

ANTIGUA AND BARBUDA



**ADVANCE PASSENGER INFORMATION AND PASSENGER
NAME RECORD BILL, 2026**

NO. OF 2026

**ANTIGUA AND BARBUDA
ADVANCE PASSENGER INFORMATION AND PASSENGER
NAME RECORD BILL 2026**

SECTIONS

**PART I
PRELIMINARY**

1. Short title and commencement.....	7
2. Interpretation.....	7
3. Application of this Act.....	13

**PART II
ADMINISTRATIVE**

4. Powers and functions of the Competent Authority	14
5. Establishment of the Passenger Information Unit.....	16
6. Functions of the Passenger Information Unit.....	17
7. Appointment and functions of Data Protection Officer	18

PART III

**COMMON PROVISIONS FOR ADVANCE PASSENGER INFORMATION AND
PASSENGER NAME RECORD**

8. Duty to provide Advance Passenger Information, Passenger Name Record data and embarkation and disembarkation data	20
9. Technical stop	20
10. Restriction on disclosure of data or documentation by the Competent Authority	21
11. Advance Passenger Information and Passenger Name Record access.....	22
12. Processing of API and PNR	23

13. Verification of API and PNR data submitted to the Competent Authority and IMPACS	24
14. Use, screening and sharing of API and PNR with regional and international security agencies	25
15. Transfer of API and PNR data to Competent Authority in another country	25

PART IV

API OPERATING PROVISIONS

16. Duty to transmit API.....	26
17. API Data Elements.....	28
18. Timeframe for submission of API data and embarkation and disembarkation data.....	28
19. Protection of API data.....	28
20. Retention of API data.....	29
21. Duty to provide API data in accordance with Act	29

PART V

PNR OPERATING PROVISIONS

22. Obligations of captain or agent of aircraft regarding the transfer of PNR data.....	30
23. Obligations of master or agent of vessel regarding the transfer of PNR data	31
24. PNR data transfer method and format.....	32
25. Transmission timeframe for PNR data.....	32
26. Automated processing of PNR data	33
27. Sensitive data	33
28. PNR data and document retention	33
29. Depersonalisation and anonymisation of PNR data	35
30. National oversight.....	36
31. Competent Authority and PIU to liaise with Regional Data Protection Officer	36
32. Competent Authority and PIU to liaise with Data Protection Officer.....	36

33. Safeguards and redress mechanisms	37
34. Contravention of this Part	37
35. Conflict of laws regarding transmission of PNR	38

PART VI

ADMINISTRATIVE PENALTIES

36. Certain contraventions may be dealt with administratively	38
37. Notice respecting administrative penalty	38
38. Opportunity to make representations	39
39. Hearing and decision.....	39
40. Appeals	40
41. Correction of decision.....	40
42. Absolute liability.....	41
43. Assessment of quantum of administrative penalty.....	41
44. Deadline for payment of administrative penalty	41
45. Recovery of administrative penalties	42
46. Consolidated Fund	42
47. Limitation Period	42

PART VII

EXCHANGE OF PNR DATA WITH OTHER PARTICIPATING STATES

48. Transfer of PNR data by the Competent Authority or PIU to other Participating States	43
49. Another Participating State requests PNR data from Competent Authority	44
50. Competent Authority or PIU requests PNR data from another Participating State.....	44

PART VIII

MISCELLANEOUS

51. Requirement to submit information electronically.....	45
---	----

52. Immunity from liability.....	45
53. Regulations	45
54. Non-Imposition of Penalties for Incomplete, Delayed or Erroneous messages resulting from technical issue	46
55. Amendment of the Schedules	46
56. Repeal	46

SCHEDULE I
SCHEDULE II
SCHEDULE III
SCHEDULE IV
SCHEDULE V
SCHEDULE VI

ANTIGUA AND BARBUDA

**ADVANCE PASSENGER INFORMATION AND PASSENGER
NAME RECORD BILL 2025**

NO. OF 2025

AN ACT to repeal and replace the Advanced Passenger Information Act, 2016; to make provision for the collection, transmission, sharing, storage and regulation of Advance Passenger Information and Passenger Name Record in respect of persons traveling to, departing from and transiting through Antigua and Barbuda, in accordance with international best practices; and to enhance the national and regional regulatory regimes and institutional cooperation frameworks governing and related to the implementation and operationalization of the **CARICOM** Advance Passenger and Crew Information System, subject to international standards and national legislation governing data protection and data privacy, and for other incidental and related matters.

ENACTED by the Parliament of Antigua and Barbuda as follows:

**PART I
PRELIMINARY**

1. Short title and commencement

(1) This Act may be cited as the Advance Passenger Information and Passenger Name Record Act 2026.

(2) This Act shall come into operation on a date as is fixed by the Minister by Notice published in the Gazette and different dates may be appointed for the coming into force of different parts of this Act.

2. Interpretation

In this Act, unless the context otherwise requires —

“advance passenger information” or **“API”** means —

- (a) a set of data detailing information concerning an aircraft or a vessel;
- (b) information concerning a passenger and crew member, or any other person traveling in an aircraft or a vessel as set out in Schedule III; and
- (c) embarkation and disembarkation data as set out in Schedule III(C);

“Advance Passenger Information and Passenger Name Record database” or **“API, PNR database”** means a centralised database established under section 6(b) for the storage, management and analysis of API and PNR data;

“agent” means a person who is authorised, in writing, by the owner, captain or master of an aircraft or vessel to perform a function under this Act on behalf of the owner, captain or master;

“aircraft” includes an aeroplane, helicopter or other means of airborne navigation by means of which persons, goods or both travel across international borders;

“anonymization of PNR data” means the process of removing or encrypting personally identifiable information (PII) from the PNR record;

“API hit” means a name or travel document present in the Watch List System;

“Associate Member State” means a Caribbean State or Territory admitted by the Conference of Heads of Government to associate membership of the Caribbean Community pursuant to Article 231 of the Revised Treaty;

“automated processing of data” means the utilisation of authorised applications, software or systems to analyse, screen and compare data against Watch Lists and other predetermined criteria with no human involvement in the subsequent decision-making process;

“captain” means the owner of an aircraft, the pilot of an aircraft so designated by the operator, or the person being in command and charged with the safe conduct of the flight;

“CARICOM” means the Caribbean Community established by Article 2 of the Revised Treaty;

“CARICOM Advance Passenger Information System” or **“CARICOM APIS”** means –

- (a) the CARICOM Electronic Manifest Single Window (CEMSIW) when used for Advance Passenger Information and Passenger Name Record data interchange; and

(b) the Advance Passenger Information and Passenger Name Record database managed by the JRCC under the authority of IMPACS;

“CARICOM Council for Security and Law Enforcement” or **“CONSLE”** means the Organ of CARICOM incorporated under Article V of the Protocol Amending the Revised Treaty of Chaguaramas to Incorporate the Council for National Security and Law Enforcement (CONSLE) as an Organ of the Community and the CARICOM Implementation Agency for Crime and Security (IMPACS) as an institution of the Community signed at Placencia, Belize on 16 February 2016;

“CARICOM Electronic Manifest Single Window” or **“CEMSIW”** means the electronic window used for the submission or transmission of API, PNR and other information required to be submitted or transmitted under this Act;

“CARICOM Member State” means a State listed in Article 3 paragraph 1 of the Revised Treaty;

“commercial aircraft” means an aircraft which engages in transporting passengers or goods for monetary gain;

“commercial vessel” means a vessel which engages in transporting passengers or goods for monetary gain;

“Competent Authority” means the entity who, for the purpose of this Act, is responsible for –

- (a) the effective and efficient collection and processing of API and PNR data of passengers and crew arriving at, transitting through and departing from Antigua and Barbuda; and
- (b) national border security and risk management measures related to the matters referred to in paragraph (a)

“Convention on Facilitation of International Maritime Traffic” or **“FAL Convention”** means the convention, adopted on 9th April 1965 and entered into force on 5th March 1967;

“Competent Authority” means the Chief Immigration Officer;

“crew member” or **“crew”** means –

in relation to an aircraft, any individual charged with performing duties essential to the operation of an aircraft during flight, including landing or take-off; and

in relation to a vessel, any individual charged with performing duties essential to the operation of the vessel and the safety and well-being of its passengers or cargo during a journey;

“data processing” –

means any operation or set of operations performed on API or PNR data for the purpose of enhancing border security, immigration control, customs clearance and other law enforcement purposes; and

includes the collection, analysis, recording, organisation, storage, adaptation or alteration, calling-up, retrieval, consultation, use, transfer, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of API or PNR data;

“Data Protection Officer” means an individual appointed under section 9 by the Competent Authority to oversee and ensure that the collection, handling, processing, storage, and transfer of Advance Passenger Information (API) and Passenger Name Record (PNR) data is done in compliance with data protection laws;

“Departure Control System” means the system used to –

- (a) support preflight or pre-voyage processes, including checking in of passengers onto aircraft or vessels; and
- (b) streamline the departure processes, ensure regulatory compliance, and enhance security measures by effectively handling API and PNR data;

“depersonalisation of PNR data” means the masking of information that enables direct identification of an individual, without hindering the use of PNR data by law enforcement agencies and entities;

“embarkation and disembarkation data” means the information set out in Schedule III(C) in relation to a passenger, crew member, or any other person traveling in an aircraft or vessel and who is expected to embark or disembark in Antigua and Barbuda;

“IATA” means the International Air Transport Association found in Havana, Cuba on the 19th April 1945;

“ICAO” means the International Civil Aviation Organisation which was formed as a result of the Convention on International Civil Aviation also known as the “Chicago Convention” signed on the 7th December, 1944;

“IMO” means the International Maritime Organisation which was formerly the Inter Governmental Maritime Consultative Organisation established by a convention adopted in Geneva in 1948 for the purpose of effectively promoting maritime safety;

“IMPACS” –

- (a) means the Implementation Agency for Crime and Security established as an Institution of CARICOM under Article VII of the Protocol Amending the Revised Treaty of Chaguaramas to Incorporate the Council for National Security and Law Enforcement (CONSLE) as an Organ of the Community and the CARICOM Implementation Agency for Crime and Security (IMOACS) as an institution of the Community signed at Placencia, Belize on 16th February 2016; and
- (b) includes its sub-agencies, namely –
 - (i) the Joint Regional Communication Centre (JRCC); and
 - (ii) the Regional Intelligence Fusion Centre (RIFC);

“INTERPOL” means the International Crime Police Organisation established by the Constitution of the International Criminal Police Organisation – INTERPOL adopted by the United Nations General Assembly at Vienna, Austria in 1956;

“JRCC” means the Joint Regional Communications Centre which is a sub-agency of IMPACS;

“master” includes a person having command or charge of a vessel other than a pilot;

