



**2021/0410(COD)**

17.05.2023

## **COMPROMISE AMENDMENTS**

on the proposal for a regulation of the European Parliament and of the Council on automated data exchange for police cooperation (“Prüm II”), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council  
(COM(2021)0784 – C9-0455/2021 – 2021/0410(COD))

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Paulo Rangel

## CA 1 - Articles 1 to 3 (Subject, purpose and scope)

### CHAPTER 1 GENERAL PROVISIONS

#### *Article 1*

##### **Subject matter**

Covers: AM 25 (rapp.), 26part (rapp.), 317 (RE)

Fall: AMs 312 (Left), 313 (Greens), 314 (S&D), 315 (S&D), 316 (S&D), 318 (ECR), 319 (Left), 320 (Greens)

This Regulation establishes a framework for the exchange of information between **Member States' competent law enforcement** authorities ~~responsible for the prevention, detection and investigation of criminal offences~~ (Prüm II). (AM 25)

This Regulation lays down the conditions and procedures for the automated searching of DNA profiles, dactyloscopic data, facial images, police records and certain vehicle registration data and the rules regarding the exchange of core data following a **confirmed match of biometric data**. (AM 26part, 317)

#### *Article 2*

##### **Purpose**

Covers: AMs 27 (rapp), 28 (rapp), 321 (S&D), 323 (RE)

Fall: AMs 322 (Left), 324 (Greens), 325 (S&D), 326 (Left), 327 (S&D), 328 (Greens), 360 (Left)

The purpose of Prüm II shall be to step up cross-border cooperation in matters covered by Part III, Title V, Chapter 5 of the Treaty on the Functioning of the European Union, particularly **by facilitating** the exchange of information between **Member States' competent law enforcement** authorities, **in full respect for the fundamental rights of ~~data subjects~~ natural persons, including the right to respect for one's private life and to the protection of personal data, in accordance with the Charter of Fundamental Rights of the European Union**. (AMs 27, 321, 323)

The purpose of Prüm II shall also be to allow for the search for missing persons and **the identification of** unidentified human remains by **Member States' competent law enforcement** authorities **in the context of a criminal investigation, provided that those authorities ~~have been~~ are empowered to conduct such searches and to carry out such identifications under national law**. (AM 28)

#### *Article 3*

##### **Scope**

Covers: AM 29 (rapp)

Fall: AMs 329 (S&D), 330 (S&D), 331 (Greens), 332 (ECR), 333 (Left)

This Regulation applies to the ~~national~~ databases, *established in accordance with national law and in compliance with, as applicable, Directive (EU) 2016/680 of the European Parliament and the Council, Regulation (EU) 2018/1725 of the European Parliament and the Council and Regulation (EU) 2016/794*, used for the automated transfer of the ~~data~~ categories of DNA profiles, dactyloscopic data, facial images, police records and certain vehicle registration data. (AMs 29)

## **CA 2 - Article 4 (Definitions)**

### **Article 4 Definitions**

Covers: AMs 30 (rapp), 31(rapp), 32 (rapp), 33 (rapp), 34 (rapp), 35 (rapp), 36 (rapp), 37 (rapp); 38 (rapp), 39 (rapp), 40 (rapp), 41 (rapp), 43 (rapp), 44 (rapp), 45 (rapp), 46 (rapp), 47 (rapp), 48 (rapp), 49 (rapp), 350part (S&D), 351 (Left), 356 (Left), 357 (RE), 358 (RE), 353 (Left), 354 (S&D), 359 (RE)

Fall: AMs 42 (rapp), 334 (Left), 335 (S&D), 336 (Greens), 337 (Left), 338 (ECR), 339 (Greens), 340 (S&D), 341 (Left), 342 (S&D), 343 (Greens), 344 (Left), 345 (ECR), 346 (S&D), 347 (S&D), 348 (Greens), 349 (Left), 352 (Left),

For the purposes of this Regulation, the following definitions apply:

- (1) 'loci' means ~~the particular molecular structure at the various~~ DNA locations **which contain identification characteristics of an analysed human DNA sample**; (AM 30)
- (2) '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~~ **loci, or the particular molecular structure at the various loci** DNA locations; (AM 31)
- (3) 'non-coding part of DNA' means chromosome regions not genetically expressed, i.e. not known to provide for any functional properties of an organism; (AM 32)
- (4) 'DNA reference data' means DNA profile and the reference number referred to in Article 9;
- (5) '**identified** ~~reference~~-DNA profile' means the DNA profile of an identified person; (AM 33)
- (6) 'unidentified DNA profile' means the DNA profile obtained from traces collected during the investigation of criminal offences and belonging to a person not yet identified;
- (7) 'dactyloscopic data' means fingerprint images, images of fingerprint latents, palm prints, palm print latents and templates of such images (coded minutiae), when they are stored and dealt with in an automated database;
- (8) 'dactyloscopic reference data' means dactyloscopic data and the reference number referred to in Article 14;
- (8b) '**unidentified dactyloscopic data**' means the dactyloscopic data obtained from traces collected during the investigation of a criminal offence which belongs to a person not yet identified; (AM34)
- (9) 'individual case' means a single investigation file;
- (10) 'facial image' means digital image of the face;
- (10a) '**facial image reference data**' means a facial image and its reference number referred to in Article 23; (AM 35)
- (10b) '**unidentified facial image**' means a facial image collected during the investigation of a criminal offence which belongs to a person not yet identified; (AM 36)

- (11) ‘biometric data’ means DNA profiles, dactyloscopic data or facial images;
- (11a) ‘alphanumeric data’ means data represented by letters, digits, special characters, spaces and punctuation marks;** (AM 37)
- (12) ‘match’ means the existence of a correspondence as a result of an automated comparison between personal data **held by the requesting Member State and personal data** recorded ~~or being recorded~~ in an information system or a database **of the requested Member State;** (AM 38)
- (13) ‘candidate’ means data with which a match occurred;
- (14) ‘requesting Member State’ means the Member State which is conducting a search through Prüm II;
- (15) ‘requested Member State’ means the Member State in ~~which~~ **whose** databases the search is conducted through Prüm II by the requesting Member State; (AM 39)
- (16) ‘police records’ means ~~any~~ **biographical** information **regarding persons convicted or suspected of having committed a serious criminal offence** available in the national ~~databases~~ register or registers recording data of competent authorities, **established** for the prevention, detection and investigation of criminal offences; (AM 40, 350part, 351)
- (17) ‘pseudonymisation’ means ~~the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person~~ **pseudonymisation as defined in Article 3, point (5), of Directive (EU) 2016/680;** (AM 41)
- (17a) ‘suspect’ means a person referred to in Article 6, point (a), of Directive (EU) 2016/680;** (AM 356, 358)
- (17b) ‘serious criminal offence’ means an offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA<sup>1</sup> or in Article 3 of Regulation (EU) 2016/794, which is punishable in the requesting Member State by a custodial sentence or a detention order for a maximum period of at least three years.** (AMs 353, 354, 359)
- (17c) ‘victim of serious crime or terrorism’ means a person that is adversely affected by an offence which corresponds or is equivalent to one of the offences referred to in Article 2(2) of Framework Decision 2002/584/JHA, if it is punishable under national law by a custodial sentence or a detention order for a maximum period of at least three years or an offence under national law which corresponds or is equivalent to one of the offences referred to in Directive (EU) 2017/541 of the European Parliament and of the Council<sup>2</sup>;** (AM 42)
- (17d) ‘personal data’ means personal data as defined in Article 3, point (1) of Directive (EU) 2016/680;** (AM 357)
- (17e) ‘designated authorities’ means the designated authorities as defined in Article 3(1), point (26), of Regulation (EU) 2017/2226 of the European Parliament and of the Council<sup>1a</sup>, Article 2(1), point (e), of Council Decision 2008/633/JHA<sup>1b</sup>, and or Article 3(1), point (21), of Regulation (EU) 2018/1240 of the European Parliament and of the Council<sup>1c</sup>;** (AM 43)
- (18) ‘Europol data’ means any **operational** personal data processed by Europol in accordance with Regulation (EU) 2016/794; (AM 44)

<sup>1</sup> Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002, p. 1)

<sup>2</sup> Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, 31.3.2017, p. 6)

(18a) '*competent law enforcement authority*' means any police, customs or other authority of a the Member States competent under national law to exercise authority and to take coercive measures for the purpose of preventing, detecting or investigating criminal offences; (AM 45)

(19) 'supervisory authority' means an independent public authority established by a Member State pursuant to Article 41 of Directive (EU) 2016/680 of the European Parliament and of the Council;

(20) 'SIENA' means the secure information exchange network application, managed by Europol *in accordance with Regulation (EU) 2016/794*, aimed at facilitating the exchange and ensuring the secure transmission of operational and strategic crime-related information between Member States and Europol; (AM 46)

(21) 'significant incident' means *significant* incident ~~unless it has a limited impact and is likely to be already well understood in terms of method or technology~~ as defined in Article 3, point (7), of Regulation (EU) .../... of the European Parliament and of the Council<sup>1a</sup> [2022/0085(COD)]; (AM 47)

(22) 'significant cyber threat' means *significant* cyber threat ~~with the intention, opportunity and capability to cause a significant incident~~ as defined in Article 3, point (11), of Regulation (EU) .../... [2022/0085(COD)]; (AM 48)

(23) 'significant vulnerability' means *significant* vulnerability ~~that will likely lead to a significant incident if it is exploited~~ as defined in Article 3, point (13) of Regulation (EU) .../... [2022/0085(COD)]; (AM 49)

(24) 'incident' means an incident within the meaning of Article 4(5) of Directive (EU) .../... of the European Parliament and of the Council<sup>41</sup> [proposal NIS 2].

## **CA3 - Chapter 2 - Section 1 - Articles to 5 to 11 (DNA)**

### **CHAPTER 2 EXCHANGE OF DATA**

[Falls AM 362 S&D]

#### **SECTION 1 DNA PROFILES**

[Falls AM 363 S&D]

#### *Article 5*

#### **Establishment of national DNA databases** (AMs 50, 364)

Covers: AMs 50 (rapp), 364 (Left), 51 (rapp), 366 (RE), 52 (rapp), 369 (Left), 53 (rapp), 371 (Left), 54 (rapp), 55 (rapp), 56 (rapp), 372 (RE)

Fall: AM 365 (Left), 367 (Greens), 368 (S&D), 370 (ID),

1. Member States shall open and keep national DNA ~~analysis files~~ *databases* for the ~~prevention, detection and~~ investigation of criminal offences. (AMs 51, 366)

Processing of data kept in those ~~files~~ *databases*, under this Regulation, shall be carried out in accordance with this Regulation *and* in compliance with the national law of the Member States applicable to the processing of those data. (AMs 52, 369)

2. Member States shall ensure the availability of DNA reference data from their national DNA analysis files *databases* as referred to in paragraph 1 **for the purposes of automated searches by other Member States pursuant to this Regulation.** (AMs 53, 371)

**2a.** DNA reference data shall not contain any **additional ~~nominal~~** data from which an individual can be directly identified. (AM 54)

**2b.** DNA reference data which is not attributed to any individual (~~Unidentified DNA profiles~~) shall be recognisable as such. (AM 55)

**2c. The Commission shall adopt an implementing act to specify the identification characteristics of a DNA profile which is to be exchanged and the minimum requirements for a match, taking into account international and European standards. That implementing act shall be adopted in accordance with the procedure referred to in Article 76(2).** (AM 56, 372)

#### Article 6

#### Automated searching of DNA profiles

[Falls AM 378 S&D and 379 ID]

Covers: AMs 57 (rapp), 381 (RE), 58 (rapp), 386 (RE), 59 (rapp), 60 (rapp), 61 (rapp), 392part (RE)

Fall: AMs 382 (S&D), 383 (Greens), 384 (Left), 385 (Greens) 387 (S&D, 388 (Left), 390 (Greens), 391 (Left), 393 (Greens), 394 (ID), 395 (Left), 396 (Greens), 397 (Greens), 398 (Left), 399 (Greens)

1. ~~For the prevention, detection and investigation of criminal offences,~~ Member States shall allow national contact points referred to in Article 29 **of other Member States** and Europol access to the DNA reference data in their DNA analysis files, ~~to conduct automated searches by comparing DNA profiles~~ **databases established for that purpose, to conduct automated searches of the DNA profiles and to compare those DNA profiles with their DNA profiles for the investigation of criminal offences.** (AMs 57, 381)

Searches ~~may~~ **shall only** be conducted ~~only~~ in individual cases, **where they are proportionate and necessary for the purposes of preventing, detecting or investigating investigation of a criminal offence,** and in compliance with the national law of the requesting Member State. (AM 58, 386)

2. Should an automated search show that a supplied DNA profile matches DNA profiles ~~stored entered~~ in the requested Member State's searched file **database or databases,** the national contact point of the requesting Member State shall receive in an automated way the DNA reference data with which a match has been found. (AM 59)

~~If there is no match, the requesting Member State shall be notified about it in an automated manner.~~ (AM 60)\*

3. The national contact point of the requesting Member State shall **manually ensure that a human review by a forensic expert is conducted in order to** confirm a match of DNA ~~profile profiles~~ data with DNA reference data held by the requested Member State following the automated supply of the DNA reference data required for confirming a match. (AM 61, 392part)

\*Provision included in article 37(3)

#### Article 7

#### Automated comparison of unidentified DNA profiles

Covers: AMs 62 (rapp), 63 (rapp), 64 (rapp), 407part (RE)

Fall: AMs 401 (S&D), 402 (Left), 403 (ID), 404 (Greens), 405 (ID), 406 (ID)

1. Member States may, via their national contact points, compare the DNA profiles of their unidentified DNA profiles with all DNA profiles from other national DNA *databases* for the investigation of criminal offences. Profiles shall be supplied and compared in an automated manner. (AM 62)

2. Should a requested Member State, as a result of the comparison referred to in paragraph 1, find that any DNA profiles supplied match any of those in its DNA ~~analysis files~~ *databases*, it shall, without delay, supply the national contact point of the requesting Member State with the DNA reference data with which a match has been found. (AM 63)

3. ***A human review by a forensic expert to confirm*** ~~The confirmation of a match of DNA profiles with DNA reference data held by the requested Member State shall be carried out *manually*~~ by the national contact point of the requesting Member State following the automated supply of the DNA reference data required for confirming a match. (AMs 64, 407part)

#### Article 8

##### Reporting about DNA analysis files

Covers: AM 65 (rapp), 409 (ID)

Fall: AMs 410 (S&D), 411 (Left)

~~Each Member State shall inform the Commission and eu-LISA of the national DNA analysis files, to which Articles 5 to 7 apply, in accordance with Article 73.\*~~

*\*Provision included in Article 72(2a)*

#### Article 9

##### Reference numbers for DNA profiles

Covers: AM 66 (rapp), 67 (rapp), 68 (rapp)

Fall:

The reference numbers for DNA profiles shall be the combination of the following:

(a) a reference number allowing Member States, in case of a match, to retrieve further data and other information in their databases referred to in Article 5 in order to supply it to one, several or all of the other Member States in accordance with ~~Articles~~ ***Article 47 and 48 or to Europol in accordance with Article 50(6)***; (AM 66)

***(aa) a reference number allowing Europol, in case of a match, to retrieve further data and other information for the purposes of Article 49(1) of this Regulation in order to supply them or it to one, several or all Member States in accordance with Regulation (EU) 2016/794***; (AM 67)

(b) a code to indicate the Member State which holds the DNA profile;

(c) a code to indicate the type of DNA profile (~~reference~~ ***identified*** DNA profiles or unidentified DNA profiles). (AM 68)

#### Article 10

### Principles of DNA reference data exchange

Covers: AMs 69 (rapp), 412 (RE), 413 (Left), 70 (rapp), 414 (RE), 71 (rapp), 415 (RE)  
Fall:

