

# Criminal Procedure and Evidence

## **CRIMINAL PROCEDURE AND EVIDENCE ACT (FINGERPRINT, DNA AND VEHICLE REGISTRATION DATA EXCHANGE) REGULATIONS 2018**

**2011-24**

**Repealed  
Subsidiary  
2018/269**

Subsidiary Legislation made under s.267.

## **CRIMINAL PROCEDURE AND EVIDENCE ACT (FINGERPRINT, DNA AND VEHICLE REGISTRATION DATA EXCHANGE) REGULATIONS 2018**

**Repealed by LN.2020/525 as from 1.1.2021**

**(LN.2018/269)**

*Commencement*      **29.11.2018**

---

### **ARRANGEMENT OF REGULATIONS.**

Regulation

#### **PART 1 PRELIMINARY**

1. Title.
2. Commencement.
3. Interpretation.
4. Authorities.

#### **PART 2 DATA PROTECTION UNDER COUNCIL DECISION 2008/615/JHA**

5. Scope of Part.
6. Provision of personal data following a DNA-profile match.
7. Provision of personal data following a dactyloscopic data match.

#### **PART 3 ACCREDITATION OF FORENSIC SERVICE PROVIDERS**

8. Scope of provisions relating to forensic providers.
9. Accreditation.
10. Recognition of results.
11. Enforcement.
12. Guidance.

**Criminal Procedure and Evidence**

**CRIMINAL PROCEDURE AND EVIDENCE ACT (FINGERPRINT,  
DNA AND VEHICLE REGISTRATION DATA EXCHANGE)  
REGULATIONS 2018**

**PART 4  
DNA PROFILES**

13. Request for the collection and supply of DNA profiles.
14. Request for the collection and supply of DNA profiles.

**PART 5  
VEHICLE REGISTRATION DATA**

15. Searches.

**PART 6  
MAJOR EVENTS**

16. Duties.
17. Exchange of data.

**PART 7  
SUPPLY OF INFORMATION TO PREVENT TERRORISM**

- 18.

**PART 8  
OTHER FORMS OF COOPERATION**

19. Interpretation of Part.
20. Joint operations.
21. Assistance.
22. Arms, ammunition and equipment.
23. Protection and assistance.
24. Liability of a seconded officer.
25. Employment relationship of a seconded officer.

**PART 9  
GENERAL PROVISIONS ON DATA PROTECTION**

26. Data protection for Parts 2, 6, 7 and 8 of these Regulations.
27. Purposes.
28. Purposes - articles 3, 4 and 9 of 2008/615/JHA.
29. Purposes - article 12 of 2008/615/JHA.
30. Designated users of the personal data communicated under Council Decision 2008/615/JHA.
31. Accuracy, current reliance and storage time of data.
32. Flagging.
33. Deletion.

# Criminal Procedure and Evidence

---

## CRIMINAL PROCEDURE AND EVIDENCE ACT (FINGERPRINT, DNA AND VEHICLE REGISTRATION DATA EXCHANGE) REGULATIONS 2018

**2011-24**

**Repealed**  
**Subsidiary**  
**2018/269**

- 34. Data subjects' rights.
- 35. Enforcement of rights.
- 36. Refund to a Member State.
- 37. Information requests.

### **PART 9** **MISCELLANEOUS**

- 38. Other agreements.

## Criminal Procedure and Evidence

---

### CRIMINAL PROCEDURE AND EVIDENCE ACT (FINGERPRINT, DNA AND VEHICLE REGISTRATION DATA EXCHANGE) REGULATIONS 2018

*In exercise of the powers conferred upon him by section 697 of the Criminal Procedure and Evidence Act 2011 and all other enabling powers, and in order to implement Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime and Council Framework Decision 2009/905/JHA of 30 November 2009 on Accreditation of forensic service providers carrying out laboratory activities, the Minister has made the following Regulations-*

#### **PART 1 PRELIMINARY**

##### **Title.**

1. These Regulations may be cited as the Criminal Procedure and Evidence Act (Fingerprint, DNA and Vehicle Registration Data Exchange) Regulations 2018.

