
First Session Thirteenth Parliament Republic of
Trinidad and Tobago



REPUBLIC OF TRINIDAD AND TOBAGO

Act No. 7 of 2026

[L.S.]

AN ACT to repeal and replace the Immigration (Advance Passenger Information) Act Chap. 18:04; to make provision for the collection, transmission, sharing, storage and regulation of Advance Passenger Information and Passenger Name Record in respect of persons travelling to, departing from and transiting through Trinidad and Tobago, and to operationalise the CARICOM Advance Passenger Information System and other related matters

[Assented to 15th May, 2026]

Enactment ENACTED by the Parliament of Trinidad and Tobago as follows:

PART I

PRELIMINARY

Short title **1.** This Act may be cited as the Advance Passenger Information and Passenger Name Record Act, 2026.

Commencement **2.** This Act comes into operation on such date as is fixed by the President by Proclamation.

Interpretation **3.** In this Act, unless the context requires otherwise—
“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 travelling in an aircraft or a vessel as set out in Part C of Schedule 1; and

(c) embarkation and disembarkation data as set out in Part C of Schedule 1;

“Advance Passenger Information and Passenger Name Record Database” or “API-PNR Database” means a centralised database established by IMPACS for the receipt, storage, processing, analysis and management of API and PNR data;

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

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

“anonymisation of PNR data” means the process of—

- (a) encrypting personal data in a PNR; or
- (b) removing personal data from a PNR;

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

“approved form” means a form approved by the Minister and published in the *Gazette*;

“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, including the CARICOM Single Market and Economy 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 Joint Regional Communication Centre under the authority of IMPACS;

“CARICOM Council for National 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 as an Organ of the Community and the CARICOM Implementation Agency for Crime and Security as an institution of the Community signed at Placencia, Belize on the 16th 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 paragraph 1 of Article 3 of the Revised Treaty;

“Chief Immigration Officer” has the meaning assigned to it under section 2 of the Immigration Act;

“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 Chief Immigration Officer;

“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;

“crew member” or “crew” means—

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

“data processing”—

- (a) means any operation or set of operations performed on API and PNR data for the purpose of enhancing border security, immigration control, customs clearance and other law enforcement purposes; and
- (b) 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 the person appointed under section 8;

“Departure Control System” means the system used to—

- (a) support pre-flight or pre-voyage process, including checking in of passengers onto aircraft or vessels; and

(b) streamline the departure process, 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 Part C of Schedule 1 in relation to a passenger, crew member, or any other person travelling in an aircraft or vessel and who is expected to embark or disembark in Trinidad and Tobago;

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

“ICAO” means the International Civil Aviation Organization established pursuant to the Convention on International Civil Aviation signed at Chicago on 7th December, 1944;

“IMO” means the International Maritime Organization which was formerly the Inter-Governmental Maritime Consultative Organisation established by the Convention on the International Maritime Organization on 6th March, 1948 adopted in Geneva;

“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 as an

Organ of the Community and the CARICOM Implementation Agency for Crime and Security 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; and

(ii) the Regional Intelligence Fusion Centre;

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

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

“Minister” means the Minister responsible for immigration;

“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 codeshare flight;

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

Schedule 2

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

“Passenger Information Unit” or “PIU” means the unit established under section 6;

“Passenger Name Record” or “PNR” means the record created by aircraft or vessel operators 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 2;

“personal data” means all information that can be used to identify an individual;

“personally identifiable information” means information that, when used alone or with other relevant data, can identify an individual;

“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 2;

“PNRGOV message” means the standard electronic message format jointly endorsed by the World Customs Organization, ICAO and IATA and used by an aircraft or vessel to submit PNR data;

“positive match” means the matching of personal or document data of 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 IMPACS *via* the CEMSIW;

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

“serious crime” means an offence against the laws of Trinidad and Tobago for which a person may be sentenced to imprisonment for a term of at least twelve months;

“technical stop” means—

- (a) the landing of an aircraft;
- (b) the berthing or anchoring of a vessel; or
- (c) the arrival or stopping of an aircraft or a vessel,

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

“terrorist offence” means any offence under Part II, Part III or Part IIIA of the Anti-Terrorism Act;

Chap. 12:07

“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 organisation responsible for the operation, management, and control of a particular vessel; and
- (b) includes an individual, a company, or an organisation 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;
- (c) criminal deportees; and
- (d) other persons of interest to law enforcement and the intelligence community.