1. **Member States and, where applicable, Europol shall take all** appropriate measures ~~shall be taken~~ to ensure confidentiality and integrity for DNA reference data being sent to other Member States **or Europol**, including their encryption. (AMs 69, 412, 413)
2. Member States **and Europol** shall take the necessary measures to guarantee the integrity **and minimum quality standards** of the DNA profiles made available or sent for comparison to the other Member States and to ensure that those measures comply with the relevant **European or** international standards for DNA data exchange. (AMs 70, 414)
3. The Commission shall adopt implementing acts ~~to establish minimum quality standards to be met by DNA profiles and to specify~~ **specifying** the relevant **European or** international standards that are to be used by Member States **and Europol** for DNA reference data exchange, **including the minimum quality standard to be met by DNA profiles**. ~~That~~ Those implementing acts shall be adopted in accordance with the procedure referred to in Article 75(2). (AMs 71, 415)

#### Article 11

### Rules for requests and answers regarding DNA profiles

Covers: AMs 72 (rapp), 73 (rapp), 74 (rapp), 421part (Greens), 422part (Left), 75 (rapp),  
Fall: AMs 416 (S&D), 417 (ID), 419 (Left), 420 (Left), 423 (S&D), 424 (ID)

1. A request for an automated search or comparison shall include only the following information:
  - (a) the code of the requesting Member State;
  - (b) the date, time and indication number of the request;
  - (c) DNA profiles and their reference numbers referred to in Article 9;
  - (d) the types of DNA profiles transmitted (unidentified DNA profiles or ~~reference~~ **identified** DNA profiles). (AM 72)
2. The answer to the request referred to in paragraph 1 shall contain only the following information:
  - (a) an indication as to whether there were one or more matches or no matches;
  - (b) the date, time and indication number of the request;
  - (c) the date, time and indication number of the answer;
  - (d) the codes of the requesting and requested Member States;
  - (e) the reference numbers of the DNA profiles from the requesting and requested Member States;
  - (f) the type of DNA profiles transmitted (unidentified DNA profiles or ~~reference~~ **identified** DNA profiles); (AM 73)
  - (g) the matching DNA profiles.
3. Automated notification of a match shall only be provided if the automated search or comparison has resulted in a match of a minimum number of loci. The Commission, **after consulting the European Data Protection Board in accordance with Article 42(2) of**



**Regulation 2018/1725**, shall adopt ~~an~~ implementing acts ~~act~~ to specify this minimum number of loci, in accordance with the procedure referred to in Article 75(2). (AM 74, 421, 422)

4. Where a search or comparison with unidentified DNA profiles results in a match, each requested Member State with matching data may insert a marking in its national database indicating that there has been a match for that DNA profile following another Member State's search or comparison.

5. Member States shall ensure that requests are consistent with ~~declarations~~ **notifications** sent pursuant to Article 8 **73(2a)**. Those ~~declarations~~ **notifications** shall be reproduced in the practical handbook referred to in Article 77. (AM 75)

## **CA 4 - Chapter 2 - Section 2 - Articles 12 to 17 (Dactyloscopic Data)**

### SECTION 2 DACTYLOSCOPIC DATA

[Falls AM 426 S&D]

#### *Article 12* **Dactyloscopic reference data**

Covers: AM 76 (rapp), 77 (rapp), 429 (RE), 78 (rapp)

Fall: AMs 427 (Left), 428 (S&D)

1. Member States shall ensure the availability of dactyloscopic reference data from ~~the file for the *their* national automated fingerprint identification systems~~ **database or databases** established for the prevention, detection and investigation of criminal offences. (AM 76, 428part)

2. Dactyloscopic reference data shall not contain any **additional ~~nominal~~** data from which an individual can be directly identified. (AMs 77, 429)

3. ~~Dactyloscopic reference data which is not attributed to any individual~~ ( Unidentified dactyloscopic data) shall be recognisable as such. (AM 78)

#### *Article 13* **Automated searching of dactyloscopic data**

[Falls AM 430 S&D]

Covers: AMs 79 (rapp), 80 (rapp), 436 (RE), 81 (rapp), 439part (RE),

Fall: 431 (Left), 433 (Greens), 432 (S&D), 434 (Left), 435 (Greens), 437 (S&D), 438 (Left), 440 (ID), 441 (Greens), 442 (Left), 443 (Left), 444 (Left)

1. For the prevention, detection and investigation of criminal offences, Member States shall allow national contact points of other Member States and Europol access to the dactyloscopic reference data in ***their national databases*** ~~the automated fingerprint identification systems which they have established~~ for that purpose, to conduct automated searches by comparing dactyloscopic reference data. (AM 79)

Searches ~~may~~ **shall only** be conducted ~~only~~ in individual cases, **where they are proportionate and necessary for the purposes of preventing, detecting or investigating a**

**criminal offence**, and in compliance with the national law of the requesting Member State. (AM 80, 436)

2. The national contact point of the requesting Member State shall **manually ensure that a human review by a forensic expert is conducted in order to** confirm a match of dactyloscopic data with dactyloscopic reference data held by the requested Member State following the automated supply of the dactyloscopic reference data required for confirming a match. (AMs 81, 439part)

#### Article 14

##### Reference numbers for dactyloscopic data

Covers: AM 82 (rapp), 83 (rapp)

Fall:

The reference numbers for dactyloscopic data shall be the combination of the following:  
(a) a reference number allowing Member States, in the case of a match, to retrieve further data and other information in their databases referred to in Article 12 in order to supply it to one, several or all of the other Member States in accordance with ~~Articles Article 47 and 48~~ **or to Europol in accordance with Article 50(6)**; (AM 82)

**(aa) a reference number allowing Europol, in case of a match, to retrieve further data and other information for the purposes of Article 49(1) in order to supply them or it to one, several or all Member States in accordance with Regulation (EU) 2016/794**; (AM 83)

(b) a code to indicate the Member State which holds the dactyloscopic data.

#### Article 15

##### Principles for the exchange of dactyloscopic data

Covers: AMs 84 (rapp), 445 (RE), 85 (rapp), 447 (RE), 86 (rapp), 448 (RE), 449 (Left), 87 (rapp)

Fall: 446 (Left)

1. The digitalisation of dactyloscopic data and their transmission to the other Member States **or Europol** shall be carried out in accordance with a uniform data format. The Commission shall adopt ~~an~~ implementing acts ~~act~~ to specify the uniform data format in accordance with the procedure referred to in Article 75(2). (AMs 84, 445)

2. Each Member State **and Europol** shall ensure that the dactyloscopic data it transmits are of sufficient quality for a comparison by the **automated comparison** fingerprint identification systems. ~~The Commission shall adopt an implementing act to specify the minimum quality standard for the comparison of dactyloscopic data. That implementing act shall be adopted in accordance with the procedure referred to in Article 75(2).~~ (AMs 85, 447)

3. Member States **and Europol** shall take **all** appropriate measures to ensure the confidentiality and integrity of dactyloscopic data being sent to other Member States, including their encryption. (AMs 86, 448, 449)

4. The Commission shall adopt ~~an~~ implementing **act** acts to specify specifying **the minimum quality standard for the comparison of dactyloscopic data** and the relevant existing **European or international** standards for dactyloscopic data exchange that are to

be used by Member States, *including the minimum quality standard for the automated comparison of dactyloscopic data.* ~~That~~ Those implementing ~~act~~ acts shall be adopted in accordance with the procedure referred to in Article 75(2). (AMs 85, 87, 447)

#### Article 16

##### Search capacities for dactyloscopic data

Covers: AMs 88 (rapp), 450 (RE), 89 (rapp), 90 (rapp)

Fall: 451 (ID), 452 (RE)

1. ~~Each Member State~~ *States and Europol* shall ensure that ~~its~~ *their* search requests do not exceed the search capacities specified by the requested Member State. (AMs 88, 450) Member States shall inform *other Member States, Europol*, the Commission and eu-LISA ~~in accordance with Article 79(8) and (10)~~ about their maximum search capacities per day for dactyloscopic data of identified persons and for dactyloscopic data of persons not yet identified. *Member States may raise those maximum search capacities. Where a Member State raises those maximum search capacities, it shall notify the other Member States, Europol, the Commission and eu-LISA of the new maximum search capacities.* (AM 89)
2. The Commission shall adopt ~~act~~ implementing ~~act~~ acts to specify the maximum numbers of candidates accepted for comparison per transmission in accordance with the procedure referred to in Article 75(2). (AM 90)

#### Article 17

##### Rules for requests and answers regarding dactyloscopic data

Covers:

Fall: AM 453 (Left)

1. A request for an automated search shall include only the following information:
  - (a) the code of the requesting Member State;
  - (b) the date, time and indication number of the request;
  - (c) the dactyloscopic data and their reference numbers referred to in Article 14.
2. The answer to the request referred to in paragraph 1 shall contain only the following information:
  - (a) an indication as to whether there were one or more matches or no matches;
  - (b) the date, time and indication number of the request;
  - (c) the date, time and indication number of the answer;
  - (d) the codes of the requesting and requested Member States;
  - (e) the reference numbers of the dactyloscopic data from the requesting and requested Member States;
  - (f) the matching dactyloscopic data.

### **CA 5 - Chapter 2 - Section 3 - Articles 18 to 20 (Vehicle Registration Data)**

#### SECTION 3

#### VEHICLE REGISTRATION DATA

[Falls AMs 454 S&D, 455 S&D]

#### Article 18

##### Automated searching of vehicle registration data

Covers: AMs 91 (rapp), 461 (S&D), 462 (Greens),

Fall: AM 456 (S&D), AM 457 (Left), 458 (Greens), 459 (S&D), 460 (Left), 463 (Left), 464 (S&D), 465 (Greens)

1. For the prevention, detection and investigation of criminal offences, Member States shall allow national contact points of other Member States and Europol access to the following national vehicle registration data, to conduct automated searches in individual cases:

(a) ~~ertain~~ data relating to owners or operators ~~keepers~~; (AM 91, 461, 462)

(b) data relating to vehicles.

2. Searches may be conducted only with a full chassis number or a full registration number.

3. Searches may be conducted only in compliance with the national law of the requesting Member State.

**4a. The data set out in in the first subparagraph, points (a) and (b), of this Article shall not go beyond the data elements specified in the implementing act adopted pursuant to Article 19(3).**

#### Article 19

##### Principles of automated searching of vehicle registration data

Covers: AMs 92 (rapp)

Fall: AM 466 (S&D), 467 (S&D), 468 (Left), 469 (Left), 470 (Left), 471 (RE)

1. For automated searching of vehicle registration data Member States shall use the European Vehicle and Driving Licence Information System (Eucaris).

2. The information exchanged via Eucaris shall be transmitted in encrypted form.

3. The Commission shall adopt ~~an~~ implementing ~~act~~ acts to specify the data elements of the vehicle registration data ~~to~~ **which may** be exchanged. ~~That~~ Those implementing ~~act~~ acts shall be adopted in accordance with the procedure referred to in Article 75(2). (AM 92)

#### Article 20

##### Keeping of logs

Covers: AMs 93 (rapp), ~~94 (rapp)~~, 474part (Left), 475 (Greens)

Fall: 472 (RE), 473 (Left), 474part (Left), 476 (S&D), 94 (rapp), 477 (RE), 478 (S&D)

1. Each Member State shall keep logs of queries that the staff of its **competent law enforcement** authorities duly authorised to exchange vehicle registration data make as well as logs of queries requested by other Member States. Europol shall keep logs of queries that its duly authorised staff make. (AM 93)

Each Member State and Europol shall keep logs of all data processing operations concerning vehicle registration data. Those logs shall include the following:

(a) the Member State or Union agency launching the request for a query;

(b) the date and time of the request;

(c) the date and time of the answer;

(d) the national databases to which a request for a query was sent;

(e) the national databases that provided a positive answer.

2. The logs referred to in paragraph 1 may be used only for the collection of statistics and data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, and for ensuring data security and integrity.

Those logs shall be protected by *all* appropriate measures against unauthorised access and erased *three years* after their creation. If, however, they are required for monitoring procedures that have already begun, they shall be erased once the monitoring procedures no longer require the logs. (AMs 474part, 94, 475)

3. For the purposes of data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, the data controllers shall have access to the logs for self-monitoring as referred to in Article 56.

## **CA 6 - Chapter 2 - Section 4 - Articles 21 to 24 (Facial Images)**

### SECTION 4 FACIAL IMAGES

[Falls AMs 479 ECR, 480 Left, 481 Greens, 482 S&D]

#### *Article 21* **Facial images**

Covers: AMs 95 (rapp), 487part (RE), 488part (S&D), 96 (rapp), 489 (RE), 97 (rapp)  
Falls: AMs 483 (S&D), 484 (ECR), 485 (S&D), 490 (Left)

1. Member States shall ensure the availability of facial images *of persons convicted or suspected of having committed a criminal offence collected in accordance with their national law* from their national databases established for the prevention, detection and investigation of criminal offences. Those data shall only include facial images and the reference number referred to in Article 23, and shall indicate whether the facial images are attributed to an individual or not. (AMs 95, 487part, 488part)  
Member States shall not make available in this context any *additional* data from which an individual can be directly identified. (AMs 96, 489)
2. ~~Facial images which are not attributed to any individual~~ (Unidentified facial images must be recognisable as such. (AMs 97)

#### *Article 22* **Automated searching of facial images**

Covers: AMs 98 (rapp), 99 (rapp), 497 (RE), 498 (S&D), 491 (Left), 100 (rapp), 505 (RE), 101 (rapp), 499 (RE), 509part (RE)  
Fall: 492 (S&D), 493 (ECR), 494 (S&D), 495 (S&D), 496 (Left), 500 (Left), 501 (Greens), 502 (S&D), 503 (Left), 504 (ID), 506 (Left)

1. For the prevention, detection and investigation of criminal offences, Member States shall allow national contact points of other Member States and Europol access to *the facial images reference data* stored in their national databases *established pursuant referred to in Article 21(1)*, to conduct automated searches. (AMs 98)  
Searches ~~may~~ *shall only* be conducted in individual cases, *where they are proportionate and necessary for the purpose of preventing, detecting or investigating a serious criminal offence*, and in compliance with the national law of the requesting Member State. *Searches for the purpose of profiling shall be prohibited.* (AMs 99, 497, 498, 491, 499, 509part)
2. The requesting Member State shall receive a list composed of matches concerning likely candidates. That Member State shall *ensure that a human review of the list is conducted by two forensic experts in order* to determine the existence of a confirmed match. (AM 100, 505)
3. ~~A minimum quality standard shall be established to allow for search and comparison of facial images. The Commission shall adopt implementing acts to specify that minimum quality standard. Those implementing acts shall be adopted in accordance with the procedure referred to in Article 75(2).~~ (AM 101)

*Article 23*

**Reference numbers for facial images**

Covers: AMs 102 (rapp)

Fall: AMs 507 (S&D), 508 (ECR)

The reference numbers for facial images shall be the combination of the following:

(a) a reference number allowing Member States, in case of a match, to retrieve further data and other information in their databases referred to in Article 21 in order to supply it to one, several or all of the other Member States in accordance with Articles 47 ~~and 48~~ **or *Europol in accordance with Article 50(6)***; (AM 102)

(b) a code to indicate the Member State which holds the facial images.

