REVIEW OF EUROPEAN AND COMPARATIVE LAW
VOLUME XXXVII
YEAR 2019

REGULATION (EU) 2017/2226 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 30 NOVEMBER 2017 ESTABLISHING AN ENTRY/EXIT SYSTEM (EES) VERSUS DATA PROTECTION – IS IT DONE IN THE RIGHT WAY?*

*Julia Wojnowska-Radzińska***

ABSTRACT

The purpose of this paper is to explore whether the processing of personal data under the Regulation 2017/226 is compatible with the principle of proportionality in the light of the Charter of Fundamental Rights of the EU and the case-law of the Court of Justice of the European Union (CJEU). The Regulation 2017/2226 provides the EES system which is the only system that collects the entry/exit data of all third-country nationals entering the Schengen territory for a short stay, whether via a land, sea or air border checkpoint. The EES replaces the current system of manual stamping of passports.

Key words: third-country nationals, personal data, principle of proportionality, data retention

---

* This paper has been written within the research stay at the Walther Schücking Institute for International Law at the Christian-Albrechts University in Kiel financed through a competition by the Faculty of Law and Administration of the Adam Mickiewicz University in Poznań.

** She is an assistant professor at the Chair of Constitutional Law at the Faculty of Law and Administration Adam Mickiewicz University in Poznan, Poland. She teaches constitutional law, international human rights law, European Migration Law and antidiscrimination law. E-mail: juliaw@amu.edu.pl

1. INTRODCUTION

Europe's external borders have seen an unprecedented rise in the number of migrants and refugees wishing to enter the EU in recent years. Migratory pressure, as well as the prevention of entry of persons seeking to enter the EU for illegitimate reasons, are serious challenges that the Union faces. According to the latest statistics "the total number of regular border crossings in 2025 is forecast to rise to 887 million, out of which around one-third are expected to be by third-country nationals traveling to Schengen countries for a short term visit"[1]. Therefore, measures to manage the external borders have to meet the dual objectives of enhancing security and facilitating travel. Under Articles 74[2] and 77(2)[3] of the Treaty on the Functioning of the European Union (TFEU), the Union has the power to adopt measures relating to the crossing of the external borders of the Member States. According to Art. 77 para. 1 b of the Treaty on the Functioning on the European Union (TFEU): "The Union shall develop a policy with a view to: carrying out checks on persons and efficient monitoring of the crossing of external borders". To achieve this goal, appropriate legal instruments have been adopted so far. One of such legal acts is

[1] COM(2016) 194 final, p. 2, http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2016/0194/COM_COM(2016)0194_EN.pdf, [date of access: 10.07.2019].

[2] Art. 74 of the TFEU states: "The Council shall adopt measures to ensure administrative cooperation between the relevant departments of the Member States in the areas covered by this Title, as well as between those departments and the Commission. It shall act on a Commission proposal, subject to Article 76, and after consulting the European Parliament".

[3] Art. 77(2) of the TFEU states: "For the purposes of paragraph 1, the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall adopt measures concerning:
(a) the common policy on visas and other short-stay residence permits;
(b) the checks to which persons crossing external borders are subject;
(c) the conditions under which nationals of third countries shall have the freedom to travel within the Union for a short period;
(d) any measure necessary for the gradual establishment of an integrated management system for external borders;
(e) the absence of any controls on persons, whatever their nationality, when crossing internal borders".

Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011[4]. This Regulation is a part of the EU legislation known as the 'smart borders package'[5]. The aim of this Regulation is to improve the effectiveness and efficiency of controls at the external borders of the Schengen Area by creating a centralised Entry/Exit System (EES) for non-EU nationals crossing the EU's external borders for a short stay. The EES is an automated IT system for registering entries and exits of travellers from non-EU countries at the external borders. Third-country nationals have the right to enter for a short stay of up to 90 days within any 180-day period either with or without the need for the prior granting a visa. The EU has a common list of countries, the citizens of which must have a visa when crossing the external borders and a list of countries, the citizens of which are exempt from that requirement[6]. Thus, the Regulation 2017/2226 applies to third-country nationals who legally enter the EU, irrespective of whether they are required to obtain Schengen visa or not. The EES collects their personal data, including biometric data, and register the time and place of their entries and exits. The system also records refusals of entry. Thereby, the EES involves the significant collection, retention and use of personal data concerning third-country nationals.

