STATUTORY INSTRUMENTS.

S.I. No. 177 of 2018

EUROPEAN UNION (PASSENGER NAME RECORD DATA) REGULATIONS 2018

S.I. No. 177 of 2018

EUROPEAN UNION (PASSENGER NAME RECORD DATA) REGULATIONS 2018

TABLE OF CONTENTS

Regulation

S.I. No. 177 of 2018

EUROPEAN UNION (PASSENGER NAME RECORD DATA) REGULATIONS 2018

I, CHARLES FLANAGAN , Minister for Justice and Equality, in exercise of the powers conferred on me by section 3 of the European Communities Act 1972 (No. 27 of 1972) and for the purpose of giving effect to Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016[1], hereby make the following regulations:

Citation and commencement

1. (1) These Regulations may be cited as the European Union (Passenger Name Record Data) Regulations 2018.

(2) These Regulations come into operation on 25 May 2018.

Interpretation

2. (1) In these Regulations—

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

"API data" means advance passenger information and includes 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;

"competent authority" means an authority competent for the prevention, detection, investigation or prosecution of terrorist offences or serious crime referred to in Regulation 9;

"competent authority of another Member State" means an authority of another Member State competent for the prevention, detection, investigation or prosecution of terrorist offences or serious crime;

"data protection officer" means a person appointed as such under Regulation 14;

"depersonalised through masking out of data elements" means rendering those elements which could serve to identify directly the data subject invisible to a user;

"Directive" means Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016;

[1]OJ No. L 119, 4.5.16, p.132

Notice of the making of this Statutory Instrument was published in "Iris Oifigiúil" of 29*th May*, 2018.

"Director" means Director of the PIU;

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

"Minister" means Minister for Justice and Equality;

"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 passenger's 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;

"PIU" means Passenger Information Unit, being—

(*a*) in the case of the State, the unit established under Regulation 4, and

(*b*) in the case of another Member State, the PIU established or designated by that other Member State;

"PNR data" means passenger name record data listed in Schedule 1, as far as collected by air carriers;

"push method" means the method whereby air carriers transfer PNR data listed in Schedule 1 into the PNR database of the authority requesting them to do so;

"serious crime" means the offences listed in Schedule 2 that are punishable by a custodial sentence or a detention order of a maximum period of at least 3 years;

"terrorist offences" means terrorist activity or terrorist linked activity within the meaning of section 4 or an offence under section 13 of the Criminal Justice (Terrorist Offences) Act 2005 (No. 2 of 2005).

(2) A word or expression that is used in these Regulations and that is also used in the Directive has, unless the context otherwise requires, the same meaning in these Regulations that it has in the Directive.

Scope

3. These Regulations provide for—

(*a*) the transfer by air carriers of passenger name record (PNR) data of passengers of extra-EU flights, and

(*b*) the processing of the data referred to in paragraph (*a*), including its collection, use and retention by the PIU and competent authorities and its exchange between other Member States.

Passenger Information Unit (PIU)

4. (1) There is established, as part of the Department of Justice and Equality, a unit to be known as the Passenger Information Unit ("PIU").

(2) The staff of the PIU shall be headed by a Director who shall be appointed by the Minister.

(3) The Director may enter into arrangements with the competent authorities designated under Regulation 9 for the secondment to the PIU of staff of the competent authorities.

(4) The Director may enter into arrangements to engage persons (on contract or otherwise) for a period of temporary service with the PIU.

(5) A staff member of the PIU or a person who is engaged by it under paragraph (4) may be designated in writing by the Director for the purpose of the performance of functions under any provision of these Regulations.

(6) The Minister shall nominate a person to perform the functions of the Director during any absence, incapacity or suspension from duty or during any vacancy in the office.

(7) The PIU shall be responsible for—

(*a*) collecting PNR data from air carriers, storing and processing those data and transferring those data, or the result of the processing of them, to the competent authorities, and

(*b*) exchanging PNR data and the result of the processing of those data with the PIUs of other Member States and with Europol in accordance with Regulations 6 and 7, respectively.