“Minister” means the Minister with responsibility for National Security;

“national border security” means the protection of national borders from the illegal movement of weapons, drugs, contraband and people, while facilitating lawful trade and travel;

“operating carrier” means the air carrier having operational control of an aircraft used for a codeshared flight;

“Participating State” means a CARICOM Member State and an Associate Member State that utilises CARICOM API to support the processing and analysis of passenger and crew data and the transmission, collection, processing and screening of API and PNR data;

“passenger” means a person not being a bona fide crew member, traveling or seeking to travel on an aircraft or vessel;

“Passenger Information Unit” or “PIU” means the authority established under section 7;

“Passenger Name Record” or “PNR” means the record created by aircraft or vessel operator or their agents, for each voyage or flight booked by or on behalf of any passenger in the reservation system, Departure Control System or equivalent system as set out in Schedule II;

“personal data” means all information that can be used to identify a natural person;

“PNR data transfer” means the transfer of PNR data to the Competent Authority and IMPACS via the CEMSIW managed by IMPACS in the format set out in Schedule II;

“PNRGOV message” means the standard electronic message format jointly endorsed by the World Customs Organization, International Civil Aviation Organisation and International Air Transport Association used by an aircraft and a vessel to submit PNR data;

“positive match” means the matching of personal or document data to an individual resulting from a comparison, whether naturally or by means of any electronic or other device, between any personal data of the individual, or between any document used by an individual for purposes of travel, against authorised databases and Watch Lists for the purposes of the implementation of this Act;

“push method” means the method used for the transfer of PNR data from the airlines, vessels or transportation operators to the Competent Authority and IMOACS via CEMSIW;

“private aircraft” means an aircraft which is not a commercial aircraft or state aircraft;

“private vessel” means a vessel which is not a commercial vessel or a state-owned vessel;

“Regional Data Protection Officer” means the individual, appointed by the Executive Director of CARICOM IMPACS, who is responsible for overseeing adherence to data protection standards during the course of cross-border data collection, data processing and data transfer among Participating States;

“regional space” means the air and maritime spaces managed by the respective governments of the CARICOM Member States in accordance with international aviation and maritime law;

“Revised Treaty” means the Revised Treaty of Chaguaramas establishing the Caribbean Community including the CARICOM Single Market and Economy signed at Nassau, The Bahamas, on 5th July 2001;

“sensitive data” –

- (a) means data that reveals an individual’s information; and
- (b) includes data that reveals an individual’s race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation;

“technical stop” means the landing of an aircraft or the berthing or anchoring of a vessel or the otherwise arrival or stopping of an aircraft or a vessel for purposes of

refuelling, unexpected essential repairs, or a similar purpose other than for taking on or discharging passengers, baggage, cargo or mail;

“terrorist offence” means any offence established under the Prevention of Terrorism Act, the Proceeds of Crime Act, the Weapons of Mass Destruction (or any other national enactment in respect of acts of terrorism;

“vessel” –

- (a) means any ship, boat, barge, yacht, or other floating or submersible transportation by means of which persons and goods can travel across international borders; and
- (b) includes a cruise line, a cargo ship and a tugboat;

“vessel operator” –

- (a) means an individual, a company, or an organization responsible for the operation, management, and control of a particular vessel; and
- (b) includes an individual, a company, or an organization responsible for overseeing the navigation, manoeuvring, and overall operation of the vessel, as well as ensuring compliance with maritime regulations, safety protocols and operational procedures;

“Watch List” means a list maintained by IMPACS and the Competent Authority that is used for the identification, tracking and monitoring of the activities or movements of criminals and suspicious travellers, including –

- (a) terrorists or persons convicted of a criminal offence;
- (b) persons suspected to be travelling on stolen and lost travel documents (SLTDs);
- (c) criminal deportees; and
- (d) other persons of interest to law enforcement and the intelligence community.

3. Application of this Act

This Act shall apply to the collection, use, retention, transfer, and protection of Advance Passenger Information and Passenger Name Record data, by the Competent Authority of Antigua and Barbuda, and IMPACS.

PART II ADMINISTRATIVE

4. Powers and functions of the Competent Authority

- (1) The Competent Authority shall –
 - (a) be responsible for overseeing and implementing the provisions of this Act;
 - (b) establish protocols, standards, issue guidelines and technical requirements for the secure transmission, storage, and processing of API and PNR data;
 - (c) oversee the operations of the PIU in the performance of its functions;
 - (d) establish secure channels and reliable systems for the timely transmission, receipt, storage, management and transfer of API and PNR data from the captain or agent of an aircraft and the master of a vessel;
 - (e) in collaboration with IMPACS, monitor compliance with API and PNT regulations and may conduct reviews or inspections of the operations of the aircraft, vessels, or transportation operators' operations to ensure adherence to the data collection and transmission requirements;
 - (f) establish data transfer agreements or arrangements with other receiving Participating States or their competent authorities, specifying the obligations, safeguards, and conditions or the usage, storage, and retention of the transferred PNR data;
 - (g) conduct audits and inspections to ensure compliance with the Act;
 - (h) establish cooperation and information sharing mechanisms with relevant national and international entities to enhance the effectiveness of API and PNR data usage;
 - (i) maintain confidentiality and data protection standards for the handling of API and PNTR data;
 - (j) provide necessary training and support to PIU personnel and persons involved in the API and PNR data management process; and
 - (k) co-ordinate with IMPACS on matters relating to API and PNR and ensure compliance with this Act.

- (2) The Competent Authority shall –
 - (a) have to access API data and PNR data or the data processing results in order to examine such information further;
 - (b) adequately manage API data and PNR data and provide an appropriate level of protection of these data in keeping with the principles of data protection, international best practices and national enactments;

- (c) verify data during physical processing of any passenger or crew member at any port of entry or departure by comparing the API information to the information contained in the travel document presented by the passenger or crew member;
- (d) liaise and coordinate with relevant national, regional and international organisations to ensure that, in so far as it is practicable, mechanisms are established which remove the requirement of passengers to submit the same information to more than one entity in respect of the same voyage or journey;
- (e) correct any erroneous data at the port of entry or departure and update the information in APIS and PNR databases after verifying it from the travel or other relevant documents of the passenger or crew member;
- (f) undertake appropriate action for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crimes as well as for border security purposes;
- (g) co-ordinate with IMPACS on all matters relating to API, PNR submissions and CEMSIW;
- (h) if requested, permit a passenger or crew from an aircraft or vessel access to his personal identifiable information maintained in the APIS database to ensure its correctness; but no passenger shall have access to any information provided by IMPACS to the Competent Authority against a Watchlist for any API hit;
- (i) process all API hits, high-risk travellers and cargo information flagged and referred by IMPACS and provide timely dispositions on these referrals, in keeping with established protocols;
- (j) determine after consultation with IMPACS the admissibility or otherwise of passengers or crew into Antigua and Barbuda;
- (k) withhold clearance for the departure of an aircraft or vessel whose captain, master or agent has not provided the API and PNR data required pursuant to section 10(3), pending submission of the data; and
- (l) assess the sufficiency, and error rates in reviewing API and PNR transmissions for each flight or voyage.

(3) Notwithstanding paragraphs (h) and (j) of subsection (2), any decision with respect to the admissibility or inadmissibility of passengers or crew from an aircraft or a vessel shall be made solely by the Competent Authority.

(4) The Competent Authority shall carry out all its activities and responsibilities in a manner consistent with the protection of personal data, principles of data protection and national enactments governing data protection and data privacy.

(5) In a situation where a PIU has not yet been established, or is not operational, the Competent Authority shall process API and PNR data and shall —

- (a) coordinate with IMPACS in carrying out an assessment of passengers prior to their scheduled arrival in or departure from Antigua and Barbuda to identify persons who require further examination by the Competent Authority; and
- (b) analyse API and PNR data for the purpose of updating or creating new criteria to be used in the screening process.

(6) In a situation referred to in subsection (5), any positive match resulting from the automated processing of API and PNR data shall be individually reviewed by non-automated means to verify whether the Competent Authority shall take action in accordance with this Act.

(7) The Competent Authority shall not take any decision —

- (a) that produces an adverse legal effect on a person or significantly affects a person only by reason of the automated processing of data; or
- (b) on the basis of a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation, unless failure to take the decision would be prejudicial to the interests of public health, public safety and national security.

5. Establishment of the Passenger Information Unit

(1) There is established a Passenger Information Unit (“PIU”) which shall comprise —

- (a) a senior Immigration Officer, nominated by the Chief Immigration Officer;
- (b) a senior officer of the Royal Police Force for Antigua and Barbuda, nominated by the Commissioner of the Police;
- (c) a senior Customs Officer, nominated by the Comptroller of Customs;
- (d) an officer of the Department of Information Technology who is responsible for Data Protection, nominated by the Minister with responsibility for Information Technology; and
- (e) three other officers appointed from law enforcement, including customs and immigration after consultation with the Minister.

(2) The senior Immigration Officer shall be head of the PIU.

6. Functions of the Passenger Information Unit

(1) The PIU shall —

- (a) receive, store, process, analyse and manage all API and PNR data transmitted by an aircraft and vessel in accordance with the provisions of this Act for the purpose of national security;
- (b) for the purpose of prevention, detection, investigation and prosecution of terrorism and serious crime –
 - (i) manage and conduct risk assessments and analysis of API and PNR data collected from an aircraft or a vessel; and
 - (ii) submit the results to the law enforcement personnel at ports of entry in Antigua and Barbuda through the use of secure tools, technologies, and intelligence methodologies;
- (c) in collaboration with the Competent Authority and IMPACS, ensure that aircraft operators, vessel operators, passengers and crew members are –
 - (i) aware of their obligations under this Act; and
 - (ii) compliant with the requirements for an aircraft or a vessel to arrive in or depart from Antigua and Barbuda;
- (d) in collaboration with the Competent Authority, liaise with and ensure effective communication and cooperation with government departments and government agencies, by –
 - (i) sharing information that it has acquired in the course of its duties under this Act; and
 - (ii) undertaking any other responsibility that shall be so assigned by the Competent Authority;
- (e) liaise, collaborate and exchange information with other national, regional and international competent authorities, including other passenger information units and national, regional and international law enforcement organisations, as required; and
- (f) where required by the Competent Authority, establish formal arrangements with national, regional and international competent authorities to support the implementation of the functions of the PIU.

(2) PIU shall carry out all its functions, activities and responsibilities in a manner consistent with the protection of personal data, principles of data protection and in accordance with the laws on data protection and data privacy.

(3) In processing API and PNR data, the PIU shall —

- (a) coordinate with IMPACS and other competent authorities in carrying out an assessment of passengers and crew prior to their scheduled arrival in or departure from Antigua and Barbuda to identify persons who require further examination by the Competent Authority; and
- (b) analyse API and PNR data for the purpose of updating or creating new criteria to be used in the screening and risk assessment process and share risk information and intelligence with IMPACS to further risk assessments and generation of risk criteria.