*Article 23a*

**Principles for the exchange of facial images**

Covers: AMs 103 (rapp), 509part (RE)

Fall:

***1. Each Member State and Europol shall ensure that the facial images in their databases are of sufficient quality for the purpose of this Regulation, in particular for automated comparison. ~~The Commission shall adopt an implementing act to specify the minimum quality standard for the comparison of facial images. That implementing act shall be adopted in accordance with the procedure referred to in Article 75(2).~~***

***2. Member States ~~and Europol~~ shall take appropriate measures to ensure the confidentiality and integrity of facial images being sent to other Member States, and Europol of facial images being sent to Member States, including their encryption.***

***3. The Commission shall adopt ~~an implementing acts to specify~~ specifying ~~the minimum quality standard for the comparison of facial images and the relevant European or international standards for facial image exchange that are to be used by Member States and Europol, including the minimum quality standard for the automated comparison of facial images. That~~ Those implementing acts shall be adopted in accordance with the procedure referred to in Article 75(2).***

*Article 24*

**Rules for requests and answers regarding facial images**

Covers:

Fall: AMs 510 (ECR), 511 (S&D), 512 (S&D), 513 (Left)

1. A request for an automated search shall include only the following information:

(a) the code of the requesting Member State;

(b) the date, time and indication number of the request;

(c) the facial images and their reference numbers referred to in Article 23.

2. The answer to the request referred to in paragraph 1 shall contain only the following information:

(a) an indication as to whether there were one or more matches or no matches;

- (b) the date, time and indication number of the request;
- (c) the date, time and indication number of the answer;
- (d) the codes of the requesting and requested Member States;
- (e) the reference numbers of the facial images from the requesting and requested Member States;
- (f) the matching facial images.

## **CA 7 - Chapter 2 - Section 5 - Articles 25 to 28 (Police Records)**

### SECTION 5 POLICE RECORDS

[Falls AMs 514 (Left), 515 (S&D), 516 (Greens)]

#### *Article 25*

#### ***National Police records indexes***

Covers: AMs 104 (rapp), 105 (rapp), 517 (S&D), 519 (RE), 520part (S&D), 106 (rapp), 523 (RE), 107 (rapp), 529part (S&D)  
Fall: 517 (S&D), 518 (S&D), 521 (ID), 522 (Left), 524 (Left), 526 (RE), 525 (RE)

1. Member States may decide to participate in the automated exchange of police records ***indexes***. ***For the purposes of such exchanges, participating*** Member States ~~participating in the automated exchange of police records~~ shall ensure the availability of ***national police records indexes which contain sets of*** biographical data of ***persons convicted or suspected of having committed a serious criminal offence*** ~~suspects and criminals~~ from their national police records indexes ***databases*** established for the ***prevention, detection and*** investigation of criminal offences. ~~Those sets~~ ***This set of data shall, if applicable and to the extent that they are*** available, ~~shall~~ contain ***only*** the following data: (AMs 105, 517, 519, 520part, 529part)

- (a) first name(s);
- (b) family name(s);
- (c) alias(es) ***and previously used name(s)***; (AM 106, 523)
- (d) date of birth;
- (e) nationality or nationalities;
- (f) place and country of birth;
- (g) gender.

***1a. Member States shall, in accordance with Article 7(2) of Directive (EU) 2016/680, ensure that the data included in the national police records indexes as listed in paragraph 1 are accurate, complete and up to date, and based on facts to be distinguished, as far as possible, from personal data based on personal assessments*** (AMs 107, 524, 526)

2. The data referred to in paragraph 1, points (a), (b), (c), (e) and (f) shall be pseudonymised.

#### *Article 26*

#### ***Automated searching of police records indexes***



Covers: AMs 108 (rapp), 109 (rapp), 110 (rapp), 529 (S&D), 530 (RE), 531part (Left), 532 (RE)

Fall: AMs 527 (S&D), 528 (S&D)

1. For the ~~prevention, detection and~~ investigation of criminal offences, Member States *participating in the automated exchange of police records indexes* shall allow national contact points of other Member States *participating in such exchanges* and Europol access to data ~~from~~ *in* their national police records indexes, to conduct automated searches. (AM 108)

Searches ~~may~~ *shall only* be conducted ~~only~~ in individual cases, *where they are proportionate and necessary for the purpose of preventing, detecting or investigating investigation of a serious criminal offence*, and in compliance with the national law of the requesting Member State. (AM 109, 529, 530, 531part, 532)

~~2. The requesting Member State shall receive the list of matches with an indication of the quality of the matches.~~

~~The requesting Member State shall also be informed about the Member State whose database contains data that resulted in the match. (AM 110)\*~~

*\*this paragraph is already covered in Article 44(4)*

#### Article 27

#### Reference numbers for police records

Covers: AM 111 (rapp)

Fall: AM 539 (S&D)

The reference numbers for police records shall be the combination of the following:

(a) a reference number allowing Member States, in the case of a match, to retrieve personal data and other information in their *national police records* indexes referred to in Article 25 in order to supply it to one, several or all of the Member States in accordance with Articles ~~47 and 48~~ **44**; (AM 111)

(b) a code to indicate the Member State which holds the police records.

#### Article 28

#### Rules for requests and answers regarding police records indexes

Covers: AM 112 (rapp), 113 (rapp)

Fall: 540 (S&D), 541 (S&D)

1. A request for an automated search *of police records indexes* shall include only the following information:

(a) the code of the requesting Member State;

(b) the date, time and indication number of the request;

(c) the ~~police records and their reference numbers~~ *data* referred to in Article ~~27~~ **25(1)**, *where available and pseudonymised in accordance with Article 25(2)*. (AM 112)

2. The answer to the request referred to in paragraph 1 shall contain only the following information:

(a) an indication as to ~~whether there were one or more matches or no~~ *the number of* matches; (AM 113)

- (b) the date, time and indication number of the request;
- (c) the date, time and indication number of the answer;
- (d) the codes of the requesting and requested Member States;
- (e) the reference numbers of the police records from the requested Member States.

## **CA 8 - Chapter 2 - Section 6 - Articles 29 to 34 (Common Provisions)**

### SECTION 6 COMMON PROVISIONS

#### *Article 29*

##### **National contact points**

Covers: AMs 114 (rapp), 115 (rapp), 543 (RE),  
Fall: AMs 542 (Greens)

1. Each Member State shall designate ~~a~~ **at least one** national contact point. (AMs 114)
2. The national contact points shall be responsible for supplying the data referred to in Articles 6, 7, 13, 18, 22 and 26.

**2a. Member States shall ensure that their national contact points are provided with adequate human, technical and financial resources, including qualified staff, to carry out their tasks under this Regulation in an adequate, effective and rapid manner.** (AMs 115, 543)

#### *Article 30*

##### **Implementing measures**

Covers: AMs 116 (rapp)  
Fall: AMs 544 (Left), 545 (Greens),

The Commission shall adopt ~~an~~ implementing acts ~~act~~ to specify the technical arrangements **to be made by the Member States with respect to** ~~for~~ the procedures set out in Articles 6, 7, 13, 18, 22 and 26. Those ~~That~~ implementing acts ~~act~~ shall be adopted in accordance with the procedure referred to in Article 75(2). (AM 116)

#### *Article 31*

##### **Technical specifications**

Covers: AM 117 (rapp)  
Fall: AMs 546 (Left), 547 (S&D), 548 (S&D), 549 (Greens), 550 (ECR)

~~Member States and Europol shall observe common technical specifications in connection with all requests and answers related to searches and comparisons of DNA profiles, dactyloscopic data, vehicle registration data, facial images and police records. The Commission shall adopt implementing acts to specify these technical specifications in accordance with the procedure referred to in Article 75(2).~~

*Article 32*

**Availability of automated data exchange at national level**

Covers: AMs 555 (S&D), 118 (rapp), 119 (rapp), 120 (rapp),

Fall: AMs 553 (Left), 554 (S&D), 556 (S&D), 557 (Greens), 558 (Left), 559 (ID), 560 (ECR), 561 (ID), 562 (Left), 563 (S&D), 564 (S&D), 565 (S&D), 566 (Left)

1. Member States shall take all necessary measures to ensure that automated searching or comparison of DNA profiles, dactyloscopic data, ~~ertain~~ vehicle registration data, facial images and police records is possible 24 hours a day and seven days a week. (AM 555)

2. National contact points shall immediately inform each other, the Commission, Europol and eu-LISA ~~where~~ of the a technical fault causing unavailability of the automated data exchange is unavailable. (AM 118)

~~Where automated data exchange is unavailable~~, National contact points shall agree on temporary alternative information exchange arrangements in accordance with the applicable Union law and national legislation ~~law~~, in for cases where automated data exchange is unavailable. (AM 119)

3. Where automated data exchange is unavailable, national contact points shall *ensure that it is re-established* ~~re-establish the automated data exchange~~ without delay. (AM 120)

*Article 33*

**Justification for the processing of data**

Covers: AMs 121 (rapp), 122 (rapp), 123 (rapp), 568 (Greens), 571 (RE), 572 (Left), 573 (S&D), 574part (Greens), 575 (RE), 576 (Left), 577 (RE), 580 (RE)

Fall: AMs 567 (Left), 569 (Left), 570 (Left), 124 (rapp), 578 (RE), 579 (Left), 581 (Left)

1. Each Member State shall keep a justification of the queries that its competent *law enforcement* authorities make. (AM 121)

Europol shall keep a justification of the queries it makes.

2. The justification referred to in paragraph 1 shall include:

(a) the purpose of the query, including a reference to the specific case or investigation *and the criminal offence, where applicable*; (AM 568, 572part, 575)

(b) an indication on whether the query concerns a suspect or a ~~perpetrator~~ *person convicted* of a criminal offence, *a victim of serious crime or terrorism, a missing person or unidentified human remains*; (AMs 122, 571, 572part, 573, 574part)

(c) an indication on whether the query aims to identify ~~an unknown~~ *a* person or obtain more data on a known person. (AM 123)

3. The justifications referred to in paragraph 2 shall only be used for *fundamental rights and* data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, and for ensuring data security and integrity. (AMs 576, 577)

Those justifications shall be protected by appropriate measures against unauthorised access and erased ~~one year~~ *three years* after their creation. If, however, they are required for monitoring procedures that have already begun, they shall be erased once the monitoring procedures no longer require the justification. (AMs 124, 578, 579)

4. For the purposes of *fundamental rights and* data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, the data

controllers shall have **unrestricted** access to those justifications for self-monitoring as referred to in Article 56. (AM 580)

*Article 34*

**Use of the universal message format**

Covers: AM 125 (rapp)

Fall: AMs 582 (Greens), 583 (ID)

1. The universal message format (UMF) standard ~~referred to in~~ **established under Article 38 of Regulation (EU)2019/818** shall be used in the development of the router referred to in Article 35 **of this Regulation** and EPRIS, **to the extent it is applicable**. (AM 125)
2. Any automated exchange of data in accordance with this Regulation shall use the UMF standard.

**CA 9 - Chapter 3 - Section 1 - Articles 35 to 41 (Architecture)**

CHAPTER 3  
ARCHITECTURE  
SECTION 1  
**Router**

*Article 35*

**The router**

Covers: AMs 126 (rapp), 127 (rapp)

Fall: AM 584 (Left), 585 (Greens)

1. A router is established for the purposes of facilitating the establishment of connections between Member States, and **between Member states and** ~~with~~ Europol, for querying with, retrieving and scoring biometric data **and for retrieving alphanumeric data** in accordance with this Regulation. (AM 126)
2. The router shall be composed of:
  - (a) a central infrastructure, including a search tool enabling the simultaneous querying of Member States' databases referred to in Articles 5, 12 and 21 ~~as well as of~~ **and** Europol data;
  - (b) a secure communication channel between the central infrastructure, Member States' **competent law enforcement authorities authorised** to use the router **in accordance with Article 36 and Europol**; (AM 127)
  - (c) a secure communication infrastructure between the central infrastructure and the European Search Portal for the purposes of Article 39.

*Article 36*

**Use of the router**

Covers: AM 128 (rapp), 586part (S&D), 587part (S&D), 588part (Left), 589part (Greens), 615 (Left)

Fall: AM 590 (ECR), 591 (Left)

The use of the router shall be reserved to the Member States' **competent law enforcement** authorities that ~~have~~ **are authorised to** access **and to the** exchange of DNA profiles, dactyloscopic data and facial images **in accordance with this Regulation**, and Europol in accordance with this Regulation and Regulation (EU) 2016/794 **where they have a demonstrable need for such access. Member States and Europol shall ensure that their authorised staff have completed relevant training, including on data protection, confidentiality, detection of biases, as well as for the accurate review of matches under the relevant data category.** (AM 128, 586part, 587part, 588part, 589part, 615).

#### Article 37

#### Queries

Covers AM 129 (rapp), 130 (rapp), 131 (rapp), 132 (rapp), 133 (rapp), 134 (rapp), 602part (S&D), 603part (Left), 604part (Greens), 608part (Greens), 609part (Left), 610 (Greens), 611 (S&D)

Fall: AM 592 (Left), 593 (Greens), 594 (Greens), 595 (Left), 596 (S&D), 597 (Greens), 598 (Left), 599 (S&D), 600 (ID), 601 (Left),

1. **The competent law enforcement authorities authorised to access** the router users referred to **pursuant to** Article 36 shall request a query **by submitting** biometric data to the router. The router shall dispatch the request for a query to the **databases of the requested** Member States ~~databases~~ and Europol data simultaneously with the data submitted by the user in accordance with **his or her** access rights. (AM 129)
2. ~~On receiving the~~ **Upon receipt of a** request for a query from the router, each requested Member State and Europol shall launch a query of their databases in an automated manner and without delay. (AM 130)
3. Any **candidates** matches resulting from the query in each Member States' databases and Europol data **queries referred to in paragraph 2** shall be sent back in an automated manner to the router. **The requesting Member State shall be notified in an automated manner where there is no match.** (AM 131)
4. The router shall rank the replies in accordance with the score of the correspondence between the biometric data used for querying and the biometric data ~~stored in~~ **supplied by** the **requested** Member States' databases and Europol data. (AM 132)
5. **The router shall return** the list of matching biometric data and their scores ~~shall be returned to the router user by the router~~ (AM 133). **That list shall be limited to the maximum number of candidates set out in the implementing act adopted pursuant to paragraph 6.** (AM 608part)
6. The Commission, **after consulting the European Data Protection Board in accordance with Article 42(2) of Regulation 2018/1725**, shall adopt ~~an~~ implementing ~~act~~ acts to specify the technical procedure for the router to query Member States' databases and Europol data, the format of the router replies, ~~and~~ the technical rules for scoring the correspondence between biometric data **and the relevant thresholds, as well as the maximum number of candidates that can be returned per search, with a view to ensuring accuracy, minimising the risk of misidentification and preventing discrimination. That** Those implementing ~~act~~ acts shall be adopted in accordance with the procedure referred to in Article 75(2). (AM 134, 602part, 603part, 604part, 608part, 609part, 610, 611).

*Article 38*  
**Quality check**

Covers AMs 135 (rapp), 613 (Greens)

Fall: AM 612 (Left), 614 (S&D), 616 (S&D), 617 (Left), 618 (ID)

The requested Member State shall check the quality of the transmitted data by means of *an* a fully automated procedure. (AM 613)

~~Should the data be unsuitable for an automated comparison,~~ The requested Member State shall inform the requesting Member State ~~about it,~~ *without delay*, via the router, *where the data are unsuitable for an automated comparison*. (AM 135)

*Article 39*

**Interoperability between the router and the Common Identity Repository for the purposes of law enforcement access**

Covers AMs 136 (rapp), 137 (rapp), 138 (rapp), 620 (RE), 622 (S&D), 623 (Left), 624 (Greens)

Fall: AMs 619 (Greens), 621 (Left)

1. *Where designated authorities are authorised to use* the router ~~users referred to in pursuant to~~ Article 36, *they* may launch a query to Member States' databases and Europol data simultaneously with a query to the Common Identity Repository, *provided that* ~~where~~ the relevant conditions under Union law are fulfilled and *that the query is launched* in accordance with their access rights. For this purpose, the router shall query the Common Identity Repository via the European Search Portal. (AM 136, 620)

2. Queries to the Common Identity Repository for law enforcement purposes shall be carried out in accordance with Article 22 of Regulation (EU) 2019/817 and Article 22 of Regulation (EU) 2019/818. Any result from the queries shall be transmitted via the European Search Portal.