---

[4] Hereinafter as the Regulation 2017/2226, Regulation, Official Journal of the European Union of 2017, L 327/20.

[5] The "Smart Borders" Package was proposed by the Commission in February 2013. Currently it encompasses a Regulation for the establishment of an Entry/Exit System and a proposed amendment to the Schengen Borders Code to integrate the technical changes needed for the Entry/Exit System. See also: Didier Bigo, Sergio Carrera, Ben Hayes, Nicholas Hernanz, Julien Jeandesboz, Justice and Home Affairs Databases and a Smart Borders System at EU External Borders An Evaluation of Current and Forthcoming Proposals, No. 52/December 2012, https://www.ceps.eu/ceps-publications/justice-and-home-affairs-databases-and-smart-borders-system-eu-external-borders/, [date of access: 10.07.2019].

[6] These lists are set out in the Regulation (EU) 2018/1806.

This article aims to identify whether the processing of personal data under the Regulation 2017/226 is compatible with the principle of proportionality in the light of the Charter of Fundamental Rights of the EU and the case-law of the Court of Justice of the European Union (CJEU). First, the key provisions regarding the EES scheme that have been adopted will be elaborated upon. Next, the problems posed by processing personal data of third-country nationals will be addressed. Then the standard developed by the CJEU concerning data retention will be analysed.

2. AIM AND CONTENT OF THE EU ENTRY/EXIT SYSTEM

The Schengen Borders Code has no provisions on the recording of travellers' cross border movements into and out of the Schengen area. Before adopting Entry/Exit System, the stamping of the travel document indicating the dates of entry and exit was the only method available to border guards and immigration authorities to calculate the duration of stay of third-country nationals and to verify if someone is overstaying[7]. However, those stamps could be difficult to interpret: they may be unreadable or the result of counterfeiting. The Regulation 2017/2226 was proposed by the European legislator in order to improve management of external borders, prevent irregular immigration by identifying 'overstayers'[8] and to facilitate the management of migration flows[9]. To this end, the European Entry/Exit System provides: the recording and storage of the date, time and place of entry and exit of third–country nationals crossing the external borders of the Schengen Area; the calculation of the duration of the authorised stay of such third-country nationals; the generation of alerts to Member States when the authorised stay has expired; and the recording and storage of the date, time and place of refusal of entry of third-country nationals whose entry for a short stay has been refused, as well as the authority of the

[7] COM(2016) 194 final, pp. 1-3.

[8] 'Overstayer' means a third-country national who does not fulfil or no longer fulfils the conditions relating to the duration of his or her authorised short stay on the territory of the Member States.

[9] Recital 15 of the Regulation 2017/2226. Further, see: COM(2016) 194 final, pp. 1-3.

Member State which has refused the entry and the reasons therefor[10]. The EES also intends to contribute to the prevention, detection and investigation of terrorist offences or of other serious criminal offences, and serve as an identification tool and an intelligence tool as well[11]. Therefore, the aim of the Entry/Exit System is twofold, namely the management of external borders[12] and the access to the EES data by law enforcement authorities for the prevention, detection and investigation of terrorist offences and other serious criminal offences. The EES is the only system that collects the entry/exit data of all third-country nationals entering the Schengen Area for a short stay, whether via a land, sea or air border checkpoint. The EES can provide data to confirm or not the presence of specific third-country nationals in the Schengen Area. The EES also uses the identification data to link entries and exits and can act as the database of last resort for identifying persons when more focused databases have failed to yield a result[13]. Moreover, the EES ensures a better identification of third-country nationals and allows for the detection of people using multiple identities[14]. Thus, the EES may be used for identifying unknown suspects, perpetrators or victims, and to consult the travel history of identified suspects[15].

