Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA

REGULATION (EU) 2019/817 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 20 May 2019

on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA

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 74 and Article 77(2)(a), (b), (d) and (e) 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[(1)],

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure[(2)],

Whereas:

(1) In its Communication of 6 April 2016 entitled Stronger and Smarter Information Systems for Borders and Security, the Commission underlined the need to improve the Union's data management architecture for border management and security. The Communication initiated a process towards achieving interoperability between EU information systems for security, border and migration management, with the aim to address the structural shortcomings related to those systems that impede the work of national authorities and to ensure that border guards, customs authorities, police officers and judicial authorities have the necessary information at their disposal.

(2) In its Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area of 6 June 2016, the Council identified various legal, technical and operational challenges in the interoperability of EU information systems and called for the pursuit of solutions.

(3) In its Resolution of 6 July 2016 on the strategic priorities for the Commission Work Programme 2017[(3)], the European Parliament called for proposals to improve and

Changes to legislation: *There are currently no known outstanding effects for the Regulation (EU) 2019/817 of the European Parliament and of the Council. (See end of Document for details)*

develop existing EU information systems, address information gaps and move towards their interoperability, as well as proposals for compulsory information sharing at EU level, accompanied by the necessary data protection safeguards.

(4) In its conclusions of 15 December 2016 the European Council called for work to continue on delivering interoperability of EU information systems and databases.

(5) In its final report of 11 May 2017, the high-level expert group on information systems and interoperability concluded that it was necessary and technically feasible to work towards practical solutions for interoperability and that interoperability could, in principle, both deliver operational gains and be established in compliance with data protection requirements.

(6) In its Communication of 16 May 2017 entitled Seventh progress report towards an effective and genuine Security Union, the Commission set out, in line with its Communication of 6 April 2016 and the findings and recommendations of the high-level expert group on information systems and interoperability, a new approach to the management of data for borders, security and migration whereby all EU information systems for security, border and migration management were to be interoperable, in a manner fully respecting fundamental rights.

(7) In its Conclusions of 9 June 2017 on the way forward to improve information exchange and ensure the interoperability of EU information systems, the Council invited the Commission to pursue the solutions for interoperability proposed by the high-level expert group.

(8) In its conclusions of 23 June 2017 the European Council underlined the need to improve interoperability between databases and invited the Commission to prepare draft legislation on the basis of the proposals made by the high-level expert group on information systems and interoperability as soon as possible.

(9) With a view to improving the effectiveness and efficiency of checks at the external borders, to contributing to prevention and combating illegal immigration and to contributing to a high level of security within the area of freedom, security and justice of the Union, including the maintenance of public security and public policy and safeguarding security in the territories of the Member States, to improving the implementation of the common visa policy, to assisting in the examination of applications for international protection, to contributing to the prevention, detection and investigation of terrorist offences and other serious criminal offences, to facilitating the identificaton of unknown persons who are unable to identify themselves or unidentified human remains in the case of a natural disaster, accident or terrorist attack, in order to maintain public trust in the Union migration and asylum system, Union security measures and Union capabilities to manage the external border, interoperability between EU information systems, namely the Entry/Exit System (EES), the Visa Information System (VIS), the European Travel Information and Authorisation System (ETIAS), Eurodac, the Schengen Information System (SIS), and the European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN) should be established in order for these EU information systems and their data to supplement each other while respecting the fundamental rights of individuals, in particular the right to

protection of personal data. To achieve this, a European search portal (ESP), a shared biometric matching service (shared BMS), a common identity repository (CIR) and a multiple-identity detector (MID) should be established as interoperability components.

(10) Interoperability between the EU information systems should allow those systems to supplement each other in order to facilitate the correct identification of persons, including unknown persons who are unable to identify themselves or unidentified human remains, contribute to combating identity fraud, improve and harmonise the data quality requirements of the respective EU information systems, facilitate the technical and operational implementation by Member States of EU information systems, strengthen the data security and data protection safeguards that govern the respective EU information systems, streamline access for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences to the EES, VIS, ETIAS and Eurodac, and support the purposes of the EES, VIS, ETIAS, Eurodac, SIS and ECRIS-TCN.

(11) The interoperability components should cover the EES, VIS, ETIAS, Eurodac, SIS, and ECRIS-TCN. They should also cover Europol data, but only to the extent of enabling Europol data to be queried simultaneously with those EU information systems.

(12) The interoperability components should process the personal data of persons whose personal data are processed in the underlying EU information systems and by Europol.

(13) The ESP should be established to facilitate technically the fast, seamless, efficient, systematic and controlled access by Member State authorities and Union agencies to the EU information systems, to Europol data and to the International Criminal Police Organization (Interpol) databases, insofar as this is needed to perform their tasks in accordance with their access rights. The ESP should also be established to support the objectives of the EES, VIS, ETIAS, Eurodac, SIS, ECRIS-TCN and Europol data. By enabling all relevant EU information systems, Europol data and the Interpol databases to be queried in parallel, the ESP should act as a single window or ‘message broker’ to search the various central systems and retrieve the necessary information seamlessly and in full respect of the access control and data protection requirements of the underlying systems.

(14) The design of the ESP should ensure that, when querying the Interpol databases, the data used by an ESP user to launch a query is not shared with the owners of Interpol data. The design of the ESP should also ensure that the Interpol databases are only queried in accordance with applicable Union and national law.