(4) Any positive match resulting from the automated processing of API and PNR data shall be individually reviewed by non-automated means to verify whether the Competent Authority shall take action in accordance with this Act.

(5) The PIU shall be equipped with the capacity for 24/7 operation, with procedures in place to minimise disruption in the event of an emergency, system outage or failure.

7. Appointment and functions of Data Protection Officer

(1) The Competent Authority shall, in accordance with relevant national enactments, appoint a qualified and experienced individual as the Data Protection Officer to oversee and ensure compliance with data protection laws and regulations relating to API data and PNR data.

(2) The DPO shall —

- (a) operate independently and autonomously in performing his duties, free from any conflicts of interest and for this purpose shall have direct access to the highest levels of management within the Competent Authority and IMPACS;
- (b) possess expert knowledge of data protection laws and regulations, as well as a deep understanding of the specific requirements and challenges associated with the collection, processing, and management of API data and PNR data;
- (c) provide advice, guidance, and recommendations to the Competent Authority and IMPACS on matters related to the processing of API data and PNR data, ensuring compliance with applicable data protection laws and regulations;
- (d) monitor the processing activities related to API data and PNR data, including data collection, storage, access, use, and sharing, to ensure compliance with legal requirements and established policies and procedures and implement related safeguards;
- (e) conduct regular risk assessments regarding the processing of API data and PNR data and identify potential risks or vulnerabilities, and shall work with

relevant departments and stakeholders to implement appropriate measures to mitigate risks and safeguard the rights and privacy of individuals;

- (f) be responsible for conducting or overseeing Data Protection Impact Assessments (DPIAs) relating to the collection, processing, and management of PNR data, and ensure that DPIAs are carried out in accordance with relevant legal requirements;
- (g) act as the main point of contact for individuals, including passengers and crew members, regarding their rights, concerns, and inquiries related to the processing of their API data and PNR data and in so doing shall facilitate the exercise of data subjects' rights and handle any complaints or data breaches;
- (h) organise and provide training programs, workshops, and awareness campaigns to enhance the Competent Authority's and IMPACS' employees' understanding of data protection principles, obligations, and best practices related to API and PNR data processing;
- (i) cooperate and maintain effective communication with IMPACS and relevant data protection authorities or regulatory bodies, providing necessary information, reports, and notifications as required by applicable laws and regulations;
- (j) prepare periodic reports on data protection activities, incidents, and compliance status for senior management and relevant stakeholders and shall ensure transparency and accountability in the processing of API data and PNR data;
- (k) provide national oversight for the protection of API data and PNR data; and
- (l) provide advice, guidance and recommendations to the Competent Authority on API data and PNR data processing to ensure compliance with applicable data protection laws.

(2) The Competent Authority and IMPACS shall provide the necessary resources, authority and support to enable the DPO to fulfil their responsibilities effectively.

(3) The DPO's official contact information, shall be made publicly available to allow individuals to contact the DPO with inquiries, concerns, or complaints related to the processing of API data and PNR data.

PART III

COMMON PROVISIONS FOR ADVANCE PASSENGER INFORMATION AND PASSENGER NAME RECORD

8. Duty to provide Advance Passenger Information, Passenger Name Record data and embarkation and disembarkation data

(1) A master, a captain or an agent of an aircraft or a vessel shall provide to the Competent Authority and IMPACS, via the CEMSIW, with the relevant API data and PNR data relating to the passenger and crew, flight or voyage as set out in Schedules I and II.

(2) The duty to provide API data and PNR data shall apply to all aircraft and vessels, regardless of size and tonnage which are—

- (a) expected to arrive in Antigua and Barbuda;
- (b) expected to depart from Antigua and Barbuda; or
- (c) in transit through Antigua and Barbuda.

(3) Where a flight is code-shared between one or more aircraft, a captain or an agent of the operating carrier shall provide API data and PNR data of all passengers and crew to the Competent Authority and IMPACS, via the CEMSIW.

(4) A passenger or a crew member traveling into and out of Antigua and Barbuda shall, via the CEMSIW, provide to the Competent Authority and IMPACS the relevant embarkation and disembarkation data as set out in Schedule III (C).

9. Technical stop

(1) Nothing in section 8 applies to an aircraft or a vessel which makes a technical stop if the technical stop is —

- (a) required by any statutory or other requirement relating to navigation;
- (b) compelled by an emergency, accident, unfavourable weather conditions, or other necessity; or
- (c) authorised by the Competent Authority.

(2) Where an aircraft or a vessel makes a technical stop for a reason outlined in subsection (1), the captain, agent. or master shall -

- (a) immediately report to the Competent Authority;

- (b) comply with any directives given by the Competent Authority in respect of any passenger or crew member, carried on the aircraft or vessel, and
- (c) not, without the consent of the Competent Authority, permit a passenger or crew member to disembark from the aircraft or vessel;

(3) Subject to any authorisation granted by the Competent Authority, neither a passenger nor a crew member on an aircraft or a vessel shall, without the consent of the Competent Authority, disembark the aircraft or vessel, and such person shall comply with any directive given by the Competent Authority.

(4) A captain, a master or an agent who contravenes this section commits offence and, where the contravention constitutes –

- (a) a first offence, is liable on summary conviction to a fine of five thousand (USD\$5,000.00) United States dollars; and
- (b) a second or repeating offence, is liable on summary conviction to a fine of twenty thousand (USD\$20,000.00) United States dollars or to imprisonment for a term of six months, or to both such fine and imprisonment.

(5) Notwithstanding subsection (4), the disembarkation of a passenger or a crew member from an aircraft or a vessel shall not constitute an offence, if the disembarkation is necessary for reasons of health, safety or the preservation of life.

10. Restriction on disclosure of data or documentation by the Competent Authority

(1) The Competent Authority shall treat all data and documentation obtained or generated in the course of his duties as confidential and such data and documentation is subject to non-disclosure obligations; and

(2) Subject to subsection (3), personnel of the Competent Authority shall refrain from disclosing any confidential data or documentation, except as expressly authorised by law or with the explicit consent of the parties involved.

(3) Personnel of the Competent Authority may disclose confidential data or documentation under the following circumstances –

- (a) when required by law or court order, subject to any applicable legal procedures and safeguards;
- (b) when necessary to fulfil the purposes for which the data or documentation was collected, provided that such disclosure is in accordance with the applicable laws, and privacy protections; and
- (c) when disclosure is required to safeguard national security, public safety, or the prevention, detection, investigation, or prosecution of serious crimes,

including terrorist offences, subject to the applicable legal framework and relevant procedures.

- (4) The Competent Authority shall —
- (a) manage all disclosed data or documentation in compliance with applicable data protection laws;
 - (b) establish and maintain appropriate technical, organisational, and administrative measures to protect the confidentiality, integrity, and security of the disclosed data or documentation;
 - (c) restrict access to disclosed data or documentation to authorised personnel who have a legitimate need-to-know for the performance of their duties;
 - (d) implement access controls, user authentication mechanisms, and monitoring systems to prevent unauthorised access or disclosure of the data or documentation;
 - (e) prohibit its personnel from making any unauthorised disclosure of confidential data or documentation, both during and after their employment or engagement with the authority; and
 - (f) implement disciplinary measures and legal remedies to address any unauthorised disclosure, including imposing penalties, suspension, or termination of employment, as considered appropriate.

11. Advance Passenger Information and Passenger Name Record access

(1) No government department or agency shall have direct access to API data and PNR data that is maintained by the Competent Authority and the PIU.

(2) Notwithstanding subsection (1), the Competent Authority may, pursuant to a written request from another government department or agency, grant limited access to the Advance Passenger Information and the Passenger Name Record data.

(3) All data shall be validated by the Competent Authority before it is transmitted to the requesting government department or agency.

(4) No person shall, without authorization, access, attempt to access, facilitate access to or cause access to API and PNR that is maintained by the Competent Authority and the PIU.

(5) A person who contravenes subsection (4) commits an offence and is liable on summary conviction to a fine of twenty thousand (USD\$20,000.00) United States dollars or imprisonment for a term of two years, or to both such fine and imprisonment.

12. Processing of API and PNR

(1) The PIU shall process API and PNR data for the following purposes –

- (a) conducting risk assessment of passengers and crew before their scheduled arrival in or departure from Antigua and Barbuda to identify individuals who require further examination for potential involvement in terrorist related activities or serious crimes;
- (b) responding, to requests received from other competent authorities and government agencies for specific cases, aimed at preventing, detecting, investigating, and prosecuting terrorist offenses or serious crimes; and
- (c) analysing API and PNR data to update or establish new criteria used in the assessments mentioned in paragraph (a) above to identify individuals involved in terrorist offenses or serious crimes.

(2) PNR data shall not be processed in such a manner as to reveal an individual's sensitive data and where PNR data reveals sensitive data, the PNR data shall be deleted immediately by the PIU.

(3) When conducting a risk assessment under subsection (1)(a), the PIU may-

- (a) compare API data and PNR data with authorised databases for the purpose of preventing, detecting, investigating, and prosecuting terrorist offenses or serious crimes, including databases of wanted persons or objects, as permitted by law; or
- (b) analyse API data and PNR data using non-discriminatory criteria and share results with the relevant authorities.

(4) The assessment of passengers and crew prior to their arrival in or departure from Antigua and Barbuda carried out under subsection (1)(a) against established criteria shall be carried out in a non-discriminatory manner.

(5) Criteria used in the assessment of passengers and crew shall —

- (a) be targeted, proportionate and specific in nature; and
- (b) be regularly reviewed in consultation with the Competent Authority and IMPACS.

(6) Notwithstanding subsection (5), a criterion for the assessment of passengers shall not, in any circumstance, be based on race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life or sexual orientation.

(7) Where PNR data collected includes data other than those listed in Schedule II any such data shall be deleted immediately and permanently upon receipt.

(8) The storage, processing and analysis of API data and PNR data shall be carried out exclusively within a secure location or locations within Antigua and Barbuda as designated by the Minister.

(9) PNR data collected in accordance with this Act shall be processed only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime and for border security purposes.

(10) Notwithstanding, subsection (9), in exceptional cases, PNR data may be processed, where necessary, for the protection of the vital interests of any individual, such as the risk of death, serious injury or threat to life or health.

(11) The Competent Authority may share PNR data with national Ministries, Departments and Agencies, where required under any enactment and in accordance with data protection principles and international best practices.

13. Verification of API and PNR data submitted to the Competent Authority and IMPACS

(1) The Competent Authority and IMPACS shall establish a robust system for the verification of API and PNR data submitted by aircraft or vessels, ensuring the accuracy, integrity, and reliability of the data collected, and the verification process shall be conducted in accordance with applicable laws, regulations, and data protection principles.