Processing of PNR Data by PIU

5. (1) The PIU shall process data only for the following purposes:

(*a*) carrying out of an assessment of passengers prior to their scheduled arrival in or departure from the State in order to identify persons who require further examination by a competent authority referred to in Regulation 9 and, where relevant, by Europol in accordance with Regulation 8, to determine whether such persons may be or may have been 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 a competent authority to provide and process PNR data in specific cases for the purpose of the prevention, detection, investigation and prosecution of terrorist offences or

serious crime and to provide a competent authority or, where appropriate, Europol, with the results of such processing;

(*c*) analysing of PNR data for the purpose of updating or creating new criteria to be used in the assessments carried out under paragraph (1)(*a*) in order to identify any person or persons who may be involved in a terrorist offence or serious crime.

(2) PNR data shall not be processed in such a manner as to reveal 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 are received by the PIU, they shall be deleted immediately.

(3) When carrying out an assessment under paragraph (1)(*a*) the PIU may—

(*a*) compare PNR data against databases relevant for the purpose of the prevention, detection, investigation and prosecution of terrorist offences or serious crime, including databases on persons or objects sought or under alert, in accordance with European Union, international and Irish law applicable to such databases, or

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

(4) An assessment of passengers prior to their arrival in or departure from the State carried out under paragraph (1)(*a*) against pre-determined criteria shall be carried out in a non-discriminatory manner.

(5) Pre-determined criteria used in the assessment of passengers—

(*a*) shall be targeted, proportionate and specific in nature,

(*b*) shall be regularly reviewed in consultation with the competent authorities, and

(*c*) shall not, in any circumstance, be based on a person's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life or sexual orientation.

(6) Where PNR data collected include data other than those listed in Schedule 1 such data shall be deleted immediately and permanently upon receipt.

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

Transfer of PNR data by PIU to other Member State and competent authorities

6. (1) Where the PIU carries out an assessment of passengers under Regulation 5(1)(*a*) and identifies a person who requires further examination by a relevant competent authority, the PIU shall, subject to paragraph (4), transmit the PNR data relating to that person and the result of the processing of those data, to the PIU's of other relevant Member States.

(2) PNR data and the result of the processing of those data transmitted to the PIU in accordance with paragraph (1) shall also be transmitted by the PIU to the relevant competent authority.

(3) PNR data relating to a person and the result of the processing of those data which is transmitted to the PIU by the PIU of another Member State shall, subject to paragraph (4), be transmitted by the PIU to the relevant competent authority.

(4) The PIU shall transmit PNR data relating to a person and the result of the processing of those data to a relevant competent authority only on a case-by-case basis and, where the person has been identified by automated processing of PNR data, where the identification has been reviewed by non-automated means.

Exchange of PNR data with other Member States

Incoming requests

7. (1) Where a reasoned request is received from the PIU of a Member State for PNR data that have not been depersonalised through masking out, or the result of the processing of those data, the PIU shall transmit any such information in its possession to the PIU of the Member State as soon as practicable.

(2) Where a reasoned request is received from the PIU of another Member State for PNR data that have been depersonalised through masking out of data elements under Regulation 11(4), or the result of the processing of those data, the PIU shall—

(*a*) where there are reasonable grounds for believing that transmitting the full data is necessary for the purpose of preventing, detecting, investigating or prosecuting terrorist offences or serious crime, and

(*b*) where the District Court, on application to it by the PIU in that regard, approves the transmission,

transfer the full data to the PIU of the other Member State.

(3) In relation to subparagraph (2)(*b*), District Court hearings of applications shall be heard otherwise than in public.

(4) Where, in cases of emergency, a reasoned request is received from the competent authority of another Member State for PNR data that have not been depersonalised through masking out, or the result of the processing of those data, the PIU shall transfer such data to the competent authority of the Member State.

