Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226

REGULATION (EU) 2018/1240 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 12 September 2018

establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty of the Functioning of the European Union, and in particular points (b) and (d) of Article 77(2) and point (a) of Article 87(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[(1)],

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

Whereas:

(1) The Communication of the Commission of 6 April 2016 entitled ‘Stronger and Smarter Information Systems for Borders and Security’ outlined the need for the Union to strengthen and improve its IT systems, data architecture and information exchange in the area of border management, law enforcement and counter-terrorism. It emphasises the need to improve the interoperability of information systems. Importantly, it sets out possible options for maximising the benefits of existing information systems and, if necessary, developing new and complementary ones to address still existing information gaps.

(2) Indeed, the Communication of 6 April 2016 identified a series of information gaps. Among them are the fact that border authorities at external Schengen borders have no information on travellers exempt from the requirement of being in possession of a visa when crossing the external borders (‘the visa requirement’). The Communication of 6 April 2016 announced that the Commission was to launch a study on the feasibility of establishing a European Travel Information and Authorisation System (ETIAS). The feasibility study was completed in November 2016. The system would determine the eligibility of visa-exempt third-country nationals prior to their travel to the Schengen Area, and whether such travel poses a security, illegal immigration or high epidemic risk.

(3) The Communication of 14 September 2016‘Enhancing security in a world of mobility: improved information exchange in the fight against terrorism and stronger external borders’ confirms the priority of securing external borders and presents concrete initiatives to accelerate and broaden the Union’s response in continuing to strengthen the management of external borders.

(4) It is necessary to specify the objectives of ETIAS, to define its technical and organisational architecture, to lay down rules concerning the operation and the use of the data to be entered into the system by the applicant and rules on the issue or refusal of the travel authorisations, to lay down the purposes for which the data are to be processed, to identify the authorities authorised to access the data and to ensure the protection of personal data.

(5) ETIAS should apply to third-country nationals who are exempt from the visa requirement.

(6) It should also apply to third-country nationals who are exempt from the visa requirement who are family members of a Union citizen to whom Directive 2004/38/EC of the European Parliament and of the Council[(3)] applies or of a national of a third country enjoying the right of free movement equivalent to that of Union citizens under an agreement between the Union and its Member States on the one hand and a third country on the other and who do not hold a residence card pursuant to Directive 2004/38/EC or a residence permit pursuant to Council Regulation (EC) No 1030/2002[(4)]. Article 21(1) of the Treaty on the Functioning of the European Union (TFEU) stipulates that every citizen of the Union shall have the right to move and reside freely within the territory of the Member States, subject to the limitations and conditions laid down in the Treaties and by the measures adopted to give them effect. The respective limitations and conditions are to be found in Directive 2004/38/EC.

(7) As confirmed by the Court of Justice[(5)], such family members have the right to enter the territory of the Member States and to obtain an entry visa for that purpose. Consequently, family members exempted from the visa obligation should have the right to obtain a travel authorisation. Member States should grant such persons every facility to obtain the necessary travel authorisation, which should be issued free of charge.

(8) The right to obtain a travel authorisation is not unconditional as it can be denied to those family members who represent a risk to public policy, public security or public health pursuant to Directive 2004/38/EC. Against this background, family members can be required to provide their personal data related to their identification and their status only insofar as these are relevant for assessment of the security threat they could represent. Similarly, examination of their travel authorisation applications should be made exclusively against security concerns, and not those related to migration risks.

(9) ETIAS should provide a travel authorisation for third-country nationals exempt from the visa requirement enabling consideration of whether their presence on the territory of the Member States does not pose or will not pose a security, illegal immigration or a high epidemic risk. A travel authorisation should therefore constitute a decision indicating that there are no factual indications or reasonable grounds to consider that

the presence of a person on the territory of the Member States poses such risks. As such, a travel authorisation is by its nature distinct from a visa; it will not require more information or place a heavier burden on applicants than a visa does. Holding a valid travel authorisation should be a new entry condition for the territory of the Member States. Mere possession of a travel authorisation should not, however, confer an automatic right of entry.