(2) The Competent Authority and IMPACS shall employ appropriate mechanisms and tools to validate the API data and PNR data provided by the captain or agent of an aircraft or the master or agent of a vessel which may include cross checking the data against reliable and authoritative sources, such as travel documents, identity databases or immigration records.

(3) The API data and PNR data shall be subject to risk assessment and analysis to identify potential anomalies, discrepancies, or patterns that may require further investigation or action.

(4) Where discrepancies or inconsistencies are identified during the verification process, the Competent Authority and IMPACS shall immediately notify the captain or agent of the relevant aircraft, the master or agent of the relevant vessel or submitter of API data and PNR data, following which the captain, master, agent or submitter shall be given an opportunity to rectify the discrepancies within a prescribed timeframe.

14. Use, screening and sharing of API and PNR with regional and international security agencies

(1) The Competent Authority and **IMPACS** shall use **API** data and **PNR** data to conduct screening of passengers and crew on an aircraft or a vessel that —

- (a) arrives in, departs from and transits through Antigua and Barbuda; and
- (b) travels within **CARICOM** in order to provide information to assist the Competent Authority and **IMPACS**, as required, and other Participating States,

against Watch Lists and approved national, regional, and international databases.

(2) The Minister shall approve national, regional and international databases to be used to conduct screenings.

(3) **CONSLE** may, from time to time, identify and update the list of approved national, regional, and international databases which are to be used to conduct screenings referred to in subsection (1).

(4) The Competent Authority and **IMPACS** may share the information contained within the **CARICOM APIS** with **INTERPOL** and any other national, regional or international intelligence, law enforcement or security agencies or centres approved by **CONSLE** in order to further national, regional or international security.

(5) **API** data and **PNR** data shall only be used for the purposes of this Act and, subject to access granted by the Competent Authority under section 11(2), to inform national compilation of statistics by Government Ministries, Departments and Agencies authorised to do so.

15. Transfer of API and PNR data to Competent Authority in another country

(1) The Competent Authority or **IMPACS** may transmit **API** data and **PNR** data to the competent authority in another country only —

- (a) in accordance with this Act; and
- (b) on ascertaining that the recipient country intends to use the data in a manner consistent with this Act.

(2) Where the level of management and protection of data in the recipient country is lower than in Antigua and Barbuda, any conflict between the provisions of this Act and enactments of a recipient country, shall be resolved prior to the transfer of data referred to in subsection (1).

(3) The Competent Authority and the competent authority of the recipient country shall resolve conflicts between the provisions of this Act and enactments in a recipient country by implementing appropriate safeguards.

(4) Appropriate safeguards may be provided for by –

(a) a legally binding and enforceable instrument between the Competent Authority in Antigua and Barbuda and the competent authority in the receiving country;

(b) binding corporate rules that are enforced by both Competent Authorities, and which expressly confer enforceable rights on a person whose API data and PNR data is requested to be transferred;

(c) a code of conduct the terms of which are agreed upon between the Competent Authority of Antigua and Barbuda and the receiving country and which has binding and enforceable commitments of the competent authority of the receiving country to apply appropriate safeguards, including as regards to the rights of the person whose API data and PNR data is being transferred; or

(d) contractual clauses between the Competent Authority of Antigua and Barbuda and the competent authority of the receiving country to apply appropriate safeguards, including as regards to the rights of the person whose API data and PNR data is being transferred.

PART IV API OPERATING PROVISIONS

16. Duty to transmit API

(1) A captain, master or agent of an aircraft or a vessel shall, via the CEMSIW, provide to the Competent Authority and IMPACS the relevant API data relating to the aircraft or vessel as set out in Schedule III and in accordance with the timeframes stipulated in Schedule IV.

(2) A captain, master or an agent of an aircraft or vessel, the Competent Authority and IMPACS shall collect, receive, process, store, retain, and transfer all API data in accordance with general data protection principles.

(3) In addition to any information provided pursuant to subsection (1), the Competent Authority may —

- (a) question any captain, master, agent, crew member or passenger in relation to the aircraft or vessel; or
- (b) request any person within the category of persons mentioned in paragraph (a) to immediately produce any document within that person's possession or control in relation to the questions put to the person.

(4) No captain, master, agent, crew member or passenger shall refuse to answer a question or knowingly give a false answer to any questions put to him by the Competent Authority pursuant to subsection (3) (a).

(5) A captain, a master, an agent, a crew member or a passenger who contravenes subsection (4) commits an offence and, where the contravention constitutes –

- (a) a first offence, the captain, master, agent, crew member or passenger is liable on summary conviction to a fine of five thousand (USD\$5,000.00) United States dollars; and
- (b) a second or repeating offence, is liable on summary conviction to a fine of twenty thousand (USD\$20,000.00) United States dollars or imprisonment for a term of six months, or to both such fine and imprisonment.]

(6) No captain, master, agent, crew member or passenger shall refuse to produce any document within that person's possession or control, or delay the production of a document, requested under subsection 3(b).

(7) A person who contravenes subsection (6) commits an offence and, where the contravention constitutes -

- (a) a first offence, is liable on summary conviction to a fine of five thousand (USD\$5,000.00) United States dollars; and
- (b) a second or repeating offence, is liable on summary conviction to a fine of twenty thousand (USD\$20,000.00) United States dollars or imprisonment for a term of six months, or to both such fine and imprisonment.]

(8) The Minister may waive the requirements of subsection (1) in such circumstances, and subject to such conditions, as the Minister may prescribe where the aircraft or vessel is —

- (a) a military or law enforcement aircraft or vessel;
- (b) on official Government business; or
- (c) on the business of a humanitarian organisation.

17. API Data Elements

A captain, a master or an agent of an aircraft or a vessel arriving in, departing from or transiting through Antigua and Barbuda shall, through the CEMSIW, transmit API data to the Competent Authority and IMPACS in a manner consistent with the list of API data elements set out in Schedule III and in accordance with the timeframes stipulated in Schedule IV.

18. Timeframe for submission of API data and embarkation and disembarkation data

(1) API data shall be submitted to the Competent Authority and IMPACS, through CEMSIW, in accordance with the timelines set out in Schedule IV (A).

(2) In the event of technical failure, a captain, a master or an agent shall transmit API data by any other appropriate electronic means, in accordance with the timelines set out in Schedule IV (A), ensuring the application of the appropriate level of data security.

(3) Embarkation and disembarkation data shall be submitted to the Competent Authority and IMPACS, through CEMSIW, in accordance with the timelines set out in Schedule IV (B).

19. Protection of API data

(1) An individual may, in the prescribed form and manner and in accordance with data protection principles and national enactments governing data protection and data privacy—

- (a) submit a request to the Competent Authority to gain access to his or her API data to check and verify its accuracy; and
- (b) where appropriate, request the correction of his or her data.

(1) The Competent Authority shall, in the prescribed form and manner –

- (a) respond to a request made under subsection (1); and
- (b) where appropriate, correct the individual's API data.

(3) An individual shall have the right to lodge a complaint before the Data Protection Officer if he or she considers that the processing of his or her API data is not in compliance with the provisions of this Act or the Data Protection Act.

20. Retention of API data

(1) API data collected under this Act for screening purposes shall be retained for a period not exceeding seven years from the date of travel of the passenger or crew member.

(2) On expiry of the data retention period stipulated under subsection (1), API data shall be deleted from each database in which they were stored, except if needed in connection with a specific case, a threat or a risk identified as being related to terrorism, serious crime or border security.

(3) Nothing contained in subsection (1) applies to the data copied from CARICOM APIS into any other security database system to which a different data retention schedule applies.

(4) Any security database that stores API data which has been sourced or copied from CARICOM APIS shall apply, at a minimum, equal levels of protection and privacy as applied by CARICOM APIS in accordance with data protection principles and international best practices.

21. Duty to provide API data in accordance with Act

(1) A captain, a master or an agent shall provide API data in accordance with this Act.

(2) Subject to subsection (5), a captain, a master or an agent who contravenes subsection (1) commits an offence and, where the contravention constitutes –

- (a) a first offence, is liable on summary conviction to a fine of five thousand (USD\$5,000.00) United States dollars; and
- (b) a second or repeating offence, is liable on summary conviction to a fine of twenty thousand (USD\$20,000.00) United States dollars or imprisonment for a term of six months, or to both such fine and imprisonment.

(3) No captain, master or agent shall intentionally or recklessly –

- (a) provide erroneous, faulty, misleading, incomplete, or false API; or
- (b) engage in, or facilitate API transfer in an incorrect format;

(4) Subject to subsection (5), a captain, a master or an agent who contravenes subsection (3) commits an offence and, where the contravention constitutes –

- (a) a first offence, is liable on summary conviction to a fine of five thousand (USD\$5,000.0) United States dollars; and

- (b) a second or repeating offence, is liable on summary conviction to a fine of twenty thousand (USD\$20,000.00) United States dollars or imprisonment for a term of six months, or to both such fine and imprisonment.

(5) Where the API data provided is inaccurate and the captain, master or agent of the aircraft or vessel satisfies the Competent Authority that the error was not made knowingly or recklessly then, notwithstanding any other provision of this Act, the captain, master or agent may not be charged for an offence pursuant to subsection (2) or (4) and no administrative penalty shall be imposed on him.

(6) A passenger or crew member –

- (a) shall provide embarkation data and disembarkation data in accordance with this Act; and
- (b) shall not intentionally or recklessly provides erroneous, misleading, incomplete, or false data.

(7) A passenger or crew member who contravenes subsection (6) commits an offence and is liable on summary conviction to a fine of four hundred (USD\$400.00) United States dollars or to imprisonment for a term of six months.

PART V PNR OPERATING PROVISIONS

22. Obligations of captain or agent of aircraft regarding the transfer of PNR data

(1) In accordance with this Act, a captain or an agent of an aircraft shall, using the push method via the CEMSIW, transfer to the Competent Authority and IMPACS PNR data which it has collected in the normal course of business in respect of passengers to be carried by the aircraft into and out of Antigua and Barbuda.

(2) Where a flight in respect of which PNR data is required to be collected and transmitted is code-shared between one or more aircraft, a captain or agent of the operating carrier shall transmit the PNR data of all passengers on the flight to the Competent Authority and IMPACS.

(3) A captain or an agent of an aircraft shall transfer PNR data to the Competent Authority and IMPACS by electronic means in accordance with the timelines stipulated in Schedule V.

(4) A captain or an agent of an aircraft may, when providing updated passenger information, limit the transmission of PNR data to an update of the information previously provided.