~~Only designated authorities defined in Article 4, point 20, of Regulation (EU) 2019/817 and Article 4, point 20, of Regulation (EU) 2019/818 may launch these simultaneous queries.~~ (AM 137)

Simultaneous queries of the Member States' databases and Europol data and the Common Identity Repository may only be launched where ~~it is likely~~ *there are reasonable grounds to believe* that data on a suspect, ~~a person convicted of or reasonably suspected of a serious criminal offence~~ perpetrator or ~~a~~ victim of a terrorist offence or other serious criminal offences ~~crime or terrorism~~ as defined respectively in Article 4, points 21 and 22, of Regulation (EU) 2019/817 and Article 4, points 21 and 22, of Regulation (EU) 2019/818 are stored in the Common Identity Repository. (AM 138, 622, 623, 624)

*Article 40*

**Keeping of logs of all data processing operations in the router (AM 625)**

Covers AMs 139 (rapp), 625 (RE), 631 (Greens)

Fall: AMs 626 (ID), 627 (Left), 628 (Left), 629 (Left), 630 (ID), 140 (rapp), 632 (Left), 633 (RE), 634 (S&D), 635 (Left)

\* *log storage period in par. 3* - 2 years (AM 140 rapp), 3 years (AM 631 Greens), 4 years (AM 632 Left, 633 RE); 5 years (AM 634 S&D)

3 years with the same reasoning used in Art. 20 and Art. 33: art. 40 Europol Regulation

1. eu-LISA shall keep logs of all data processing operations in the router. Those logs shall include the following:

- (a) the Member State or Union agency launching the request for a query;
- (b) the date and time of the request;
- (c) the date and time of the answer;
- (d) the national databases or Europol data to which a request for a query was sent;
- (e) the national databases or Europol data that provided an answer;
- (f) where applicable, the fact that there was a simultaneous query to the Common Identity Repository.

2. Each Member State shall keep logs of queries that ***the staff of*** its competent ***law enforcement*** authorities ~~and the staff of those authorities~~ duly authorised to use the router make as well as logs of queries requested by other Member States. (AM 139)

Europol shall keep logs of queries that its duly authorised staff make.

3. The logs referred to in paragraphs 1 and 2 may be used only for the collection of statistics and data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, and for ensuring data security and integrity.

Those logs shall be protected by appropriate measures against unauthorised access and erased ***three years*** after their creation. If, however, they are required for monitoring procedures that have already begun, they shall be erased once the monitoring procedures no longer require the logs. (AM 631)

4. For the purposes of data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, the data controllers shall have access to the logs for self-monitoring as referred to in Article 56.

#### *Article 41*

#### **Notification procedures in case of technical impossibility to use the router**

Covers AMs 141 (rapp), 142 (rapp), 143 (rapp), 637 (RE)

Fall: AM 636 (Left), 638 (ID), 639 (Left), 640 (Left), 641 (ID)

1. Where it is technically impossible to use the router to query one or several national databases or Europol data because of a failure of the router, the ***competent law enforcement authorities referred to in Article 36 and Europol*** ~~router users~~ shall be notified in an

automated manner by eu-LISA. eu-LISA shall take measures to address the technical impossibility to use the router without delay. (AM 141)

2. Where it is technically impossible to use the router to query one or several national databases because of a failure of the national infrastructure in a Member State, that Member State shall notify the other Member States, *Europol*, eu-LISA and the Commission in an automated manner. *The Member State concerned* shall take *appropriate* measures to address the technical impossibility to use the router without delay. (AMs 142, 637)

3. Where it is technically impossible to use the router to query Europol data because of a failure of the infrastructure of Europol, Europol shall notify the Member States, eu-LISA and the Commission in an automated manner. Europol shall take *appropriate* measures to address the technical impossibility to use the router without delay. (AM 143)

### **CA 10 - Chapter 3 - Section 2 - Articles 42 to 46 (EPRIS)**

#### SECTION 2 EPRIS

Fall: AMs 642 (Greens), 643 (Left), 644 (S&D)

#### *Article 42* EPRIS

Covers: AMs 144 (rapp)

Fall: 645 (S&D), 646 (S&D), 647 (S&D)

1. For the automated searching of *national* police records *indexes* referred to in Article 26, Member States and Europol shall use the European Police Records Index System (EPRIS).

2. EPRIS shall be composed of: (AM 144)

(a) a central infrastructure, including a search tool enabling the simultaneous querying of Member States' databases;

(b) a secure communication channel between the EPRIS central infrastructure, Member States and Europol.



*Article 43*  
**Use of EPRIS**

Covers: AMs 145 (rapp), 146 (rapp), 649 (RE)

Fall: AMs 648 (S&D)

1. For the purposes of searching *national* police records *indexes* via EPRIS, *at least two of* the following sets of data shall be used: (AM 145)
  - (a) first name(s);
  - (b) family name(s);
  - (c) date of birth.
2. Where available, the following sets of data may also be used:
  - (a) alias(es) *and previously used name(s)*; (AM 146, 649)
  - (b) nationality or nationalities;
  - (c) place and country of birth;
  - (d) gender.
3. The data referred to in points (a) and (b) of paragraph 1 and in points (a), (b) and (c) of paragraph 2 used for queries shall be pseudonymised.

*Article 44*  
**Queries**

Covers: AMs 147 (rapp), 148 (rapp), 149 (rapp), 150 (rapp), 151 (rapp)

Fall: 650 (S&D), 651 (Left), 652 (S&D), 653 (Left), 654 (S&D), 655 (Left), 656 (Left), 657 (S&D), 658 (S&D), 659 (S&D), 660 (Left)

1. Member States and Europol shall request a query by submitting the data referred to in Article 43.  
EPRIS shall dispatch the request for a query to the Member States' ~~databases~~ *national police records indexes* with the data submitted by the requesting Member State *or Europol* and in accordance with this Regulation. (AM 147)
2. On receiving the request for a query from EPRIS, each requested Member State shall launch a query of their national police records index in an automated manner and without delay.
3. Any matches resulting from the query in each *requested* Member State's ~~database~~ *police records indexes* shall be sent back in an automated manner to EPRIS. (AM 148)
4. The list of matches shall be returned to the requesting Member State *and Europol* by EPRIS. The list of matches shall indicate the quality of the match as well as the Member State(s) whose database(s) contains data that resulted in the match(es). (AM 149)
5. Upon reception of the list of matches, the requesting Member State shall decide the matches for which a follow-up is necessary and send a reasoned follow-up request containing any additional relevant information to the requested Member State(s) via SIENA.
6. The requested Member State(s) shall process such requests without delay to decide whether to share the data stored in their database.  
Upon confirmation, the requested Member State(s) shall share the data referred to in Article 43 where available. This exchange of *data information* shall take place via SIENA. (AM 150)

7. The Commission shall adopt ~~an~~ implementing ~~act~~ acts to specify the technical procedure for EPRIS to query Member States' databases and the format of the replies. These ~~That~~ implementing acts shall be adopted in accordance with the procedure referred to in Article 75(2). (AM 151)

*Article 45*  
**Keeping of logs**

Covers: AMs 152 (rapp), 153 (rapp), 663 (RE), 664 (RE), 665 (Left)  
Fall: 661 (RE), 662 (S&D)

1. Europol shall keep logs of all data processing operations in EPRIS. Those logs shall include the following:

- (a) the Member State or Union agency *Europol* launching the request for a query; (AM 663)
- (b) the date and time of the request;
- (c) the date and time of the answer;
- (d) the national databases to which a request for a query was sent;
- (e) the national databases that provided an answer.

2. Each *participating* Member State shall keep logs of the requests for queries that *the staff of* its competent *law enforcement* authorities ~~and the staff of those authorities~~ duly authorised to use EPRIS make. Europol shall keep logs of requests for queries that its duly authorised staff make. (AM 152)

3. The logs referred to in paragraphs 1 and 2 may be used only for data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, and for ensuring data security and integrity.

Those logs shall be protected by appropriate measures against unauthorised access and erased ~~one year~~ *three years* after their creation. (AM 153, 664, 665)

If, however, they are required for monitoring procedures that have already begun, they shall be erased once the monitoring procedures no longer require the logs.

4. For the purposes of data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, the data controllers shall have access to the logs for self-monitoring as referred to in Article 56.

7. The Commission shall adopt implementing acts to specify the technical procedure for EPRIS to query Member States' databases and the format of the replies. These implementing acts shall be adopted in accordance with the procedure referred to in Article 75(2).

*Article 46*

**Notification procedures in case of technical impossibility to use EPRIS**

Covers: AMs 154 (rapp), 667 (S&D), 668 (S&D)

Fall: 666 (S&D), 669 (ID)

1. Where it is technically impossible to use EPRIS to query one or several national ~~databases~~ ***police records indexes*** because of a failure of the infrastructure of Europol, Member States shall be notified in an automated manner by Europol. Europol shall take measures to address the technical impossibility to use EPRIS ~~without delay~~ ***in a timely manner***. (AM 154, 667)

2. Where it is technically impossible to use EPRIS to query one or several national databases because of a failure of the national infrastructure in a Member State, that Member State shall notify Europol and the Commission in an automated manner. Member States shall take measures to address the technical impossibility to use EPRIS ~~without delay~~ ***in a timely manner***. (AM 668)

**CA 11 - Chapter 4 - Articles 47 & 48 (Exchange of core data)**

CHAPTER 4

**EXCHANGE OF DATA FOLLOWING A MATCH**

*Article 47*

**Exchange of core data**

Covers AMs 156 (rapp), 157 (rapp), 158 (rapp), 159 (rapp), 671 (RE), 670 (S&D), 675 (Greens)

Fall: 672 (Left), 673 (Greens), 674 (Greens)

1. Where the procedures referred to in ~~Articles~~ ***Article 6, 7, 13 or 22*** show a match between the data used for the search or comparison and data held in the database of the requested Member State(s), and upon ***manual*** confirmation of this match by ***qualified staff of*** the requesting Member State, the requested Member State shall return a set of core data via the router within 24 hours. ***Where a judicial authorisation is required under national law, the set of core data shall be returned within 72 hours.*** (AMs 156, 671)

~~That set of core data, if available, shall contain the following data:~~

- ~~(a) first name(s);~~
- ~~(b) family name(s);~~
- ~~(c) date of birth;~~
- ~~(d) nationality or nationalities;~~
- ~~(e) place and country of birth;~~
- ~~(f) gender.~~

***1a. Where the confirmed match concerns identified data of a person, the ~~that~~ set of core data referred to in paragraph 1 shall, to the extent available, contain the following data, if available:***

- (a) first name or names;***
- (b) family name or names;***
- (c) alias or aliases and previously used name or names;***

(d) date of birth;  
(e) nationality or nationalities;  
(f) place and country of birth;  
(g) gender;  
(h) the date on which and the place where the biometric data were acquired;  
(i) the criminal offence for which the biometric data were acquired;  
(j) the criminal case number;  
(k) the competent law enforcement authority responsible for the criminal case. (AM 157)

**Ib.** Where the confirmed match concerns unidentified data or traces, the ~~that~~ set of core data referred to in paragraph 1 shall, to the extent available, contain the following data, ~~if available~~:

(a) the date on which and the place where the biometric data were acquired;  
(b) the criminal offence for which the biometric data were acquired;  
(c) the criminal case number;  
(d) the competent law enforcement authority responsible for the criminal case. (AM 158)

**Ic.** The release of core data by the requested Member State shall be subject to the decision of a human, ~~as required by Article 11 of Directive (EU) 2016/680~~. (AM 159)

**Id.** The requested Member State(s) ~~may~~ shall only refuse to share the core data where:

(a) the judicial authorisation required under the national law of the requested Member State was refused;  
(b) there are objective reasons to believe sharing core data would disproportionately infringe the fundamental rights of the data subject; or  
(c) there are objective reasons to believe sharing core data would jeopardise the success of an ongoing investigation of a criminal offence.

The justification for such refusals must be provided promptly to the requesting Member State and in any event within the time limits provided in paragraph 1. (AMs 670, 675)

*Article 48*  
**Use of SIENA**

Covers AMs 160 (rapp), 676 (S&D)  
Falls: AM 677 (Left)

Any exchange which is not explicitly provided for in this Regulation between Member States' competent authorities or with Europol, at any stage of one of the procedures under this Regulation, shall take place via SIENA. (AMs 160, 676)

**CA 12 - Chapter 5 - Articles 49 & 50 (Europol)**

CHAPTER 5  
**EUROPOL**

*Article 49*  
**Access by Member States to third country-sourced biometric data stored by Europol**

Covers AMs 161 (rapp), 162 (rapp)

Falls: 678 (Greens), 679 (S&D), 680 (Left), 681 (S&D), 682 (Left)

1. ***Without prejudice to any restrictions indicated by the provider of the information to Europol in accordance with Article 19(2) of Regulation (EU) 2016/794***, Member States shall, in accordance with Regulation (EU) 2016/794, have access to, and be able to search via the router, biometric data which has been provided to Europol by third countries ~~third-country authorities~~ for the purposes of Article 18(2), points (a), (b) and (c), of Regulation (EU) 2016/794. (AMs 161)
2. Where ~~this procedure~~ ***the search referred to in paragraph 1*** results in a match between the data used for the search and ***third-country-sourced data held by Europol data***, the follow-up shall take place in accordance with Regulation (EU) 2016/794. (AM 162)

#### Article 50

#### Access by Europol to data stored in Member States' databases

Covers AMs 163 (rapp), 165 (rapp), 166 (rapp), 167 (rapp), 168 (rapp), 697 (RE)

Falls: AMs 683 (Left), 684 (S&D), 685 (S&D), 687 (S&D), 688 (Left), 689 (Greens), 690 (Greens), 691 (S&D), 692 (Greens), 693 (S&D), 694 (Greens), 695 (S&D), 696 (Greens), 698 (Left), 699 (S&D)

1. ***Where necessary to achieve ~~its~~ the objectives set out in Article 3 of Regulation (EU) 2016/794 and ~~carry out its tasks~~***, Europol shall, in accordance with Regulation (EU) 2016/794, have access ***for the purposes of Article 18(2) point (a) and (c), of Regulation (EU) 2016/794*** to data which are stored by Member States in their national databases in accordance with this Regulation. (AM 163)
2. Europol queries performed with biometric data as a search criterion shall be carried out using the router.
3. Europol queries performed with vehicle registration data as a search criterion shall be carried out using Eucaris.
4. Europol queries performed with ~~police records~~ ***biographical data of suspects and convicted persons as referred to in Article 25*** as a search criterion shall be carried out using EPRIS. (AM 165)
5. Europol shall carry out the searches in accordance with paragraph 1 only ***for the purpose of Article 18(2) point (a) of Regulation (EU) 2016/794***, when carrying out its tasks referred to in Regulation (EU) 2016/794. (AM 166)
6. Where the procedures referred to in ~~Articles~~ ***Article 6, 7, 13 or 22*** show a match between the data used for the search or comparison and data held in the national database of the requested Member State(s), and upon ~~manual confirmation of that~~ ***human review of that match by qualified staff of Europol in accordance with this Regulation and the transmission of the name of the third country which provided the data***, the requested Member State shall decide whether to return a set of core data via the router within 24 hours. ***Where a judicial authorisation is required under national law, the core data shall be returned within 72 hours.*** That set of core data, if available, shall contain the following data: (AM 167, 697)

- (a) first name(s);
- (b) family name(s);
- (c) date of birth;
- (d) nationality or nationalities;
- (e) place and country of birth;
- (f) gender.