##### **Commencement.**

2. These Regulations come into operation on the day of publication.

##### **Interpretation.**

3. In these Regulations-

“automated search” means an online access procedure for consulting the databases of one, more than one, or all of the Member States or of the participating countries;

“automated search procedure” means direct access to the automated files of another body where the response to the search procedure is fully automated;

“blocked” and “blocking” mean the marking of stored personal data with the aim of limiting their processing in future;

“caution” has the meaning in section 2(1) of the Criminal Procedure and Evidence Act 2011;

“competent law enforcement authorities” means those bodies responsible for the prevention, detection or investigation of criminal offences;

“convicted” includes a reference to-

- (a) a person who has been given a caution in respect of the offence which, at the time of the caution, the person has admitted;
- (b) a person who has been found not guilty of the offence by reason of insanity; or
- (c) a person who has been found to be under a disability and to have done the act charged in respect of the offence;

and for the purposes of this definition, an absolute discharge in respect of an offence does not count as a conviction;

“Council Decision 2008/615/JHA” means Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime;

“Council Decision 2008/616/JHA” means Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime;

“Council Framework Decision” means Council Framework Decision 2009/905/JHA of 30 November 2009 on Accreditation of forensic service providers carrying out laboratory activities;

“dactyloscopic data” means fingerprint images, images of fingerprint latents, palm prints, palm print latents and templates of such images (coded minutiae);

“data controller” has the same meaning as “controller” under section 2 of the Data Protection Act 2004;

“data subject” has the same meaning as under section 2 of the Data Protection Act 2004;

“DNA-profile” means a letter or number code which represents a set of identification characteristics of the non-coding part of an analysed human DNA sample; the particular molecular structure at the various DNA locations (loci);

## **Criminal Procedure and Evidence**

---

### **CRIMINAL PROCEDURE AND EVIDENCE ACT (FINGERPRINT, DNA AND VEHICLE REGISTRATION DATA EXCHANGE) REGULATIONS 2018**

- “forensic service provider” means any person that carries out forensic laboratory activities at the request of competent law enforcement or judicial authorities;
- “GRA” means the Gibraltar Regulatory Authority established under section 3(1) of the Gibraltar Regulatory Authority Act 2000 or such person or agency as the Minister may, from time to time, appoint;
- “laboratory activity” means any measure taken in a laboratory when locating and recovering traces on items, as well as developing, analysing and interpreting forensic evidence, with a view to providing expert opinions or exchanging forensic evidence;
- “latent” means any fingerprint or palm print that through processing has been made visible for the purpose of creating an image;
- “loci” means any set of identification characteristics of the non-coding part of an analysed human DNA sample, being the particular molecular structure at the various DNA locations;
- “Member State” means a Member State of the European Union;
- “national unit” means the national unit set up for the purposes of Part 2 of these Regulations and staffed by officers of the Royal Gibraltar Police;
- “non-coding part of an analysed human DNA sample” means chromosome regions not genetically expressed, being those regions not known to provide for any functional properties of an organism;
- “personal data” has the same meaning as under section 2 of the Data Protection Act 2004;
- “processing of personal data” means an operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, sorting, retrieval, consultation, use, disclosure by supply, dissemination or otherwise making available, alignment, combination, blocking, erasure or destruction of data and shall also include notification of whether or not “a hit” exists;
- “recordable offence” has the same meaning as under section 2(1) of the Criminal Procedure and Evidence Act 2011 and includes cautions;

“reference DNA-profile” means any DNA-profile of an identified person;

“referencing” means the marking of stored personal data without the aim of limiting their processing in the future;

“result of a laboratory activity” means any analytical outputs and directly associated interpretation;

“UKAS” means the United Kingdom Accreditation Service, a company limited by guarantee incorporated in England and Wales under number 3076190;

“unidentified DNA-profile” means any DNA-profile collected during the investigation of a criminal offence and belonging to a person not yet identified; and

“vehicle registration data” means the data-set as specified in Chapter 3 of the Annex to Council Decision 2008/616/JHA.

## **Authorities.**

4.(1) The national contact point within Gibraltar for the purpose of supplying data as referred to in articles 6 and 11 of Council Decision 2008/615/JHA is the Royal Gibraltar Police.

