Subsidiary Legislation made under s.67.

IMMIGRATION (PASSENGER NAME RECORD) RULES 2018

(LN. 2018/120)

Commencement **24.5.2018**

Transposing-
Directive 2016/681/EU

ARRANGEMENT OF REGULATIONS.

Regulation

IMMIGRATION (PASSENGER NAME RECORD) RULES 2018

Subsidiary 2018/120

In exercise of the powers conferred upon it by section 67 of the Immigration, Asylum and Refugee Act and all other enabling powers, and in order to transpose into the law of Gibraltar Directive 2016/681/EU 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, the Government has made the following Rules-

Title and commencement.

1.(1) These Rules may be cited as the Immigration (Passenger Name Record) Rules 2018 and come into operation on the day of publication.

(2) These Rules operate without prejudice to and in conjunction with the Immigration (Passenger Data) Rules 2014 in relation to Advanced Passenger Information ("API").

(3) These Rules shall apply to all inbound and outbound flights to and from Gibraltar.

Interpretation.

2.(1) In these Rules-

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

"API" means Advanced Passenger Information, as defined in the Immigration (Passenger Data) Rules 2014;

"flight" means any scheduled or non-scheduled inbound or outbound flight by an air carrier to and from Gibraltar including both direct flights and flights with any stop-overs;

"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;

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

"push method" means the method whereby air carriers transfer PNR data listed in Schedule 2 into the database of the authority requesting them;

"terrorist offences" means the offences under Gibraltar Law referred to in Terrorism Act 2005;

"serious criminal offences" refer to criminal offences in Gibraltar that attract a maximum custodial sentence of at least three years and are of the nature listed in Schedule 3 of these Rules;

"supervisory authority" as defined in section 21 of the Data Protection Act 2004 as the Gibraltar Regulatory Authority acting as a Data Protection Commissioner;

"PIU" means the Passenger Information Unit as defined in Rule 3 of these Rules; and

"the Act" should be taken to mean the Immigration, Asylum and Refugee Act.

(2) Other terms used in these Rules shall be construed consistently with equivalent terms used in the Directive 2016/681/EU 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.

Passenger information unit.

3.(1) The Passenger Information Unit shall be the competent authority for the prevention, detection, investigation or prosecution of terrorist offences and of serious crime.

(2) 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 processing them to the competent authorities referred to in Schedule 1; and

(b) exchanging both PNR data and the result of processing those data with the PIUs of Member States and with Europol.

(3) The PIU shall be composed of the Principal Immigration Officer and any other staff which may be necessary for its operation.

Data protection officer.

4.(1) The PIU shall appoint a data protection officer responsible for monitoring the processing of PNR data and implementing relevant safeguards.

(2) The data subject has the right to contact the data protection officer on all issues relating to the processing of that data subject's PNR data.

Processing of PNR data.

5.(1) If PNR data transferred by air carriers includes data other than that listed in Schedule 2, the PIU shall delete such data immediately and permanently upon receipt.

(2) The PIU 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 Gibraltar to identify persons who require further examination by the Competent Authorities in Schedule 1 and where relevant, by Europol in accordance with the Europol Regulations 2017, in view of the fact that such persons may be involved in a terrorist or serious criminal offence;

(b) responding, on a case-by-case basis to a duly reasoned request based on sufficient grounds from the competent authorities to provide and process PNR data in specific cases for the purposes of preventing, detecting, investigating and prosecuting terrorist or serious criminal offences and to provide the 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 subrule (3)(b) in order to identify any persons who may be involved in a terrorist or serious criminal offence.

(3) When carrying out the assessment referred to in subrule (2)(a), the PIU 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 all laws in Gibraltar applicable to such databases; or

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

(4) Any assessment of pre-determined criteria shall be carried out in a non-discriminatory manner and shall not 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) Any positive match resulting from the automated processing of PNR data conducted under subrule (2)(a), shall be individually reviewed by non-automated means to verify whether the competent authority needs to take action.

(6) PNR data shall be transmitted by the PIU of persons identified in accordance with subrule (2)(a) to the competent authorities. 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) The data protection officer shall have access to all data processed by the PIU.