7. Europol's use of information obtained from a search made in accordance with paragraph 1 **and 5**, and from the exchange of core data in accordance with paragraph 6, shall be subject to the consent of the Member State in ~~which~~ **whose** database the match occurred. If the Member State allows the use of such information, its handling by Europol shall be governed by Regulation (EU) 2016/794. (AM 168)

### **CA 13 - Chapter 6 - Articles 51 to 61a (Data Protection)**

*(Corresponds to Articles 51 - 62a in voting list)*

#### **CHAPTER 6 DATA PROTECTION**

##### *Article 51*

##### **Purpose of the data processing** (AM 169)

Covers AMs 169 (rapp), 170 (rapp), 171 (rapp), 172 (rapp), 173 (rapp), 174 (rapp), 175 (rapp), 701 (RE), 703part (Left), 704 (RE), 710 (RE), 712 (RE), 713part (Left), 714part (RE) 718 (RE), 719 (S&D), 722part (S&D), 724 (S&D),  
Fall: AMs 702 (S&D), 705 (Left), 706 (S&D), 707 (Greens), 708 (S&D), 709 (ECR), 711 (S&D), 715 (S&D), 716 (Greens), 720 (S&D), 721 (S&D), 723 (S&D)

1. Processing of personal data **received** by the requesting Member State or Europol shall be permitted solely for the purposes for which the data have been supplied by the requested Member State in accordance with this Regulation. ***Without prejudice to Directive (EU) 2016/680 and Regulation (EU) 2018/1725, as applicable,*** processing for other purposes shall be permitted solely with the prior authorisation of the requested Member State ***or Europol, as relevant.*** (AM 170, 701, 703part)

2. Processing of data supplied pursuant to ~~Articles~~ **Article 6, 7, 13, 18 or 22 or 26** by the ~~searching or comparing~~ **requesting** Member State ***or Europol*** shall be permitted solely ***where necessary*** in order to: (AMs 171, 704)

(a) establish whether the compared DNA profiles, dactyloscopic data, vehicle registration data, facial images and police records match;

***(aa) exchange a set of core data pursuant to Article 47;*** (AMs 172, 710)

(b) prepare and submit a police ***or judicial*** request for legal assistance if those data match; (AM 173)

(c) logging within the meaning of Articles 20, 40 and 45. (AMs 174, 712)

3. ~~The personal data received by the requesting Member State or Europol may process the data supplied to it in accordance with Articles 6, 7, 13 or 22 solely where this is necessary for the purposes of this Regulation. The supplied data shall be deleted immediately following data comparison or automated replies to searches unless further processing~~ **by the requesting Member State is strictly necessary and proportionate** for the purposes of the prevention, detection and investigation of criminal offences. (AMs 175, 713part, 714part)

4. Data supplied in accordance with Article 18 may be used by the requesting Member State solely where this is **strictly necessary and proportionate to achieve** the purposes of this Regulation. The data supplied shall be deleted immediately following automated replies to searches unless further processing is necessary for recording pursuant to Article 20. The requesting Member State shall use the data received in a reply solely for the procedure for which the search was made. (AMs 717, 718)

~~4a. Without prejudice to the powers of national supervisory authorities pursuant to Article 47 of Directive (EU) 2016/680, Prior to connecting their national databases to the router, EPRIS or Eucaris, Member States shall conduct a data protection impact assessment as referred to in Article 27 of Directive (EU) 2016/680 and consult the supervisory authority as referred to in Article 28 of that Directive. The supervisory authority may use any of its powers referred to in Article 47 of Directive (EU) 2016/680, in accordance with paragraph 5 of Article 28 of that Directive.~~ (AM 719)

~~4b. Member States shall ensure that data subjects are provided with information pursuant to Article 13 of Directive (EU) 2016/680 to allow them to exercise their rights.~~ (AM 722part)

~~4c. The European Data Protection Board shall issue guidelines on the implementation of Directive (EU) 2016/680 concerning the criminal databases and cross-border exchanges of personal data, in particular concerning accuracy, strict necessity and how to ensure ensuring respect for the right to data protection.~~ (AM 724)

## Article 52

### Accuracy, relevance and data retention

Covers AMs 176 (rapp), 177 (rapp), 178 (rapp), 179 (rapp), 180 (rapp), 726 (RE), 727 (RE), 728 (RE), 729 (RE)

Fall: AMs 725 (Left)

1. Member States *and Europol* shall ensure the accuracy and current relevance of personal data *which are processed pursuant to this Regulation*. Should a requested Member State *or Europol* become aware that ~~incorrect~~ data *that are incorrect and/or no longer up to date* or data which should not have been supplied have been supplied, this shall be notified without delay to any requesting Member State. All requesting Member States concerned shall be obliged to correct or delete the data accordingly *without undue delay*. Moreover, personal data supplied shall be corrected if they are found to be incorrect. If the requesting Member State *or Europol* has reason to believe that the supplied data are incorrect or should be deleted the requested Member State shall be informed *without delay*. (AM 176, 726)

*Member States and Europol shall put in place appropriate measures for updating their databases, including as regards acquittals of ~~acquitted~~ persons whose personal data are in the databases.* (AM 727)

2. Where a data subject contested the accuracy of data in possession of a Member State *or Europol*, where the accuracy cannot be reliably established by the Member State concerned *or Europol* and where it is requested by the data subject, the data concerned shall be marked with a flag. Where such a flag exists, Member States *or Europol* may remove it only with the permission of the data subject or based on a decision of the competent court or *national supervisory authority or the European Data Protection Supervisor, as relevant*. (AM 177)

3. Data supplied which should not have been supplied or received shall be deleted. Data which are lawfully supplied and received shall be deleted:

- (a) where they are not or no longer necessary for the purpose for which they were supplied;
- (b) following the expiry of the maximum period for keeping data laid down under the national law of the requested Member State where the requested Member State *or Europol* informed the requesting Member State of that maximum period at the time of supplying the data. (AM 178, 728);

*(ba) following the expiry of the maximum period for keeping data laid down in Regulation (EU) 2016/794.* (AM 179)

Where there is reason to believe that the deletion of data would prejudice the interests of the data subject, the data shall be ~~blocked~~ *restricted* instead of being deleted. ~~Blocked-Restricted~~ data *shall be supplied processed* solely for the purpose which prevented their deletion. (AM 180, 729)

## Article 53

### Data Processor

Covers AMs 181 (rapp), 731 (RE)

Fall: AM 730 (Left)



1. eu-LISA shall be the processor within the meaning of Article 3, point (12), of Regulation (EU) 2018/1725 for the processing of personal data via the router.

2. Europol shall be the processor for the processing of personal data via EPRIS.

**2a. Member States shall be the processors for the processing of personal data via Eucaris.** (AMs 181, 731)

#### *Article 54*

#### **Security of processing**

Covers AM 182 (rapp), 183 (rapp)

Fall: AM 732 (Left), 733 (Left), 734 (Left), 735 (Left), 736 (Left), 737 (Left), 738 (Left)

1. Europol, eu-LISA and Member States' **competent law enforcement** authorities shall ensure the security of the processing of personal data that takes place pursuant to this Regulation. Europol, eu-LISA and Member States' **competent law enforcement** authorities shall cooperate on security-related tasks. (AM 182)

2. Without prejudice to Article 33 ~~91~~ of Regulation (EU) 2018/1725 and Article 32 of Regulation (EU) 2016/794, eu-LISA and Europol shall take the necessary measures to ensure the security of the router and EPRIS respectively as well as their related communication infrastructure. (AM 183)

3. In particular, eu-LISA and Europol shall adopt the necessary measures concerning the router and EPRIS respectively, including a security plan, a business continuity plan and a disaster recovery plan, in order to:

(a) physically protect data, including by making contingency plans for the protection of critical infrastructure;

(b) deny unauthorised persons access to data-processing equipment and installations;

(c) prevent the unauthorised reading, copying, modification or removal of data media;

(d) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of recorded personal data;

(e) prevent the unauthorised processing of data and any unauthorised copying, modification or deletion of data;

(f) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment;

(g) ensure that persons authorised to access the router and EPRIS have access only to the data covered by their access authorisation, by means of individual user identities and confidential access modes only;

(h) ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment;

(i) ensure that it is possible to verify and establish what data have been processed in the router and EPRIS, when, by whom and for what purpose;

(j) prevent the unauthorised reading, copying, modification or deletion of personal data during the transmission of personal data to or from the router and EPRIS or during the transport of data media, in particular by means of appropriate encryption techniques;

(k) ensure that, in the event of interruption, installed systems can be restored to normal operation;

(l) ensure reliability by making sure that any faults in the functioning of the router and EPRIS are properly reported;

(m) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure compliance with this Regulation and to assess those security measures in the light of new technological developments.

#### *Article 55*

### **Security incidents**

Covers AMs 184 (rapp), 185 (rapp), 740 (RE), 741part (Left), 742 (RE), 743 (Left), 745 (Greens)

Fall: AM 739 (Left), 744 (Left)

1. Any event that has or may have an impact on the security of the router or EPRIS and may cause damage to or loss of data stored in them shall be considered to be a security incident, in particular where unauthorised access to data may have occurred or where the availability, integrity and confidentiality of data has or may have been compromised.

2. Security incidents shall be managed *in close cooperation between the Member States concerned or Europol and eu-LISA, as relevant*, so as to ensure a quick, effective and proper response. (AM 740)

3. Without prejudice to Article 34 of Regulation (EU) 2016/794 *and Article 92 of Regulation (EU) 2018/1725*, Europol shall notify CERT-EU of significant cyber threats, significant vulnerabilities and significant incidents without undue delay and in any event no later than 24 hours after becoming aware of them. Actionable and appropriate technical details of cyber threats, vulnerabilities and incidents that enable proactive detection, incident response or mitigating measures shall be disclosed to CERT-EU without undue delay. (AM 184, 741part)

In the event of a security incident in relation to the central infrastructure of the router *and without prejudice to Articles 34 and 92 of Regulation (EU) 2018/1725*, eu-LISA shall notify CERT-EU of significant cyber threats, significant vulnerabilities and significant incidents without undue delay and in any event no later than 24 hours after becoming aware of them. Actionable and appropriate technical details of cyber threats, vulnerabilities and incidents that enable proactive detection, incident response or mitigating measures shall be disclosed to CERT-EU without undue delay. (AM 185, 742, 743)

4. Information regarding a security incident that has or may have an impact on the operation of the router or on the availability, integrity and confidentiality of the data shall be provided by the Member States and Union agencies concerned to the Member States and Europol without delay and reported in compliance with the incident management plan to be provided by eu-LISA.

5. Information regarding a security incident that has or may have an impact on the operation of EPRIS or on the availability, integrity and confidentiality of the data shall be provided by the Member States and Union agencies concerned to the Member States without delay and reported in compliance with the incident management plan to be provided by Europol.

***5a(new). This Article is without prejudice to the reporting obligations pursuant to Articles 34, 35, 92 and 93 of Regulation (EU) 2018/1725 and Articles 30 and 31 of Directive (EU) 2016/680. (AM 745)***

#### *Article 56*

#### **Self-monitoring**

Covers AM 186 (rapp), 187 (rapp), 188 (rapp), 746 (RE), 747 (RE), 748 (Greens), 751 (RE), 752 (RE)

Fall: AMs 749 (RE), 750 (Left), 753 (RE)

1. Member States ~~and the relevant Union agencies~~ shall ensure that each authority entitled to use Prüm II takes the measures necessary to monitor its compliance with this Regulation and cooperates, where necessary, with the supervisory authority. ***Europol shall take the measures necessary to monitor its compliance with this Regulation and shall cooperate, where necessary, with the European Data Protection Supervisor. (AMs 186, 187, 746)***

2. The data controllers shall ***implement*** ~~take~~ the necessary ***technical and organisational*** measures ***to ensure effective supervision*** and monitor the compliance of data processing pursuant to this Regulation, including through frequent verification of the logs referred to in Articles 20, 40 and 45 ***concerning the admissibility of queries, the lawfulness of data processing and data security and integrity***, and cooperate, where necessary ***and as appropriate***, with the supervisory authorities and with the European Data Protection Supervisor. (AMs 188, 748, 751)

***3. The data controllers and Europol shall be provided with adequate human, financial and technical resources to fulfil their tasks pursuant to this Article. (AM 752)***

#### *Article 57*

#### **Penalties**

COM-Text

Falls: AM 754 (RE)

Member States shall ensure that any misuse of data, processing of data or exchange of data contrary to this Regulation is punishable in accordance with national law. The penalties provided shall be effective, proportionate and dissuasive.

#### *Article 58*

#### **Burden of proof**

*Deleted with the corrigendum*

*Article 58*  
*(Corresponds to Article 59 in voting list)*

**Liability**

COM-Text

Falls: AM 755 (Left)

If any failure of a Member State to comply with its obligations under this Regulation causes damage to the router or EPRIS, that Member State shall be liable for such damage, unless and in so far as eu-LISA, Europol or another Member State bound by this Regulation failed to take reasonable measures to prevent the damage from occurring or to minimise the impact.

*Article 59*  
*(Corresponds to Article 60 in voting list)*

**Audits by the European Data Protection Supervisor**

Covers AMs 761 (RE), 758 (RE), 759 (Left), 760 (Greens)

Fall: AMs 756 (ID), 757 (Left), 762 (Left)

1. The European Data Protection Supervisor shall ensure that an audit of personal data processing operations by eu-LISA and Europol for the purposes of this Regulation is carried out in accordance with relevant international auditing standards at least every four years. A report of that audit shall be sent to the European Parliament, to the Council, to the Commission, to the Member States and to the Union agency concerned. Europol and eu-LISA shall be given an opportunity to make comments before the reports are adopted.