The EES operates at the external borders of the EU countries which apply the Schengen acquis in full. However, the Member States which apply the Schengen acquis in full must introduce the EES at their internal borders with the Member States which do not yet apply the Schengen acquis in full but operate the EES. The Member States which apply the Schengen acquis in full and the Member States which do not yet apply the Schengen acquis in full but operate the EES must introduce the EES at their internal borders with the Member States which do not yet apply the Schengen acquis in full and do not operate the EES[16].

According to Article 7 of the Regulation 2017/2226 the EES consists of: a central system which will operate a computerised central database of

---

[10] Art. 1(1) of the Regulation 2017/2226.
[11] Art. 1(2) of the Regulation 2017/2226.
[12] Art. 4 of the Regulation 2017/2226.
[13] Recital 22 of the Regulation 2017/2226.
[14] Ibidem.
[15] Art. 6 of the Regulation 2017/2226.
[16] Art. 4 of the Regulation 2017/2226.

biometric[17] and alphanumeric data[18] (a mix of letters and numbers); a national uniform interface in each participating country; a secure communication channel between the EES central system and the central system of the VIS; a secure and encrypted communication infrastructure between the EES central system and the national uniform interfaces (identical interfaces for all the EU countries connect their border infrastructures to the EES central system); a data repository to obtain customisable reports and statistics; a web service to enable non-EU nationals to verify their remaining authorised stay. Furthermore the EES includes an automated calculator that indicates the maximum duration of authorised stay for third-country nationals registered in the EES. The automated calculator must inform the competent authorities: on entry, of the maximum duration of authorised stay of third-country nationals and whether the number of authorised entries of a short-stay visa issued for one or two entries has been exhausted; during checks or verifications carried out within the territory of the Member States, of the remaining authorised stay or duration of overstay of the third-country nationals; on exit, of any overstay of third-country nationals; when examining and deciding on short-stay visa applications, of the maximum remaining duration of authorised stay based on intended entry dates[19].

The EES encompasses the collection, storage and use of alphanumeric data and biometric data concerning third-country nationals entering and exiting the EU, as detailed in Articles 15 to 18 of the Regulation 2017/2226. At the borders at which the EES is operated, the border authority must create the individual file of a third-country national subject to a visa requirement by entering the following data: surname (family name); first name or names (given names); date of birth; nationality or nationalities; sex; the type and number of the travel document or documents and the three-letter code of the issuing country of the travel document or documents; the date of expiry of the validity of the travel document or documents; and the facial image. The facial image must be taken

[17] "Biometric data" means fingerprint data and facial image.

[18] "Alphanumeric data" means data represented by letters, digits, special characters, spaces and punctuation marks.

[19] Art. 11(2) of the Regulation 2017/2226.

live[20]. It should be indicated that for third-country nationals who require visas, the facial image will be the only biometric data included in the EES since their fingerprints are already stored in the VIS. Moreover, the exact information on date and time of entry, border crossing point and the authority that authorised the entry, must also be entered[21]. On each exit of a third-country national subject to a visa requirement at a border at which the EES is operated, date and time of exit, as well as the border crossing point of the last exit must be registered.

According to visa-exempt third-country nationals the border authority must create the individual file of them by entering the same data as for third-country nationals subject to a visa requirement and, in addition, fingerprint data from the right hand and the corresponding fingerprint data from the left hand[22]. It should be noted that 'fingerprint data' means the data relating to the four fingerprints of the index, middle finger, ring finger and little finger from the right hand and from the left hand[23]. Children under the age of 12 must be exempt from the requirement to give fingerprints[24]. Persons for whom fingerprinting is physically impossible must be exempted from the requirement to give fingerprints. However, where the physical impossibility is of a temporary nature, that fact must be recorded in the EES and the person must be required to give the fingerprints on exit or at the subsequent entry. This information must be deleted from the EES once the fingerprints have been given. The border authorities must be entitled to request further clarification on the grounds for the temporary impossibility to give fingerprints. Member States must ensure that appropriate procedures guaranteeing the dignity of the person are in place in the event of difficulties encountered in the capturing of fingerprints[25].