4. 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 and IMPACS. Application of this Act

PART II ADMINISTRATIVE

5. (1) The Competent Authority shall—

- (a) be responsible for implementing the provisions of this Act; Functions and powers of the Competent Authority
- (b) establish protocols and standards, and 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 PNR laws, regulations and requirements, and may conduct reviews or inspections of aircraft,

vessels or the operations of transportation operators to ensure adherence to the data collection and transmission requirements;

- (f) establish data transfer agreements or arrangements with the competent authorities of other Participating States, specifying the obligations, safeguards, and conditions for the use, storage, and retention of the transferred PNR data;
- (g) conduct audits and inspections to ensure compliance with this 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 PNR 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) In addition to the functions under subsection (1), the Competent Authority shall—

- (a) have access to API and PNR data or the data processing results in order to examine such information further;
- (b) manage API and PNR data adequately and provide an appropriate level of protection of API and PNR data in keeping with the Data Protection Act, international best practices and any other written law;

-
- (c) verify data during physical processing of any passenger or crew member at any port of entry or departure by comparing the advance passenger information to the information contained in the travel document presented by the passenger or crew member;
 - (d) liaise and co-ordinate 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 the CARICOM APIS and the API-PNR Database 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 and PNR submissions and CEMSIW;
 - (h) if requested, permit a passenger or crew member from an aircraft or vessel access to his personal data maintained in the CARICOM APIS to ensure its correctness, but no passenger shall have access to any information provided by IMPACS to the Competent Authority against a Watch List 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 Trinidad and Tobago;
 - (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 9(1), 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 subsection (2)(h) and (j), 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 of its activities and responsibilities in a manner consistent with the Data Protection Act.

(5) Where the PIU is not operational, the Competent Authority shall process API and PNR data and shall —

- (a) co-ordinate with IMPACS in carrying out an assessment of passengers prior to their scheduled arrival in or departure from Trinidad and Tobago 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) Where subsection (5) applies, 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.

6. (1) There is established a unit within the Establishment of the Passenger Information Unit Immigration Department to be known as “the Passenger Information Unit”, which shall be headed by a Director who shall be an immigration officer of senior rank—

- (a) appointed by the Public Service Commission; or
- (b) engaged on contract by the Permanent Secretary in accordance with the Guidelines on Contract Employment established by the Chief Personnel Officer for such purpose, and who shall hold office for three years, but may be eligible for reappointment.

(2) There shall be a Deputy Director of the PIU who shall be an immigration officer of senior rank—

- (a) appointed by the Public Service Commission; or

(b) engaged on contract by the Permanent Secretary in accordance with the Guidelines on Contract Employment established by the Chief Personnel Officer for such purpose, and who shall hold office for three years, but may be eligible for reappointment.

(3) In addition to the Director and Deputy Director, the PIU shall include—

(a) a data protection officer employed in the Ministry and assigned to the PIU by the Permanent Secretary; and

(b) such number of immigration officers and other employees of the Immigration Department assigned to the PIU by the Permanent Secretary, after consultation with the Chief Immigration Officer.

(4) The PIU shall be assisted by persons designated as authorised officers under subsection (5).

(5) The Minister may designate—

(a) a police officer;

(b) a customs officer; or

(c) any other person,

to be an authorised officer for a specific period and purpose.

(6) The Director, Deputy Director and other staff of the PIU, and authorised officers designated under subsection (5), shall be positively vetted and suitably qualified and experienced persons.

7. (1) The PIU shall—

(a) receive, store, process, analyse and manage all API and PNR data transmitted by an aircraft or 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 terrorist offences and serious crimes—
- (i) manage and conduct risk assessments and analysis of API and PNR data collected from an aircraft or vessel; and
 - (ii) submit the results to the law enforcement personnel at ports of entry in Trinidad and Tobago, through the use of appropriate 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 vessel to arrive in or depart from Trinidad and Tobago;
- (d) in collaboration with the Competent Authority, liaise with and ensure effective communication and cooperation with Ministries and Government departments and agencies, by—
- (i) sharing information that it has acquired in the course of its duties under this Act; and
 - (ii) undertaking any other responsibility assigned by the Competent Authority;

-
- (e) where required by the Competent Authority, 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; 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) The PIU shall carry out all its functions, activities and responsibilities in a manner consistent with the Data Protection Act.
- (3) In processing API and PNR data, the PIU shall—
- (a) co-ordinate with IMPACS and other competent authorities in carrying out an assessment of passengers and crew prior to their scheduled arrival in or departure from Trinidad and Tobago 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 to operate twenty-four hours a day, seven days a week, with procedures in place to minimise disruption in the event of an emergency, system outage or failure.