(15) The Interpol database of Stolen and Lost Travel Documents (SLTD database) enables authorised entities responsible for preventing, detecting or investigating terrorist offences or other serious criminal offences in Member States, including immigration and border control authorities, to establish the validity of a travel document. ETIAS queries the SLTD database and the Interpol Travel Documents Associated with Notices database (TDAWN database) in the context of assessing whether a person applying for a travel authorisation is likely for instance to migrate irregularly or could pose a threat to security. The ESP should enable queries against the SLTD and TDAWN databases using an individual's identity data or travel document data. Where personal data are

transferred from the Union to Interpol through the ESP, the provisions on international transfers in Chapter V of Regulation (EU) 2016/679 of the European Parliament and of the Council[4], or the national provisions transposing Chapter V of Directive (EU) 2016/680 of the European Parliament and of the Council[5] should apply. This should be without prejudice to the specific rules laid down in Council Common Position 2005/69/JHA[6] and Council Decision 2007/533/JHA[7].

(16) The ESP should be developed and configured in such a way that it only allows such queries to be performed using data related to persons or travel documents held in an EU information system, in Europol data or in the Interpol databases.

(17) To ensure the systematic use of the relevant EU information systems, the ESP should be used to query the CIR, the EES, VIS, ETIAS, Eurodac and ECRIS-TCN. However, a national connection to the different EU information systems should remain in order to provide a technical fall back. The ESP should also be used by Union agencies to query Central SIS in accordance with their access rights and in order to perform their tasks. The ESP should be an additional means to query Central SIS, Europol data and the Interpol databases, complementing the existing dedicated interfaces.

(18) Biometric data, such as fingerprints and facial images, are unique and therefore much more reliable than alphanumeric data for the purposes of identifying a person. The shared BMS should be a technical tool to reinforce and facilitate the work of the relevant EU information systems and the other interoperability components. The main purpose of the shared BMS should be to facilitate the identification of an individual who is registered in several databases, by using a single technological component to match that individual's biometric data across different systems, instead of several components. The shared BMS should contribute to security, as well as financial, maintenance and operational benefits. All automated fingerprint identification systems, including those currently used for Eurodac, VIS and SIS, use biometric templates comprised of data derived from a feature extraction of actual biometric samples. The shared BMS should regroup and store all these biometric templates – logically separated according to the information system from which the data originated – in one single location, thereby facilitating cross-system comparisons using biometric templates and enabling economies of scale in developing and maintaining the EU central systems.

(19) The biometric templates stored in the shared BMS should be comprised of data derived from a feature extraction of actual biometric samples and obtained in such a way that reversing the extraction process is not possible. Biometric templates should be obtained from biometric data but it should not be possible to obtain that same biometric data from the biometric templates. As palm print data and DNA profiles are only stored in SIS and cannot be used to perform cross-checks with data present in other information systems, following the principles of necessity and proportionality, the shared BMS should not store DNA profiles or biometric templates obtained from palm print data.

(20) Biometric data constitute sensitive personal data. This Regulation should lay down the basis and the safeguards for processing such data for the purpose of uniquely identifying the persons concerned.

(21) The EES, VIS, ETIAS, Eurodac and ECRIS-TCN require accurate identification of the persons whose personal data are stored in them. The CIR should therefore facilitate the correct identification of persons registered in those systems.

(22) Personal data stored in those EU information systems may relate to the same persons but under different or incomplete identities. Member States dispose of efficient ways to identify their citizens or registered permanent residents in their territory. The interoperability between EU information systems should contribute to the correct identification of persons present in those systems. The CIR should store the personal data that are necessary to enable the more accurate identification of the individuals whose data are stored in those systems, including their identity data, travel document data and biometric data, regardless of the system in which the data were originally collected. Only the personal data strictly necessary to perform an accurate identity check should be stored in the CIR. The personal data recorded in the CIR should be kept for no longer than is strictly necessary for the purposes of the underlying systems and should be automatically deleted when the data are deleted from the underlying systems in accordance with their logical separation.

(23) A new processing operation consisting of the storage of such data in the CIR instead of the storage in each of the separate systems is necessary to increase the accuracy of identification through the automated comparison and matching of the data. The fact that identity data, travel document data and biometric data are stored in the CIR should not hinder in any way the processing of data for the purposes of the EES, VIS, ETIAS, Eurodac or ECRIS-TCN, as the CIR should be a new shared component of those underlying systems.

(24) It is therefore necessary to create an individual file in the CIR for each person registered in the EES, VIS, ETIAS, Eurodac or ECRIS-TCN, to achieve the purpose of correct identification of persons within the Schengen area and to support the MID for the dual purpose of facilitating identity checks for *bona fide* travellers and combating identity fraud. The individual file should store all the identity information linked to a person in a single place and make it accessible to duly authorised end-users.

(25) The CIR should thus facilitate and streamline access by authorities responsible for preventing, detecting or investigating terrorist offences or other serious criminal offences to the EU information systems that are not established exclusively for purposes of prevention, detection or investigation of serious crime.

(26) The CIR should provide for a shared container for identity data, travel document data and biometric data of persons registered in the EES, VIS, ETIAS, Eurodac and the ECRIS-TCN. It should be part of the technical architecture of these systems and serve as the shared component between them for storing and querying the identity data, travel document data and biometric data they process.

(27) All records in the CIR should be logically separated by automatically tagging each record with the name of the underlying system owning that record. The access controls of the CIR should use these tags to determine whether to allow access to the record.