2. Without prejudice to Article 43(3) of Regulation (EU) 2016/794, eu-LISA and Europol shall supply information requested by the European Data Protection Supervisor to it, grant the European Data Protection Supervisor access to all the documents it requests and to their logs referred to in Articles 40 and 45 and allow the European Data Protection Supervisor access to all their premises at any time. ***This paragraph is without prejudice to the powers of the European Data Protection Supervisor pursuant to Article 58 of Regulation (EU) 2018/1725 (AMs 758, 759, 760)***

2a. ***The European Data Protection Supervisor shall be provided with the staff and financial resources necessary ~~corresponding to the needs identified~~ to carry out the audits referred to in paragraph 1. (AM 761)***

*Article 60*  
*(Corresponds to Article 61 in voting list)*

**Cooperation between supervisory authorities and the European Data Protection Supervisor**

Covers AM 189 (rapp) 764 (RE)  
Fall: AM 763 (RE), 765 (Left)

1. The supervisory authorities and the European Data Protection Supervisor shall, each acting within the scope of their respective competences, cooperate actively within the framework of their respective responsibilities ~~and~~ **to** ensure the coordinated supervision of the application of this Regulation, in particular if the European Data Protection Supervisor or a supervisory authority finds major discrepancies between practices of Member States or finds potentially unlawful transfers using the Prüm II communication channels. (AM 189)
2. In the cases referred to in paragraph 1 of this Article, coordinated supervision shall be ensured in accordance with Article 62 of Regulation (EU) 2018/1725.
3. The European Data Protection **Supervisor and the European Data Protection Board** shall send a joint report of its activities under this Article to the European Parliament, to the Council, to the Commission, to Europol and to eu-LISA by 2 years after entry into operation of the router and EPRIS and every two years thereafter. That report shall include a chapter on each Member State prepared by the supervisory authority of the Member State concerned. (AM 764)

#### *Article 61*

*(Corresponds to Article 62 in voting list)*

#### ***Transfer ~~Communication~~ of personal data to third countries and international organisations (AM 190)***

Covers AM 190 (rapp), 191 (rapp), 192 (rapp), 766 (Greens), 767 (RE)  
Fall: AM 768 (Greens)

***1. Any data obtained by a requesting Member State in accordance with this Regulation shall require the consent of the requested Member State in order to be transferred. A requesting Member State shall transfer ~~any~~ personal data it has obtained in accordance with this Regulation to a third country or an international organisation only in accordance with Chapter V of Directive (EU) 2016/680 and where the requested Member State has granted its authorisation prior to the transfer. (AM 191, 766)***

***1a. Europol shall transfer personal ~~any~~ data it has obtained in accordance with this Regulation to a third country or an international organisation only where the conditions laid down in Article 25 of Regulation (EU) 2016/794 are fulfilled and the requested Member State has granted its authorisation prior to the transfer. (AM 192, 767)***

#### *Article 61a*

*(Corresponds to Article 62a in voting list)*

#### ***Relation to other legal acts on data protection***

Covers AM 768 (Greens)

***Any processing of personal data for the purposes of this Regulation shall be carried out in compliance with this Chapter and without prejudice to Directive (EU) 2016/680, Regulation (EU) 2018/1725 and Regulation (EU) 2016/794, as applicable.***

**CA 14 - Chapter 7 - Articles 62 to 65 (Responsibilities)**

*(Corresponds to Articles 63 - 66 in voting list)*

CHAPTER 7  
**RESPONSIBILITIES**

*Article 62*

*(Corresponds to Article 63 in voting list)*

**Responsibilities of Member States**

Covers AMs 193 (rapp), 194 (rapp), 195 (rapp), 196 (rapp), 197 (rapp), 392part (RE), 407part (RE), 439part (RE), 505part (RE), 773 (RE), 774 (RE)

Fall: AMs 769 (Left), 770 (Left), 771 (Left), 772 (Left), 775 (RE), 776 (Left)

1. Each Member State shall be responsible for:

- (a) the connection to the infrastructure of the router;
- (b) the integration of the existing national systems and infrastructures with the router;
- (c) the organisation, management, operation and maintenance of its existing national infrastructure and of its connection to the router;
- (d) the connection to the infrastructure of EPRIS;
- (e) the integration of the existing national systems and infrastructures with EPRIS
- (f) the organisation, management, operation and maintenance of its existing national infrastructure and of its connection to EPRIS;
- (g) the management of, and arrangements for, access by the duly authorised staff of the competent national **law enforcement** authorities to the router in accordance with this Regulation and the creation and regular update of a list of those staff and their profiles; (AM 193)
- (h) the management of, and arrangements for, access by the duly authorised staff of the competent national **law enforcement** authorities to EPRIS in accordance with this Regulation and the creation and regular update of a list of those staff and their profiles; (AM 194)
- (i) the management of, and arrangements for, access by the duly authorised staff of the competent national **law enforcement** authorities to Eucaris in accordance with this Regulation and the creation and regular update of a list of those staff and their profiles; (AM 195)
- (j) the manual confirmation **by qualified staff** of a match as referred to in Article 6(3), Article 7(3), Article 13(2) **and** Article 22(2) ~~and Article 26(2)\*~~; (392part, 407part, 439part, 505part)
- (k) ensuring the availability of the data necessary for the exchange of data in accordance with Article 6, Article 7, Article 13, Article 18, Article 22 and Article 26;
- (l) the exchange of information in accordance with Article 6, Article 7, Article 13, Article 18, Article 22 and Article 26;
- (m) **correcting, updating or** deleting any data received from a requested Member State within **24** hours following the notification from the requested Member State that the personal data submitted was incorrect, **is** no longer up-to-date or was unlawfully transmitted. (AMs 196, 773)

(n) compliance with the *minimum* data quality requirements established in this Regulation. (AM 774)

2. Each Member State shall be responsible for connecting their competent national *law enforcement* authorities to the router, EPRIS and Eucaris. (AM 197)

\* covered by Art.44(4)

#### Article 63

*(Corresponds to Article 64 in voting list)*

#### **Responsibilities of Europol**

Covers AMs 198 (rapp)

Fall: 777 (Left), 778 (Greens)

1. Europol shall be responsible for the management of, and arrangements for the access by its duly authorised staff to the router, EPRIS and Eucaris in accordance with this Regulation.

2. Europol shall also be responsible for the processing of the queries of Europol data by the router. Europol shall adapt its information systems accordingly.

3. Europol shall be responsible for any technical adaptations in Europol infrastructure required for establishing the connection to the router and to Eucaris.

**3a. Without prejudice to Article 26(6c) of Regulation (EU) 2016/794 and Europol's searches pursuant to Article 50(4) of this Regulation, Europol shall not have access to any of the personal data processed through EPRIS.** (AM 198)

4. Europol shall be responsible for the development of EPRIS in cooperation with the Member States. EPRIS shall provide the functionalities laid down in Articles 42 to 46.

Europol shall provide the technical management of EPRIS. Technical management of EPRIS shall consist of all the tasks and technical solutions necessary to keep the EPRIS central infrastructure functioning and providing uninterrupted services to Member States 24 hours a day, 7 days a week in accordance with this Regulation. It shall include the maintenance work and technical developments necessary to ensure that EPRIS functions are at a satisfactory level of technical quality, in particular as regards the response time for interrogation of the national databases in accordance with the technical specifications.

5. Europol shall provide training on the technical use of EPRIS.

6. Europol shall be responsible for the procedures referred to in Articles 49 and 50.

#### Article 64

*(Corresponds to Article 65 in voting list)*

#### **Responsibilities of eu-LISA during the design and development phase of the router**

No AMs were tabled - COM wording

#### Article 65

*(Corresponds to Article 66 in voting list)*

#### **Responsibilities of eu-LISA following the start of operations of the router**

Covers AM 199 (rapp), 605 (Greens), 606 (Left), 607 (S&D)

Fall: AMs 779 (Left), 780 (Left)

1. Following the entry into operations of the router, eu-LISA shall be responsible for the technical management of the central infrastructure of the router, including its maintenance and technological developments. In cooperation with Member States, it shall ensure that the best available technology is used, subject to a cost-benefit analysis. eu-LISA shall also be responsible for the technical management of the necessary communication infrastructure.

Technical management of the router shall consist of all the tasks and technical solutions necessary to keep the router functioning and providing uninterrupted services to Member States and to Europol 24 hours a day, 7 days a week in accordance with this Regulation. It shall include the maintenance work and technical developments necessary to ensure that the router functions at a satisfactory level of technical quality, in particular as regards availability and the response time for submitting requests to the national databases and Europol data in accordance with the technical specifications.

The router shall be developed and managed in such a way as to ensure fast, efficient and controlled access, full and uninterrupted availability of the router, and a response time in line with the operational needs of the competent *law enforcement* authorities of the Member States and Europol. (AM 199)

***1a (new). eu-LISA shall make publicly available information on technology supplied by private parties, including the supplier, for the purposes of its tasks referred to in paragraph 1. (AMs 605, 606, 607)***

2. Without prejudice to Article 17 of the Staff Regulations of Officials of the European Union, laid down in Council Regulation (EEC, Euratom, ECSC) No 259/68, eu-LISA shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality to its staff required to work with data stored in the interoperability components. This obligation shall also apply after such staff leave office or employment or after the termination of their activities.

eu-LISA shall not have access to any of the personal data processed through the router.

3. eu-LISA shall also perform tasks related to providing training on the technical use of the router.

## **CA 15 - Chapter 8 - Articles 66 to 69 (Amendments to other instruments)**

*(Corresponds to Articles 67 - 70 in voting list)*

### **CHAPTER 8 AMENDMENTS TO OTHER EXISTING INSTRUMENTS**

#### *Article 66*

*(Corresponds to Article 67 in voting list)*

#### **Amendments to Decisions 2008/615/JHA and 2008/616/JHA**

Covers

Fall: AMs 779 (Left), 780 (Left)



1. In Decision 2008/615/JHA, Articles 2 to 6 and Sections 2 and 3 of Chapter 2 are replaced with regard to the Member States bound by this Regulation from the date of application of the provisions of this Regulation related to the router as set out in Article 73.

Therefore, Articles 2 to 6 and Sections 2 and 3 of Chapter 2 of Decision 2008/615/JHA are deleted from the date of application of the provisions of this Regulation related to the router as set out in Article 73.

2. In Decision 2008/616/JHA, Chapters 2 to 5 and Articles 18, 20 and 21 are replaced with regard to the Member States bound by this Regulation from the date of application of the provisions of this Regulation related to the router as set out in Article 73.

Therefore, Chapters 2 to 5 and Articles 18, 20 and 21 of Decision 2008/616/JHA are deleted from the date of application of the provisions of this Regulation related to the router as set out in Article 73.

#### Article 67

*(Corresponds to Article 68 in voting list)*

#### **Amendments to Regulation (EU) 2018/1726**

Covers AM 200 (rapp), 201 (rapp)

Fall:

Regulation (EU) 2018/1726 is amended as follows:

(1) the following Article 13a is inserted:

“Article 13a

#### **Tasks related to the router**

In relation to Regulation (EU) .../... of the European Parliament and of the Council\* [*this Regulation*], the Agency shall perform the tasks related to the router conferred on it by that Regulation.

---

\* Regulation (EU) [number] of the European Parliament and of the Council of xy on [officially adopted title] (OJ L ...)”

in Article 17, paragraph 3 is replaced by the following:

‘3. The seat of the Agency shall be Tallinn, Estonia.

The tasks relating to development and operational management referred to in Article 1(4) and (5) and Articles 3 to 8 and Articles 9, 11 and 13a shall be carried out at the technical site in Strasbourg, France.

A backup site capable of ensuring the operation of a large-scale IT system in the event of failure of such a system shall be installed in Sankt Johann im Pongau, Austria.’

*in Article 19(1), the following point (~~eea~~) is added after point (ee):*

*‘(eea) adopt the reports on the state of play of ~~on~~ the development of the router referred to in Article 35 of Regulation (EU) .../... of the European Parliament and of the Council [2021/0410(COD)] pursuant to Article ~~79(2)~~ 78(2) of that Regulation;’ (AM 200)*

***in Article 19(1), point (ff) is ~~points (ff) and (hh)~~ are replaced by the following:***

***‘(ff) adopt the reports on the technical functioning of SIS II pursuant to Article 50(4) of Regulation (EC) No 1987/2006 and Article 66(4) of Decision 2007/533/JHA respectively, of the VIS pursuant to Article 50(3) of Regulation (EC) No 767/2008 and Article 17(3) of Decision 2008/633/JHA, of the EES pursuant to Article 72(4) of Regulation (EU) 2017/2226, ~~and~~ of ETIAS pursuant to Article 92(4) of Regulation (EU) 2018/1240 **and of the router referred to in Article 35 of Regulation (EU) ... [2021/0410(COD)] pursuant to Article 78(5) of that Regulation (EU) ...;*****

(ff) — adopt the reports on the technical functioning of the following:

***‘(i) — SIS II pursuant to Article 60(7) ~~50(4)~~ of Regulation (EU) 2018/1861 of the European Parliament and of the Council ( ~~8~~ ) ~~(EC) No 1987/2006~~ and Article 74(8) ~~66(4)~~ of Regulation (EU) 2018/1862 of the European Parliament and of the Council ( ~~9~~ ) ~~Decision 2007/533/JHA;~~’***

(ii) — VIS pursuant to Article 50(3) of Regulation (EC) No 767/2008 and Article 17(3) of Decision 2008/633/JHA;

(iii) — EES pursuant to Article 72(4) of Regulation (EU) 2017/2226;

(iv) — ETIAS pursuant to Article 92(4) of Regulation (EU) 2018/1240;

(v) — ECRIS TCN and the ECRIS reference implementation pursuant to Article 36(8) of Regulation (EU) 2019/816;

(vi) — the interoperability components pursuant to Article 78(3) of Regulation (EU) 2019/817 and Article 74(3) of Regulation (EU) 2019/818;

(vii) — the e-CODEX system pursuant to Article 16(1) of Regulation (EU) 2022/850;

***(viii) — ~~the router referred to in Article 35 of Regulation (EU) ... [2021/0410(COD)] pursuant to Article 78(5) of that Regulation (EU) ...;~~’***

***in Article 19(1), point (hh) is replaced by the following:***

***‘(hh) adopt formal comments on the European Data Protection Supervisor’s reports on ~~the~~ its audits **carried out** pursuant to Article 56(2) of Regulation (EU) 2018/1861 ~~Article 45(2) of Regulation (EC) No 1987/2006~~, Article 42(2) of Regulation (EC) No 767/2008, Article 31(2) of Regulation (EU) No 603/2013, Article 56(2) of Regulation (EU) 2017/2226, Article 67 of Regulation (EU) 2018/1240, Article 29(2) of Regulation (EU) 2019/816, ~~and~~ Article 52 of Regulations (EU) 2019/817 and (EU) 2019/818 **and Article 60(1) 59(1) of Regulation (EU) ... [2021/0410(COD)]** and ensure appropriate follow-up of those audits;’*** (AM 201)

*Article 68*  
*(Corresponds to Article 69 in voting list)*  
**Amendments to Regulation (EU) 2019/817**

No AMs were tabled - COM wording

*Article 69*  
*(Corresponds to Article 70 in voting list)*  
**Amendments to Regulation (EU) 2019/818**

Covers AM 202 (rapp), 203 (rapp)

Fall:

Regulation (EU) 2019/818 is amended as follows:

(1) in Article 6(2), the following point (d) is added:

“(d) a secure communication infrastructure between the ESP and the router established by Regulation (EU) .../... of the European Parliament and of the Council\* [*this Regulation*].

\* Regulation (EU) [number] of the European Parliament and of the Council of xy on [officially adopted title] (OJ L ...)”

(2) In Article 39, paragraphs 1 and 2 are replaced by the following:

“1. A central repository for reporting and statistics (CRRS) is established for the purposes of supporting the objectives of the SIS, Eurodac, ECRIS-TCN, in accordance with the respective legal instruments governing those systems, and to provide cross-system statistical data and analytical reporting for policy, operational and data quality purposes. The CRRS shall also support the objectives of **Regulation (EU) .../... of the European Parliament and of the Council\* [2021/0410(COD)]..**” (AM 202)

“2. eu-LISA shall establish, implement and host in its technical sites the CRRS containing the data and statistics referred to in Article 74 of Regulation (EU) 2018/1862 and Article 32 of Regulation (EU) 2019/816 logically separated by EU information system. eu-LISA shall also collect the data and statistics from the router referred to in Article ~~64(1)~~ **71(1)** of Regulation (EU) .../... \* [*this Regulation* ]. Access to the CRRS shall be granted by means of controlled, secured access and specific user profiles, solely for the purpose of reporting and statistics, to the authorities referred to in Article 74 of Regulation (EU) 2018/1862, Article 32 of Regulation (EU) 2019/816 and Article 64(1) of Regulation (EU) .../... \* [*this Regulation* ].” (AM 203)

**CA 16 - Chapter 9 - Articles 70 to 79 (Final Provisions)**

*(Corresponds to Articles 71 - 80 in voting list)*

CHAPTER 9  
FINAL PROVISIONS

Article 70

*(Corresponds to Article 71 in voting list)*

**Reporting and statistics**

Covers 204 (rapp), 205 (rapp), 206 (rapp), 207 (rapp), 784 (Left), 786 (Greens), 208 (rapp), 209 (rapp), 210 (rapp), 211 (rapp), 212 (rapp), 213 (rapp), 214 (rapp),  
Fall: 782 (Left), 783 (Left), 784 (Left), 785 (Left), 787 (Left), 788 (Left), 789 (Left)

1. The duly authorised staff of the competent **law enforcement** authorities of Member States, the Commission, Europol and eu-LISA shall have access to ~~consult~~ the following data related to the router, **as relevant**, solely for the purposes of reporting and statistics: (AM 204)

(a) number of queries per Member State and by Europol, **per category of data**; (AM 205)

~~(b) number of queries per category of data;~~ (AM 206)

(c) number of queries to each of the connected databases;

(d) number of matches against each Member State's database per category of data;

(e) number of matches against Europol data per category of data;

(f) number of confirmed matches where there were exchanges of core data; ~~and~~ (AM 207)

**(fa) number of confirmed matches where there were no exchanges of core data;** (AM 208)

**(fb) number of unconfirmed matches and** (AM 784, 786)

(g) number of queries to the Common Identity Repository via the router.