8. (1) The President shall appoint a positively vetted and suitably qualified and experienced individual as the Data Protection Officer to oversee and ensure compliance with this Act.

Appointment and
functions of Data
Protection Officer

(2) A person appointed under subsection (1) shall hold office for three years and is eligible for reappointment.

(3) A person appointed under subsection (1) shall, before he performs the functions of the Data Protection Officer, take and subscribe to the oath of office set out in Schedule 3.

(4) The DPO shall—

- (a) operate independently in performing his duties, free from any conflicts of interest and for this purpose shall have direct access to the Competent Authority and the highest levels of management within the Immigration Department and IMPACS;
- (b) possess expert knowledge of the Data Protection Act, as well as a deep understanding of the specific requirements and challenges associated with the collection, processing and management of API and PNR data;
- (c) provide advice, guidance and recommendations to the Competent Authority and IMPACS on matters related to the processing of API and PNR data, ensuring compliance with the Data Protection Act;

- (d) monitor the processing activities related to API and PNR data, including data collection, storage, access, use and sharing, to ensure compliance with legal requirements and established policies and procedures and to implement related safeguards;
- (e) conduct regular risk assessments regarding the processing of API 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 relating to the collection, processing and management of API and PNR data, and ensure that these assessments 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 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 programmes, workshops and awareness campaigns to enhance the understanding of the Competent Authority and employees of IMPACS, 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 any written law;
- (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 and PNR data;
- (k) provide national oversight for the protection of API and PNR data; and
- (l) provide advice, guidance and recommendations to the Competent Authority on API and PNR data processing to ensure compliance with this Act and the Data Protection Act.

(5) The Government shall provide the necessary resources, and the Competent Authority and IMPACS shall provide the necessary cooperation and support, to enable the DPO to fulfil his responsibilities effectively.

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

PART III

COMMON PROVISIONS FOR ADVANCE PASSENGER INFORMATION AND PASSENGER NAME RECORD

9. (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 and PNR data relating to the passengers and crew and the flight or voyage as set out in Schedules 1 and 2.

Duty to provide API and PNR data and embarkation and disembarkation data

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

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

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

(4) A master, a captain or an agent of an aircraft or vessel travelling into or out of Trinidad and Tobago shall, *via* the CEMSIW, provide to the Competent Authority and IMPACS the relevant embarkation and disembarkation data as set out in Part C of Schedule 1.

Part C
Schedule 1
Technical stop

10. (1) Nothing in section 9 applies to an aircraft or 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 vessel makes a technical stop for a reason specified in subsection (1), the captain, agent or master—

- (a) shall immediately report to the Competent Authority;
- (b) shall 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) shall 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 vessel shall, without the consent of the Competent Authority, disembark the aircraft or vessel, and such person shall comply with any directions given by the Competent Authority.

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

- (a) a first offence, is liable on summary conviction to a fine of thirty-five thousand dollars; and
- (b) a second or subsequent offence, is liable on summary conviction to a fine of one hundred and forty thousand dollars and imprisonment for six months.

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

- 11. (1)** The Competent Authority shall ensure that—
- (a) all data and documentation obtained or generated in the course of its functions and responsibilities are treated as confidential and that such data and documentation are subject to non-disclosure obligations; and
- (b) its personnel refrain from disclosing any confidential data or documentation, except as provided for by subsection (2), expressly authorised by any written law or with the explicit consent of the parties involved.
- Restriction on disclosure of data or documentation by the Competent Authority

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

- (a) when required by law or court order;
- (b) when necessary to fulfil the purposes for which the data or documentation was collected, provided that such disclosure is in accordance with the Data Protection Act; and
- (c) when disclosure is required to safeguard national security, public safety, or the prevention, detection, investigation or prosecution of terrorist offences or serious crimes.

(3) The Competent Authority shall—

- (a) manage all disclosed data or documentation in compliance with the Data Protection Act;
- (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 Competent Authority; and

(f) initiate disciplinary proceedings and seek other legal remedies to address any unauthorised disclosure, including imposing penalties, suspension or termination of employment, as considered appropriate.

12. (1) No Ministry or Government department or agency shall have direct access to API 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 access to API and PNR data, and such access may be limited or controlled.