(10) ETIAS should contribute to a high level of security, to the prevention of illegal immigration and to the protection of public health by providing an assessment of visitors prior to their arrival at the external border crossing points.

(11) ETIAS should contribute to the facilitation of border checks performed by border guards at the external border crossing points. It should also ensure a coordinated and harmonised assessment of third-country nationals subject to the travel authorisation requirement who intend to travel to Member States. Furthermore, it should enable applicants to be better informed of their eligibility to travel to Member States. In addition, ETIAS should contribute to the facilitation of border checks by reducing the number of refusals of entry at the external borders and by providing border guards with certain additional information related to flags.

(12) ETIAS should also support the objectives of the Schengen Information System (SIS) related to alerts on third-country nationals subject to a refusal of entry and stay, on persons wanted for arrest for surrender purposes or extradition purposes, on missing persons, on persons sought to assist with a judicial procedure and on persons for discreet checks or specific checks. For this purpose, ETIAS should compare relevant data from application files against relevant alerts in SIS. Where the comparison reveals a correspondence between personal data in the application file and alerts on third-country nationals subject to a refusal of entry and stay or on persons wanted for arrest for surrender purposes or extradition purposes, the application file should be processed manually by the ETIAS National Unit of the Member State responsible. The assessment performed by the ETIAS National Unit should lead to a decision whether to issue a travel authorisation or not. Where the comparison reveals a correspondence between personal data in the application file and alerts on missing persons, on persons sought to assist with a judicial procedure and on persons for discreet checks or specific checks, this information should be transferred to the SIRENE bureau and should be dealt with in accordance with the relevant legislation relating to SIS.

(13) The conditions for issuing a travel authorisation should be coherent with the specific objectives associated with the different types of alerts recorded in SIS. In particular, the fact that applicants would be subject to an alert on persons wanted for arrest for surrender purposes or extradition purposes or to an alert on persons for discreet checks or specific checks should not prevent them from being issued with a travel authorisation with a view to Member States taking appropriate action in accordance with Council Decision 2007/533/JHA[(6)].

(14) ETIAS should consist of a large-scale information system, the ETIAS Information System, the ETIAS Central Unit and the ETIAS National Units.

(15) The ETIAS Central Unit should be part of the European Border and Coast Guard Agency. The ETIAS Central Unit should be responsible for verifying, in cases where the automated application process has reported a hit, whether the applicant's personal data correspond to the personal data of the person having triggered that hit. Where a hit is confirmed or where doubts remain, the ETIAS Central Unit should initiate the manual processing of the application. It should ensure that the data it enters in the applications files are up to date and define, establish, assess *ex ante*, implement, evaluate *ex post*, revise and delete the specific risk indicators, ensuring that the verifications that are performed and their results are recorded in the application files. It should also carry out regular audits of the processing of applications and of the implementation of the ETIAS screening rules, including by regularly assessing their impact on fundamental rights, in particular with regard to privacy and personal data protection. It should furthermore be responsible for fulfilling a number of support tasks such as ensuring the necessary notifications are sent and providing information and support. It should be operational 24 hours a day, 7 days a week.

(16) Each Member State should establish an ETIAS National Unit responsible for examining applications and deciding whether to issue or refuse, annul or revoke travel authorisations. The ETIAS National Units should cooperate with each other and with the European Union Agency for Law Enforcement Cooperation (Europol) for the purpose of assessing applications. The ETIAS National Units should be provided with adequate resources to fulfil their tasks in accordance with the deadlines set out in this Regulation. In order to facilitate the decision-making process and the exchange of information between Member States and to reduce translation costs and response times, it is preferable that all ETIAS National Units communicate in a single language.