It should be stressed that the EES as an immigration database contains a wide range of personal data and thus may be recognised as "a model

---

[20] Art. 16(1) of the Regulation 2017/2226.
[21] Art. 16(2) of the Regulation 2017/2226.
[22] Art. 17(1) of the Regulation 2017/2226.
[23] Art. 3(1) point 16 of the Regulation 2017/2226.
[24] Art. 17(3) of the Regulation 2017/2226.
[25] Art. 17(4) of the Regulation 2017/2226.

for generalised surveillance of movement"[26]. On the one hand, "the deployment of electronic personal data in order to classify and govern the movement of people across borders has become a key feature of the contemporary war on terror"[27]. Using this data, the third-country national is profiled and encoded in terms of degrees of risk. Thus, the EU has adopted pre-emptive data surveillance practice to monitor actual and potential risks and sources of them through the EES. The EES serves to sift out risky persons from the flow of third-country nationals at the borders. As a result, they are differentiating between two kinds of risky foreigners: "immigration violators" and "guilty" individuals known as transgressors of the law[28]. According to V. Mitsilegas, "border control measures have [therefore] been developed as security measures, and data obtained in the context of immigration and border control (…) are now also viewed as security data which must be accessible not only to immigration authorities but also to intelligence and law enforcement authorities, for security purposes"[29]. On the other hand, regardless of whether individuals are aware of being targets of mass surveillance, the indiscriminate interception and collection of data has important ramifications with regard to the rule of law and fundamental rights of third-country nationals. Biometric data included in the EES belongs to sensitive personal data under the EU data protection law as it encompasses "personal data resulting from specific technical pro-

---

[26] Valsamis Mitsilegas, "The law of the border and the borders of law. Rethinking border control from the perspective of the individual", In: Rethinking Border Control for a Globalizing World. A preferred future, ed. Leanne Weber, London/New York: Routledge, 2016, 17. See also: Valsamis Mitsilegas, Niovi Vavoula, "The normalization of surveillance movement in an era of reinforcing privacy standards", In: Handbook on Migration and Security, ed. Philippe Bourbeau, Edward Elgar Publishing, 2017, 243.

[27] William Walters, "Putting the migration-security complex in its place", In: Risk and the War on Terror, eds. Louise Amoore, Marieke de Goede, London/New York: Routledge, 2008, 170.

[28] Charlotte Epstein, "Evolving risk. Using biometrics to protect the borders", In: Risk and the War on Terror, eds. Louise Amoore, Marieke de Goede, London/New York: Routledge, 2008, 188.

[29] Valsamis Mitsilegas, "The law of the border and the borders of law. Rethinking border control from the perspective of the individual", In: Rethinking Border Control for a Globalizing World. A preferred future, ed. Leanne Weber, London/New York: Routledge, 2016, 19.

cessing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data"[30]. What is more, the EES applies to all third-country nationals, not merely those who have been identified as potentially "risky" or even "guilty". In fact, it embraces large population of travellers irrespective of the country they come from, shifting the focus of risk from suspect individuals and individual groups to "suspect population"[31].

3. EES DATA PROCESSING

The EES registers entry, exit and refusal of entry of third-country nationals, storing information on their identity, their travel documents as well as biometric data with a view to identify any person who does not fulfil or no longer fulfils the conditions of duration of the authorised stay in the territory of the Member States at the same time facilitating crossings for the large majority of 'bona fide' third-country travellers[32]. As the European Data Protection Supervisor has noticed "the sheer volume of personal data that would be processed through this system will make the EES one of the largest European databases"[33].

The Regulation 2017/2226 explicitly stresses that any processing of the EES data should be proportionate to the objectives pursued and nec-

---

[30] See: Art. 4 point 14 and Art. 9 of the Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[31] Niovi Vavoula, "EU Immigration Databases Under Scrutiny: Towards the Normalisation of Surveillance of Movement in an Era of "Privacy Spring"?", In: Data Protection and Privacy under Pressure. Transatlantic tensions, EU surveillance, and big data, eds. Gert Vermeulen, Eva Lievens, Maklu, 2017: 238.

[32] Recital 6 of the Regulation 2017/2226.