**The data shall be aggregated.** It shall not be possible to identify individuals from the data. (AM 209)

2. The duly authorised staff of the competent **law enforcement** authorities of Member States, Europol and the Commission shall have access to consult the following data related to Eucaris, solely for the purposes of reporting and statistics: (AM 210)

(a) number of queries per Member State and by Europol;

(b) number of queries to each of the connected databases; and

(c) number of matches against each Member State's database.

**The data shall be aggregated.** It shall not be possible to identify individuals from the data. (AM 211)

3. The duly authorised staff of the competent **law enforcement** authorities of Member States, the Commission and Europol shall have access to consult the following data related to EPRIS, solely for the purposes of reporting and statistics: (AM 212)

(a) number of queries per Member State and by Europol;

(b) number of queries to each of the connected indexes; and

(c) number of matches against each Member State's database.

It shall not be possible to identify individuals from the data.

4. eu-LISA shall store the data referred to in ~~those paragraphs~~. **paragraph 1 of this Article in the central repository for reporting and statistics established by pursuant to Article 39 of Regulation (EU) 2019/818.** (AM 213)

The data shall allow the **competent law enforcement** authorities referred to in ~~paragraph 1 of the Member States, Europol, eu-LISA and the Commission~~ to obtain customisable reports and statistics to enhance the efficiency of law enforcement cooperation. (AM 214)

Article 71

*(Corresponds to Article 72 in voting list)*

**Costs**

Covers

Fall: AMs 790 (Left), 791 (Greens), 792 (ECR), 793 (Left), 794 (S&D), 795 (Left)

1. Costs incurred in connection with the establishment and operation of the router and EPRIS shall be borne by the general budget of the Union.
2. Costs incurred in connection with the integration of the existing national infrastructures and their connections to the router and EPRIS as well as costs incurred in connection with the establishment of national facial images databases and police national indexes for the prevention, detection and investigation of criminal offences shall be borne by the general budget of the Union.

The following costs shall be excluded:

- (a) Member States' project management office (meetings, missions, offices);
  - (b) hosting of national IT systems (space, implementation, electricity, cooling);
  - (c) operation of national IT systems (operators and support contracts);
  - (d) design, development, implementation, operation and maintenance of national communication networks.
3. Each Member State shall bear the costs arising from the administration, use and maintenance of the Eucaris software application referred to in Article 19(1).
  4. Each Member State shall bear the costs arising from the administration, use and maintenance of their connections to the router and EPRIS.

Article 72

*(Corresponds to Article 73 in voting list)*

**Notifications**

Covers AMs 215 (rapp), 216 (rapp), 217 (rapp), 218 (rapp), 219 (rapp), 220 (rapp)

Fall:

1. Member States shall notify eu-LISA of the **competent law enforcement** authorities referred to in Article 36, which may use or have access to the router. (AM 215)
2. eu-LISA shall notify the Commission of the successful completion of the tests referred to in Article 73(1), point (b).
  - 2a. Each Member State shall notify the other Member States, the Commission, eu-LISA and Europol of the content of ~~their~~ its national DNA databases to which Articles 5, 6 and 7 apply.** (AM 216)
  - 2b. Each Member States shall inform the other Member States, the Commission, eu-LISA and Europol of the content of ~~their~~its national dactyloscopic databases to which Articles 12 and 13 apply.** (AM 217)
  - 2c. Each Member States shall inform the other Member States, the Commission, eu-LISA and Europol of the content of ~~their~~its national facial images databases to which Articles 21 and 22 apply.** (AM 218)
  - 2d. Member States participating in automated exchanges of police records pursuant to Articles 25 and 26 shall notify the other Member States, the Commission and Europol of the content of ~~their~~its national police records indexes, the national databases used for the establishment of those indexes and the conditions for automated searches.** (AM 219)

3. Member States shall notify the Commission, Europol and eu-LISA of ~~the~~ ***their*** national contact ~~points~~ ***point designated pursuant to Article 29. The Commission shall compile a list of the national contact points of which it has been notified and make it available to all Member States.*** (AM 220)

Article 73

*(Corresponds to Article 74 in voting list)*

**Start of operations**

Covers AMs 221 (rapp), 222 (rapp), 223 (rapp), 224 (rapp), 797 (RE), 225 (rapp), 226 (rapp), 227 (rapp), 228 (rapp), 229 (rapp)

Fall: AMs 796 (Left), 798 (Left), 799 (Left), 800 (Left)

1. The Commission shall determine the date from which the Member States and ~~the Union agencies~~ ***Europol*** may start using ***the*** router by means of an implementing act once the following conditions have been met: (AM 221)

(a) the measures referred to in Articles ***5(2c), 10(3), 15(4), 19(3), 23a(3), 30 and 37(6)*** have been adopted;

(b) eu-LISA has declared the successful completion of a comprehensive test of the router, which it has conducted in cooperation with the Member States' ***competent law enforcement*** authorities and Europol. (AM 222)

In that implementing act the Commission shall also determine the date from which the Member States and ~~the Union agencies~~ ***Europol shall must*** start using ***the*** router. That date shall be one year after the date determined in accordance with the first subparagraph. (AM 223)

The Commission may postpone the date from which the Member States and the Union agencies ~~must~~ ***are to*** start using ***the*** router by one year ~~six months~~ at most where an assessment of the implementation of the router has shown that such a postponement is necessary. ~~That implementing act shall be adopted in accordance with the procedure referred to in Article 75(2).~~ (AM 224, 797)

2. The Commission shall determine the date from which the Member States and ~~the Union agencies~~ ***Europol*** are to start using EPRIS by means of an implementing act once the following conditions have been met: (AM 225)

(a) the measures referred to in Article 44(7) have been adopted;

(b) Europol has declared the successful completion of a comprehensive test of EPRIS, which it has conducted in cooperation with the Member States' ***competent law enforcement*** authorities. (AM 226)

3. The Commission shall determine the date from which Europol is to make available third country-sourced biometric data to Member States in accordance with Article 49 by means of an implementing act once the following conditions have been met:

(a) the router is in operation;

(b) Europol has declared the successful completion of a comprehensive test of the connection, which it has conducted in cooperation with the Member States' ***competent law enforcement*** authorities' and eu-LISA. (AM 227)

4. The Commission shall determine the date from which Europol is to have access to data stored in Member States' databases in accordance with Article 50 by means of an implementing act once the following conditions have been met:

(a) the router is in operation;

(b) Europol has declared the successful completion of a comprehensive test of the connection, which it has conducted in cooperation with the Member States' *competent law enforcement* authorities and eu-LISA. (AM 228)

**4a. The implementing acts referred to in this Article shall be adopted in accordance with the procedure referred to in Article 75(2).** (AM 229)

Article 74

*(Corresponds to Article 75 in voting list)*

**Transitional provisions and derogations**

No AMs were tabled - COM wording

Article 75

*(Corresponds to Article 76 in voting list)*

**Committee procedure**

No AMs were tabled - COM wording

Article 76

*(Corresponds to Article 77 in voting list)*

**Advisory group**

No AMs were tabled - COM wording

Article 77

*(Corresponds to Article 78 in voting list)*

**Practical handbook**

Covers AMs 801 (RE), 802 (Greens), 803 (S&D), 804 (Left), 805 (RE)

Fall:

The Commission shall, in close cooperation with the Member States, Europol, ~~and~~ eu-LISA, **the European Data Protection Board, the European Data Protection Supervisor and the European Union Agency for Fundamental Rights Agency** make available a practical handbook for the implementation and management of this Regulation. The practical handbook shall provide technical and operational guidelines, recommendations and best practices. The Commission shall adopt the practical handbook in the form of a recommendation *by ... [six months after entry into force of this Regulation]. The Commission shall regularly and where necessary update the practical handbook.* (AMs 801, 802, 803, 804, 805)

Article 78

*(Corresponds to Article 79 in voting list)*

**Monitoring and evaluation**

Covers AMs 230 (rapp), 231 (rapp), 232 (rapp), 809 (Greens), 810 (RE), 811part (Left), 233 (rapp), 813 (RE), 234 (rapp), 235 (rapp), 236 (rapp), 818 (RE)

Fall: 806 (Left), 807 (Left), 808 (Left), 812 (Left), 814 (Left), 815 (S&D), ~~816 (RE)~~, 817 (S&D), 819 (S&D), 820 (S&D), 821 (Left), 822 (S&D), 823 (Left)

1. eu-LISA and Europol shall, respectively, ensure that procedures are in place to monitor the development of the router and of EPRIS in light of objectives relating to planning and costs and to monitor ~~the~~ **their** functioning ~~of the router and of EPRIS~~ in light of objectives relating to the technical output, cost-effectiveness, security and quality of service. (AM 230)
2. By [*one year after entry into force of this Regulation*] and every year thereafter during the development phase of the router, eu-LISA shall ~~respectively~~ submit a report to the European Parliament and to the Council on the state of play of the development of the router. That report shall contain detailed information about the costs incurred and information as to any risks which may impact the overall costs to be borne by the general budget of the Union in accordance with Article 71. (AM 231)  
Once the development of the router is finalised, eu-LISA shall submit a report to the European Parliament and to the Council explaining in detail how the objectives, in particular relating to planning and costs, were achieved as well as justifying any divergences.
3. By [*one year after entry into force of this Regulation*] and every year thereafter during the development phase of EPRIS, Europol shall submit a report to the European Parliament and to the Council ~~on the state of preparation for the implementation of this Regulation and~~ on the state of play of the development of EPRIS including detailed information about the costs incurred and information as to any risks which may impact the overall costs to be borne by the general budget of the Union in accordance with Article 71. (AM 232)  
Once the development of EPRIS is finalised, Europol shall submit a report to the European Parliament and to the Council explaining in detail how the objectives, in particular relating to planning and costs, were achieved as well as justifying any divergences.
4. For the purposes of technical maintenance, eu-LISA and Europol shall have access to the necessary information relating to the data processing operations performed in the router and EPRIS respectively. ***This shall exclude access to any personal data.*** (AM 809, 810, 811part)
5. Two years after the start of operations of the router and every two years thereafter, eu-LISA shall submit to the European Parliament, to the Council and to the Commission a report on the technical functioning of the router, including the security thereof.
6. Two years after the start of operations of EPRIS and every two years thereafter, Europol shall submit to the European Parliament, to the Council and to the Commission a report on the technical functioning of EPRIS, including the security thereof.
7. ~~Three~~ **Two** years after the start of operations of the router and EPRIS as referred to in Article 73 and every four years thereafter, the Commission shall produce an overall evaluation of Prüm II, including: (AM 233, 813)
  - (a) an assessment of the application of this Regulation ***for each Member State and Europol;*** (AM 813)
  - (b) an examination of the results achieved against the objectives of this Regulation and its impact on fundamental rights;
  - (c) the impact, effectiveness and efficiency of Prüm II performance and its working practices in light of its objectives, mandate and tasks;
  - (d) an assessment of the security of Prüm II.***The Commission shall pay due attention to any Member State subject to a procedure referred to in Article 7 of the Treaty on the European Union (AM 818)***  
The Commission shall transmit the evaluation report to the European Parliament, the Council, the European Data Protection Supervisor and the European Agency for Fundamental Rights.



8. The Member States and Europol shall provide eu-LISA and the Commission with the information necessary to draft the reports referred to in paragraphs 2 and 5. This information shall not jeopardise working methods or include information that reveals sources, staff members or investigations of the ~~designated~~ **competent law enforcement** authorities. (AM 234)

9. The Member States shall provide Europol and the Commission with the information necessary to draft the reports referred to in paragraphs 3 and 6. This information shall not jeopardise working methods or include information that reveals sources, staff members or investigations of the ~~designated~~ **competent law enforcement** authorities. (AM 235)

10. **Without prejudice to confidentiality requirements and the protection of ongoing investigations**, Member States, eu-LISA and Europol shall provide the Commission with the information necessary to produce the evaluations referred to in paragraph 7. Member States shall also provide the Commission with the number of confirmed matches against each Member State's database per category of data. (AM 236)

#### Article 79

*(Corresponds to Article 80 in voting list)*

#### **Entry into force and applicability**

No AMs were tabled - COM wording

### **CA 17 - Title & Citations**

Covers: AM 1 (rapp), 2 (rapp), 239 (RE), 240 (RE)

Fall: AMs 237 (S&D), 238 (RE)

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,  
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2), Article 87(2), point (a), and Article 88(2) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee<sup>1</sup>, (AM 1)

~~Having regard to the opinion of the Committee of the Regions<sup>29</sup>~~ (AM 2, AM 239)

**Having regard to the opinion of the European Data Protection Supervisor<sup>1a</sup>** (AM 240)

Acting in accordance with the ordinary legislative procedure,

<sup>1</sup> OJ C 323, 26.8.2022, p. 69

<sup>1a</sup> *EDPS Opinion on the Proposal for a Regulation on automated data exchange for police cooperation, of 2 March 2022*

## CA 18 - Recitals

Covers: AMs 241 (RE), 242 (RE), 3 (rapp), 244 (RE), 245part (S&D), 4 (rapp), 5 (rapp), 249part (S&D), 250part (S&D), 6 (rapp), 253 (Left), 254 (RE), 302 (S&D), 255 (RE), 7 (rapp), 257part (S&D), 23 (rapp), 8 (rapp), 263 (RE), 264 (Left), 9 (rapp), 265 (S&D), 10 (rapp), 267 (RE), 272 (RE), 12 (rapp), 267 (RE), 279 (S&D), 13 (rapp), 280 (RE), 14 (rapp), 283 (RE), 284part (S&D), 15 (rapp), 286 (S&D), 287 (RE), 16 (rapp), 17 (rapp), 293 (S&D), 18 (rapp), 294 (RE), 295 (Greens), 296part (S&D), 19 (rapp), 297 (S&D), 298 (Left), 303 (S&D), 304part (S&D), 20 (rapp), 21 (rapp), 305 (RE), 307 (RE), 308 (RE), 309 (RE), 24 (rapp), 311 (RE), 23 (rapp), 816 (RE), 818 (RE)

Fall: AMs 243 (Left), 246 (ID), 247 (Left), 248 (Left), 251 (ECR), 252 (Greens), 256 (Left), 258 (Greens), 259 (ID), 260 (S&D), 261 (ECR), 262 (S&D), 11 (rapp), 266 (Left), 268 (S&D), 269 (ECR), 270 (Greens), 271 (S&D), 273 (Left), 274 (S&D), 275 (S&D), 276 (ECR), 277 (Greens), 278 (Left), 281 (Greens), 282 (Left), 285 (Left), 288 (Left), 289 (Greens), 290 (S&D), 291 (S&D), 292 (Left), 299 (Greens), 300 (S&D), 301 (Left), 306 (S&D), 310 (Left)

(1) The Union has set itself the objective of offering its citizens an area of freedom, security and justice without internal frontiers, in which the free movement of persons is ensured. That objective should be achieved by means of, among others, appropriate measures to prevent and combat crime **and other threats to public security**, including organised crime and terrorism **in line with the EU Security Union Strategy**. (AM 241)

(2) That objective requires that law enforcement authorities exchange data, in an efficient and timely manner, in order to effectively ~~fight crime~~ **prevent, detect and investigate criminal offences**. (AM 242)