(17) To meet its objectives, ETIAS should provide an online application form that the applicant should fill in with declarations relating to his or her identity, travel document, residence information, contact details, level of education and job group, any status he or she holds of family member to Union citizens or third-country nationals enjoying the right of free movement and not holding a residence card pursuant to Directive 2004/38/EC or a residence permit pursuant to Regulation (EC) No 1030/2002, where the applicant is minor, details of the person responsible for him or her, and answers to a set of background questions.

(18) ETIAS should accept applications introduced on behalf of the applicant for travellers who are themselves not in a position to create an application, for whatever reason. In such cases, the application should be submitted by a third party authorised by the traveller or legally responsible for him or her, provided this person's identity is included in the application form. It should be possible for travellers to authorise commercial intermediaries to create and submit an application on their behalf. The ETIAS Central Unit should act upon any reports of abuses by commercial intermediaries appropriately.

(19) Parameters for ensuring the completeness of an application and the coherence of the data submitted should be established to verify the admissibility of applications for a travel authorisation. For instance, such verification should preclude the use of travel documents which will expire in less than three months, have expired or were

issued more than 10 years previously. The verification should be undertaken before the applicant is invited to pay the fee.

(20) In order to finalise the application, applicants should be required to pay a travel authorisation fee. The payment should be managed by a bank or a financial intermediary. The data required for securing the electronic payment should only be provided to the bank or financial intermediary operating the financial transaction and not form part of data stored in ETIAS.

(21) Most of the travel authorisations should be issued within minutes, though a reduced number could require longer, especially in exceptional cases. In such exceptional cases, it may be necessary to request additional information or documentation from the applicant, to process that additional information or documentation and, following examination of the information or documentation provided by the applicant, to invite him or her to an interview. Interviews should only be conducted in exceptional circumstances, as a last resort and when serious doubts remain regarding the information or documentation provided by the applicant. The exceptional nature of interviews should lead to less than 0,1 % of applicants being invited to an interview. The number of applicants invited to an interview should be subject to regular review by the Commission.

(22) The personal data provided by the applicant should be processed by ETIAS for the sole purposes of assessing whether the entry of the applicant into the Union could pose a security, illegal immigration or high epidemic risk in the Union.

(23) The assessment of such risks cannot be carried out without processing the personal data to be provided in a travel authorisation application. The personal data in the applications should be compared with the data present in a record, file or alert registered in an EU information system or database (the ETIAS Central System, SIS, the Visa Information System (VIS), the Entry/Exit System (EES) or Eurodac), in Europol data or in the Interpol databases (the Interpol Stolen and Lost Travel Document database (SLTD) or the Interpol Travel Documents Associated with Notices database (TDAWN)). The personal data in the applications should also be compared against the ETIAS watchlist and against specific risk indicators. The categories of personal data that should be used for comparison should be limited to the categories of data present in those EU information systems that are consulted, in Europol data, in Interpol databases, in the ETIAS watchlist or in the specific risk indicators.

(24) The comparison should take place by automated means. Whenever such comparison reveals that a correspondence (a ‘hit’) exists between any of the personal data or combination thereof in the application and the specific risk indicators or the personal data either in a record, file or alert in the above information systems or in the ETIAS watchlist, the application should be processed manually by the ETIAS National Unit of the Member State responsible. The assessment performed by the ETIAS National Unit should lead to the decision to issue the travel authorisation or not to do so.

(25) It is expected that the vast majority of applications will obtain a positive answer by automated means. No refusal, annulment or revocation of a travel authorisation should be based only on the automated processing of personal data in the applications. For this

reason, the applications generating a hit should be processed manually by an ETIAS National Unit.

(26) Applicants who have been refused a travel authorisation should have the right to appeal. Appeals should be conducted in the Member State that has taken the decision on the application and in accordance with the national law of that Member State.