(5) Where, in cases of emergency under Regulation 7(4), a reasoned request is received from the competent authority of another Member State for PNR data that have been depersonalised through masking out, or the result of the processing of those data, the PIU shall—

(*a*) where there are reasonable grounds for believing that transmitting the full data is necessary for the purpose of preventing, detecting, investigating or prosecuting terrorist offences or serious crime, and

(*b*) where the District Court, on application to it by the PIU in that regard, approves the transmission,

transfer the full data to the competent authority of the other Member State.

(6) In relation to subparagraph (5)(*b*), District Court hearings of applications shall be heard otherwise than in public.

(7) Where, in exceptional circumstances, a request is received from the PIU of a Member State to obtain PNR data at a time other than that provided for in Regulation 10(4) and there are reasonable grounds to believe that the data requested is necessary to respond to a specific and actual threat related to terrorist offences or serious crime, the PIU may request the air carrier to transfer the requested PNR data to the PIU in accordance with Regulation 10(6) and the PIU shall, in turn, transfer the PNR data to the PIU of the requesting Member State.

Outgoing requests

(8) The PIU may make a reasoned request for PNR data to the PIU of a Member 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. Such a request may be based on one or more data elements and shall set out the reasons for the request.

(9) In cases of emergency a competent authority may make a direct request for PNR data to the PIU of another Member State where there are reasonable grounds to believe that the request constitutes an emergency and that the data is necessary for the prevention, detection, investigation or prosecution of a terrorist offence or serious crime. In such a case, a copy of the request shall also be sent to the PIU by the competent authority. In all other cases, a competent authority shall channel its requests through the PIU.

(10) In exceptional circumstances, the PIU may request the PIU of another Member State to request an air carrier to transfer PNR data to the PIU of that other Member State at a time other than the time at which the air carrier transfers PNR data to the PIU of that Member State and to transfer those data to the PIU where access to the PNR data requested is necessary to respond to a specific and actual threat related to terrorist offences or serious crime.

Request for PNR data from Europol

8. (1) Where an electronic and duly reasoned request is received from Europol on a case-by-case basis for PNR data that have not been depersonalised through masking out, or the result of the processing of those data, the PIU shall transfer any such information to Europol, where, having considered the request, there are reasonable grounds to believe that the transmission of the requested data will substantially contribute to the prevention, detection or investigation of the offence concerned.

(2) Where a reasoned request is received from Europol for PNR data that have been depersonalised through masking out, or the result of the processing of those data, the PIU shall—

(*a*) where there are reasonable grounds for believing that transmitting the full data will substantially contribute to the prevention, detection or investigation of the offence concerned, and

(*b*) where the District Court, on application to it by the PIU in that regard, approves the transmission,

transmit the full data to Europol.

(3) In relation to subparagraph (2)(*b*), District Court hearings of applications shall be heard otherwise than in public.

Competent authorities

9. (1) The authorities listed in Schedule 3 are entitled to request or receive PNR data or the result of processing that data from the PIU or the PIU of another Member State in order to examine that information further or to take appropriate action for the purpose of preventing, detecting, investigating and prosecuting terrorist offences or serious crime.

(2) Where a competent authority requests from the PIU PNR data that have been depersonalised through masking out, or the result of the processing of those data, disclosure of the full PNR data shall be permitted only—

(*a*) where there are reasonable grounds for believing that transmitting the full data is necessary for the purpose of preventing, detecting, investigating or prosecuting terrorist offences or serious crime, and

(*b*) where the District Court, on application to it by the PIU in that regard, approves the transmission.

(3) In relation to subparagraph (2)(*b*), District Court hearings of applications shall be heard otherwise than in public.

(4) PNR data and the result of the processing of those data may be further processed by a national competent authority only for the purpose of the prevention, detection, investigation and prosecution of terrorist offences or serious crime.