(5) A captain or an agent of an aircraft shall also transfer PNR data to the Competent Authority and IMPACS on a case-by-case basis, at the request of the Competent Authority and IMPACS at times other than those provided for in subsection (3) where access to that data is required in order to respond to a specific and actual threat related to terrorist offences or serious crime.

(6) A captain or agent of an aircraft shall maintain records of PNR data transfers, including the date, time and details of the transmission, for a specified period as required by the Competent Authority.

(7) A captain or an agent of an aircraft shall cooperate fully with the Competent Authority and IMPACS in relation to the transfer of PNR data, providing any additional information or assistance as required for the purpose of national security, law enforcement or other authorised purposes.

(8) A captain or an agent of an aircraft shall comply with all requirements under this Act.

23. Obligations of master or agent of vessel regarding the transfer of PNR data

(1) A master or an agent of a vessel shall, in accordance with this Act, transfer by the push method to the Competent Authority and IMPACS via the CEMSIW all PNR data which it has collected in the normal course of business in respect of passengers and crew to be carried by that vessel into and out of Antigua and Barbuda.

(2) Where a commercial vessel or private vessel in respect of which PNR data is required to be collected and transmitted is code-shared between one or more vessels, a captain or an agent of the operating carrier shall transmit the PNR data of all passengers and crew on the vessel to the Competent Authority and IMPACS.

(3) A master or an agent of a vessel shall transfer PNR data to the Competent Authority and IMPACS by electronic means in accordance with the timelines specified in Schedule I.

(4) A master or an agent of a vessel, when providing updated passenger information, may limit the transmission of PNR data to an update of the information previously provided.

(5) A master or an agent of a vessel shall also transfer PNR data to the Competent Authority and IMPACS on a case-by-case basis, at the request of the Competent Authority and IMPACS at times other than those provided for in subsection (3) where access to that data is required in order to respond to a specific and actual threat related to terrorist offences or serious crime.

(6) A master or an agent of a vessel shall maintain records of PNR data transfers, including the date, time and details of the transmission, for a period specified by the Competent Authority.

(7) A master or an agent of a vessel shall cooperate fully with the Competent Authority and IMPACS in relation to the transfer of PNR data, providing any additional information or assistance as required for the purpose of national security, law enforcement or other authorised purposes.

(8) A master or an agent of a vessel shall accurately complete and submit information, including such information related to health, crew effects, ship stores and dangerous goods to the Competent Authority and IMPACS, through the CEMSIW for processing, in accordance with the data elements as reflected in Schedule VI, pursuant to the FAL Convention, as updated.

(9) A master or an agent of a vessel shall comply with all requirements under this Act.

24. PNR data transfer method and format

(1) Subject to subsections (3) and (4), the captain or agent of an aircraft or the master or agent of a vessel arriving at, departing from or transiting through Antigua and Barbuda shall transfer PNR data, collected in the course of their normal business operations to the Competent Authority and IMPACS through the CEMSIW by the push method, using the PNRGOV message format.

(2) The captain or agent of an aircraft or the master or agent of a vessel arriving at, departing from or transiting through Antigua and Barbuda shall not be required to filter PNR data prior to the transmission of the data to the Competent Authority and IMPACS.

(3) In the event of a technical failure, or any other exceptional case, the captain or agent of an aircraft or the master or agent of a vessel shall transfer PNR data by any other appropriate electronic means as an alternative to the push method.

(2) The PNR data to be transmitted under this section shall be consistent with the data elements set out in Schedule II.

25. Transmission timeframe for PNR data

(1) Subject to subsection (2), the captain, master or agent of an aircraft or a vessel operating a flight or voyage arriving at, departing from or transiting through Antigua and Barbuda shall transfer PNR data to the Competent Authority and IMPACS in accordance with Schedule I or Schedule V, as the case may be.

(2) In the event of a cancellation of a scheduled flight or voyage after the first transmission of PNR data, no further transmission shall be required.

(3) Where access to PNR data is required to respond to a specific threat to the public or in the interest of national security, an aircraft or a vessel shall be required to provide the Competent Authority and IMPACS, with PNR data prior to, between, or after the scheduled transmission timelines specified in Schedule I or V, as the case may be.

26. Automated processing of PNR data

(1) Automated processing of PNR data shall be based on objective, precise and reliable criteria that effectively indicate the existence of a risk, without leading to unlawful differentiation among individuals.

(2) Automated processing of PNR data shall not be discriminatory.

(3) In accordance with national enactments related to data protection and data privacy, a decision which produces significant adverse actions on individuals, affecting their legal interests, rights or other legal entitlements, as provided for under national enactments, shall not be made on the sole basis of the automated processing of PNR data.

27. Sensitive data

(1) Subject to subsection (3), no person shall process PNR data that is sensitive data.

(2) Subject to subsection (3), PNR data containing sensitive data shall be immediately deleted if received by the Competent Authority and IMPACS.

(3) Notwithstanding subsections (1) and (2), sensitive data may be processed in exceptional and immediate circumstances to protect the vital interests of an individual.

28. PNR data and document retention

(1) PNR data provided by a captain or an agent of an aircraft, or a master or agent of a vessel to the Competent Authority and IMPACS shall be retained in a database of the Competent Authority and IMPACS for a period of seven years after its transfer.

(2) PNR data transferred in accordance with subsection (1) shall be deleted permanently upon the expiration of the period of seven years after the PNR data is transferred.

(3) PNR data or the results of the processing of such data that have been transferred to a Competent Authority by the PIU shall be deleted permanently —

- (a) on the expiration of a period of seven years after they were transferred; or
- (b) where the data were retained for the purpose of the prevention, detection, investigation or prosecution of a terrorist offence or serious crime and proceedings for such offence are brought against any person, on the day on which final judgment is given in the proceedings,

whichever occurs later.

(4) The Competent Authority shall retain the result of the assessment of passengers and crew for as long as is necessary to inform the competent authorities and passenger information units of other Participating States of a positive match.

(5) Where the result of automated processing has, following individual review by non-automated means, proven to be negative it may be retained to avoid future false positive matches for as long as the underlying data are not destroyed in accordance with this Act.

(6) The PIU, under the supervision of the Competent Authority shall maintain documentation relating to all of its processing systems and procedures and that documentation shall contain at least —

- (a) the name and contact details of the organisation and personnel of the PIU entrusted with the processing of PNR data and the different levels of access authorisation;
- (b) the requests made by the competent authorities and the PIUs of other Participating States; and
- (c) all requests for and transfers of PNR data to a third country.

(7) The PIU shall keep records of its processing operations involving collection, consultation, disclosure and erasure of PNR data.

(8) Records kept under subsection (7) in relation to consultation and disclosure shall show, in particular —

- (a) the purpose, date and time of such operations; and
- (b) as far as possible, the identity of the member of staff of the PIU who consulted or disclosed the PNR data and the identity of the recipients of those data.

(9) Records kept under subsection (7) shall be —

- (a) used solely for the purposes of verification, self-monitoring, ensuring data integrity and security, and auditing; and
- (b) kept for a period of seven years.

(10) The PIU shall, on request, make available to the Data Protection Officer all documentation required to be maintained under this Act.

(11) The PIU shall put in place and implement appropriate technical and organisational measures and procedures to ensure a high level of security appropriate to the risks represented by the nature and processing of PNR data.

(12) Where a personal data breach occurs and this is likely to result in a high risk to the protection of the personal data concerned or affect the privacy of the data subject adversely, the breach shall be communicated to the data subject and to the Data Protection Officer without undue delay.

29. Depersonalisation and anonymisation of PNR data

(1) PNR data transferred by a captain or an agent of an aircraft, or a master or an agent of a vessel to the Competent Authority and IMPACS via the CEMSIW shall, after a period of six months from the date of the transfer, be depersonalised, no longer enabling direct identification of the passengers or crew, except when used in connection with an identifiable ongoing case, threat or risk related to the purposes stipulated in this Act or investigations.

(2) The following data elements shall be removed to facilitate the depersonalisation of PNR data referred to in subsection (1) –

- (a) passenger and crew name or names, including the names of other passengers and crew on the PNR and number of passengers and crew on the PNR travelling together;
- (b) address and contact information;
- (c) all forms of payment information, including billing address, to the extent that it contains any information which could serve to directly identify the passenger and crew to whom the PNR data relate, or any other person;
- (d) frequent flyer or traveller information;
- (e) any general remarks relating to the PNR data to the extent that they contain any information which could serve to directly identify the passenger and crew to whom the PNR data relate; and

(3) Depersonalised data shall be retained for statistical, analytical or research purposes, provided that it does not infringe upon the privacy rights of the individuals.

(4) PNR data may be re-personalised only if needed in connection with an identifiable ongoing case, threat or risk related to the purposes stipulated in this Act, upon authorisation by the appropriate authority.

(5) PNR data shall be deleted or anonymised after it has been retained for a period of seven years, except when used in connection with an identifiable ongoing case, threat or risk related to the purposes stipulated in this Act.

(6) Nothing contained in subsection (1) applies to PNR data copied from the databases managed by the Competent Authority and IMPACS into any other security database system to which a different data retention schedule applies.

(7) Any security database that stores PNR data which has been sourced or copied from databases managed by the Competent Authority and IMPACS shall apply, at a minimum, equal levels of protection and privacy in accordance with data protection principles and international best practices.

30. National oversight

The Data Protection Officer shall provide national oversight for the protection of PNR data.

31. Competent Authority and PIU to liaise with Regional Data Protection Officer

(1) The Competent Authority and the PIU shall liaise with and provide the requisite support and information to the Regional Data Protection Officer.

(2) The Competent Authority and IMPACS shall provide the Regional Data Protection Officer with the information necessary for him or her to perform his or her duties and tasks effectively and independently.

(3) The Regional Data Protection Officer shall have access to all data pertinent to the processing of API and PNR by the Competent Authority and IMPACS.

(4) In circumstances where the Regional Data Protection Officer considers that the processing of any data has not been lawful or was not done in accordance with this Act, the Regional Data Protection Officer may refer the matter to the Executive Director of IMPACS.

(5) The Regional Data Protection Officer shall coordinate and collaborate with the national data protection officers of Participating States.

32. Competent Authority and PIU to liaise with Data Protection Officer

(1) The Competent Authority and PIU shall liaise with and provide the requisite support and information to the Data Protection Officer who shall be appointed in accordance with relevant national enactments.

(2) The Competent Authority and the PIU shall provide the Data Protection Officer with the resources and information to perform his or her duties and tasks effectively and independently.

(3) The Data Protection Officer shall have access to all data processed by the Competent Authority.

(4) In circumstances where the Data Protection Officer considers that the processing of any data has not been lawful or was not done in accordance with this Act, the Data Protection Officer may refer the matter to the Competent Authority.