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

(9) Subrule (2)(a) shall not prevent the right of entry of persons enjoying their right to free movement into Gibraltar pursuant to section 55J of the Act.

Obligations on air carriers.

6.(1) Air carriers shall use the "push method" to transfer PNR data listed in Schedule 2 to the database of the PIU for both flight arrivals and departures within Gibraltar.

(2) API data referred to in point 18 of Schedule 2 shall be transferred by "push method" to the database of the PIU, regardless of the technical means by which it is collected.

(3) Data shall be transferred 24 to 48 hours before scheduled flight departure time and immediately after the boarding gate has closed.

(4) Transmission at any time other than in subrule (3) shall be permitted in response to a specific and actual threat related to a terrorist or serious criminal offence.

Exchange of information between Member States.

7.(1) The PIU shall transmit all relevant and necessary PNR data or the result of processing those data to the corresponding PIUs of a Member State.

Received information shall be transmitted to the competent authorities listed in Schedule 1.

(2) The PIU shall have the right to request that the PIU of any Member State provide it with PNR data that are kept in the Member State's database and that have not been depersonalised. Such a request shall be a reasonable for the purpose of a specific case of prevention, detection, investigation or prosecution of terrorist or serious criminal offences.

(3) The PIU of a Member State shall have the right to make the request described in subrule (2) of the PIU in Gibraltar.

(4) If such data as requested in subrule (3) has been depersonalised pursuant to rule 9, the PIU shall only provide the full PNR data where it is reasonably believed that it is necessary for the purpose referred to in rule 5(2)(b), only when authorised by an authority referred to in rule 9(3)(b).

(5) The competent authorities of a Member State may request the PIU provide them with PNR data from the PIU database only when necessary in cases of emergency and under the above conditions in subrule (2).

(6) The PIU shall have the right to request that the PIU of a Member State provide access to PNR data when necessary to respond to a specific and actual threat related to terrorist or serious criminal offences.

(7) Existing channels between Gibraltar and competent authorities in Member States shall be used for cooperation.

Transfer of data to third countries.

8.(1) The PIU may transfer PNR data and the result of processing such data that is stored by the PIU in accordance with Rule 9 on data retention and depersonalisation, only on a case-by-case basis and if-

(a) the conditions laid down in regulation 15 of the Data Protection (Police And Judicial Cooperation in Criminal Matters) Regulations 2014;

(b) the transfer is necessary for the purposes referred to in rule 5(2);

(c) the third country agrees to transfer the data to another third country only where it is strictly necessary for the purposes of

these Rules referred to in rule 5(2) and only with the express authorisation of the PIU; and

(d) the same conditions in rule 7(2) are met.

(2) Notwithstanding Regulation 15 of the Data Protection (Police and Judicial Cooperation in Criminal Matters) Regulations 2014, transfers of PNR data without prior consent of the Member State from which the data were obtained shall be permitted in exceptional circumstances and only if-

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

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

(3) The PIU shall transfer PNR data to the competent authorities of third countries only under conditions consistent with these Rules and upon ascertaining that the recipients intend to make use of that PNR data in accordance with those conditions and safeguards.

(4) The data protection officer of the PIU that has transferred PNR data, shall be informed each time the PIU transfers PNR Data.

Period of data retention and depersonalisation.

9.(1) PNR data provided by air carriers to the PIU shall be retained in a database at the PIU for a period of 5 years after the transfer to the PIU.

(2) Upon expiry of a period of 6 months after the transfer of the PNR data referred to in subrule (1), all PNR data shall be depersonalised through masking out the following data elements which could serve to directly identify the passenger to whom the PNR data related-

(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 directly identify the passenger to whom the PNR data relates or any other persons;

(d) frequent flyer information;

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

(f) any API data that has been collected.

(3) Upon expiry of the period of 6 months referred to in subrule (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 rule 3(2)(b); and

(b) approved by:

(i) a judge of the Supreme Court of Gibraltar; or

(ii) a competent authority listed in Schedule 1 subject to informing,

the data protection officer of the PIU and to an ex-post review by that data protection officer.