(5) Paragraph (4) is without prejudice to law enforcement or judicial powers where other offences, or indications thereof, are detected in the course of enforcement action further to such processing.

(6) A competent authority 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 transfer of PNR data

10. (1) An air carrier shall, in accordance with this Regulation, transfer by the push method to the database of the PIU all PNR data which it has collected in the normal course of business in respect of passengers to be carried by that air carrier on an extra-EU flight.

(2) Where a flight in respect of which PNR data is required to be collected and transmitted is code-shared between one or more air carriers, the air carrier which operates the flight shall transmit the PNR data of all passengers on the flight to the PIU.

(3) Where an air carrier collects API data, but does not retain those data by the same technical means as for other PNR data, it shall transfer the API data to the PIU by the push method and such data shall be considered as PNR data for the purposes of these Regulations.

(4) An air carrier shall—

(*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,

transfer PNR data to the PIU—

(i) by electronic means by using the common protocols and supported data formats adopted in accordance with Article 17(2) of the Directive, or

(ii) in the event of technical failure or difficulty, by any other appropriate means ensuring the same level of technical and organisational security.

(5) An air carrier may, when providing updated passenger information under paragraph (4)(*b*), limit the transmission of PNR data to an update of the information previously provided.

(6) An air carrier shall also transfer PNR data to the PIU, on a case-by-case basis, at the request of the PIU at times other than those provided for in paragraph (4) where access to that data is required in order to respond to a specific and actual threat related to terrorist offences or serious crime.

(7) An air carrier shall comply with a requirement under this Regulation.

Period of data retention and depersonalisation

11. (1) PNR data provided by an air carrier to the PIU shall be retained in a database of the PIU for a period of 5 years after their transfer to the PIU.

(2) PNR data transferred in accordance with paragraph (1) shall be deleted permanently upon the expiration of the period of 5 years after they were transferred.

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

(*a*) upon the expiration of a period of 5 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) PNR data transferred by an air carrier to the PIU shall, after a period of 6 months from their transfer, be depersonalised through masking out the following data elements which could serve to identify directly the passenger to whom the PNR data relate:

(*a*) passenger name or names, including the names of other passengers on the PNR and number of passengers on the PNR travelling together;

(*b*) address and contact information;

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

(*d*) frequent flyer information;

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

(*f*) any API data that have been collected.

(5) The result of the assessment of passengers under Regulation 5(1)(*a*) shall only be retained by the PIU for as long as is necessary to inform the competent authorities in accordance with Regulation 6(2) and to inform the PIUs of other Member States in accordance with Regulation 6(1) of a positive match.

(6) Where the result of automated processing has, following individual review by non-automated means in accordance with Regulation 6(4), proven to be negative it may be retained in order to avoid future false positive matches for as long as the underlying data are not destroyed in accordance with this Regulation.

Retention of documentation

12. (1) The PIU shall maintain documentation relating to all of its processing systems and procedures. That documentation shall contain at least—

(*a*) the name and contact details of the organisation and personnel of the PIU entrusted with the processing of PNR data and the different levels of access authorisation,

(*b*) the requests made by the competent authorities and the PIUs of other Member States, and

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

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

(3) Records kept under paragraph (2) 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.

(4) Records kept under paragraph (2) 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 5 years.

(5) The PIU shall, on request, make available to the Data Protection Commission all documentation required to be maintained under this Regulation.

(6) 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.

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

Restriction of disclosure of data or documentation

13. The Director of the PIU shall ensure that all—

(*a*) documentation created by or on behalf of the PIU in relation to processing systems and procedures and all records kept by the PIU in accordance with Regulation 12, and

(*b*) data retained in accordance with Regulation 11,

are kept securely and that only such persons as are authorised in writing by him or her shall be permitted to have access to such documentation or data.

Data protection officer

14. (1) The Director shall appoint a data protection officer responsible for monitoring the processing of PNR data and for data protection safeguards under these Regulations.