33. Safeguards and redress mechanisms

(1) An individual shall have the same right to the protection of his or her personal data, including the right to be informed, the right of access, the right of rectification and the right to an adequate remedy, in accordance with the Data Protection Act, 2013, best practices and national enactments and policy in relation to the protection of personal data.

(2) An agent of an aircraft or a vessel shall inform every passenger of his rights related to the protection of his or her personal data referred to in subsection (1).

(3) An individual shall have the right to lodge a complaint before the Data Protection Officer in circumstances where he or she considers that the processing of his or her personal data constitutes a violation of this Act.

34. Contravention of this Part

- (1) A captain, a master or an agent who contravenes a section in this Part commits an offence.
- (2) Subject to section 37, where a contravention referred to in subsection (1) constitutes –
 - (a) a first offence, the captain, master or agent is liable on summary conviction to a fine of five thousand (USD\$5,000.00) United States dollars; and
 - (b) second or repeating offence, the captain, master or agent is liable on summary conviction to a fine of twenty thousand (USD\$20,000.00) United States dollars or imprisonment for a term of six months, or to both such fine and imprisonment.

35. Conflict of laws regarding transmission of PNR

In the event of a conflict of laws between the provisions of this Part and those of the legislation of another country regarding the transmission of PNR data by an aircraft or a vessel, the penalties provided for under this Part shall be suspended during the period the authorities of the two States are attempting to resolve the conflict and until it is demonstrated that the two States have attempted to resolve the conflict.

PART VI ADMINISTRATIVE PENALTIES

36. Certain contraventions may be dealt with administratively

- (1) This Part applies to contraventions of the provisions of Part IV and Part V.
- (2) Any person who contravenes any of the provisions of Part IV or Part V may, with their consent, pay an administrative penalty, as prescribed in Regulations made under this Act, in lieu of court proceedings.

37. Notice respecting administrative penalty

(1) If the Competent Authority reasonably suspects that a person contravened a provision referred to in Part IV or Part V, the Competent Authority shall, before making a determination, issue to the person a notice, in writing.

- (2) A notice issued under subsection (1) shall –
 - (a) be in the prescribed form;
 - (b) include the name of the person who is the subject of the notice;
 - (c) specify the section that the person is alleged to have contravened;
 - (d) set out the circumstances alleged to constitute the contravention to which the notice relates;
 - (e) inform the person, in clear language, of the person's right to make representation under section 38;
 - (f) inform the person that a request to make a representation shall be submitted within 30 days after the date on which the person receives the notice, failing which the Competent Authority shall, immediately make a determination in lieu of representation; and
 - (g) a preliminary assessment of the amount of the administrative penalty.

38. Opportunity to make representations

(1) Before making a determination in respect of an alleged contravention of a section referred to in section 36, the Competent Authority shall provide the person referred to in section 37(1) the opportunity to make representations in respect of the alleged contravention.

(2) A person who wishes to make representations pursuant to subsection (1) shall, in writing, submit a request to the Competent Authority within 30 days after the date on which the person receives the notice issued under section 37(1).

(3) Subject to subsection (4), if a person makes a request in accordance with subsection (2), the Competent Authority shall –

- (a) conduct a written, electronic or oral hearing, or any combination thereof, as the Competent Authority, in his sole
- (b) determine the circumstances and the place in which, and the process by which, the hearing shall be conducted; and
- (c) by notice in writing, specify the form and content of materials to be provided for the hearing and the deadline for the submission of materials.

(4) If a person fails to submit materials to the Competent Authority in accordance with what is specified under subsection (3)(c), the Competent Authority is not required to conduct a hearing and shall immediately proceed to make a determination and issue a decision in respect of the alleged contravention.

39. Hearing and decision

(1) Where a person makes a request under section 38(2) and, where required, submits any materials in accordance with a notice issued under section 38(3)(c), the Competent Authority shall, within forty (40) days of receipt of the request and the submission any materials, conduct a hearing in respect of the alleged contravention.

(2) Within twenty-one (21) days of the date of completion of representations, the Competent Authority shall make a determination in respect of the alleged contravention and issue a decision, in writing.

(3) If, on a balance of probabilities, the Competent Authority is satisfied that a person has contravened a provision referred to in section 36, the Competent Authority shall serve the person with a decision requiring the person to pay an administrative penalty in the amount specified in the decision.

(4) A decision shall –

- (a) be in the prescribed form;
- (b) specify reasons for the decision;
- (c) specify the name of the person who is liable for the administrative penalty;
- (d) set out the contravention in relation to which the administrative penalty is imposed;
- (e) specify the amount of the administrative penalty;
- (f) specify the date by which the administrative penalty is to be paid; and
- (g) notify the person of his or her right to appeal to the High Court.

(5) An administrative penalty shall be paid within the deadline specified in the notice issued under subsection (4).

(6) Where an administrative penalty is imposed under this Part, a prosecution for an offence under this Act in respect of the same contravention may not be brought against the person.

(7) If the Competent Authority does not, within twenty-one (21) days after the person has made representations under this Part, issue a decision in respect of the alleged contravention, the Competent Authority shall notify the person, in writing, that he is not required to pay an administrative penalty.

40. Appeals

(1) A person aggrieved by a decision of the Competent Authority made under this Part may, within the prescribed period and in the prescribed manner, appeal to the High Court.

(2) The decision of the High Court is final.

41. Correction of decision

(1) The Competent Authority may, within 15 days of issuing a decision under section 39, amend the decision to correct –

- (a) a typographical error, arithmetical error or other similar error; or
- (b) an obvious error or omission.

(2) The discretion given to the Competent Authority under subsection (1) is exercisable with or without a hearing and –

- (a) on the initiative of the Competent Authority; or
- (b) at the request of the person who is the subject of the decision.

(3) If the Competent Authority corrects a decision under subsection (1) the Competent Authority shall give notice in writing to the person who is the subject of the decision.

42. Absolute liability

A requirement that a person pay an administrative penalty applies even if the person exercised due diligence to prevent the contravention or failure in relation to which the administrative penalty is imposed.

43. Assessment of quantum of administrative penalty

(1) In establishing the amount of an administrative penalty in a particular case, a director must consider the following matters, if applicable –

- (a) the nature of the contravention or failure;
- (b) the real or potential adverse effect of the contravention or failure;
- (c) whether the contravention or failure was deliberate;
- (d) any economic benefit derived by the person from the contravention or failure;
- (e) whether the person exercised due diligence to prevent the contravention or failure;
- (f) the person's efforts to correct the contravention or failure;
- (g) the person's efforts to prevent the recurrence of the contravention or failure; and
- (h) any other factors that, in the opinion of the Competent Authority, are relevant.

(2) If the contravention or failure continues for more than one day, separate administrative penalties, each not exceeding the applicable maximum administrative penalty, may be imposed for each day the contravention or failure continues.

44. Deadline for payment of administrative penalty

A person who is the subject of a decision made under this Part shall pay the administrative penalty within thirty (30) days after the later of –

- (a) the date the decision is served on the person;
- (b) if the decision was corrected under section 43, the date in which the person received the notice of correction;
- (c) if the person appeals the imposition of the administrative penalty -

- (i) the date the person receives a copy of the order of the Court, if the Court confirms or varies the administrative penalty; or
- (ii) the date on which a new decision is served on the person, if the Court sends the matter back to the Competent Authority with directions.

45. Recovery of administrative penalties

(1) Subject to a decision of the Court cancelling a decision made under section 41, an administrative penalty imposed under this Part may be recovered as a debt due to the government.

(2) If a person fails to pay an administrative penalty, the Competent Authority may file a certificate in a court that has jurisdiction and, upon filing, the certificate has the same force and effect, and all proceedings may be taken on it, as if it was a judgement of the court with which it is filed.

(3) A certificate filed under subsection (2) may be in the prescribed form, shall be signed by the Competent Authority and shall contain –

- (a) the name of the person who is liable for the penalty;
- (b) the contravention in relation to which the penalty is imposed; and
- (c) the amount of the penalty.

46. Consolidated Fund

All revenue derived from administrative penalties shall be paid into the Consolidated Fund.

47. Limitation Period

A notice under section 37 may not be served more than 3 years after the later of –

- (a) the date the alleged contravention to which the notice relates occurred; or
- (b) the date on which evidence of the alleged contravention first came to the knowledge of the Competent Authority.

PART VII
EXCHANGE OF PNR DATA WITH OTHER PARTICIPATING STATES

48. Transfer of PNR data by the Competent Authority or PIU to other Participating States

(1) Subject to subsection (4) and upon receiving a request from the competent authority of a Participating State, the Competent Authority may share PNR data with the competent authority of the Participating State in accordance with applicable laws, regulations, and international agreements.

(2) The transfer of PNR data shall be limited to the purposes specified under this Act, including national security, public safety, immigration control, and the prevention, detection, investigation, and prosecution of serious crimes, including terrorist offences.

(3) The PIU, acting on the approval and guidance of the Competent Authority, shall transfer PNR data in compliance with data protection laws and regulations, including appropriate security measures to safeguard the confidentiality, integrity, and protection of the data during transmission and at the receiving end.

(4) The Competent Authority shall transfer PNR data when there is a lawful basis and a demonstrated necessity for such transfer, as determined by the Competent Authority.

(5) The Competent Authority shall assess the proportionality and necessity of the transfer, considering factors such as the gravity of the threat, the relevance of the data, and the availability of alternative means to achieve the stated purposes.

(6) The PIU, acting on the approval and guidance of the Competent Authority, shall transfer the necessary and proportionate PNR data required for the specified purposes, ensuring that the transferred data is limited to what is essential and relevant.

(7) The Competent Authority shall establish clear guidelines regarding the retention periods of transferred PNR data by the competent authority of the receiving Participating States, ensuring that the data is retained for no longer than necessary for lawful purposes.

(8) The PIU, acting on the approval and guidance of the Competent Authority, shall engage in mutual assistance and information exchange with the competent authority of the receiving Participating States, ensuring timely and efficient sharing of relevant information related to the transferred PNR data.

(9) The PIU shall establish mechanisms to facilitate feedback, communication, and coordination with the receiving entities, addressing queries, providing clarifications, and responding to requests for additional information or cooperation.

(10) The Competent Authority shall oversee and monitor the transfer of PNR data by the PIU, ensuring compliance with the legal provisions and applicable agreements.

(11) The Competent Authority shall establish an accountability framework to assess the lawfulness, necessity, and effectiveness of the transfers, conducting periodic audits, and assessments to evaluate the compliance of the PIU with the established requirements.

(12) The Competent Authority shall provide regular reports to relevant government bodies or legislative committees on the transfers of PNR data, including the number of transfers, the receiving entities, and the purposes for which the data was transferred.

(13) The Competent Authority shall establish a transparent transfer process, subject to the limitations imposed by law or national security considerations.