(2) The national contact point within Gibraltar for the purpose of supplying data as referred to in article 12 of Council Decision 2008/615/JHA is the Driver and Vehicle Licensing Department.

(3) Subject to subregulation (4), the national contact point within Gibraltar for the purpose of supplying data as referred to in articles 13 and 14 of Council Decision 2008/615/JHA is the Royal Gibraltar Police.

(4) Subregulation (3) shall not affect the operation of the Gibraltar Football Information Point designated under the International Football Matches Security Regulations 2014.

(5) The national contact point within Gibraltar for the purpose of supplying information as referred to in article 16 of Council Decision 2008/615/JHA is the Commissioner of Police.

## **PART 2**

### **DATA PROTECTION UNDER COUNCIL DECISION 2008/615/JHA**

#### **Scope of Part.**

5. When, in accordance with articles 3, 4 or 9 of Council Decision 2008/615/JHA, a Member State searches or compares any DNA-profile or dactyloscopic data it holds against DNA-profiles or dactyloscopic data held by Gibraltar, the national unit must ensure that those searches or comparisons are only against-

- (a) unidentified DNA-profiles;
- (b) reference DNA-profiles relating to persons who have been convicted of a recordable offence; and
- (c) dactyloscopic data relating to persons who have been convicted of a recordable offence.

**Provision of personal data following a DNA-profile match.**

6.(1) Subject to subregulations (2) to (4), where, pursuant to a search or comparison made by a Member State under articles 3 or 4 of Council Decision 2008/615/JHA, a match is shown between any DNA-profile held by that Member State and any DNA-profile held by Gibraltar, the national unit shall provide the reference data with which a match has been found and may provide the personal data it holds relating to the matched DNA-profile to the Member State that made the search or comparison.

(2) The national unit must not provide the personal data where-

- (a) the Member State that made the search or comparison has not requested the personal data relating to the matched DNA-profile;
- (b) the matched DNA-profile does not include ten or more matching loci;
- (c) the personal data relates to a person aged under 18, unless the request for the personal data is received by the national unit following a formal request for mutual legal assistance to the Commissioner of Police for the exchange of criminal records; or
- (d) subject to subregulations (3) and (4), both the DNA-profile held by the Member State and the DNA-profile held by Gibraltar are reference DNA-profiles.

(3) In the circumstances set out in subregulation 2(d), the national unit may, unless one or more of subregulations 2(a) to 2(c) apply, request that the Member State requesting the personal data provides dactyloscopic data for the person to whom the reference DNA-profile relates.

(4) Where-

- (a) the Member State requesting the personal data provides dactyloscopic data in response to a request under subregulation (3); and
- (b) there is a match with dactyloscopic data held by Gibraltar;

the national unit may, subject to subregulation (2)(c), provide the personal data it holds relating to the matched dactyloscopic data.

### **Provision of personal data following a dactyloscopic data match.**

7.(1) Subject to subregulation (2), where, pursuant to a search made by a Member State under article 9 of Council Decision 2008/615/JHA, a match is shown between any dactyloscopic data held by that Member State and any dactyloscopic data held by Gibraltar, the national unit may provide the personal data it holds relating to the matched dactyloscopic data to the Member State that made the search.

(2) The national unit must not provide the personal data it holds relating to the matched dactyloscopic data to the Member State that made the search or comparison where-

- (a) the Member State that made the search has not requested the personal data relating to the matched dactyloscopic data; or
- (b) the personal data relates to a person aged under 18, unless the request for the personal data is received by the national unit following a formal request for mutual legal assistance to the Commissioner of Police for the exchange of criminal records.

## **PART 3**

### **ACCREDITATION OF FORENSIC SERVICE PROVIDERS**

#### **Scope of provisions relating to forensic providers.**

8.(1) This Part applies to any laboratory activity resulting in-

- (a) a DNA-profile; or

## Criminal Procedure and Evidence

---

### CRIMINAL PROCEDURE AND EVIDENCE ACT (FINGERPRINT, DNA AND VEHICLE REGISTRATION DATA EXCHANGE) REGULATIONS 2018

(b) dactyloscopic data.

(2) Nothing in this Part affects rules on the judicial assessment of evidence.