[33] EDPS Opinion on the Second EU Smart Borders Package, Recommendations on the revised Proposal to establish an Entry/Exit System, Opinion 06/2016, 21 September 2016, p. 8, https://edps.europa.eu/sites/edp/files/publication/16-09-21_smart_borders_en.pdf, [date of access: 10.07.2019].

essary for the performance of the tasks of the competent authorities[34]. As it has already been discussed, the EES pursues two objectives. Based on the second objective of the EES, the system seeks to improve internal security by preventing, detecting and investigating terrorist offences or other serious criminal offences. According to recital 22 of the Regulation 2017/2226, in the fight against terrorist offences and other serious criminal offences, it is necessary that designated authorities have the most up-to-date information and that as a result the information contained in the EES is available to the designated authorities of the Member States and the European Police Office (Europol), subject to the conditions laid down in the Regulation 2017/2226. It is apparent from the case-law of the Court of Justice of the EU (CJEU) that the fight against international terrorism in order to maintain international peace and security constitutes an objective of general interest[35]. Therefore, the EES data may be used as an identity verification tool both in cases where the third–country national has destroyed his or her documents and where designated authorities are investigating a crime through the use of fingerprints or facial images and wish to identify an individual[36]. In other words, the EES may provide data to confirm or not the presence of specific third-country nationals in the Schengen Area. The data recorded in the EES may also help to construct evidence by tracking the travel routes of a person suspected of having committed a crime or of a crime victim[37].

However, the access to the EES for the purpose of preventing, detecting or investigating terrorist offences or other serious criminal offences constitutes an interference with the fundamental rights privacy[38] and

---

[34] Recital 19 of the Regulation 2017/2226.

[35] Commission Staff Working Document, Impact Assessment, Annexes to the Impact Assessment report on the introduction of an Entry Exit System, part 3/3, SWD(2016) 115 final, Brussels April 2016, p. 136, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/securing-eu-borders/legal-documents/docs/20160406/smart_borders_package_-_20160406_-_impact_assessment_-_part_3_en.pdf, [date of access: 12.07.2019].

[36] Recital 22 of the Regulation 2017/2226.

[37] Ibidem.

[38] Art. 7 of the Charter: "Everyone has the right to respect for his or her private and family life, home and communications".

protection of personal data[39] of third-country nationals whose personal data is processed in the EES. According to the principle of proportionality enshrined in Art. 52(1)[40] of the Charter of Fundamental Rights of the EU any interference with those fundamental rights must be limited to the extent which is necessary in a democratic society to protect a legitimate and proportionate interest, and must be proportionate to the legitimate objective to be achieved. The principle of proportionality is a common feature of decision-making in terms of the human rights issue that "seeks to police the justification of state interference with human rights, ensuring that the State places no greater limitation on rights than necessary"[41]. Furthermore, the Court of Justice of the EU has given precise guidance how personal data must be processed in order to meet the requirements of the principle of proportionality[42]. The Court has explicitly underlined that the proportionality test in connection with limitations to Article 7 and

[39] Art. 8 of the Charter: "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority".

[40] Art. 52(1) of the Charter states: "Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others".

[41] Andrew Legg, The Margin of Appreciation in International Human Rights Law: Deference and Proportionality, Oxford University Press, 2012, 178.

[42] See: *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, Joined Cases No. C293/12 and C594/12, Judgment of 8 April 2014 of the Court of Justice of the EU; *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others*, Joined Cases C-203/15 and C-698/, Judgment of 21 December 2016 of the Court of Justice of the EU; Opinion 1/15 of the Court of Justice of the European Union of 26 July 2017 pursuant to Article 218(11) TFEU on the Draft agreement between Canada and the European Union (Passenger Name Records). See also: Marie-Pierre Granger, Kristina Irion, "The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection", European Law Review, No. 6(2014): 835–854.

