_between_Mexico_and_the_European_Union_on_PNR_data_transmission%20.pdf (last accessed June 18, 2023)
6. EU-Japan PNR agreement: Council authorises opening of negotiations, 18 February 2020, https://www.consilium.europa.eu/en/press/press-releases/2020/02/18/eu-japan-pnr-agreement-council-authorises-opening-of-negotiations/(last accessed June 18, 2023)
7. easyJet Notice of cyber security incident (19 May 2020), http://otp.investis.com/clients/uk/easyjet1/rns/regulatorystory.aspx?cid=2&newsid=1391756 (last accessed 19 June 2023)
8. SITA Statement on the Security Incident (4 March 2021), https://www.sita.aero/pressroom/news-releases/sita-statement-about-security-incident/ (last accessed 19 June 2023)
9. Press Release No 105/22 Luxembourg, 21 June 2022, Judgment of the Court in Case C-817/19 | Ligue des droits humains
10. Aviation is facing a rising wave of cyber-attacks in the wake of COVID (8 August 2022), https://www.shlegal.com/insights/aviation-is-facing-a-rising-wave-of-cyber-attacks-in-the-wake-of-covid (last accessed 19 June 2023).