#### **Accreditation.**

9.(1) Competent law enforcement authorities must use an accredited forensic service provider to conduct any laboratory activity that is within scope of these regulations and is requested in relation to the prevention, detection or investigation of criminal offences.

(2) A forensic service provider is accredited if they are either-

- (a) accredited by UKAS as complying with the standard EN ISO/IEC 17025:2005, as amended from time to time, on the general requirements for the competence of testing and calibration laboratories; or
- (b) are otherwise accredited in accordance with article 4 of the Council Framework Decision.

(3) The requirement of accreditation only applies in relation to laboratory work that is carried out after the commencement of these Regulations.

#### **Recognition of results.**

10. A competent law enforcement authority must recognise the result of a laboratory activity accredited either under regulation 9(2)(a) or (b) as being equally reliable.

#### **Enforcement.**

11.(1) If the Minister with responsibility for Justice becomes aware that a person has not complied with its duties under this Part, the Minister may, by notice to that person, specify-

- (a) measures that the person must take to ensure that that person complies with this Part; and
- (b) the deadline by which those measures must be taken.

(2) The Minister with responsibility for Justice must consider any representations about the notice received from the person to whom the notice is addressed, and may amend or withdraw the notice.

(3) If the specified measures have not been taken by the specified deadline, the Minister may apply to the magistrates' court for an order requiring the person to comply with the notice or otherwise carry out its duties under this Part.

## **Guidance.**

12. The Minister with responsibility for Justice may give guidance to a person responsible for the prevention, detection or investigation of criminal offences with respect to the practical implementation of this Part, and a person to whom such guidance is given must have regard to it.

## **PART 4 DNA PROFILES**

### **Request for the collection and supply of DNA profiles.**

13.(1) Where there is no DNA profile match for a person undergoing an investigation or criminal proceedings and that person is present in a Member State, the Royal Gibraltar Police may request assistance from that Member State in accordance with subregulation (2) in order to obtain a DNA profile of the person.

(2) The Royal Gibraltar police must, when requesting collection and examination of cellular material from a person and supply of the DNA profile obtained, make the request for assistance-

- (a) to the competent authority in the Member State where the person is present;
- (b) in the form of a statement or an investigation warrant;
- (c) show the requirements under section 88 or 89 of the Criminal Procedure and Evidence Act 2011 would be fulfilled if the person was in Gibraltar; and
- (d) specify the purpose for which the DNA profile is required.

### **Request for the collection and supply of DNA profiles.**

14.(1) Subject to subregulations (2) and (3), where the Royal Gibraltar Police receives a request from a competent authority of a Member State for the collection and examination of cellular material and supply of the DNA profile obtained for an identified person and the person is present in

## Criminal Procedure and Evidence

---

### CRIMINAL PROCEDURE AND EVIDENCE ACT (FINGERPRINT, DNA AND VEHICLE REGISTRATION DATA EXCHANGE) REGULATIONS 2018

Gibraltar, the Royal Gibraltar Police must ensure the collection and examination of the person's cellular material and provide the DNA profile obtained to the competent authority of the Member State.

(2) The request, referred to in subregulation (1), received from a competent authority must-

- (a) specify the purpose for which the DNA profile is required;
- (b) be in the form of a statement or an investigation warrant issued by the competent authority of the Member State, as required by the law of the Member State; and
- (c) show the requirements under the law of the Member State for collecting and examining cellular material would be fulfilled if the person were present in the Member State.

(3) The collection and examination of the person's cellular material must be carried out in accordance with section 88 or 89 of the Criminal Procedure and Evidence Act 2011.

(4) The Royal Gibraltar Police must provide the DNA profile referred to in this regulation in accordance with the Data Protection Act 2004.

### PART 5 VEHICLE REGISTRATION DATA

#### Searches.

15.(1) The national contact point of a Member State designated for the purposes of article 12 of Council Decision 2008/615/JHA shall be allowed access to the vehicle registration data database held by the contact point in regulation 4(2) in accordance with subsections (2) to (4).

(2) The access must be in the form of an automated search which relates to-

- (a) data relating to the owner or operator of the vehicle; and
- (b) data relating to the vehicle.

