CHAPTER 584

PASSENGER NAME RECORD (DATA) ACT

AN ACT to provide for the transposition of Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

28th May, 2018*

ACT XVII of 2018 as amended by XX of 2018.

ARRANGEMENT OF ACT

		Articles
Part I	Preliminary Provisions	1-3
Part II	General Provisions	4
Part III	Passenger Name Records	5-15
Part IV	Implementing measures	16-20

PART I

Short title.

1. The short title of this Act is the Passenger Name Record (Data) Act.

Scope.

2. This Act is transposing Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

Applicability.

3. (1) This Act provides for:

(a) the transfer by air carriers of passenger name record (hereinafter referred to as "PNR") data of passengers of extra-EU flights to Malta, and the processing of such data, including its collection, use, and retention from Member States and its exchange between Malta and other EU Member States;

(b) the transfer by air carriers of PNR data of passengers of intra-EU flights to Malta and the processing of such data, including its collection, use, and retention from Member States and its exchange between Malta and other EU Member States.

(2) PNR data collected in accordance with this Act may be processed only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, as provided for in article 7(2)(a), (b) and (c).

*See Legal Notice 170 of 2018.

PART II

Interpretation.

4. For the purposes of this Act, and unless the context otherwise requires, the following definitions shall apply:

"air carrier" means an air transport undertaking with a valid operating licence or equivalent permitting it to carry out carriage of passengers by air;

Cap. 217.

"Board" means the Immigration Appeals Board as constituted by article 25A of the Immigration Act;

"data subject" means an identified or identifiable natural person in accordance with Article 4(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, regarding the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

"Europol" means the European Union Agency for Law Enforcement Cooperation as established by Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (hereinafter referred to as the "Europol Regulation");

"EU Member State" means a Member State of the European Union;

"extra-EU flight" means any scheduled or non-scheduled flight by an air carrier flying from a third country and planned to land on the territory of an EU Member State or flying from the territory of an EU Member State and planned to land in a third country, including in both cases flights with any stop-overs in the territory of EU Member States or third countries;

"intra-EU flight" means any scheduled or non-scheduled flight by an air carrier flying from the territory of an EU Member State and planned to land on the territory of one or more of the other EU Member States, without any stop-overs in the territory of a third country;

"Minister" means the Minister responsible for home affairs and national security;

"national competent authority" means the authorities listed in Schedule A which shall be the authorities competent for the prevention, detection, investigation or prosecution of

terrorist offences and serious crimes;

"national supervisory authority" means the Information and Data Protection Commissioner as referred to in the Data Protection Act; Cap. 586.

"passenger" means any person, including persons in transfer or transit and excluding members of the crew, carried or to be carried in an aircraft with the consent of the air carrier, such consent being manifested by that person's registration in the passengers list;

"passenger name record" or "PNR" means a record of each passenger's travel requirements which contains information necessary to enable reservations to be processed and controlled by the booking and participating air carriers for each journey booked by or on behalf of any person, whether it is contained in reservation systems, departure control systems used to check passengers onto flights, or equivalent systems providing the same functionalities;

"Principal Immigration Officer" means the person appointed to such office by the Prime Minister under article 3 of the Immigration Act, and includes, within the limits of any authority granted by the Principal Immigration Officer under article 3(3) of the Immigration Act, any public officer acting under such authority; Cap. 217.

"push method" means the method whereby air carriers transfer PNR data collected in the course of their business listed in Schedule B into the database of the National Passenger Information Unit requesting them;

"reservation system" means the air carrier's internal system, in which PNR data is collected for the handling of reservations;

"serious crime" means the offences listed in Schedule C that are punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of an EU Member State;

"terrorist offences" means the offences under the Criminal Code and any other national legislation regulating the combating of terrorism; Cap. 9.