(2) A data subject may contact the data protection officer, as a single point of contact, on all issues relating to the processing of that subject's PNR data.

(3) The Director shall—

(*a*) ensure that the data protection officer is involved in an appropriate and timely manner in all matters relating to the protection of personal data,

(*b*) support the data protection officer in performing the tasks referred to in paragraph (4) by providing access to processing operations and the resources necessary to carry out these tasks, and

(*c*) assist the data protection officer in maintaining his or her expert knowledge in relation to data protection matters.

(4) The tasks of the data protection officer shall include the following:

(*a*) informing and advising the Director and members of the PIU who are processing PNR data of their obligations under these Regulations;

(*b*) providing advice on awareness-raising activities, staff training, and the allocation of responsibilities in relation to data protection, as well as advising on and monitoring the carrying out of data protection impact assessments;

(*c*) monitoring compliance with these Regulations concerning data protection and with the policies of the data controller in relation to the protection of personal data, including audit activity;

(*d*) acting as a contact point for issues related to the processing of personal data.

Functions of Data Protection Commission

15. (1) The Data Protection Commission (subsequently in this Regulation referred to as the "Commission") is responsible for advising on and monitoring the application of these Regulations within the State with a view to protecting fundamental rights in relation to the processing of personal data.

(2) The Commission shall—

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

(*b*) verify the lawfulness of the data processing under these Regulations, and

(*c*) conduct investigations, inspections and audits, either on its own initiative or on the basis of a complaint referred to in paragraph (2)(*a*).

(3) The Commission shall, upon request, advise any data subject on the exercise of the data protection rights laid down in these Regulations.

Transfer of data to third countries

16. (1) The PIU may, on a case-by-case basis, transfer PNR data and the results of the processing of such data that are retained by the PIU in accordance with Regulation 11 to a third country, if—

(*a*) such transfer is in accordance with the Data Protection Act 2018,

(*b*) the transfer is necessary for the purpose of the prevention, detection, investigation and prosecution of a terrorist offence or serious crime,

(*c*) the third country concerned agrees to transfer the data to another third country only where it is strictly necessary for the purpose of the prevention, detection, investigation and prosecution of a terrorist offence or serious crime, and only with the authorisation of the Director of the PIU, and

(*d*) the conditions laid down in Regulation 7(1) and (2) are met.

(2) Where a reasoned request is received from a third country for PNR data that have been depersonalised through masking out, or the result of any processing of those data, the PIU shall—

(*a*) where there are reasonable grounds for believing that transmitting the full data is necessary for the purpose of preventing, detecting, investigating or prosecuting terrorist offences or serious crime, and

(*b*) where the District Court, on application to it by the PIU in that regard, approves the transmission,

transmit the full data to the third country concerned, in accordance with the requirements of this Regulation.

(3) In exceptional circumstances, the PIU may permit the transfer of PNR data to a third country without the prior consent of the other Member State from which the PNR data were obtained, only if—

(*a*) such transfers are essential in order to respond to a specific and actual threat related to terrorist offences or serious crime in another Member State or third country, and

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

(4) Where a transfer takes place in accordance with paragraph (3), the PIU shall inform the PIU of the Member State from which the PNR data was originally received without delay and a record of the transfer shall be made.

(5) PNR data shall only be transferred to the competent authorities of third countries in accordance with the terms and conditions of these Regulations and upon ascertaining that the use the recipients intend to make of the PNR data is consistent with those conditions and safeguards.

(6) The data protection officer shall be informed of all transfers of PNR data to a third country made in accordance with this Regulation.

Offence — non-compliance by air carrier with Regulation 10

17. (1) An air carrier who fails to comply with Regulation 10 commits an offence and is liable—

(*a*) on summary conviction, to a class A fine, or

(*b*) on conviction on indictment, to a fine not exceeding €250,000.