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

(4) No person shall, without authorisation, access, attempt to access, facilitate access to, or cause access to API and PNR data 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 one hundred and forty thousand dollars and imprisonment for two years.

13. (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 Trinidad and Tobago to identify individuals who require further examination for potential involvement in terrorist offences, other 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 offences 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 offences 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 and PNR data with authorised databases for the purpose of preventing, detecting, investigating, and prosecuting terrorist offences or serious crimes, including databases of wanted persons or objects, as permitted by law; or
- (b) analyse API 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 Trinidad and Tobago carried out under subsection (1)(a) against established criteria shall be carried out in a non-discriminatory manner.

(5) The 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 2, the data shall be deleted immediately and permanently upon receipt.

(8) The storage, processing and analysis of API and PNR data shall be carried out exclusively within a secure location or locations within Trinidad and Tobago, 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 crimes 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 Ministries or Government departments and agencies, where required under the Data Protection Act or any other written law.

14. (1) The Competent Authority and IMPACS shall establish a robust system for the verification of API and PNR data submitted in respect of an aircraft or vessel, ensuring the accuracy, integrity and reliability of the data collected.

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

(2) The Competent Authority and IMPACS shall employ appropriate mechanisms and tools to validate the API 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 and PNR data shall be subject to risk assessment and analysis to identify potential anomalies, discrepancies, inconsistencies or patterns that may require further investigation or action.

(4) Where any anomaly, discrepancy or inconsistency is 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 the submitter of the API and PNR data, following which the captain, master, agent or submitter shall be given an opportunity to rectify the anomaly, discrepancy or inconsistency within seven days or such other period as the Minister may, by Order, prescribe.

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

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

- (a) arrives in, departs from or transits through Trinidad and Tobago; or
- (b) travels within CARICOM,

against Watch Lists and approved national, regional and international databases in order to provide information to assist competent authorities, IMPACS and Participating States.

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

(3) 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.

(4) The API and PNR data shall only be used for the purposes of this Act and, subject to access granted by the Competent Authority under section 12(2), to inform national compilation of statistics by Ministries and Government departments and agencies authorised to do so.

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

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

- (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 a recipient country is lower than in Trinidad and Tobago, any conflict between the provisions of this Act and the laws of the 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 a recipient country shall resolve conflicts between the provisions of this Act and the laws of the 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 and the competent authority in a recipient country;

- (b) binding rules that are enforced by both the Competent Authority and the competent authority in a recipient country, and which expressly confer enforceable rights on a person whose API and PNR data is requested to be transferred;
- (c) a code of conduct, the terms of which are agreed upon between the Competent Authority and the competent authority of a recipient country and which impose binding and enforceable commitments on the competent authority of the recipient country to apply appropriate safeguards, including as regards to the rights of the person whose API and PNR data is being transferred; or
- (d) contractual clauses between the Competent Authority and the competent authority of a recipient country to apply appropriate safeguards, including as regards to the rights of the person whose API and PNR data is being transferred.

PART IV
API OPERATING PROVISIONS

Duty to transmit API
data

17. (1) A captain, master or agent of an aircraft or 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 1.

Schedule 1

(2) The Competent Authority, IMPACS or a captain, master or an agent of an aircraft or vessel, shall collect, receive, process, store, retain and transmit all API data in accordance with this Act and the Data Protection Act.

(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 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, master, agent, crew member or 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 thirty-five thousand dollars; or
- (b) a second or subsequent offence, is liable on summary conviction to a fine of one hundred and forty thousand dollars and imprisonment for six months.

(6) No person shall refuse to produce, 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 thirty-five thousand dollars; and

(b) a second or subsequent offence, is liable on summary conviction to a fine of one hundred and forty thousand dollars and imprisonment for six months.

(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.

API data elements

18. A captain, master or an agent of an aircraft or vessel arriving at, departing from or transiting through Trinidad and Tobago 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 1.

Schedule 1

Timeframe for submission of API data and embarkation and disembarkation data
Part A
Schedule 4

19. (1) API data shall be submitted to the Competent Authority and IMPACS, through CEMSIW, in accordance with the timeframe set out in Part A of Schedule 4.

(2) In the event of technical failure, the captain, master or agent of an aircraft or vessel shall transmit API data by any other appropriate electronic means in accordance with the timeframes set out in Part A of Schedule 4, ensuring the application of the appropriate level of data security.

Part A
Schedule 4

(3) Embarkation and disembarkation data shall be submitted to the Competent Authority and IMPACS, through CEMSIW, in accordance with the timeframe set out in Part B of Schedule 4.