"third country" means a country which is not a Member State of the European Union:

Provided that Denmark is to be regarded as a third country for the purposes of this Act in accordance with the Treaty on European Union and the Treaty on the Functioning of

the European Union - consolidated version of the Treaty on European Union - Protocols - Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007, and Articles 1 and 2 of the Protocol No. 22 on the position of Denmark annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union;

"to depersonalise through masking out of data elements" means to render those data elements which could serve to identify directly the data subject invisible to a user.

PART III

Passenger Information Unit. *Amended by: XX.2018.35.*

5. (1) There shall be established a National Passenger Information Unit (hereinafter referred to as "NPIU") which shall fall within the responsibilities of the Commissioner of Police.

(2) The NPIU shall be the authority competent to process PNR data for the prevention, detection, investigation or prosecution of terrorist offences and of serious crime.

(3) The NPIU shall be responsible for:

(a) collecting PNR data from air carriers, storing and processing this data and transferring this data or the result of processing it to the competent authorities referred to in article 8;

(b) exchanging both PNR data and the result of processing this data with the PIUs of other EU Member States and with Europol in accordance with articles 10 and 11:

S.L. 586.08.

Provided that PNR data shall be collected and processed in accordance with the Data Protection (Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties) Regulations.

(4) The NPIU shall be provided with adequate resources to fulfil all its tasks. Staff members of the NPIU may be seconded from national competent authorities.

Data Protection Officer in the NPIU. *Amended by: XX.2018.35.*

6. (1) The Commissioner of Police shall appoint a Data Protection Officer for the NPIU, responsible for monitoring the processing of PNR data and implementing relevant safeguards.

(2) The Commissioner of Police shall ensure that the Data Protection Officer has the means to perform his duties and tasks in

S.L. 586.08.

accordance with the Data Protection (Processing of Personal Data by Competent Authorities for the Purposes of the Prevention,

Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties) Regulations.

(3) The Commissioner of Police shall ensure that a data subject can exercise the right to contact the Data Protection Officer, as a single point of contact, on all issues relating to the processing of that data subject's PNR data.

Processing of PNR data.

7. (1) The PNR data transferred by the air carriers shall be collected by the NPIU as provided for in article 9. Where the PNR data transferred by air carriers includes data other than that listed in Schedule B, the NPIU shall delete such data immediately and permanently upon receipt.

(2) The NPIU shall process PNR data only for the following purposes:

(a) carrying out an assessment of passengers prior to their scheduled arrival in or departure from Malta to identify persons who require further examination by national competent authorities or competent authorities of other EU Member States, and where relevant, by Europol in accordance with article 11, in view of the fact that such persons may be involved in a terrorist offence or serious crime;

(b) responding, on a case-by-case basis, to a duly reasoned request based on sufficient grounds from competent authorities to provide and process PNR data in specific cases for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime, and to provide competent authorities or, where appropriate, Europol with the results of such processing; and

(c) analysing PNR data for the purpose of updating or creating new criteria to be used in the assessments carried out under sub-article (3)(b) in order to identify any person who may be involved in a terrorist offence or serious crime.

(3) When carrying out the assessment referred to in sub-article (2)(a), the NPIU may:

(a) compare PNR data against databases relevant for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, including databases on persons or objects sought or under alert, in accordance with Union, international and national rules applicable to such databases; or

(b) process PNR data against pre-determined criteria.

(4) Any assessment of passengers prior to their scheduled

arrival or departure in Malta performed under sub-article (3)(b) against pre-determined criteria shall be carried out in a non-discriminatory manner. Those pre-determined criteria must be targeted, proportionate and specific:

Provided that pre-determined criteria shall be set and regularly reviewed by the NPIU in cooperation with the national competent authorities. The criteria shall in no circumstances be based on a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation.

(5) The NPIU shall ensure that any positive match resulting from the automated processing of PNR data conducted under sub-article (2)(a) is individually reviewed by non-automated means to verify whether any of the national competent authorities needs to take action under national law.

(6) The NPIU shall transmit the PNR data of persons identified in accordance with sub-article (2)(a) or the result of processing that data for further examination to the national competent authorities or to the competent authorities of other EU Member States. Such transfers shall only be made on a case-by-case basis and, in the event of automated processing of PNR data, after individual review by non-automated means.