(2) It is a defence for an air carrier charged with an offence under this Regulation to show that the air carrier took all reasonable steps to ensure compliance with Regulation 10.

(3) An offence under this Regulation may be brought and prosecuted summarily by the Director.

Offences by bodies corporate

18. (1) If an offence under Regulation 17 is committed by a body corporate and the offence is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of, a person who is a director, manager, secretary or other similar officer of the body, or is a person who was purporting to act in any such capacity, that person as well as the body corporate commits an offence and is liable to be proceeded against and punished as if that person had committed the first-mentioned offence.

(2) If the affairs of a body corporate are managed by its members, paragraph (1) applies in relation to the acts and omissions of a member of the body in connection with the member's functions of management as if the member were a director or manager of it.

Reporting of statistical information

19. (1) On a yearly basis from the next year following the making of these Regulations, not later than May 31 in each year, the Director shall submit to

the Minister a report containing statistical information on PNR data provided to the PIU.

(2) The statistics required to be provided in accordance with paragraph (1) shall as a minimum cover—

(*a*) the total number of passengers whose PNR data have been collected and exchanged, and

(*b*) the number of passengers identified for further information.

(3) The statistics provided under this Regulation shall not contain any personal data.

SCHEDULE 1

Regulation 2

Passenger name record (PNR) data

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, email 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 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 data listed in numbers 1 to 18 above.

SCHEDULE 2

Regulation 2

Serious crime

1. ***Participation in a criminal organisation.***

An offence under—

section 21 or 21A of the Offences against the State Act 1939 (No. 13 of 1939)

section 6 of the Offences against the State (Amendment) Act 1998 (No. 39 of 1998)

section 72 or 73 of the Criminal Justice Act 2006 (No. 26 of 2006)

2. ***Trafficking in human beings.***

An offence under—

section 3 of the Child Trafficking and Pornography Act 1998 (No. 22 of 1998)

section 2 of the Illegal Immigrants (Trafficking) Act 2000 (No. 29 of 2000)

section 2, 4 or 5 of the Criminal Law (Human Trafficking) Act 2008 (No. 8 of 2008)

3. ***Sexual exploitation of children and child pornography.***

An offence under—

section 3, 4, 5 or 6 of the Child Trafficking and Pornography Act 1998 (No. 22 of 1998)

section 249(1) of the Children Act 2001 (No. 24 of 2001)

section 176(2) of the Criminal Justice Act 2006 (No. 26 of 2006)

section 2 or 3 of the Criminal Law (Sexual Offences) Act 2006 (No. 15 of 2006)

section 3, 4, 5, 6, 7 or 8 of the Criminal Law (Sexual Offences) Act 2017 (No. 2 of 2017)

4. ***Illicit trafficking in narcotic drugs and psychotropic substances.***

An offence under—

section 3, 15, 15A, 15B, 17, 19 or 21 of the Misuse of Drugs Act 1977 (No. 12 of 1977)

section 34 of the Criminal Justice Act 1994 (No. 15 of 1994)

section 3(1), 4, 5(1), 8(6) or 10(8) of the Criminal Justice (Psychoactive Substances) Act 2010 (No. 22 of 2010)

section 14 of the Customs Act 2015 (No. 18 of 2015)

5. ***Illicit trafficking in weapons, munitions and explosives.***

An offence under—

section 4, 5, 31, 40, 43 or 81 of the Explosives Act 1875 (1875 c. 17)

section 2, 3, 4(1) or 5 of the Explosive Substances Act 1883 (1883 c. 3)

section 2, 15, 16 or 17 of the Firearms Act 1925 (No. 17 of 1925)

section 27A or 27B of the Firearms Act 1964 (No. 1 of 1964)

section 7, 8 or 12 of the Firearms and Offensive Weapons Act 1990 (No. 12 of 1990)

section 14 of the Customs Act 2015 (No. 18 of 2015)