(3) Subject to subsection (4), searches must be related to-

- (a) the prevention and investigation of a criminal offence;

- (b) an offence coming within the jurisdiction of the courts or the public prosecution service of the Member State; or
- (c) to maintain public security, and

must be carried out in compliance with the searching Member States' national law.

(4) Searches by the national contact point of a Member State must be conducted with a full chassis number or a full registration number.

## **PART 6 MAJOR EVENTS**

### **Duties.**

16.(1) The national contact point appointed under regulation 4(3) shall be responsible for coordinating and facilitating police information exchanges in connection with criminal offences and in maintaining public order and security for a major event with a cross-border dimension, in particular for a sporting event or European Council meeting.

(2) The information exchanges referred to in subregulation (1) may also involve other law enforcement authorities in Gibraltar.

(3) The national contact point appointed under regulation 4(3) shall facilitate, coordinate or organise the implementation of international police cooperation in connection with public order and security for a major event with a cross-border dimension, in particular for a sporting event or European Council meeting.

### **Exchange of data.**

17.(1) The national contact point appointed under regulation 4(3) shall engage, whether at the request of a national contact point of a Member State concerned or on its own initiative, in mutual exchange of general information and non-personal data and, subject to subregulation (3), personal data.

(2) The general information exchanged in connection with a major event with a cross-border dimension, in particular for a sporting event or European Council meeting, shall comprise strategic, operational and tactical information.

## **Criminal Procedure and Evidence**

---

### **CRIMINAL PROCEDURE AND EVIDENCE ACT (FINGERPRINT, DNA AND VEHICLE REGISTRATION DATA EXCHANGE) REGULATIONS 2018**

(3) Subject to subregulation (4), personal data shall be exchanged in accordance with Part 9.

(4) Subject to subparagraph (5), personal data may be supplied to a national contact point of a Member State where-

- (a) a final conviction, or
- (b) other circumstances give rise to a reason to believe a data subject will commit a criminal offence,

at the event or pose a threat to public order and security.

(5) Personal data supplied in accordance with this regulation must-

- (a) only be processed for the purposes of this regulation and for the specified events for which they were supplied;
- (b) be deleted without delay once the purposes referred to in this regulation have been achieved or may no longer be achieved and in any event be deleted after a year.

#### **PART 7**

#### **SUPPLY OF INFORMATION TO PREVENT TERRORISM**

18.(1) For the prevention of terrorist offences the Commissioner of Police may in individual cases, either on his own initiative or following a request from a Member State, supply a Member State's national contact point with information in subregulation (2) in relation to a data subject where particular circumstances give reason to believe the data subject will commit criminal offences as referred to in articles 1, 2 and 3 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combatting terrorism.

(2) The information referred to in subregulation (1) relating to the data subject is-

- (a) his full name or alias;
- (b) his date of birth;
- (c) his place of birth; and
- (d) a description of the circumstances which give rise to the belief referred to in subregulation (1).

(3) The Commissioner of Police may impose such conditions as he sees fit on the use made by the Member State of data transmitted in accordance with this regulation.

(4) Where the Commissioner of Police requests or receives information in relation to a data subject and particular circumstances give reason to believe the data subject will commit criminal offences as referred to in articles 1, 2 and 3 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combatting terrorism, the Commissioner of Police must comply with the conditions regulating the information imposed by the national contact point of the Member State that sent the information.

## **PART 8 OTHER FORMS OF COOPERATION**

### **Interpretation of Part.**

19.(1) In this Part-

“competent authority” means the authority competent to take decisions, act or to take decisions and act within a Member State, and in the case of Gibraltar means the Commissioner of Police;

“joint investigation team” means an investigation team formed in accordance with-

- (a) Council Framework Decision 2002/465/JHA of 13 June 2002 on joint investigation teams, as the same may be amended from time to time;
- (b) any other European Union measure on joint investigation teams adopted under European Union law;
- (c) any international agreement which has been extended to or which applies to Gibraltar; and

“seconded member” or “seconded officer” means a member of the joint operation or officer providing assistance who is not from the place in which the team is operating.

(2) This Part shall be without prejudice to any other existing provision or arrangements on the setting up of a joint investigation team.