Article 8 of the Charter of Fundamental Rights of the EU "is to be understood as a very strict one because "simple" necessity and meeting objectives of general interest is not enough. The scrutiny requires that the objectives are genuinely met and the necessity is a strict one"[43]. In the *Digital Rights Ireland* case the CJEU has pointed out two very important issues. Firstly, the CJEU stresses that the EU provisions must lay down clear and precise rules governing the scope and application of the measures interfering with the personal data[44]. Secondly, these provisions have to provide for minimum safeguards so that the persons whose data has been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data[45]. The Court has held that protection of the right to privacy requires i any event that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary[46]. Moreover, the Court presents the view that "(…) since general access to all retained data, regardless of whether there is any link, at least indirect, with the intended purpose, cannot be regarded as limited to what is strictly necessary, the national legislation concerned must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data of subscribers or registered users. In that regard, access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime. (…) In order to ensure, in practice, that those conditions are fully respected, it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent

[43] Mark D. Cole, Teresa Quintel, Data Retention under the Proposal for an EU Entry/Exit System (EES). Analysis of the impact on and limitations for the EES by Opinion 1/15 on the EU/Canada PNR Agreement of the Court of Justice of the European Union, Legal Opinion, October 2017, p. 27, https://orbilu.uni.lu/bitstream/10993/35446/1/Legal%20Opinion.PDF, [date of access: 12.07.2019].

[44] *Digital Rights Ireland*, para. 54.

[45] Ibidem.

[46] Ibidem, para. 52.

administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime"[47].

Recital 29 of the Regulation 2017/2226 indicates that "to protect personal data and to exclude systematic searches, the processing of EES data should only take place in specific cases and when it is necessary for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences. The designated authorities and Europol should only request access to the EES when they have reasonable grounds to believe that such access will provide information that will substantially assist them in preventing, detecting or investigating terrorist offences or other serious criminal offences". Further, Article 32 of the Regulation specifies the conditions to be met for law enforcement authorities to get access to the EES data through an electronic reasoned request, as well as the additional conditions laid down for the purpose of identifying an unknown suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence[48]. Article 32(2) stipulates that a prior search does not have to be conducted if there are reasonable grounds to believe that a comparison with the systems of the other Member States would not lead to the verification of the identity of the data subject or in a case of urgency where there is the need to prevent an imminent danger to the life of a person associated with a terrorist offence or another serious criminal offence. Those reasonable grounds must be included in the electronic or written request sent by the operating unit of the designated authority to

---

[47] *Maximillian Schrems v. Data Protection Commissioner*, Case C-362/14, Judgement of 6 October 2015 of the Court of Justice of the EU, paras. 119 and 120.

[48] Art. 32(1) states: „Designated authorities may access the EES for consultation where all of the following conditions are met: (a) access for consultation is necessary for the purpose of the prevention, detection or investigation of a terrorist offences or another serious criminal offence; (b) access for consultation is necessary and proportionate in a specific case; (c) evidence or reasonable grounds exist to consider that the consultation of the EES data will contribute to the prevention, detection or investigation of any of the criminal offences in question, in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under a category covered by this Regulation.

the central access point. Thus, there appears a question, how a designated authority would know in advance, without performing any search in the systems of the other Member States, if any relevant data would be found in those systems. What is more, under Art. 29(3) each Member State must designate a central access point which must have access to the EES. The central access point must verify that the conditions to request access to the EES laid down in Article 32 are fulfilled. Nevertheless, national designated authorities requesting access to the EES data and verifying authorities granting such access can be part of the very same authorities. Article 29(3) states namely that: "the designated authority and the central access point may be part of the same organisation if permitted under national law, but the central access point shall act fully independently of the designated authorities when performing its tasks under this Regulation. The central access point shall be separate from the designated authorities and shall not receive instructions from them as regards the outcome of the verification which it shall carry out independently". Thus, the current wording of the discussed provision does not prevent unlawful access. It should be noted that the verifying authority has to be effectively independent from the designated authority in order to guarantee a proper verification of compliance with the conditions. Moreover, it is worth mentioning that in accordance with the settled case-law of the CJEU, the access by the competent national authorities should be "(…) made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued (…)"[49]. Unfortunately, the review by a court or an independent authority as required by the CJEU in *Digital Rights Ireland*, *Tele2/Watson* and in *Opinion 1/15* is not an obligation foreseen under the Regulation 2017/2226.