(7) It shall be ensured that the Data Protection Officer has access to all data processed by the NPIU:

Provided that if the Data Protection Officer considers that processing of any data has not been lawful, the Data Protection Officer may refer the matter to the national supervisory authority.

(8) The storage, processing and analysis of PNR data by the NPIU shall be carried out exclusively within a secure location or locations.

(9) The consequences of the assessments of passengers referred to in sub-article (2)(a) shall not jeopardise the right of entry of persons enjoying the Union right of free movement into the territory of the EU Member State concerned as laid down in the Free Movement of European Union Nationals and their Family Members Order. Where assessments are carried out in relation to intra-EU flights between EU Member States to which Regulation (EU) No. 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) applies, the consequences of such assessments shall comply with that Regulation.

S.L. 460.17.

Functions of Competent Authorities.

8. (1) The national competent authorities shall be entitled to request and/or receive PNR data or the result of processing

that data from the NPIU, in order to analyse that information further or to take appropriate action for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime.

(2) The PNR data and the result of processing that data received by the NPIU may be further processed by the national competent authorities only for the specific purposes of preventing, detecting, investigating or prosecuting terrorist offences or serious crime.

(3) Sub-article (2) of this article shall be without prejudice to the powers of the national law enforcement or judicial authorities where other offences, or indications thereof, are detected in the course of enforcement action further to such processing.

(4) The national competent authorities shall not take any decision that produces an adverse legal effect on a person or significantly affects a person only by reason of the automated processing of PNR data. Such decisions shall not be taken 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.

Obligations on air carriers regarding transfers of data.

9. (1) Air carriers landing in or departing from Malta, shall transfer by the "push method" to the database of the NPIU, the PNR data listed in Schedule B, to the extent that they have already collected such data in the normal course of their business:

Provided that where the flight is code-shared between one or more air carriers the obligation to transfer the PNR data of all passengers on the flight shall be on the air carrier that operates the flight.

(2) Where Malta is the destination of a stop-over by both an extra-EU and/or an intra-EU flight, the air carrier concerned shall also transfer the PNR data of all passengers as provided in sub-article (1).

(3) In the event that the air carriers have collected any advance passenger information (hereinafter referred to as "API") data listed under item 18 of Schedule B, but do not retain that data by the same technical means as for other PNR data, air carriers shall also transfer that data to the NPIU in the same manner as referred to in sub-article (1). In the case of such transfer, all the provisions of this Act shall also apply in relation to that API data.

(4) Air carriers shall transfer PNR data by electronic means using the common protocols, supported data formats, and transmission protocols as adopted by the Commission of the European Union by implementing acts or, in the event of technical failure, by any other appropriate means ensuring an appropriate level of data security, as follows:

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

(b) immediately after flight closure, that is once the passengers have boarded the aircraft in preparation for departure and it is no longer possible for passengers to board or leave.

(5) The NPIU shall permit air carriers to limit the transfer referred to in sub-article (4)(b) to updates of the transfers referred to in sub-article (4)(a).

(6) Where access to PNR data is necessary to respond to a specific and actual threat related to terrorist offences or serious crime, air carriers shall, on a case-by-case basis, transfer PNR data at other points in time than those mentioned in sub-article (4), upon request from the NPIU.

Exchange of information between the NPIU and corresponding PIUs of other EU Member States.

10. (1) All relevant and necessary PNR data or the result of processing that data, relating to persons identified by the NPIU in accordance with article 7(2), shall be transmitted by the NPIU to the corresponding PIUs of the other EU Member States.

(2) The NPIU shall transmit all the relevant and necessary PNR data or the result of processing that data from corresponding PIUs of other EU Member States to national competent authorities, only on a case-by-case basis and, in the event of automated processing of PNR data after individual review by non-automated means.