### **Joint operations.**

## Criminal Procedure and Evidence

---

### CRIMINAL PROCEDURE AND EVIDENCE ACT (FINGERPRINT, DNA AND VEHICLE REGISTRATION DATA EXCHANGE) REGULATIONS 2018

20.(1) By mutual agreement with the competent authority of a Member State, the Commissioner of Police may set up a joint operation.

(2) A joint operation set up pursuant to subregulation (1) shall be-

- (a) for maintaining public order and security;
- (b) preventing criminal offences;
- (c) for a limited period; and

shall be subject to the procedures and safeguards of the Joint Investigation Teams Regulations 2014.

(3) In pursuance of subregulation (2) read “joint operation” for “joint investigation team” for regulations 5 to 13 and in the Schedule of the Joint Investigation Teams Regulations 2014.

#### **Assistance.**

21.(1) The Commissioner of Police shall provide a competent authority of a Member State with assistance in the form of-

- (a) prompt notification of situations with a cross-border impact and exchange any relevant information;
- (b) coordinating and implementing the necessary policing measures within Gibraltar in situations with a cross-border impact;
- (c) as far as possible, dispatching officers, specialists and advisers and supplying equipment, at the request of the Member State in which the situation has arisen,

in connection with mass gatherings and major events, disasters and serious accidents, in order to prevent criminal offences and maintain public order and security.

(2) The Commissioner of Police may accept assistance from a competent authority of a Member State in the form of-

- (a) prompt notification of situations with a cross-border impact and exchange of relevant information;

- (b) coordinating and implementing the necessary policing measures within Gibraltar in situations with a cross-border impact;
- (c) as far as possible, dispatching officers, specialists and advisers and supplying equipment, at the request of the Commissioner of Police when a situation has arisen,

in connection with mass gatherings and major events, disasters and serious accidents, in order to prevent criminal offences and maintain public order and security.

### **Arms, ammunition and equipment.**

22.(1) The Minister, as he sees fit, may by Order permit officers seconded from a Member State to a joint operation, as provided for in regulation 20, or assistance, as provided for in regulation 21, to wear the national uniform of the seconding Member State and carry such arms, ammunition and equipment as they are competent and permitted to under the seconding Member State's national law when present in Gibraltar.

(2) If the Minister has not made an order under subregulation (1), the seconded officers may not wear the national uniform of the seconding Member State or carry such arms, ammunition and equipment as they are competent and permitted to under the seconding Member State's national law when present in Gibraltar.

(3) The Commissioner of Police may in individual cases, where the nature of the situation requires it, following an Order by the Minister under subregulation (1), permit arms, ammunition and equipment to be used for purposes beyond self-defence or in the defence of others.

(4) The use of arms, ammunition and equipment as provided under this regulation shall be subject to Gibraltar law.

(5) The Commissioner of Police shall inform the competent authority of a Member State as to the arms, ammunitions and equipment permitted and of the conditions of their use permitted by this Regulation.

(5) Where a seconded officer uses a vehicle in action under this regulation within Gibraltar he shall be subject to the road traffic legislation applicable to police officers in Gibraltar, including right of way and privileges enjoyed by a police officer while driving.

### **Protection and assistance.**

## Criminal Procedure and Evidence

---

### CRIMINAL PROCEDURE AND EVIDENCE ACT (FINGERPRINT, DNA AND VEHICLE REGISTRATION DATA EXCHANGE) REGULATIONS 2018

23. Where the Minister makes an Order under regulation 22 a seconded officer of a Member State shall be entitled to equal protection and assistance in the course of the duties agreed and permitted under this Part as an officer of the Royal Gibraltar Police.

#### **Liability of a seconded officer.**

24. For the purposes of establishing whether any offence has been committed and in the prosecution of any such offence, a seconded officer in Gibraltar shall be treated as though he were a member of the Royal Gibraltar Police.

#### **Employment relationship of a seconded officer.**

25. A seconded officer operating under this Part shall remain subject to the employment law provisions applicable in their own Member State, and in the case of a seconded officer from Gibraltar to the employment law provisions applicable in Gibraltar, in particular in relation to disciplinary rules.