(3) The objective of this Regulation is therefore to improve, streamline and facilitate the exchange of criminal information **and vehicle registration data** between Member States' **competent** law enforcement authorities **for the purposes of preventing, detecting and investigating criminal offences**, but also with the European Union Agency for Law Enforcement Cooperation established by Regulation (EU) No 2016/794 of the European Parliament and of the Council<sup>30</sup> (Europol) ~~as the Union criminal information hub~~, **in full compliance with fundamental rights and data protection rules**. (AMs 3, 244, 245part)

(4) Council Decisions 2008/615/JHA31 and 2008/616/JHA32 laying down rules for the exchange of information between authorities responsible for the prevention and investigation of criminal offences by providing for the automated transfer of DNA profiles, dactyloscopic data and certain vehicle registration data, have proven important for tackling terrorism and cross-border crime, **thereby protecting the internal security of the Union and the safety of its citizens**. (AM 4)

(5) This Regulation should lay down the conditions and procedures for the automated ~~transfer~~ **search and exchange** of DNA profiles, dactyloscopic data, **certain** vehicle registration data, facial images and police records, **in the context of a criminal investigation**. This should be without prejudice to the processing of any of these data in the Schengen Information System (SIS) or the exchange of supplementary information related to them via the SIRENE bureaux

*pursuant to Regulation (EU) 2018/1862 of the European Parliament and of the Council<sup>1a</sup> or to the rights of individuals whose data is processed therein. (AM 5, 249part, 250part)*

*<sup>1a</sup> Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (OJ L 312, 7.12.2018, p. 56).*

(6) ~~The~~ **Any** processing of personal data and the exchange of personal data for the purposes of this Regulation *should be carried out in compliance with Chapter 6 of this Regulation and, as applicable, Directive (EU) 2016/680 of the European Parliament and the Council<sup>1a</sup>, Regulation (EU) 2018/1725 of the European Parliament and the Council<sup>1b</sup> and Regulation (EU) 2016/794. The processing and exchange of personal data for the purposes of this Regulation* should not result in discrimination against persons on any grounds. It should fully respect human dignity and integrity and other fundamental rights, including the right to respect for one's private life and to the protection of personal data, in accordance with the Charter of Fundamental Rights of the European Union. (AM 6, 253, 254, 302)

*<sup>1a</sup> Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).*

*<sup>1b</sup> Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).*

(7) By providing for the automated search or comparison of DNA profiles, dactyloscopic data, *certain* vehicle registration data, facial images and police records, the purpose of this Regulation is also to allow for the search of missing persons and *the identification of unidentified* human remains *in the context of a criminal investigation*. This should be without prejudice to the entry of SIS alerts on missing persons and the exchange of supplementary information on such alerts under Regulation (EU) 2018/1862 of the European Parliament and of the Council.<sup>33</sup> (AM 7, 257part)

*(7a) Since the objectives of this Regulation, namely to step up cross-border police cooperation and to allow Member States' competent law enforcement authorities to search for missing persons and identify unidentified human remains, cannot be sufficiently achieved by the Member States but can rather, by reason of the scale and effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In*

*accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.* (AM 23)

(8) The Directive (EU) .../... [*on information exchange between law enforcement authorities of Member States*] provides a coherent Union legal framework to ensure that **competent** law enforcement authorities have equivalent access to information held by other Member States when they need it to fight crime and terrorism. To enhance information exchange, that Directive formalises and clarifies the **rules and** procedures for information sharing between Member States **States' competent law enforcement authorities**, in particular for investigative purposes, including the role of the 'Single Point of Contact' for such exchanges, and making full use of Europol's information exchange channel SIENA. Any exchange of information **between competent law enforcement authorities** beyond what is provided for in this Regulation ~~should be~~ *is* regulated by Directive (EU) .../... [*on information exchange between law enforcement authorities of Member States*]. (AM 8, 263)

*(8a) Member States should designate one or more national contact points for the exchanges under this Regulation, depending on their national organisation structures. However, in order to streamline the exchanges under this Regulation, Member States should seek to have only one national contact point, where possible.*

(9) For the automated searching of **certain** vehicle registration data, Member States **and Europol** should use the European Vehicle and Driving Licence Information System (Eucaris) set up by the Treaty concerning a European Vehicle and Driving Licence Information System (EUCARIS) designed for this purpose. ~~Eucaris should connect~~ **which connects** all participating Member States in a network. There is no central component needed for the communication to be established as each Member State communicates directly to the other connected Member States, **and Europol communicates directly to the connected databases. The automated search and exchange of driving licence data is excluded from the scope of this Regulation.** (AM 9, 265)

(10) The identification of a criminal is essential for a successful criminal investigation and prosecution. The automated searching of facial images of ~~suspects and convicted criminals~~ **persons convicted or suspected of having committed a criminal offence collected in accordance with national law** should provide for additional information for successfully identifying criminals and fighting crime. **Given the sensitivity of the data concerned, it should only be possible to conduct automated searches for the purpose of preventing, detecting or investigating a serious criminal offence. In addition, a human review of the list of candidates by two forensic experts should be ensured in order to determine the existence of a confirmed match.** (AMs 10, 267)

(11) The automated search or comparison of biometric data (~~DNA profiles, dactyloscopic data and facial images~~) between authorities responsible for the prevention, detection and investigation of criminal offences under this Regulation should only concern data contained in **Union's or Member States' databases** established for the prevention, detection and investigation of criminal offences, **in accordance with this Regulation.** (AM 272)

(12) Participation in the **automated search and** exchange of police records **indexes** should remain voluntary. Where Member States decide to participate, in the spirit of reciprocity, it should not be possible for them to query other Member States' databases if they do not make their own data available for queries by other Member States. **Given the sensitivity of the data**

*concerned, exchanges of police record indexes under this Regulation should only concern data of persons convicted or suspected of having committed a serious criminal offence. In addition, it should only be possible to conduct automated searches for the purpose of investigating a serious criminal offence* (AM 12, 267, 279)

*(12a) Member States should ensure that data included in their national police record indexes are accurate, complete and up to date and should implement safeguards, in particular pseudonymisation, to protect queried personal data.* (AM 13)

*(12b) The exchange of police record indexes under this Regulation does not concern criminal records exchanged through the existing European Criminal Records Information System (ECRIS) framework.* (AM 280)

(13) In recent years, Europol has received a large amount of biometric data of ~~suspected and suspects and persons~~ convicted ~~terrorists and criminals~~ *for terrorism and criminal offences* from several ~~third countries~~ *third-country authorities in accordance with Regulation (EU) 2016/794, in particular battlefield information from war zones. It has often not been possible to make full use of such data because they are not always available to the competent law enforcement authorities of the Member States.* Including third country-sourced data stored at Europol in the Prüm framework and thus making this data available to *competent* law enforcement authorities *in line with the Agency's role as the Union central criminal information hub* is necessary for better prevention and investigation of *serious* criminal offences. It also contributes to building synergies between different law enforcement tools, *and ensures that data is used in the most efficient manner.* (AMs 14, 283, 284)

(14) Europol should be able to search Member States' databases under the Prüm framework with data received from ~~third countries~~ *third-country authorities, in full respect of the rules and conditions provided for in Regulation (EU) 2016/794*, in order to establish cross-border links between criminal cases *in respect of which Europol is competent*. Being able to use Prüm data, next to other databases available to Europol, should ~~allow establishing~~ *enable a* more complete and informed analysis *to be carried out on the criminal investigations and should allow thereby allowing* Europol to provide better support to Member States' *competent* law enforcement authorities *when conducting criminal investigations*. In case of a *confirmed* match between data used for the search and data held in Member States' databases, Member States may supply Europol with the information necessary for it to fulfil its tasks. (AMs 15, 286, 287)

(15) Decisions 2008/615/JHA and 2008/616/JHA provide for a network of bilateral connections between the national databases of Member States. As a consequence of this technical architecture, each Member State ~~should~~ *had to* establish at least 26 connections, that means a connection with each Member State *participating in the automated exchanges*, per data category. The router and the European Police Records Index System (EPRIS) established by this Regulation ~~should~~ *will* simplify the technical architecture of the Prüm framework and serve as connecting points between all Member States. The router should require a single connection per Member State in relation to biometric data and EPRIS should require a single connection per *participating* Member State in relation to police records. (AM 16)

(16) The router should be connected to the European Search Portal established by Article 6 of Regulation (EU) 2019/817 of the European Parliament and of the Council and Article 6 of Regulation (EU) 2019/818 of the European Parliament and of the Council to allow Member

States' *competent law enforcement* authorities and Europol to launch queries to national databases under this Regulation simultaneously to queries to the Common Identity Repository established by Article 17 of Regulation (EU) 2019/817 and Article 17 of Regulation (EU) 2019/818 for law enforcement purposes *in accordance with Article 22 of Regulation (EU) 2019/817 and Article 22 of Regulation (EU) 2019/818. Those two Regulations should therefore be amended accordingly. Moreover, Regulation (EU) 2019/818 should be amended with a view to enabling the storage of reports and statistics of the router in the Common Repository for Reporting and Statistics.* (AM 17, 293)

(17) In case of a match between the data used for the search or comparison and data held in the national database of the requested Member State(s), and upon *manual* confirmation of this match by *qualified staff* of the requesting Member State, the requested Member State should return a limited set of core data, *to the extent that they are available*, via the router within 24 hours. *Where the requested Member State needs to obtain a judicial authorisation prior to the transmission of the core data, the 24-hour deadline should not apply and, instead, the Member State should ensure that the core data are returned within 72 hours.* The deadline ~~would~~ *will* ensure fast communication exchange between Member States' *competent law enforcement* authorities. Member States should retain control over the release of this limited set of core data. *In exceptional circumstances, it might be objectively justified for Member States to refuse sharing the set of core data. Such refusal and its justification should be provided promptly to the requesting Member State within the time limits established under this Regulation.* A certain degree of *H*uman intervention should be maintained at key points in the process, including for *the decision to launch a query, to confirm a match, for the decision to launch a request to receive core data following a confirmed match, and* the decision to release personal data to the requesting Member State, in order to ensure that there would be no automated exchange of core data. (AM 18, 294, 295, 296part)

~~(18) Any exchange between Member States' authorities or with Europol at any stage of one of the processes described under this Regulation, which is not explicitly described in this Regulation, should take place via SIENA to ensure that a common, secure and reliable channel of communication is used by all Member States.~~ (AM 19, 297, 298)

(19) The universal message format (UMF) standard should be used in the development of the router and EPRIS. Any automated exchange of data in accordance with this Regulation should use the UMF standard. Member States' *competent law enforcement* authorities and Europol are encouraged to use the UMF standard also in relation to any further exchange of data between them in the context of the Prüm II framework. The UMF standard should serve as a standard for structured, cross-border information exchange between information systems, authorities or organisations in the field of Justice and Home Affairs. (AM 20)

(20) Only non-classified information should be exchanged via the Prüm II framework.

(21) Certain aspects of the Prüm II framework cannot be covered exhaustively by this Regulation given their technical, highly detailed and frequently changing nature. Those aspects include, for example, technical arrangements and specifications for automated searching procedures, the standards for data exchange, *including minimum quality standards*, and the data elements to be exchanged. In order to ensure uniform conditions for the implementation of this Regulation implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council. (AM 21, 305)

***(21a) Data quality in the context of automated comparison is an essential prerequisite to ensure the efficiency of this Regulation and reduce the risk of false matches. Adequate standards should be determined at EU level by means of implementing acts for data exchanged in the framework of this Regulation. (AM 307)***

***(21b) Given the scale and sensitivity of the personal data exchanged for the purposes of this Regulation, and the existence of different national rules for storing information on individuals in national databases, it is important to ensure that the databases used for the automated searching of DNA profiles, dactyloscopic data, facial images, police records and certain vehicle registration data are established in accordance with national law and, as applicable, Directive (EU) 2016/680 of the European Parliament and the Council, Regulation (EU) 2018/1725 of the European Parliament and the Council and Regulation (EU) 2016/794. Therefore, prior to connecting their national databases to the router, EPRIS or Eucaris, Member States should conduct a data protection impact assessment as referred to in Article 27 of Directive (EU) 2016/680 and consult the supervisory authority as referred to in Article 28 of that Directive, in order to ensure that data in the national databases has been stored in accordance with the applicable legislation. (AM 264, 255)***

***(21c) Member States and Europol should ensure that data exchanged in the framework of this Regulation are accurate and up-to-date. In accordance with the principles of data protection, Member States and Europol should make sure that any data transmitted that is found to be incorrect, inaccurate or outdated is corrected or deleted, as appropriate, and any correction or deletion is communicated to all recipients without delay. (AM 308)***

***(21d) Strong monitoring of the implementation of this Regulation is of utmost importance. In particular, compliance with rules for processing personal data should be subject to effective safeguards, and regular monitoring and audits by data controllers, supervisory authorities and the European Data Protection Supervisor should be ensured. Provisions allowing for a regular checking of the admissibility of queries and the lawfulness of data processing should also be in place. Member States and Europol should ensure adequate human, technical and financial resources for these purposes. (AM 309).***

***(21e) Supervisory authorities and the European Data Protection Supervisor should ensure coordinated supervision of the application of this Regulation within the framework of their responsibilities, in particular where they find major discrepancies between Member State's practices, find potentially unlawful transfers or potential politically-motivated requests. (AM 763)***

***(21f) When implementing this Regulation, Member States and Europol should take note of the developing case law from the European Court of Justice in relation to the use of biometric databases (AM 303)***

***(21g) Member States and third countries who are permitted access to the PRUM II framework should be full members of the Council of Europe with full rights of representation therein, and signatories of the European Convention on Human Rights and its Court. (AM 304)***

***(21h) Two years following the start of operations of the router and EPRIS, and every four years thereafter, the European Commission should produce an evaluation report that includes an assessment of the application of this Regulation by the Member States and***



*Europol, in particular of their compliance with the relevant data protection safeguards and paying due attention to any Member State subject to a procedure referred to in Article 7 of the Treaty of the European Union. The report should also include an examination of the results achieved against the objectives of this Regulation and its impact on fundamental rights, while also evaluating its impact, performance, effectiveness, efficiency, security and working practices.* (AM 816, 818)

(22) As this Regulation provides for the establishment of the new Prüm framework, relevant provisions of Decisions 2008/615/JHA and 2008/616/JHA should be deleted. Those Decisions should therefore be amended accordingly.

(23) As the router should be developed and managed by the European Union Agency for the Operational Management of Large-Scale Information Systems in the Area of Freedom, Security and Justice established by Regulation (EU) 2018/1726 of the European Parliament and of the Council (eu-LISA), it is ~~therefore~~ necessary to amend Regulation (EU) 2018/1726 by adding that to the tasks of eu-LISA. ~~In order to allow for the router to be connected to the European Search Portal to carry out simultaneous searches of the router and the Common Identity Repository it is therefore necessary to amend Regulation (EU) 2019/817. In order to allow for the router to be connected to the European Search Portal to carry out simultaneous searches of the router and the Common Identity Repository and in order to store reports and statistics of the router on the Common Repository for Reporting and Statistics it is therefore necessary to amend Regulation (EU) 2019/818. Those Regulations should therefore be amended accordingly.~~ (AM 22)

(24) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(25) [In accordance with Article 3 of the Protocol (No 21) on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union, Ireland has notified its wish to take part in the adoption and application of this Regulation.] OR [In accordance with Articles 1 and 2 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, and without prejudice to Article 4 of that Protocol, Ireland is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.]

(26) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council and delivered an opinion on ~~[XX]~~ **2 March 2022**<sup>1x</sup>. (AM 24, 311)

<sup>1x</sup>*OJ C 225, 9.6.2022, p. 6*