(3) As soon as practicable, the NPIU shall provide the corresponding PIU of any other EU Member State with PNR data kept in the database of the NPIU, which have not yet been depersonalised through masking out of data elements in accordance with article 13(2), and if necessary, the result of any processing of that data, if it has already been carried out pursuant to article 7(2)(a), when requested by such PIU of any other EU Member State.

(4) The request mentioned in sub-article (3), shall be duly reasoned and may be based on any one data element or a combination of such elements, as deemed necessary by the requesting PIU of any other EU Member State, for a specific case of prevention, detection, investigation or prosecution of terrorist offences or serious crime.

(5) In the event that the requested data has been depersonalised through masking out of data elements in accordance with article 13(2), the NPIU shall only provide the requesting EU Member State with the full PNR data where it is reasonably believed that it is necessary for the purpose referred to in article 7(2)(b) and only when authorised to do so by the national supervisory authority referred to in article 13(3)(b).

(6) The NPIU may process reasoned requests received directly from competent authorities of other EU Member States, to provide them with PNR data kept in its database, only in cases of emergency and under the conditions laid down in sub-articles (3), (4) and (5). A copy of the request shall always be sent to the corresponding PIU of the requesting EU Member State. In all other cases the NPIU shall only process requests from competent authorities when such requests are channelled through the corresponding PIU of the other EU Member State where the competent authority concerned is established.

(7) Exceptionally, where access to PNR data is necessary to respond to a specific and actual threat related to terrorist offences or serious crime, the NPIU shall obtain and provide the requesting PIU of another EU Member State with PNR data, in accordance with article 9(6).

(8) Exchange of information under this article may take place using any existing channels for cooperation between the national competent authorities and competent authorities of other EU Member States. The language used for the request and the exchange of information shall be the one applicable to the channel used.

(9) The NPIU shall have the right to request other corresponding PIUs of other EU Member States to be provided with PNR data in the circumstances covered in the previous sub-articles.

Conditions for access to PNR data by Europol.

11. (1) The NPIU shall transmit PNR data or processing results after receiving an electronic and duly reasoned request from the Europol National Unit, within the limits of its competences and for the performance of its tasks, for the transmission of specific PNR data or the result of processing that data:

Provided that such a request from Europol may be submitted when this is strictly necessary to support and strengthen action by the EU Member States to prevent, detect or investigate a specific terrorist offence or serious crime in accordance with the Europol Regulation.

(2) The request shall set out reasonable grounds on the basis of which Europol considers that the transmission of PNR data or the result of processing PNR data will substantially contribute to the prevention, detection or investigation of the criminal offence concerned.

S.L. 164.02.

(3) Exchange of information under this article shall take place through the Simplification of Exchange of Information or Intelligence between the Malta Police Force and other State Agencies of the Member States of the European Union having similar powers Regulations (hereinafter referred to as "SIENA") and in accordance with the Europol Regulation. The language used for the request and

the exchange of information shall be that applicable to SIENA.

Transfer of data to third countries. *Amended by: XX.2018.35.*

12. (1) The NPIU may transfer PNR data and the result of processing such data that is stored by the NPIU in accordance with article 13 to a third country, only on a case-by-case basis and if:

S.L 586.08.

(a) the conditions laid down in the Data Protection (Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties) Regulations are met;

(b) the transfer is necessary for the purposes of this Act referred to in article 3(2);

(c) the third country agrees to transfer the data to another third country only where it is strictly necessary for the purposes of this Act referred to in article 3(2), and only with the express authorisation of the NPIU; and

(d) the same conditions as those laid down in article 10(3), (4) and (5) are met.

S.L. 586.08.

(2) Notwithstanding the Data Protection (Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties) Regulations, a transfer of PNR data without prior consent of the EU Member State from which the data was obtained shall be permitted in exceptional circumstances and only if:

(a) such transfer is essential to respond to a specific and actual threat related to terrorist offences or serious crime in an EU Member State or a third country; and

(b) prior consent cannot be obtained in good time.