### **PART 9 GENERAL PROVISIONS ON DATA PROTECTION**

#### **Data protection for Parts 2, 6, 7 and 8 of these Regulations.**

26.(1) The following provisions in this Part on data protection shall apply to Parts 2, 6, 7 and 8 of these Regulations.

(2) Personal data shall be exchanged in accordance with-

- (a) the Data Protection Act 2004;
- (b) any other applicable international law; and
- (c) to the extent that these are not already provided for under paragraphs (a) and (b), taking account of—
  - (i) the principles of Convention No 108 of the Council of Europe of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data; and
  - (ii) Recommendation No R (87)15 of the Committee of Ministers of the Council of Europe of 17 September

1987 regulating the use of personal data in the police sector.

## **Purposes.**

27.(1) Subject to subregulation (2), personal data communicated under Council Decision 2008/615/JHA shall be used solely for the purposes for which Council Decision 2008/615/JHA stipulates the personal data may be communicated for, and the transmission or receipt of that data must be recorded both in the source data file and in the data file on which it is entered.

(2) Personal data communicated under Council Decision 2008/615/JHA may be used for a purpose other than that for which it was communicated where prior authorisation is sought from and approved by the Commissioner of Police.

(3) Where a national contact point or competent authority receives approval from a Member State for the use of personal data communicated by it for a purpose other than that referred to in subregulation (1), the use of that data shall be subject to the provisions of these Regulations and any other applicable Gibraltar law.

(4) Where a national contact point or competent authority receives a request from a Member State for an authorisation to use personal data communicated to it for a purpose other than the purpose for which it originally sent the personal data, the national contact point or competent authority may only grant such an authorisation in so far as Gibraltar law permits.

## **Purposes - articles 3, 4 and 9 of 2008/615/JHA.**

28.(1) Subject to subregulation (2) and (3), the processing of data, supplied pursuant to article 3, 4 or 9 of Council Decision 2008/615/JHA by means of a search or comparison, by the national authority or competent authority, shall be permitted solely in order to-

- (a) establish whether the compared DNA profiles or dactyloscopic data match;
- (b) prepare and submit a police or judicial request for legal assistance in compliance with national law if those data match;
- (c) record within the meaning of article 30 of Council Decision 2008/615/JHA.

(2) The national authority or competent authority administering the data file, referred to in subregulation (1), may process the data supplied to it in accordance with articles 3, 4 and 9 solely where this is necessary for the purposes of comparison, providing automated replies to searches or recording pursuant to article 30 of Council Decision 2008/615/JHA.

(3) The supplied data, referred to in subregulation (2), shall be deleted immediately following data comparison or automated replies to searches unless further processing is necessary for the purposes mentioned under paragraphs (1)(b) and (c).

**Purposes - article 12 of 2008/615/JHA.**

29.(1) A national contact point or competent authority administering a data file may for the purpose of providing automated replies to search procedures or recordings under article 30 of Council Decision 2008/615/JHA use data supplied in accordance with article 12 of Council Decision 2008/615/JHA.

(2) The data supplied under subregulation (1) shall be deleted immediately following automated replies to searches unless further processing is necessary for recording pursuant to article 30 of Council Decision 2008/615/JHA.

(3) A national contact point or competent authority who carries out a search under this regulation may use data received in a reply solely for the procedure for which the search was made.

**Designated users of the personal data communicated under Council Decision 2008/615/JHA.**

30. Data referred to in regulation 27 may only be used by the-

- (a) judicial authorities; and
- (b) departments and authorities,

carrying out tasks or performing duties in connection with the purposes referred to in regulation 27.

**Accuracy, current reliance and storage time of data.**

31.(1) Where data is communicated pursuant to Parts 2, 6, 7 and 8 of these Regulations the sender of that data must ensure the accuracy thereof.

(2) Where a data controller has established, either on its own initiative or further to a request by the data subject that data has been provided that is inaccurate or should not have been communicated, the data controller must immediately inform the recipients.

(3) Where the data controller is the recipient of data from a Member State and the data controller is notified that the data is inaccurate or should not have been provided, the data controller must correct or destroy the data, or indicate that the data is inaccurate or was unlawfully communicated.

(4) Nothing in this regulation shall be construed as a derogation from the protections provided elsewhere in these Regulations or in the Data Protection Act 2004.