Furthermore, the provisions of the Regulation 2017/2226 regarding data retention raise serious concerns whether the requirements of proportionality have been met. The Regulation specifies that "the personal data stored in the EES should be kept for no longer than strictly necessary for the purposes for which the data are processed"[50]. To this end, the Europe-

[49] *Digital Rights Ireland*, para. 62, *Opinion 1/15*, paras. 202 and 208.

[50] Recital 32 of the Regulation 2017/222.

an legislator has differentiated the data retention period, providing for a retention period of three years and one day for all entry and exit records of all third-country nationals following the date of the last exit record or of the refusal of entry record if there is no entry record within three years from the date of the last exit record or refusal of entry record[51], and five years and one day for third-country nationals who have not exited the territory of the Member States within the authorised period of stay[52]. The justification for the three-year retention period for third-country nationals who have respected the duration of authorised stay is based on border management purposes, decreased border crossing time and the facilitation of expedited border crossings[53]. In turn, the five-year retention period for third-country nationals who have not exited the territory of the Member States within the authorised period of stay is necessary to support the identification and return process[54]. Moreover, the European legislator specifies, that these retention periods are necessary to allow border guards to conduct the necessary risk analysis and to analyse the travel history of the applicant in order to assess the use of previous visas and whether the conditions of stay have been respected[55]. According to recital 34 "the travel history available in the EES should therefore cover a period of time which is sufficient for the purpose of visa issuance".

However, the CJEU has explicitly recognised that the retention of personal data must be "based on objective criteria in order to ensure that it is limited to what is strictly necessary"[56]. Taking into consideration that

---

[51] Art. 34(1) of the Regulation 2017/222.

[52] Art. 34(3).

[53] Recital 32.

[54] Recital 33.

[55] Recital 34.

[56] Digital Rights Ireland, para. 64, Tele2/Watson, para. 57, Opinion 1/15, para. 206. See also: Mark D. Cole, Fran-ziska Boehm, Data Retention after the Judgement of the Court of Justice of the European Union, June 30, 2014, pp. 1-107, https://www.greens-efa.eu/legacy/fileadmin/dam/Documents/Studies/Data_protection/FB_MDC_Study_Data_Retention_Judgment_June_2014_FINAL_EXEC_SUMM.pdf, [date of access: 15.07.2019]. Moreover, the CJEU recognized that: "Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons (…) without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the

third-country nationals are in principle not suspected of unlawful conduct or under investigation, "it is doubtful whether the general improvement of management of the EU's external borders can be regarded as an objective that is to be regarded as compelling in the same way as the fight against terrorism and serious crime"[57]. In other words, the EES affects, in general, millions of people every year. No distinction is made on the basis of the data retention period possible usefulness for the objectives pursued or according to the persons concerned. Moreover, the Regulation 2017/2226 does not include any possibility to vary the period of retention based on objective criteria[58] in order to ensure that the period is limited to what is strictly necessary. In this regard, it is difficult to uphold that the three-year retention period of data is proportionate and limited to what is strictly necessary and does not represent the least intrusive measure. The European legislator should fully justify the proportionality of a retention period of personal data for three years, in view of the objective of reducing border check delays and improving border checks for third country nationals. The retention of third-country nationals' personal data after they have left the EU might be only proportionate to the second objective of the EES. But even in such circumstances, as M. Cole indicates, "it might be more adequate and therefore only then proportionate to store the data in databases established purely for the LE purposes and not in a general border management database"[59]. It should be also added that the EES scheme is to be assessed both globally, taking into consideration the already existing large-scale IT systems in the EU, namely VIS, SIS or the Eurodac database[60].

---

limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are spe-cific, strictly restricted and capable of justifying the interference which both access to that data and its use entail" (*Maximillian Schrems v. Data Protection Commissioner*, para. 93).

[57] Mark D. Cole, Teresa Quintel, Data Retention under the Proposal for an EU Entry/Exit System (EES). Analysis of the impact on and limitations for the EES by Opinion 1/15 on the EU/Canada PNR Agreement of the Court of Justice of the European Union, Legal Opinion, October 2017, p. 30.