Part B
Schedule 4

20. (1) An individual may, in the approved form and manner and in accordance with the Data Protection Act and any other written law—

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

(2) The Competent Authority shall in the approved form—

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

in the prescribed manner.

(3) An individual shall have the right to lodge a complaint before the DPO if he considers that the processing of his API data is not in compliance with the provisions of this Act, the Data Protection Act or any other written law.

21. (1) Subject to subsection (2), 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 crew member or passenger.

(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.

Failure to provide
API data

22. (1) A captain, master or agent who fails to provide API data in accordance with this Act commits an offence and, where the contravention constitutes—

- (a) a first offence, is liable on summary conviction to a fine of thirty-five thousand dollars; or
- (b) a second or subsequent offence, is liable on summary conviction to a fine of one hundred and forty thousand dollars and imprisonment for six months.

(2) No captain, master or agent shall intentionally or recklessly—

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

(3) Subject to subsection (4), a captain, master or agent who contravenes subsection (2) commits an offence and, where the contravention constitutes—

- (a) a first offence, is liable on summary conviction to a fine of thirty-five thousand dollars; or
- (b) a second or subsequent offence, is liable on summary conviction to a fine of one hundred and forty thousand dollars and imprisonment for six months.

(4) Where the API data provided is inaccurate and the captain, master or agent of the aircraft or vessel satisfies the Competent Authority the error was not made knowingly or recklessly then, notwithstanding

any other provision of this Act, the captain, master or agent shall not be liable for an offence under subsection (3) and no administrative fine shall be imposed on him.

(5) 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 provide erroneous, misleading, incomplete or false data.

(6) A passenger or crew member who contravenes subsection (5) commits an offence and is liable on summary conviction to a fine of two thousand, eight hundred dollars and imprisonment for six months.

PART V PNR OPERATING PROVISIONS

23. (1) In accordance with section 25, a captain or agent of an aircraft shall transfer to the Competent Authority and IMPACS, all 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 Trinidad and Tobago.

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

(2) Where a flight in respect of which PNR data is required to be collected and transmitted is code-shared between two 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 agent of an aircraft shall transfer PNR data to the Competent Authority and IMPACS by electronic means in accordance with the timeframe stipulated in Schedule 5.

Schedule 5

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

Schedule 5

(5) Notwithstanding the timeframe provided for in Schedule 5, a captain or 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 where access to that data is required in order to respond to a specific and actual threat related to any terrorist offence 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 specific period as required by the Competent Authority.

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

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

24. (1) In accordance with section 25, a master or agent of a vessel shall transfer to the Competent Authority and IMPACS, 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 Trinidad and Tobago.

(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 two or more vessels, a master or 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 agent of a vessel shall transfer PNR data to the Competent Authority and IMPACS by electronic means in accordance with the timeframe specified in Schedule 6.

Schedule 6

(4) A master or 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) Notwithstanding the timeframe provided for in Schedule 6, a master or 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 where access to that data is required in order to respond to a specific and actual threat related to any terrorist offence or serious crime.

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

(8) For the purposes of the FAL Convention, a master or agent of a vessel shall accurately complete, and submit to the Competent Authority and IMPACS, in the form set out in Schedule 7.

Schedule 7

25. (1) Subject to subsections (3) and (4), the captain or agent of an aircraft or the master or agent of a vessel arriving in, departing from or transiting through Trinidad and Tobago shall transfer PNR data collected in the course of normal business operations to the

PNR data transfer
method and format

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 in, departing from or transiting through Trinidad and Tobago 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.

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

Schedule 2

Transmission
timeframe for PNR
data

26. (1) Subject to subsection (2), the captain, master or agent of an aircraft or vessel operating a flight or voyage arriving in, departing from or transiting through Trinidad and Tobago shall transfer PNR data to the Competent Authority and IMPACS in accordance with Schedule 2 and, as the case may be, Schedule 5 or 6.

Schedule 5 or
Schedule 6

(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 vessel shall be required to provide the Competent Authority and IMPACS, with PNR data prior to, between, or after the scheduled transmission timeframes specified in Schedule 5 or Schedule 6, as the case may be.

Schedule 5 or
Schedule 6

Automated
processing of PNR
data

27. (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) A decision which produces any significant adverse action on an individual, affecting his legal interests or rights or other legal entitlements, shall not be made on the sole basis of the automated processing of PNR data.