49. Another Participating State requests PNR data from Competent Authority

(1) Where a request for PNR data is received from the competent authority, or the passenger information unit, of another Participating State, but the data have not been depersonalised through masking out, the PIU in consultation with the Competent Authority may transmit any such information in its possession to the competent authority or passenger information unit of the requesting Participating State if it believes that transmitting the data is necessary for the purpose of preventing, detecting, investigating or prosecuting terrorist offences or serious crime.

(2) In exceptional circumstances, where a request for PNR data is received from a competent authority or passenger information unit of a Participating State at a time other than that provided for under this Act, the PIU may request the captain or agent of the aircraft or the master or agent of the vessel to transfer the requested PNR data and in turn transfer the PNR data to the competent authority in the requesting Participating State.

(3) A request made under subsection (2) can only be facilitated where there are reasonable grounds to believe that the data requested is necessary to respond to a specific and actual threat related to terrorist offences or serious crime.

50. Competent Authority or PIU requests PNR data from another Participating State

(1) The Competent Authority or the PIU may submit a request for PNR data to the competent authority, or the passenger information unit, of a Participating State where

there are reasonable grounds to believe that the request is necessary for the prevention, detection, investigation or prosecution of a terrorist offence or serious crime.

(2) A request made under subsection (1) may be based on one or more data elements and shall include the reasons for the request.

(3) The Competent Authority or the PIU may in exceptional circumstances, request the competent authority or passenger information unit of another Participating State to request the transfer of PNR data by a captain, a master or an agent of an aircraft or vessel to the passenger information unit of that Participating State at a time other than the time at which the aircraft transfers the PNR data to the passenger information unit of that Participating State and to transfer the PNR data to the passenger information unit where access to the PNR data is necessary to respond to a specific or actual threat related to terrorist offence or serious crime.

PART VIII MISCELLANEOUS

51. Requirement to submit information electronically

Information required to be submitted under this Act shall be submitted electronically.

52. Immunity from liability

(1) Any person acting under the direction of the Competent Authority or IMPACS shall not be held liable for any direct, indirect, incidental, consequential, or special damages including but not limited to financial loss, personal injury, or reputational harm, arising from or in connection with the collection, receipt, processing, use, disclosure, or transfer of API and PNR data.

(2) Subsection (1) shall not apply to any act or omission arising from negligence or wilful misconduct.

53. Regulations

(1) The Minister may make Regulations to give effect to the principles and provisions of this Act.

(2) Notwithstanding the generality of subsection (1), the Minister may make Regulations —

- (a) specifying the circumstances in which and the conditions under which the Minister may waive the requirements set out in section 18(1);

- (b) to provide for procedures for the gathering of information and the collaboration and sharing of information with the agencies mentioned in this Act;
- (c) determining the composition, procedural operations institutional and other arrangements of the PIU to ensure its effective and efficient operations;
- (d) designating Competent Authorities to receive API and PNR data;
- (e) establishing approved watchlists or criteria and databases to be used for national processing in conjunction with API and PNR data; and
- (f) any other matter required to be prescribed under this Act.

54. Non-Imposition of Penalties for Incomplete, Delayed or Erroneous messages resulting from technical issue

Notwithstanding any provision under this Act in respect of the imposition of penalties, an aircraft or vessel operator shall not be penalised or held otherwise responsible for incomplete, delayed or erroneous messages resulting from a technical issue.

55. Amendment of the Schedules

The Minister may, by Order published in the Gazette, amend the Schedules.

56. Repeal

The Advanced Passenger Information Act 2016, No. 3 of 2016 is hereby repealed.

SCHEDULE I

TIMELINES FOR ELECTRONIC SUBMISSION OF PNR DATA BY A MASTER OR AGENT OF A VESSEL

(Sections 8(1), 25(3) and 27)

(1) An aircraft shall transfer PNR data to the Competent Authority and IMPACS by electronic means via the CEMSIW in accordance with the following timelines -

(a) forty-eight (48) hours before the scheduled voyage departure time; and

(b) twenty-four (24) hours before the scheduled voyage departure time; and

(c) time zero which represents the actual time of departure, that is once the passengers and crew have boarded the vessel in preparation for departure and it is no longer possible for passengers and crew to board or leave; or

(d) in the event of technical failure or difficulty, by any other appropriate means with a tolerance of 30 minutes after the departure ensuring the same level of technical and organisational security.

(2) Where a voyage is cancelled, submissions in keeping with the timeframes articulated above prior to the cancellation are still required. Only submissions due after time of cancellation are not required.

(3) In emergency situations, submissions shall be made as soon as practicable where deemed necessary by the Competent Authority.

SCHEDULE II

PASSENGER NAME RECORD (PNR) DATA ELEMENTS

(Sections 10(1), 14(7) and 26(5))

(a) Passenger Name Record or PNR Data

As available in the traveller's Passenger Name Record in the Aircraft or Vessel Reservation System including all historical changes to the PNR listed which shall include

-

- (1) PNR record locator
- (2) Date of reservation or date of issue of ticket
- (3) Date(s) of intended travel
- (4) Name(s)
- (5) Address and contact information (telephone number, e-mail address)
- (6) All forms of payment information, including billing address
- (7) Complete travel itinerary for specific PNR
- (8) Frequent flyer information
- (9) Travel agency or travel agent
- (10) Travel status of passenger, including confirmations, check-in status, no show or go show information
- (11) Split or divided PNR information
- (12) General remarks (including all available information on unaccompanied children less than eighteen years of age, such as name and gender of the minor, language(s) spoken, name and contact details of the guardian on departure and relationship to the minor, name and contact details of guardian on arrival and relationship to the minor, departure and arrival agent)
- (13) Ticketing field information, including ticket number, date of ticket issuance and one-way tickets, automated ticket fare quote fields
- (14) Seat number and other seat information
- (15) Code share information
- (16) All baggage information
- (17) Number and other names of travellers on PNR
- (18) Any API data collected
- (19) All historical changes to the PNR listed in numbers 1 to 18

(b) Additional data elements -

- (i) Visa Number (if applicable)
- (ii) Issue Date of Visa
(Place where Visa is issued)
- (iii) Place of Issuance of the Visa (Place where Visa was issued)
- (iv) Other Document Number used for Travel (if applicable)
(The other document number used for travel when the official travel document is not required)
- (v) Type of Other Document used for Travel (supporting travel document)
(Indicator to identify the type of other document used for travel)
- (vi) Primary Residence -
 - (aa) Country of Primary Residence
(Country where passenger resides most of the year)
 - (bb) Address
(location identification such as - street name and number)
 - (cc) City
 - (dd) State or Province or County
 - (ee) Postal Code
- (vii) Destination Address -
 - (aa) Address where the passenger will be staying in the territory of disembarkation
 - (bb) City
 - (cc) State or Province or County
 - (dd) Postal Code

(c) Data relating to the Reporting Party -

- (i) Reporting Party Name
- (ii) Reporting Party Telephone Number
- (iii) Reporting Party Facsimile Number
- (iv) Reporting Party Electronic Mail Address

SCHEDULE III

ADVANCE PASSENGER INFORMATION DATA ELEMENTS AND EMBARKATION AND DISEMBARKATION DATA ELEMENTS

(Sections 10(4), 18(1) and (19))

(A) AIRCRAFT

(a) Data relating to the flight (Header Data)-

- (i) Flight Identification
(IATA or ICAO Airline code and flight number, Registration Number)
- (ii) Scheduled Departure Date
(Date of Scheduled departure of aircraft based on local time of departure location)
- (iii) Scheduled Departure Time
(Time of scheduled departure of aircraft based on local time of arrival location)
- (iv) Scheduled Arrival Date
(Date of the scheduled arrival of aircraft based on local time of arrival location)
- (v) Scheduled Arrival Time
(Time of scheduled arrival of aircraft based on local time of arrival location)
- (vi) Last Place or Port of Call of Aircraft
(Aircraft departed from this last foreign place or port of call to go to “place or port of aircraft initial arrival”)

- (vii) Place or Port of Aircraft Initial Arrival
(Place or port in the country of destination where the aircraft arrives from the last place or port of call of aircraft)
- (viii) Subsequent Place or Port of Call within the country or regional space
- (ix) Number of Persons on board including-
the total number of passengers on Board; and
the total number of crew members

(b) Data relating to each individual on board -

- (i) Official Travel Document Number
(Passport or other Government approved travel documents)
- (ii) Issuing State or Organisation of the Official Travel Document
(Name State or Organisation responsible for the issuance of the official document)
- (iii) Official Travel Document Type
(Indicator to identify type of official travel document)
- (iv) Expiration Date of Official Travel Document (Expiration date of the official travel document)
- (v) Surname or Given Name(s)
(Family name and given name(s) of the holder as it appears on the travel document)
- (vi) Nationality
(Nationality of the holder of the travel document)
- (vii) Date of Birth
(Date of birth of the holder)
- (viii) Gender
(Gender of the holder)
- (ix) Traveller's Status

(Passenger, crew, in-transit)

- (x) Place or Port of Original Embarkation
(Place or port on that journey where traveller first boarded for foreign travel)
- (xi) Port or Place of Clearance
(Place or port where the traveller is cleared by the border control agencies)
- (xii) Place or Port of Onward Foreign Destination
(Foreign place or port where the traveller is transiting)

(c) Data relating to the Reporting Party -

- (i) Reporting Party Name
- (ii) Reporting Party Telephone Number
- (iii) Reporting Party Facsimile Number
- (iv) Reporting Party Electronic Mail Address

(B) VESSEL

(a) Data relating to the voyage (Header Data) -

- (i) Vessel Identification
(IMO or Registration number)
- (ii) Country of Registration
(Country where the vessel is registered)
- (iii) Agent or Owner (where applicable)
(Name of Agent for the vessel or where no Agent, Name of Owner)
- (iv) Call Sign (if applicable)
- (v) Scheduled Departure Date
(Date of Scheduled departure of vessel based on local time of departure location)
- (vi) Scheduled Departure Time

(Time of scheduled departure of vessel based on local time of arrival location)

- (vii) **Scheduled Arrival Date**
(Date of the scheduled arrival of vessel based on local time of arrival location)
- (viii) **Scheduled Arrival Time**
(Time of scheduled arrival of vessel based on local time of arrival location)
- (ix) **Last Place or Port of Call of Vessel**
(Vessel departed from this last foreign place or port of call to go to “place or port of vessel initial arrival”)
- (x) **Place or Port of Vessel Initial Arrival**
(Place or port in the country of destination where the vessel arrives from the last place or port of call of vessel)
- (xi) **Subsequent Place or Port of Call within the country or regional space**
- (xii) **Number of Persons on board including-**
 - a. the total number of passengers on Board; and
 - b. the total number of crew members