6. ***Corruption.***

An offence under—

section 1 (inserted by section 2 of the Prevention of Corruption (Amendment) Act 2001 (No. 27 of 2001)) of the Prevention of Corruption Act 1906 (1906 c. 34)

section 8 of the Prevention of Corruption (Amendment) Act 2001 (No. 27 of 2001)

7. ***Fraud, including that against the financial interests of the European Union.***

Conspiracy to defraud

An offence under—

section 119 of the Registration of Title Act 1964 (No. 16 of 1964)

section 2 of the Criminal Damage Act 1991 (No. 31 of 1991)

section 1078 of the Taxes Consolidation Act 1997 (No. 39 of 1997)

section 102 of the Finance Act 1999 (No. 2 of 1999)

section 4, 6, 7, 9, 10, 11, 25, 26, 27, 28, 29, 42, 43, 44, 45 or 51 of the Criminal Justice (Theft and Fraud Offences) Act 2001 (No. 50 of 2001)

section 119 of the Finance Act 2001 (No. 7 of 2001)

subsection (3) or (4) of section 78 of the Finance Act 2005 (No. 5 of 2005)

section 251, 252, 253, 254, 255, 262 or 262A of the Social Welfare Consolidation Act 2005 (No. 26 of 2005)

section 17 or 19 of the Criminal Justice Act 2011 (No. 22 of 2011)

section 14 of the Customs Act 2015 (No. 18 of 2015)

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

An offence under—

section 33, 34, 35, 36, 37 or 38 of the Criminal Justice (Theft and Fraud Offences) Act 2001 (No. 50 of 2001)

section 7, 8, 9 or 10 of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (No. 6 of 2010)

9. ***Computer-related crime / cybercrime.***

An offence under—

section 2, 3 or 4 of the Criminal Damage Act 1991 (No. 31 of 1991)

section 9 of the Criminal Justice (Theft and Fraud Offences) Act 2001 (No. 50 of 2001)

section 2, 3, 4, 5 or 6 of the Criminal Justice (Offences Relating to Information Systems) Act 2017 (No. 11 of 2017)

section 8 of the Criminal Law (Sexual Offences) Act 2017 (No. 2 of 2017)

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

An offence under—

section 3 or 4 of the Local Government (Water Pollution) Act 1977 (No. 1 of 1977)

section 32 of the Waste Management Act 1996 (No. 10 of 1996)

11. ***Facilitation of unauthorised entry and residence.***

An offence under section 2 of the Illegal Immigrants (Trafficking) Act 2000 (No. 29 of 2000)

12. ***Murder, grievous bodily injury.***

Murder

An offence under—

section 18 or 19, in relation to assault, of the Criminal Justice (Public Order) Act 1994 (No. 2 of 1994)

section 3, 4, 5, 6 or 13 of the Non-Fatal Offences against the Person Act 1997 (No. 26 of 1997)

13. ***Illicit trade in human organs and tissue.***

An offence under section 2 or 4 of the Criminal Law (Human Trafficking) Act 2008 (No. 8 of 2008)

14. ***Kidnapping, illegal restraint and hostage-taking.***

An offence under—

section 15, 16 or 17 of the Non-Fatal Offences against the Person Act 1997 (No. 26 of 1997)

section 9 of the Criminal Justice (Terrorist Offences) Act 2005 (No. 2 of 2005)

15. ***Organised and armed robbery.***

An offence under—

section 4, 12, 13, 14, 15, 17 or 18 of the Criminal Justice (Theft and Fraud Offences) Act 2001 (No. 50 of 2001)

section 71, 71A, 72 or 73 of the Criminal Justice Act 2006 (No. 26 of 2006)

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

An offence under section 4, 12, 13, 14, 15, 17 or 18 of the Criminal Justice (Theft and Fraud Offences) Act 2001 (No. 50 of 2001)