The NPIU shall be informed without delay and the transfer shall be duly recorded and subject to an *ex-post* verification.

(3) The NPIU shall transfer PNR data to the competent authorities of third countries only under conditions consistent with this Act and only upon ascertaining that the use the recipients intend to make of the PNR data is consistent with those conditions and safeguards.

(4) The Data Protection Officer of the NPIU shall be informed each time the NPIU transfers PNR data pursuant to this article.

Period of data retention and depersonalisation.

13. (1) The NPIU shall ensure that the PNR data provided by the air carriers is retained in a database at the NPIU for a period of five years from the date of its transfer to the PIU of the EU Member State on whose territory the flight is landing or departing.

(2) Upon expiry of a period of six months from the date of the transfer of the PNR data referred to in sub-article (1), all PNR data shall be depersonalised through masking out the following data elements which could serve to identify directly the passenger to whom the PNR data relates:

(a) name(s), including the names of other passengers on the PNR and number of travellers on the PNR travelling together;

(b) address and contact information;

(c) all forms of payment information, including billing address, to the extent that it contains any information which could serve to identify directly the passenger to whom the PNR relate or any other persons;

(d) frequent flyer information;

(e) general remarks to the extent that they contain any information which could serve to identify directly the passenger to whom the PNR relate; and

(f) any API data that has been collected.

(3) Upon expiry of the period of six months referred to in sub-article (2), disclosure of the full PNR data shall be permitted only where it is:

(a) reasonably believed that it is necessary for the purposes referred to in article 7(2)(b); and

(b) approved by:

(i) a judicial authority; or

(ii) the national supervisory authority to verify whether the conditions for disclosure are met, following a request made by the Data Protection Officer of the NPIU who carries out an expost review of such disclosure.

(4) The NPIU shall ensure that the PNR data is deleted permanently upon expiry of the period referred to in sub-article (1):

Provided that this obligation shall be without prejudice to cases where specific PNR data has been transferred to a national

competent authority or competent authority of other EU Member States and used in the context of specific cases for the purposes of preventing, detecting, investigating or prosecuting terrorist offences or serious crime, in which case data retention shall be regulated by the national law relevant to such competent authorities.

(5) The result of the processing referred to in article 7(2)(a) shall be kept by the NPIU only as long as necessary to inform the national competent authorities and, in accordance with article 10(1), to inform the corresponding NPIUs of other EU Member States of a positive match. Where the result of automated processing has, further to individual review by non-automated means as referred to in article 7(5), proven to be negative, it may be stored so as to avoid future "false" positive matches for as long as the underlying data is not deleted under sub-article (4).

Protection of personal data. *Amended by: XX.2018.35.*

14. (1) In respect of all processing of personal data pursuant to this Act, every passenger shall have the same right to protection of his personal data, rights of access, rectification, erasure and restriction and rights to compensation and judicial redress as laid down in the Data Protection (Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties) Regulations.

S.L. 586.08.

(2) The NPIU and national competent authorities shall ensure confidentiality of processing and data security in accordance with the Data Protection (Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties) Regulations, which shall apply to all processing of personal data pursuant to this Act.

S.L. 586.08.

(3) This Act is without prejudice to the applicability of the Data Protection Act and the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 regarding the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC, to the processing of personal data by air carriers (hereinafter referred to as the "General Data Protection Regulation").

Cap. 586.

(4) The NPIU and the national competent authorities shall not process PNR data which reveals a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation. In the event that PNR data revealing such information is received by the NPIU and the national competent authorities, it shall be deleted immediately.

(5) The NPIU shall maintain documentation relating to all processing systems and procedures under their responsibility. This documentation shall contain at least:

(a) the name and contact details of the organisation and personnel in the NPIU entrusted with the processing of the PNR data and the different levels of access authorisation;

(b) the requests made by competent authorities and PIUs of other EU Member States;

(c) all requests for and transfers of PNR data to a third country.

The NPIU shall make all documentation available, upon request, to the national supervisory authority.