(b) Data relating to each individual on board -

- (i) **Official Travel Document Number**
(Passport or other Government approved travel documents)
- (ii) **Issuing State or Organisation of the Official Travel Document**
(Name State or Organisation responsible for the issuance of the official document)
- (iii) **Official Travel Document Type**
(Indicator to identify type of official travel document)
- (iv) **Expiration Date of Official Travel Document**

(Expiration date of the official travel document)

- (v) Surname or Given Name(s)
(Family name and given name(s) of the holder as it appears on the travel document)
- (vi) Nationality
- (vii) Date of Birth
(Date of birth of the holder)
- (viii) Gender
(Gender of the holder)
- (ix) Traveller's Status (Passenger, crew, in-transit)
- (x) Place or Port of Original Embarkation
(Place or port on that journey where traveller first boarded for foreign travel)
- (xi) Port or Place of Clearance
(Place or port where the traveller is cleared by the border control agencies)
- (xii) Place or Port of Onward Foreign Destination
(Foreign place or port where the traveller is transiting)

(c) Data relating to the Reporting Party -

- (i) Reporting Party Name
- (ii) Reporting Party Telephone Number
- (iii) Reporting Party Facsimile Number
- (iv) Reporting Party Electronic Mail Address

(C) EMBARKATION AND DISEMBARKATION DATA

(a) Data elements relating to flight or voyage information -

- (i) Residential status
- (ii) Vessel Type
- (iii) Airline/Vessel name

- (iv) Airline/Vessel registration ID
- (v) Country of embarkation
- (vi) Port of embarkation
- (vii) Intended date of arrival

(b) Data elements relating to personal information -

- (i) First name
- (ii) Last name
- (iii) Gender
- (iv) Date of birth
- (v) Nationality
- (vi) Country of birth
- (vii) Country of residence
- (viii) Zip code
- (ix) State
- (x) City
- (xi) Address
- (xii) Email
- (xiii) Telephone number
- (xiv) Approval of processing information

(c) Data elements relating to document information -

- (i) Travel document type
- (ii) Travel document number
- (iii) Travel document issue country
- (iv) Travel document expiry date
- (v) Proof of travel document

(d) Data elements relating to destination information -

- (i) Purpose of visit
- (ii) Accommodation type
- (iii) Other accommodation type
- (iv) Destination name
- (v) Destination address
- (vi) Destination city
- (vii) Length of stay

(e) Data elements relating to health information -

- (i) Symptoms over the past seven 7 days
- (ii) Countries visited within the last 21 days

(f) Data elements relating to customs -

- (i) Total pieces of Luggage
- (ii) Bringing of plants and livestock
- (iii) Bringing of pharmaceuticals
- (iv) Bringing of narcotics
- (v) Bringing of weapons
- (vi) Bringing of commercial merchandise
- (vii) Bringing of currency
- (viii) Bringing of animal products
- (ix) Bringing of disease agents
- (x) Bringing of soil
- (xi) Items to declare

SCHEDULE IV

TIMEFRAME FOR SUBMISSION OF API AND EMBARKATION AND DISEMBARKATION DATA

(Sections 18(1), 19 and 20)

(A) Timeframe for submission of API

1. In case of commercial aircraft, no later than 40 minutes prior to departure from the last port of call.
2. In case of a private aircraft, no later than 40 minutes prior to the departure from the last port of call.
3. In case of a vessel arriving from outside the regional space, no later than 24 hours prior to arrival.
4. In case of a vessel arriving from a destination within the regional space, no later than 1 hour prior to the arrival of the vessel from the last port of call.
5. In the event of any changes to the flight or vessel header data or data relating to an individual on board, an updated API file is required prior to departure of the aircraft or vessel.
6. In emergency situations, submissions shall be made as soon as practicable where deemed necessary by the Competent Authority.

(B) Timeframe for submission of Embarkation and Disembarkation data

Passenger and Crew shall be required to submit embarkation and disembarkation data within 72 hours (including the day of arrival/departure) prior to their arrival into and departure from Antigua and Barbuda.

SCHEDULE V

TIMELINES FOR ELECTRONIC SUBMISSION OF PNR DATA BY A CAPTAIN OR AGENT OF AN AIRCRAFT

(Section 24(3) and 27)

An aircraft shall transfer PNR data to the Competent Authority and IMPACS by electronic means via the CEMSIW in accordance with the following timelines -

- (a) 48 hours before the scheduled flight departure time; and
- (b) 24 hour(s) before the scheduled flight departure time; and
- (c) time zero which represents the actual time of departure where flight closure has been completed, that is once the passengers and crew have boarded the aircraft in preparation for departure and it is no longer possible for passengers and crew to board or leave;
- (d) in the event of technical failure or difficulty, by any other appropriate means with a tolerance of 30 minutes after the departure ensuring the same level of technical and organisational security;
- (e) where a flight is cancelled, submissions in keeping with the timeframes articulated above prior to the cancellation are still required. Only submissions due after time of cancellation are not required; or
- (f) in emergency situations, submissions shall be made as soon as practicable where deemed necessary by the Competent Authority.

SCHEDULE VI

DATA ELEMENTS TO BE SUBMITTED UNDER THE FAL CONVENTION

(Section 25(8))

GENERAL DECLARATION

(IMO FAL Form 1)

		<input type="checkbox"/> Arrival	<input type="checkbox"/> Departure
1.1 Name and type of ship		1.2 IMO number	
1.3 Call sign		1.4 Voyage number	
ture		3. Date and time of arrival/departure	
4. Flag State of ship	5. Name of master	6. Last port of call/Next port of call	
7. Certificate of registry (Port; date; number)		8. Name and contact details of ship's agent	
9. Gross tonnage	10. Net tonnage		
11. Brief particulars of the voyage (previous and subsequent ports of call; underline where the remaining cargo will be discharged)			

12. Brief description of the cargo		
13. Number of crew	14. Number of passengers	15. Remarks
Attached documents (indicate number of copies)		
16. Cargo Declaration	17. Ship's Stores Declaration	
18. Crew List	19. Passenger List	20. The ship's requirements in terms of waste and residue reception facilities
21. Crew's Effects Declaration (only on arrival)	22. Maritime Declaration of Health (only on arrival)	
23. Date and signature by the master, authorised agent or officer		

For official use

10. Date and signature by the master, authorised agent or officer

SHIP'S STORES DECLARATION

(IMO FAL Form 3)

		[] Arrival	[] Departure	Page Number
1.1 Name of ship		1.2 IMO number		
1.3 Call sign		1.4 Voyage number		
2. Port of arrival/departure		3. Date of arrival/departure		
4. Flag State of ship		5. Last port of call/Next port of call		
6. Number of persons on board		7. Period of stay		
8. Name of article	9. Quantity	10. Location on board	11. Official use	
12. Date and signature by master, authorised agent or officer				

9. Date and signature by the master, authorised agent or officer					

DANGEROUS GOODS MANIFEST

(IMO FAL Form 7)

(As required by SOLAS 74, chapter VII, regulations 4.2 and 7-2.2, MARPOL, Annex III, regulation 4.2 and chapter 5.4, paragraph 5.4.3.1 of the IMDG Code)

1.1 Name of ship		1.2 IMO number		1.3 Call sign		Page Number				
1.4 Voyage number		2. Flag State of ship		3. Port of loading		4. Port of discharge				
5. Stowage Position	6. Reference Number	7. Marks & Numbers - Freight container identification No(\$)	8. UN Number	9. Proper Shipping Name/(Technical Specifications)	10. Class/ (Subsidiary Risk(s))	11. Packing Group	12. Additional Information/Marine Pollutant/Flash point/etc.	13. Number and kind of packages	14. Mass (kg) or Volume (L)	15. Em S
16. Shipping Agent										
16.1 Place and date										
Signature of Agent										

Passed the House of Representatives on
The day of , 2026.

Passed the Senate on the day of
, 2026.

Speaker

President

Clerk to the House of Representatives

Clerk to the Senate

EXPLANATORY MEMORANDUM

This a Bill to repeal and replace the Advance Passenger Information Act 2016. The Bill is a key component to modernising the legal framework as it relates to Advance Passenger Information and Passenger Name Record.

Part I - Preliminary

This Part contains Clauses 1 and 2 which are standard provisions.

Clause 1 provides that the Act shall be cited as the

Advance Passenger Information and Passenger Name Record Bill 2025. Clause 2 provides that the Act shall come into operation on a date fixed by the Minister by Notice published in the Gazette and different dates may be appointed for the coming into force of different parts of the Act.

Part II - Administrative

This Part contains clauses 4 to 7. The Part details the powers and functions of the Competent authority, the Chief Immigration Officer. It also provides for the establishment of the Passenger Information Unit and outlines its functions. Additionally, this part provides for the appointment of a Data Protection Officer whose functions are, among other things, to oversee and ensure compliance with data protection laws and regulations relating to advance passenger information data and passenger name record data.

Part III - Common Provisions for Advance Passenger Information and Passenger Information Name Record

This Part contains clauses 8 to 15. This part imposes an obligation on the master, captain or agent of an aircraft or vessel to provide relevant advance passenger information and passenger name record in accordance with the provisions of the Act. It further stipulates restrictions on disclosure of certain information by the Competent Authority, and limits access to advance passenger information and passenger name records. This Part discusses the processing, use, screening and sharing of advance passenger information and passenger name record data, and provides guidelines for Transfer of data to Competent Authority in other countries

Part IV - API Operating Provisions

This Part contains imposes a duty on the captain, master or agent of an aircraft or vessel to transmit advance passenger information data in accordance with the provisions of the Act. It details elements of advance passenger information data, timeframes for submission of API data and embarkation and disembarkation data. This Part further details the protection and retention of API data.

Part V - PNR Operating Provisions

This Part contains imposes a duty on the captain, master or agent of an aircraft or vessel to transmit passenger name record data in accordance with the provisions of the Act, and outlines guidelines for the transfer of this type of data.

Part VI - Administrative Penalties

This Part outlines the administrative penalties which are applicable where a person breaches any provisions of Part IV and V. It details steps taken by the Competent Authority in the event of such breach, the deadlines for payment of administrative fines and the recovery of such fines. It also provides that the person alleged to be in breach has an opportunity make representations, and if necessary, that person may appeal to the High Court.

Part VII - Exchange of PNR data with other Participating States

This Part provides guidelines for the exchange of passenger name record information with other Participating States. It also details the process by which other Competent Authorities may make a request for PNR.

Part VIII - Miscellaneous

This Part contains miscellaneous clauses. It also stipulates that information required to be submitted under this Act is to be done electronically. This part details the immunity of persons acting under the direction of the Competent Authority and also outlines the power of the Minister to make regulations.

Hon. Sir Steadroy C. O. Benjamin KGCN
*Attorney General and
Minister with responsibility for Immigration*