17. ***Counterfeiting and piracy of products.***

An offence under—

section 92 of the Trade Marks Act 1996 (No. 6 of 1996)

section 140 or 141 of the Copyright and Related Rights Act 2000 (No. 28 of 2000)

section 33, 34, 35, 36, 37 or 38 of the Criminal Justice (Theft and Fraud Offences) Act 2001 (No. 50 of 2001)

18. ***Forgery of administrative documents and trafficking therein.***

An offence under section 25, 26, 27, 28 or 29 of the Criminal Justice (Theft and Fraud Offences) Act 2001 (No. 50 of 2001)

19. ***Illicit trafficking in hormonal substances and other growth promoters.***

An offence under—

Regulation 69 of the European Communities (Animal Remedies) (No. 2) Regulations 2007 (S. I. No. 786 of 2007)

Regulation 34 of the European Communities (Control of Animal Remedies and their Residues) Regulations 2009 (S. I. No. 183 of 2009)

20. ***Illicit trafficking in nuclear or radioactive materials.***

An offence under section 38 of the Radiological Protection Act 1991 (No. 9 of 1991)

21. ***Rape.***

Rape

22. ***Crimes within the jurisdiction of the International Criminal Court.***

An offence under section 7, 8 or 11 of the International Criminal Court Act 2006 (No. 30 of 2006)

23. ***Unlawful seizure of aircraft/ships.***

An offence under—

section 11 of the Air Navigation and Transport Act 1973 (No. 29 of 1973)

section 3 of the Air Navigation and Transport Act 1975 (No. 9 of 1975)

section 10 of the Criminal Law (Jurisdiction) Act 1976 (No. 14 of 1976)

section 2 of the Maritime Security Act 2004 (No. 29 of 2004)

24. ***Sabotage.***

An offence under section 2 of the Criminal Damage Act 1991 (No. 31 of 1991)

25. ***Trafficking in stolen vehicles.***

An offence with a view to trafficking a stolen vehicle under—

section 112(2) (inserted by section 3 of the Road Traffic Act 1984 (No. 16 of 1984)) of the Road Traffic Act 1961 (No. 24 of 1961)

section 10 of the Criminal Law (Jurisdiction) Act 1976 (No. 14 of 1976)

section 4, 14, 17 or 18 of the Criminal Justice (Theft and Fraud Offences) Act 2001 (No. 50 of 2001)

26. ***Industrial espionage.***

An offence under—

section 4, 9, or 15 of the Criminal Justice (Theft and Fraud Offences) Act 2001 (No. 50 of 2001)

section 2, 3, 4, 5 or 6 of the Criminal Justice (Offences Relating to Information Systems) Act 2017 (No. 11 of 2017)

SCHEDULE 3

Regulation 9

Competent authorities

Department of Justice and Equality (including Irish Naturalisation and Immigration Service)

Garda Síochána

Office of the Revenue Commissioners

Department of Employment Affairs and Social Protection

Permanent Defence Force

L.S.

GIVEN under my Official Seal,
24 May 2018.

CHARLES FLANAGAN,
Minister for Justice and Equality.

BAILE ÁTHA CLIATH
ARNA FHOILSIÚ AG OIFIG AN tSOLÁTHAIR
Le ceannach díreach ó
FOILSEACHÁIN RIALTAIS,
52 FAICHE STIABHNA, BAILE ÁTHA CLIATH 2
(Teil: 01 - 6476834 nó 1890 213434; Fax: 01 - 6476843)
nó trí aon díoltóir leabhar.

_____

DUBLIN
PUBLISHED BY THE STATIONERY OFFICE
To be purchased from
GOVERNMENT PUBLICATIONS,
52 ST. STEPHEN'S GREEN, DUBLIN 2.
(Tel: 01 - 6476834 or 1890 213434; Fax: 01 - 6476843)
or through any bookseller.

_____

ISBN 978-1-4468-7493-6

€6.60

9 781446 874936

Wt. (B33492). 285. 5/18. Essentra. Gr 30-15.