## **Flagging.**

32.(1) Where a data subject contests the accuracy of data held by a national contact point or competent authority and the accuracy or inaccuracy is not established, the data subject may request the data be marked with a flag.

(2) Where a data subject requests that data be marked in accordance with subregulation (1) the data controller shall mark the data with a flag.

(3) A data controller may make an application to remove a flag on specific data by applying to-

- (a) the data subject;
- (b) the magistrates' court; or
- (c) the GRA.

(4) The data controller may remove a flag where a person named in subregulation (3)(a) to (c) grants permission to remove the flag.

(5) The magistrates' court or the GRA may grant permission to a data controller to remove a flag on data after hearing submissions as to why the data is accurate; the data subject may make representations at the hearing.

## **Deletion.**

33.(1) Personal data supplied, which should not have been supplied or received, shall be deleted by a data controller.

(2) Data lawfully supplied and received shall be deleted-

- (a) if the data are no longer necessary for the purpose for which they were supplied;
- (b) following the expiry of the maximum period for retention of data, if such period was communicated upon receipt.

(3) Where a national contact point or competent authority receive personal data without a prior request for such data, the national contact point or competent authority shall immediately check if the data are necessary for the purposes for which they were supplied.

(4) Where a national contact point or competent authority has reason to believe that a deletion would prejudice the interests of a data subject, the data shall be blocked instead of being deleted.

(5) Data blocked in accordance with subregulation (4) may only be supplied or used for the purpose which prevented the deletion of the data.

**Data subjects' rights.**

34.(1) A data subject may request information from a data controller in relation to the data processed in respect of his person, namely-

- (a) the origin of the data;
- (b) the recipient or groups of recipient;
- (c) the intended purpose of the processing; and
- (d) the legal basis for the processing.

(2) A data controller must reply to a request by a data subject made under subregulation (1) in general comprehensible terms and without unacceptable delays.

(3) A data controller may impose a reasonable fee for requesting information in relation to a data subject pursuant to subregulation (1) and must be satisfied that the person requesting the data is the data subject.

(4) A data controller must satisfy himself that the person requesting the data is the data subject by requiring production of his passport or identification card.

(5) Where the data on the data subject is inaccurate, it shall be corrected by the data controller and where the data on the data subject was unlawfully processed the data shall be deleted by the data controller.

(6) The data controller shall inform the data subject when the task in subregulation (5) is completed.

## **Enforcement of rights.**

35.(1) A data subject may apply to the magistrates' court where his rights in relation to data protection have been interfered with.

(2) A court may grant such damages as it deems appropriate and rectification or erasure of the data subjects' data as it deems fit.

## **Refund to a Member State.**

36.(1) Where a national contact point or competent authority within Gibraltar receives incorrect data on a data subject and a court awards damages to the data subject, the national contact point or competent authority may recover the sum of damages in full from the Member State which supplied the personal data.

(2) Where a national contact point or competent authority within Gibraltar sends incorrect data on a data subject to a Member State and a court awards damages to the data subject in the Member State and the Member State requests repayment of the damages, the national contact point or competent authority shall repay the damages awarded by the court.

## **Information requests.**

37.(1) A national contact point or competent authority within Gibraltar who has sent personal data on a data subject may request from the Member State to which the personal data was sent, information on the processing of the supplied data and the result obtained.

(2) A national contact point or competent authority within Gibraltar who has received personal data on a data subject from a Member State and receives a request, from the Member State to which the personal data was sent, for information on the processing of the supplied data and the result obtained, shall inform the Member State accordingly.

## **PART 9 MISCELLANEOUS**

**2011-24**

**Repealed**  
**Subsidiary**  
**2018/269**

## Criminal Procedure and Evidence

---

### CRIMINAL PROCEDURE AND EVIDENCE ACT (FINGERPRINT, DNA AND VEHICLE REGISTRATION DATA EXCHANGE) REGULATIONS 2018

#### **Other agreements.**

38.(1) These Regulations are without prejudice to-

- (a) agreements or arrangements between Gibraltar and Member States or third countries; and
- (b) existing agreements on legal assistance or mutual recognition of court decisions.