(4) PNR data shall be deleted permanently upon expiry of the period referred to in subrule (1). This obligation is without prejudice to cases where exceptions are provided for in these Rules or in Gibraltar law.

(5) The result of processing data referred to in rule 3(2)(a) shall be kept by the PIU only as long as necessary to inform the competent authorities and, in accordance with rule 5(1) to inform the PIUs of Member States of a positive match.

Protection of personal data.

10.(1) In respect of all processing of personal data pursuant to these Rules, every passenger shall have the same right to protection of their personal data, rights of access, rectification, erasure and restriction and rights to compensation and redress as provided for by the laws of Gibraltar.

(2) Regulation 21 and 22 of the Data Protection (Police and Judicial Cooperation in Criminal Matters) Regulations 2014 shall apply to all processing of personal data pursuant to these Rules.

(3) These Rules are without prejudice to the obligations of air carriers to take appropriate technical and organisational measures to protect the security and confidentiality of personal data pursuant to the Data Protection Act 2004.

(4) The processing of PNR data revealing a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation shall be prohibited. Any PNR data revealing such information received by the PIU shall be erased immediately.

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

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

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

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

(6) The PIU shall keep records of the following operations-

(a) collection;

(b) consultation;

(c) disclosure; and

(d) erasure.

(7) The operations named in subrules (7)(b) and (c) shall show 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 those data.

(8) The records shall be used solely for the purposes of-

(a) verification;

(b) self-monitoring;

(c) ensuring data integrity and data security; and

(d) auditing.

(9) The PIU shall make all documentation available upon request, to the supervisory authority.

(10) Where a personal data breach is likely to result in a high risk for the protection of the personal data or adversely affect the privacy of the data subject, the PIU shall communicate that breach to the data subject and to the supervisory authority without undue delay.

Offences.

11. A person who fails to comply with an obligation imposed on him by rules 3 to 10 commits an offence.

Penalties.

12.(1) A person guilty of an offence under rule 11 shall be liable, on summary conviction, to a fine not exceeding level 5 on the standard scale.

Supervisory authority.

13.(1) The supervisory authority shall be the Gibraltar Regulatory Authority.

(2) The 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 reasonable time;

(b) verify the lawfulness of the data processing, conduct investigations, inspection and audits in accordance with Gibraltar law, either on its own initiative or on the basis of a complaint described in subrule (2)(a).

(3) The supervisory authority shall upon request, advise any data subject on the exercise of their rights.

Data formats.

14. All protocols and supported data formats shall be adhered to in accordance with Article 16 of the Directive 2016/681/EU.

Carrier's liability.

15. Compliance with these Rules shall be without prejudice to any obligations under the Carrier's Liability Act 2002.

SCHEDULE 1

HM Attorney General
HM Customs
The Chief Secretary of HM Government of Gibraltar
The Gibraltar Coordinating Centre for Criminal Intelligence & Drugs
The Gibraltar Finance Intelligence Unit
The Ministry for Justice
The Royal Gibraltar Police

SCHEDULE 2

Passenger name record data as far as collected by air carriers

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 numbers 1 to 18

SCHEDULE 3

1. participation in a criminal organisation
2. human trafficking
3. sexual exploitation of children and child pornography
4. illicit trafficking in narcotic drugs and psychotropic substances
5. illicit trafficking in weapons, munitions and explosives
6. corruption
7. fraud, including that against the financial interests of the Union
8. laundering of the proceeds of crime and counterfeiting of currency, including the euro
9. computer-related crime/cybercrime
10. environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties
11. facilitation of unauthorised entry and residence
12. murder, grievous bodily harm
13. illicit trade in human organs and tissue
14. kidnapping, illegal restraint and hostage-taking
15. organised and armed robbery
16. illicit trafficking in cultural goods, including antiques and works of art
17. counterfeiting and piracy of products
18. forgery of administrative documents and trafficking therein
19. illicit trafficking in hormonal substances and other growth promoters
20. illicit trafficking in nuclear or radioactive materials
21. rape
22. crimes within the jurisdiction of the International Criminal Court
23. unlawful seizure of aircraft/ships
24. sabotage
25. trafficking in stolen vehicles
26. industrial espionage