28. (1) Subject to subsection (3), no person shall ^{Sensitive data} 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.

29. (1) PNR data provided by a captain or 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. ^{PNR data and document retention}

(2) PNR data retained 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 another competent authority by the PIU shall be deleted permanently either—

- (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 passenger information units 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 the breach 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.

30. (1) PNR data transferred by a captain or agent of an aircraft, or a master or 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 investigation, case, threat or risk related to the purposes of this Act.

Depersonalisation
and anonymisation
of PNR data

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

- (a) the name or names of each passenger and crew member, including the names and number of passengers and crew members on the PNR who are travelling together;
- (b) address and contact information of each passenger and crew member;
- (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 or crew member to whom the PNR data relates, or any other person;
- (d) frequent flyer or traveller information; and
- (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 or crew member to whom the PNR data relates.

(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 investigation, case, threat or risk related to the purposes of this Act, upon authorisation by the Competent 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 investigation, case, threat or risk related to the purposes of this Act.

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

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

31. Subject to the Data Protection Act, the Data Protection Officer shall provide national oversight for the protection of PNR data.

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

Competent Authority
and PIU to liaise
with Regional Data
Protection Officer

(2) The Competent Authority and IMPACS shall provide the Regional Data Protection Officer with the information necessary for him to perform his 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 data 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 Data Protection Officer or the Executive Director of IMPACS.

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

Competent Authority
and PIU to liaise
with Data Protection
Officer

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

(2) The Competent Authority and the PIU shall provide the Data Protection Officer with the resources and information to perform his 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.

Safeguards and
redress mechanisms

34. (1) An individual shall have the same right to the protection of his personal data in any API or PNR 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 and any other written law in relation to the protection of his personal data.

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

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

Contravention of this
Part

35. (1) A captain, master or agent who contravenes a provision in this Part commits an offence.

(2) 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 thirty-five thousand dollars; and

- (b) a second or subsequent offence, the captain, master or agent is liable on summary conviction to a fine of one hundred and forty thousand dollars and imprisonment for six months.

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

PART VI

EXCHANGE OF PNR DATA WITH OTHER PARTICIPATING STATES

37. (1) Subject to subsection (4), upon receiving a request from the competent authority of a Participating State, the Competent Authority may share PNR data with that competent authority in accordance with this Act and the Data Protection Act.

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

(3) The PIU, acting on the approval and guidance of the Competent Authority, shall transfer PNR data in compliance with this Act and the Data Protection Act, 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 such PNR data as is proportionate and necessary to achieve the stated 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 a recipient Participating State, 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 a recipient Participating State, 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 co-ordination with the competent authorities of recipient Participating States, including by addressing queries, providing clarification, 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, including by ensuring compliance with this Act, the Data Protection Act and applicable agreements.

(11) The Competent Authority shall establish an accountability framework to assess the lawfulness, necessity, and effectiveness of the transfers, including by 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 Ministries and Government departments and agencies 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.

38. (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 has not been depersonalised, the PIU in consultation with the Competent Authority may transmit PNR data 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 crimes.

Request from
another
Participating State

(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 to the PIU, and the PIU may, in turn, transfer the PNR data to the competent authority in the requesting Participating State.

(3) A request made under subsection (2) shall 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 crimes.

39. (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

Request for PNR
data from another
Participating State
by the Competent
Authority or PIU

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 under subsection (1) may be made with respect to 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, master or 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 captain, master or agent is required to transfer the PNR data to the passenger information unit of that Participating State, and to transfer the PNR data to the PIU, where access to the PNR data is necessary to respond to a specific or actual threat related to any terrorist offence or serious crime.

PART VII

MISCELLANEOUS

Requirement to
submit information
electronically

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

Administrative fines

41. (1) Where the Competent Authority has reasonable cause to believe that a person has committed a summary offence specified in the First Column of Schedule 8, the Competent Authority may issue to that person a notice offering the person the opportunity to discharge any liability to conviction in respect of that offence by payment of the administrative fine specified in the Second Column of that Schedule.

Schedule 8

(2) Where a person is given a notice under this section, criminal proceedings shall not be taken against him for the offence specified in the notice until the expiration of twenty-one days commencing from the day after which the notice was served.

(3) Where a person fails to pay the administrative fine referred to in subsection (1), that person is liable to be prosecuted for the offence.