(27) The ETIAS screening rules should be used to analyse an application file by enabling a comparison between the data recorded in it and specific risk indicators corresponding to previously identified security, illegal immigration or high epidemic risks. The criteria used for defining the specific risk indicators should in no circumstances be based solely on a person's sex or age. They should also in no circumstances be based on information revealing a person's colour, race, ethnic or social origin, genetic features, language, political or any other opinion, religion or philosophical belief, trade union membership, membership of a national minority, property, birth, disability, or sexual orientation. The specific risk indicators should be defined, established, assessed *ex ante*, implemented, evaluated *ex post*, revised and deleted by the ETIAS Central Unit following consultation of an ETIAS screening board composed of representatives of the ETIAS National Units and the agencies involved. To help ensure the respect of fundamental rights in the implementation of the ETIAS screening rules and specific risk indicators, an ETIAS Fundamental Rights Guidance Board should be established. The secretariat for its meetings should be provided by the Fundamental Rights Officer of the European Border and Coast Guard Agency.

(28) An ETIAS watchlist should be established for the purposes of identifying connections between data in an application file and information related to persons who are suspected of having committed or having taken part in a terrorist offence or other serious criminal offence or regarding whom there are factual indications or reasonable grounds, based on an overall assessment of a person, to believe that they will commit a terrorist offence or other serious criminal offences. The ETIAS watchlist should form part of the ETIAS Central System. Data should be entered into the ETIAS watchlist by Europol, without prejudice to the relevant provisions on international cooperation in Regulation (EU) 2016/794 of the European Parliament and of the Council[(7)], and by Member States. Before entering data into the ETIAS watchlist, it should be determined that the data are adequate, accurate and important enough to be included in the ETIAS watchlist and that their entry would not lead to a disproportionate number of applications being processed manually. The data should be regularly reviewed and verified to ensure their continued accuracy.

(29) The continuous emergence of new forms of security threats, new patterns of illegal immigration and high epidemic risks requires effective responses using modern means. Since these means often involve the processing of significant amounts of personal data, appropriate safeguards should be introduced to keep the interference with the right to protection of private life and to the right of protection of personal data limited to what is necessary in a democratic society.

(30) Personal data in ETIAS should therefore be kept secure. Access to them should be limited to strictly authorised personnel. In no circumstances should access be used to

reach decisions based on any form of discrimination. The personal data stored should be kept securely in the facilities of the European Agency for the operational management of large-scale information systems in the area of freedom, security and justice (eu-LISA) in the Union.

(31) Issued travel authorisations should be annulled or revoked as soon as it becomes evident that the conditions for issuing them were not or are no longer met. In particular, where a new alert for refusal of entry and stay or an alert reporting a travel document as lost, stolen, misappropriated or invalidated is entered in SIS, SIS should inform ETIAS. ETIAS should then verify whether this new alert corresponds to a valid travel authorisation. Where a new refusal of entry and stay alert has been issued, the ETIAS National Unit of the Member State responsible should revoke the travel authorisation. Where the travel authorisation is linked to a travel document reported as lost, stolen, misappropriated or invalidated in SIS, or reported as lost, stolen or invalidated in SLTD, the ETIAS National Unit of the Member State responsible should manually process the application file. Following a similar approach, new data entered into the ETIAS watchlist should be compared with the application files stored in ETIAS in order to verify whether those new data correspond to a valid travel authorisation. In such cases, the ETIAS National Unit of the Member State that entered the new data, or the Member State of first intended stay in the case of data entered by Europol, should assess the hit and, where necessary, revoke the travel authorisation. It should also be possible to revoke a travel authorisation at the request of the applicant.

(32) When, in exceptional circumstances, a Member State considers it necessary to allow a third-country national to travel to its territory on humanitarian grounds, for reasons of national interest or because of international obligations, it should have the possibility to issue a travel authorisation valid only for a limited territory and period.

(33) Prior to boarding, air and sea carriers and international carriers transporting groups overland by coach should have the obligation to verify that travellers are in possession of a valid travel authorisation. The ETIAS file itself should not be accessible to carriers. Carriers should have secure access to the ETIAS Information System to allow them to consult it using travel document data.

(34) The technical specifications for accessing the ETIAS Information System through the carrier gateway should limit the impact on passenger travel and carriers to the extent possible. For this purpose, integration with the EES should be considered.