[58] For instance, there is an evidence that the retained data can make an effective contribution to combatting serious crime.

[59] Ibidem, para. 31.

[60] See: EDPS Opinion on the Second EU Smart Borders Package, Recommendations on the revised Proposal to establish an Entry/Exit System, Opinion 06/2016, 21 September 2016, p. 21.

4. CONCLUSIONS

The increasing traveller flows and the principle of a thorough border check on all third-country nationals have increased waiting times at borders in such a way that it already constitutes a problem for many Member States. While the Member States remain responsible for controlling their own border, the EU's common policy in support of the Member States' efforts should be continuously developed and strengthened in response to new threats, shifts in migratory pressure and any shortcomings identified, using new technology extensively and proportionately. The Entry/Exit System (EES) is a new solution established not only to contribute to the modernisation of the external border management by improving the quality and efficiency of the external border controls of the Schengen Area but also to reinforce internal security and the fight against terrorism and serious crime. The EES system is the only system that collects the entry/exit data of all third-country nationals entering the Schengen Area for a short stay, whether via a land, sea or air border checkpoint. Nevertheless, the processing of personal data of third-country nationals under the EES is significant and intrusive, taking into consideration the number of persons affected by this scheme, the type of information processed, the means used for processing such information and the diverse objectives pursued. Processing of personal data by the EES constitutes an interference with fundamental rights of third-country nationals, which in order to be in accordance with the law, must be proportionate to the objectives pursued. Provided that the continued storage and use of the EES data would be based on objective criteria showing that they could contribute to the fight against terrorism and serious crimes, and considering that the access to the data by designated authorities would be subject to prior review carried out either by a court, or by an independent administrative authority, a five-year retention period would not exceed the limits of what is strictly necessary for the purposes of combating terrorism and serious transnational crime.

REFERENCES

Cole D. Mark, Boehm Franziska. 2014. Data Retention after the Judgement of the Court of Justice of the European Union: 1-107. July 15, 2019 https://www.greens-efa.eu/legacy/fileadmin/dam/Documents/Studies/Data_protection/FB_MDC_Study_Data_Retention_Judgment_June_2014_FINAL_EXEC_SUMM.pdf

Cole D. Mark, Quintel Teresa. 2017. Data Retention under the Proposal for an EU Entry/Exit System (EES). Analysis of the impact on and limitations for the EES by Opinion 1/15 on the EU/Canada PNR Agreement of the Court of Justice of the European Union, Legal Opinion: 1-37. July 12, 2019 https://orbilu.uni.lu/bitstream/10993/35446/1/Legal%20Opinion.PDF

Epstein Charlotte. 2008, "Evolving risk. Using biometrics to protect the borders". In: Risk and the War on Terror, eds. Louise Amoore, Marieke de Goede, 178-193. London/New York: Routledge.

Granger Marie-Pierre, Irion Kristina. 2014. "The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection". European Law Review 6: 835–854.

Legg Andrew. 2012. The Margin of Appreciation in International Human Rights Law: Deference and Proportionality. Oxford University Press.

Mitsilegas Valsamis. 2016. "The law of the border and the borders of law. Rethinking border control from the perspective of the individual". In: Rethinking Border Control for a Globalizing World. A preferred future, ed. Leanne Weber, 15-31. London/New York: Routledge.

Mitsilegas Valsamis, Vavoula Niovi. 2017 "The normalization of surveillance movement in an era of reinforcing privacy standards". In: Handbook on Migration and Security, ed. Philippe Bourbeau, 232-251. Edward Elgar Publishing.

Vavoula Niovi. 2017. "EU Immigration Databases Under Scrutiny: Towards the Normalisation of Surveillance of Movement in an Era of "Privacy Spring"?". In: Data Protection zand Privacy under Pressure. Transatlantic tensions, EU surveillance, and big data, eds. Gert Vermeulen, Eva Lievens, 215-248. Maklu.

Walters William. 2008. "Putting the migration-security complex in its place". In: Risk and the War on Terror, eds. Louise Amoore, Marieke de Goede, 158-177. London/New York: Routledge.