(4) Payment of an administrative fine under this section shall be made to the Competent Authority and a certificate that payment of the penalty was made to the Competent Authority by the specified date shall, if the certificate purports to be signed by an officer authorised by the Competent Authority, be admissible as evidence of the facts stated therein.

(5) All monies received under this section shall be credited to the Consolidated Fund.

(6) A notice under subsection (1) shall—

- (a) specify the offence alleged;
- (b) give such particulars of the offence as are necessary for giving reasonable information of the allegation; and
- (c) state—

- (i) that criminal proceedings shall not be laid until the expiration of twenty-one days from the date of service of the notice where payment of the administrative fine is made and the commission of the offence is discontinued;
- (ii) the amount of the administrative fine and the fact that it is to be paid to the Competent Authority; and
- (iii) that the Competent Authority shall not accept any payments in respect of a notice under subsection (1) after the expiration of the twenty-one days.

(7) In any proceedings for an offence to which this section applies, no reference shall be made to the giving of any notice under this section or to the payment or non-payment of an administrative fine thereunder unless in the course of the proceedings or in some document which is before the court in connection with the proceedings, reference has been made by, or on behalf of the accused to the giving of such a notice, or, as the case may be, to such payment.

(8) A person who is aggrieved by a decision of the Competent Authority to impose an administrative fine under this section, may, within thirty days of being informed of that decision, appeal to the High Court.

Immunity from
liability

42. (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.

Regulations

43. (1) The Minister may make regulations to give effect to 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 17(1) as provided for in section 17(8);
- (b) to provide for procedures for the gathering of information by, and the sharing of information and collaboration among, the agencies mentioned in this Act;

- (c) prescribing the composition of the PIU, and such procedural operations and institutional and other arrangements as may be required to ensure the effectiveness and efficiency of its operations;
- (d) designating Competent Authorities to receive API and PNR data;
- (e) establishing approved Watch Lists, 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.

44. Notwithstanding any provision under this Act in respect of the imposition of penalties, no person shall be penalised or held otherwise responsible for incomplete, delayed or erroneous messages resulting from a technical issue. Non-imposition of penalties

45. The Minister may, by Order, amend any of the Schedules. Amendment of Schedules

46. The Immigration (Advance Passenger Information) Act is repealed. Repeal Chap. 18:04

SCHEDULE 1

ADVANCE PASSENGER INFORMATION DATA ELEMENTS AND EMBARKATION AND DISEMBARKATION DATA ELEMENTS

*[Sections 3, 9(1) and (4),
18(1) and 19]*

PART A

AIRCRAFT

- (a) Data relating to the flight (Header Data)—
 - (i) Flight Identification
(IATA or ICAO Airline code and flight number,
Registration Number)

SCHEDULE 1—CONTINUED

- (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]—
 - 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

SCHEDULE 1—CONTINUED

- (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

PART 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)

SCHEDULE 1—CONTINUED

- (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)

SCHEDULE 1—CONTINUED

- (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

PART 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

SCHEDULE 1—CONTINUED

- (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

SCHEDULE 1—CONTINUED

- (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 2

PASSENGER NAME RECORD (PNR) DATA ELEMENTS

*[(Sections 3, 9(1), 13(7), 25(4)
and 26(1)]*

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

SCHEDULE 2—CONTINUED

(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

(c) 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)

SCHEDULE 2—CONTINUED

(vi) Primary Residence—

(aa) Country of Primary Residence

(Country where passenger resides most
of the year)

(ab) Address

(location identification such as—street
name and number)

(ac) City

(ad) State or Province or County

(ae) Postal Code

(vii) Destination Address—

(aa) Address where the passenger will be
staying in the territory of disembarka-
tion

(ab) City

(ac) State or Province or County

(ad) Postal Code

(d) 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 3

*[Section 8(3)]*FORM OF OATH (AFFIRMATION) OF OFFICE FOR THE
DATA PROTECTION OFFICER

I, A.B., having been appointed Data Protection Officer do swear by
 (solemnly affirm) that I bear true
 faith and allegiance to Trinidad and Tobago and will uphold the
 Constitution and the law, that I will conscientiously, impartially
 and to the best of my knowledge, judgment and ability discharge
 the functions of my office and do right to all manner of people after
 the laws and usages of Trinidad and Tobago without fear or favour,
 affection or ill-will.

SCHEDULE 4

TIMEFRAMES FOR SUBMISSION OF API AND EMBARKATION AND
DISEMBARKATION DATA*(Section 19)*

PART 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.

PART 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 Trinidad and Tobago.