(35) With a view to limiting the impact of the obligations set out in this Regulation on international carriers transporting groups overland by coach, user-friendly mobile solutions should be made available.

(36) Within two years following the start of operations of ETIAS, the appropriateness, compatibility and coherence of provisions referred to in Article 26 of the Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders[8] for the purposes of the ETIAS provisions for overland transport by coaches should be assessed by the Commission. The recent evolution of overland transport by coaches should be

taken into account. The need for amending provisions concerning overland transport by coaches referred to in Article 26 of that Convention or this Regulation should be considered.

(37) In order to ensure compliance with the revised conditions for entry, border guards should check whether travellers are in possession of a valid travel authorisation. Therefore, during the standard border check process, border guards should read travel document data electronically. This operation should trigger a query in different databases as provided under the Regulation (EU) 2016/399 of the European Parliament and of the Council[9] (Schengen Borders Code), including a query in ETIAS which should provide the up-to-date travel authorisation status. If there is no valid travel authorisation, the border guard should refuse entry and should complete the border check process accordingly. If there is a valid travel authorisation, the decision to authorise or refuse entry should be taken by the border guard. Certain data in the ETIAS file should be accessible to border guards to assist them in carrying out their tasks.

(38) Where the ETIAS National Unit of the Member State responsible considers that some aspects of the application for a travel authorisation deserve further examination by the border authorities, it should be able to attach a flag to the travel authorisation it issues, recommending a second line check at the border crossing point. It should also be possible for such a flag to be attached at the request of a consulted Member State. Where the ETIAS National Unit of the Member State responsible considers that a specific hit triggered during the processing of the application constitutes a false hit or where the manual processing shows that there were no grounds for refusing a travel authorisation, it should be able to attach a flag to the travel authorisation it issues to facilitate border checks by providing border authorities with information related to the verifications that have been carried out and to limit the negative consequences of false hits on travellers. Operational instructions for border authorities for handling travel authorisations should be provided in a practical handbook.

(39) Since the possession of a valid travel authorisation is a condition of entry and stay for certain categories of third-country national, the immigration authorities of the Member States should be able to consult the ETIAS Central System when a prior search has been conducted in the EES and this search indicates that the EES does not contain an entry record corresponding to the presence of the third-country national on the territory of the Member States. Immigration authorities of the Member States should have access to certain information stored in the ETIAS Central System, in particular for the purpose of returns.

(40) In the fight against terrorist offences and other serious criminal offences and given the globalisation of criminal networks, it is imperative that designated authorities responsible for the prevention, detection or investigation of terrorist offences and other serious criminal offences (‘designated authorities’) have the necessary information to perform their tasks effectively. Access to data contained in the VIS for such purposes has already proven effective in helping investigators to make substantial progress in cases related to trafficking in human beings, terrorism or drug trafficking. VIS does not contain data on visa-exempt third-country nationals.

(41) Access to the information contained in ETIAS is necessary to prevent, detect and investigate terrorist offences as referred to in Directive (EU) 2017/541 of the European Parliament and of the Council[(10)] or other serious criminal offences as referred to in Council Framework Decision 2002/584/JHA[(11)]. In a specific investigation and in order to establish evidence and information related to a person suspected of having committed a serious crime or to a victim of a serious crime, designated authorities may need access to the data generated by ETIAS. The data stored in ETIAS may also be necessary to identify the perpetrator of a terrorist offence or other serious criminal offences, especially when urgent action is needed. Access to ETIAS for the purpose of preventing, detecting or investigating terrorist offences or other serious criminal offences constitutes an interference with the fundamental rights to respect for the private life of individuals and to the protection of personal data of those persons whose personal data are processed in ETIAS. Therefore, the data in ETIAS should be retained and made available to the designated authorities of the Member States and to Europol only subject to the strict conditions set out in this Regulation. This will ensure that the processing of data stored in ETIAS is limited to what is strictly necessary for the prevention, detection and investigation of terrorist offences and other serious criminal offences in accordance with requirements laid down in the jurisprudence of the Court, in particular in the Digital Rights Ireland case[(12)].