(6) The NPIU shall keep records of the processing operations, which shall consist of, at least, the collection, consultation, disclosure and erasure:

Provided that the records of consultation and disclosure shall show, in particular, the purpose, date and time of such operations and, as far as possible, the identity of the person who consulted or disclosed the PNR data and the identity of recipients of that data. The records shall be used solely for the purposes of verification, of self-monitoring, of ensuring data integrity and data security or of auditing. The NPIU shall make the records available, upon request, to the national supervisory authority.

(7) The records referred to in sub-article (6) shall be kept for a period of five years.

(8) The NPIU shall implement appropriate technical and organisational measures and procedures to ensure a high level of security appropriate to the risks represented by the processing and the nature of the PNR data.

(9) The Commissioner of Police shall ensure that where a personal data breach is likely to result in a high risk for the protection of the personal data or affect the privacy of the data subject adversely, the NPIU shall communicate that breach to the data subject and to the national supervisory authority without undue delay.

Penalties.

15. (1) An air carrier which, as a result of a technical or non-technical fault, fails to transmit, in full or in part, PNR data in accordance with article 9 or does not do so in the required format, shall be liable to pay to the Principal Immigration Officer such penalty as may be established by him, being not less than three thousand euro (€3,000) and not exceeding five thousand euro (€5,000):

Provided that, in relation to extra-EU flights, an air carrier that has been found liable to pay a penalty under the Communication of Passenger Data by Air or Sea Carriers Order, shall not be sanctioned under this Act in relation to the non-transmission of the same set of data.

S.L. 460.18.

(2) Such penalty shall be recoverable by the Principal Immigration Officer, after the term within which an appeal to the Board may be entered has elapsed without an appeal having been entered, or after the decision of such Board, as a civil debt due to the Government and the provisions of article 466 of the Code of Organization and Civil Procedure shall, notwithstanding any other provision to the contrary, *mutatis mutandis* apply to such debt.

Cap. 12.

(3) An air carrier who feels aggrieved by any decision of the Principal Immigration Officer under sub-article (1) may, within twenty working days of the notification of the decision, enter an appeal to the Board against such decision and the Board shall have jurisdiction to hear and determine such appeals.

(4) In the case where the NPIU is in breach of its obligations under this Act or the Data Protection Act and any other regulation made under the said Act, it shall be liable to such penalty as may be established by the national supervisory authority pursuant to the provisions of the Data Protection Act and/or any other sanctions imposed by the courts of justice.

Cap. 586.

PART IV

The National Supervisory Authority.

16. (1) The national supervisory authority is responsible for advising on and monitoring the application within its territory of the logging provisions adopted by the NPIU and the national competent authorities pursuant to the Data Protection (Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties) Regulations.

S.L. 568.08.

(2) The national supervisory authority shall conduct activities under sub-article (1) with a view to protecting fundamental rights in relation to the processing of personal data.

(3) The national supervisory authority shall:

(a) deal with complaints lodged by any data subject, investigate the matter and inform the data subjects of the progress and the outcome of their complaints within a reasonable period of time;

(b) verify the lawfulness of the data processing, conduct investigations, inspection and audits in accordance with national law, either on its own initiative or on the basis of a complaint lodged by any data subject as referred to in sub-article (3)(a).

(4) The national supervisory authority shall, upon request, advise any data subject on the exercise of the rights laid down in provisions adopted pursuant to this Act.

Common protocols and supported data formats.

17. (1) All transfers of PNR data by air carriers to the NPIU for the purposes of this Act shall be made by electronic means that provide sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out:

Provided that in the event of a technical failure, the PNR data may be transferred by any other appropriate means having the same level of security maintained and ensuring that the Data Protection Act and any other regulation made thereunder are complied with:

Cap. 586.

Provided further that this sub-article shall apply for as long as the common protocols and supported data formats referred to in sub-articles (2), (3) and (4) are not available.

(2) The PNR data shall be transferred in a supported data format to ensure their readability by all parties involved.