SCHEDULE 5

TIMEFRAMES FOR ELECTRONIC SUBMISSION OF PNR DATA BY A
CAPTAIN OR AGENT OF AN AIRCRAFT*[Sections 23(3) and
(5) and 26]*

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

- (a) 48 hours before the scheduled flight departure time;
and
- (b) 24 hours before the scheduled flight departure time;
and

SCHEDULE 5—CONTINUED

- (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 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; or
- (f) in emergency situations, submissions shall be made as soon as practicable where deemed necessary by the Competent Authority.

SCHEDULE 6

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

[(Sections 24(3) and (5) and 26(3)]

A vessel shall transfer PNR data to the Competent Authority and IMPACS by electronic means *via* the CEMSIW in accordance with the following timeframes:

- (a) 48 hours before the scheduled voyage departure time;
and
- (b) 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;
- (e) 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;
- (f) in emergency situations, submissions shall be made as soon as practicable where deemed necessary by the Competent Authority.

SCHEDULE 7

DATA ELEMENTS TO BE SUBMITTED UNDER THE FAL CONVENTION

[Section 24(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	
2. Port of arrival/departure		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

SCHEDULE 7—CONTINUED

SHIP'S STORES DECLARATION
(IMO FAL Form 3)

		<input type="text"/> Arrival	<input type="text"/> 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				

SCHEDULE 7—CONTINUED

CREW LIST
(IMO FAL Form 5)

				<input type="checkbox"/> Arrival		<input type="checkbox"/> Departure		<input type="checkbox"/> Page Number			
1.1 Name of ship				1.2 IMO number		1.3 Call sign		1.4 Voyage number			
2. Port of arrival/departure						4. Flag State of ship		5. Last port of call			
6. No.	7. Family name	8. Given names	9. Rank or rating	10. Nationality	11. Date of birth	12. Place of birth	13. Gender	14. Nature of identity document	15. Number of identity document	16. Issuing State of identity document	17. Expiry date of identity document
18. Date and signature by the master, authorised agent or officer											

SCHEDULE 8

(Section 41)

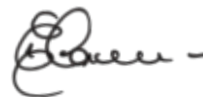
ADMINISTRATIVE FINES

No.	FIRST COLUMN <i>Description of Offence</i>	SECOND COLUMN <i>Administrative Fine</i>
1.	Section 10: Failure to comply with requirements <i>re. technical stop</i>	<i>(a)</i> on first occasion - \$5,000 <i>(b)</i> on second occasion - \$7,500 <i>(c)</i> on third or subsequent occasion - \$10,000
2.	Section 12: Unauthorised access to API-PNR data	<i>(a)</i> on first occasion - \$5,000 <i>(b)</i> on second occasion - \$7,500 <i>(c)</i> on third or subsequent occasion - \$10,000
3.	Section 17(4) and (5): Refusing to answer or giving a false answer to the Competent Authority	<i>(a)</i> on first occasion - \$5,000 <i>(b)</i> on second occasion - \$7,500 <i>(c)</i> on third or subsequent occasion - \$10,000
4.	Section 17(6) and (7): Refusing to produce document to Competent Authority	<i>(a)</i> on first occasion - \$5,000 <i>(b)</i> on second occasion - \$7,500 <i>(c)</i> on third or subsequent occasion - \$10,000
5.	Section 22(1): Failure to provide API data	<i>(a)</i> on first occasion - \$5,000 <i>(b)</i> on second occasion - \$7,500 <i>(c)</i> on third or subsequent occasion - \$10,000
6.	Section 22 (3): Providing erroneous, etc. API data or engaging in or facilitating API transfer in an incorrect format	<i>(a)</i> on first occasion - \$5,000 <i>(b)</i> on second occasion - \$7,500

SCHEDULE 8—CONTINUED

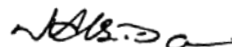
		(c) on third or subsequent occasion - \$10,000
7.	Section 22 (6): Failure to provide embarkation and disembarkation data or provision of erroneous, etc. data by passenger or crew member	(a) on first occasion - \$5,000 (b) on second occasion - \$7,500 (c) on third or subsequent occasion - \$10,000
8.	Section 35: Contravention of Part V	(a) on first occasion - \$5,000 (b) on second occasion - \$7,500 (c) on third or subsequent occasion - \$10,000

Passed in the House of Representatives this 10th day of April, 2026.



Clerk of the House

Passed in the Senate this 21st day of April, 2026.



Clerk of the Senate