(3) All transfers of PNR data by air carriers to the NPIU for the purposes of this Act shall be made electronically by using secure methods conforming to those common protocols, which shall be common to all transfers to ensure the security of the PNR data during transfer.

(4) All air carriers are required to select and identify to the NPIU the common protocol and data format that they intend to use for their transfers, provided the NPIU is satisfied that the data formats and transmission protocols provide an adequate level of security.

(5) It shall be ensured that the necessary technical measures are adopted to be able to use those common protocols and data formats within one year from the date of the adoption of the common protocols and supported data formats referred to in sub-articles (2), (3) and (4).

Statistical Data.

18. (1) On a yearly basis, the NPIU shall provide the European Commission with a set of statistical information on PNR data:

Provided that these statistics shall not contain any personal data.

(2) The statistics shall as a minimum cover:

(a) the total number of passengers whose PNR data has been collected and exchanged;

(b) the number of passengers identified for further examination.

Bilateral or Multilateral Agreements or Arrangements.

19. (1) This Act does not preclude the application of bilateral or multilateral agreements or arrangements entered into by Malta and other EU Member States on exchange of information between competent authorities that are in force on 24 May 2016, insofar as such agreements or arrangements are compatible with this Act.

Cap. 586.

(2) This Act is without prejudice to the applicability of the Data Protection Act and any regulations thereunder as well as Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(3) This Act is without prejudice to any obligations and commitments of EU Member States or of the European Union by virtue of bilateral or multilateral agreements with third countries.

Power to make Regulations.

20. (1) The Minister responsible for home affairs and national security may make regulations prescribing anything which is by this Act to be prescribed and generally for carrying the purposes or provisions of this Act into effect.

(2) The Minister may also by regulations amend or vary the Schedules to this Act, add schedules to this Act and amend or vary such other schedules.

SCHEDULE A

1. Malta Police Force.
2. Principal Immigration Officer.
3. Malta Security Service.
4. Financial Investigation and Analysis Unit.
5. Customs Department.
6. Judicial Authorities.

SCHEDULE B

1. PNR record locator.
2. Date of reservation/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/travel agent.
10. Travel status of passenger, including confirmations, check-in status, no-show or go-show information.
11. Split/divided PNR information.
12. General remarks (including all available information on unaccompanied minors under 18 years, such as name and gender of the minor, age, language(s) spoken, name and contact details of 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 the PNR.

18. Any advance passenger information (API) data collected (including the type, number, country of issuance and expiry date of any identity document, nationality, family name, given name, gender, date of birth, airline, flight number, departure date, arrival date, departure port, arrival port, departure time and arrival time).

19. All historical changes to the PNR listed in items 1 to 18.

SCHEDULE C

1. Participation in a criminal organization.

2. Terrorism.

3. Trafficking in human beings.

4. Sexual exploitation of children and child pornography.

5. Illicit trafficking in narcotic drugs and psychotropic substances.

6. Illicit trafficking in weapons, munitions and explosives.

7. Corruption.

8. Fraud, including that against the financial interests of the Union.

9. Laundering of the proceeds of crime and counterfeiting of currency, including the euro.

10. computer-related crime/cybercrime.

11. Environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties.

12. Facilitation of unauthorised entry and residence.

13. Murder, grievous bodily injury.

14. Illicit trade in human organs and tissue.

15. Kidnapping, illegal restraint and hostage-taking.

16. Organised and armed robbery.

17. Illicit trafficking in cultural goods, including antiques and works of art.

18. Counterfeiting and piracy of products.

19. Forgery of administrative documents and trafficking therein.

20. Illicit trafficking in hormonal substances and other growth promoters.

21. Illicit trafficking in nuclear or radioactive materials.

22. Rape.

23. Crimes within the jurisdiction of the International Criminal Court.

24. Unlawful seizure of aircraft/ships.

25. Sabotage.

26. Trafficking in stolen vehicles.

27. Industrial espionage.