(42) In particular, access to data stored in ETIAS for the purpose of preventing, detecting or investigating terrorist offences or other serious criminal offences should only be granted following a reasoned request by the operating unit of a designated authority explaining its necessity. In cases of urgency, where there is a need to prevent an imminent danger to the life of a person associated with a terrorist offence or another serious criminal offence, the verification of whether the conditions were fulfilled should take place after access to such data has been granted to the designated competent authorities. This *ex post* verification should take place without undue delay and in any event no later than seven working days after the processing of the request.

(43) It is therefore necessary to designate the authorities of the Member States that are authorised to request such access for the specific purposes for the prevention, detection or investigation of terrorist offences or of other serious criminal offences.

(44) The central access point(s) should act independently of the designated authorities and should verify that the conditions to request access to the ETIAS Central System are fulfilled in the concrete case at hand.

(45) Europol is the hub for information exchange in the Union. It plays a key role in cooperation between Member States' authorities responsible for cross-border criminal investigations by supporting the Union-wide prevention, analysis and investigation of crime. Consequently, Europol should also have access to the ETIAS Central System within the framework of its tasks and in accordance with Regulation (EU) 2016/794 in specific cases where this is necessary for Europol to support and strengthen action by Member States to prevent, detect or investigate terrorist offences or other serious criminal offences.

(46) To exclude systematic searches, the processing of data stored in the ETIAS Central System should take place only in specific cases and only 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 ETIAS when they have reasonable grounds to believe that such access will provide information that will assist them in preventing, detecting or investigating a terrorist offence or other serious criminal offence.

(47) The personal data recorded in ETIAS should be kept for no longer than is necessary for the purposes for which the data are processed. In order for ETIAS to function, it is necessary to keep the data related to applicants for the validity period of the travel authorisation. After the validity period has expired, the data should only be stored with the explicit consent of the applicant and only for the purpose of facilitating a new ETIAS application. A decision to refuse, annul or revoke a travel authorisation could indicate a security, illegal immigration or high epidemic risk posed by the applicant. Where such a decision has been issued, the data should therefore be kept for five years from the date of that decision, in order for ETIAS to be able to take into account accurately the higher risk possibly posed by the applicant concerned. If the data giving rise to this decision are deleted earlier, the application file should be deleted within seven days. After the expiry of such period, the personal data should be deleted.

(48) Personal data stored in the ETIAS Central System should not be made available to any third country, international organisation or private party. As an exception to that rule, however, it should be possible to transfer such personal data to a third country where the transfer is subject to strict conditions and necessary in the individual case for the purposes of return. In the absence of an adequacy decision by means of implementing act pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council[13] or of appropriate safeguards to which transfers are subject pursuant to that Regulation, it should exceptionally be possible to transfer data stored in ETIAS to a third country for the purposes of return, but only where the transfer is necessary for important reasons of public interest as referred to in that Regulation.

(49) It should also be possible to transfer personal data obtained by Member States pursuant to this Regulation to a third country in an exceptional case of urgency, where there is an imminent danger associated with a terrorist offence or where there is an imminent danger to the life of a person associated with a serious criminal offence. An imminent danger to the life of a person should be understood as covering a danger arising from a serious criminal offence committed against that person such as grievous bodily injury, illicit trade in human organs and tissue, kidnapping, illegal restraint and hostage-taking, sexual exploitation of children and child pornography, and rape.

(50) In order to ensure public awareness of ETIAS, particularly among third-country nationals subject to the travel authorisation requirement, information concerning ETIAS, including the relevant Union legislation, and the procedure for the application for a travel authorisation should be made available to the general public through a public website and an application for mobile devices to be used for applying to ETIAS. This information should also be disseminated through a common leaflet and by any other

appropriate means. In addition, applicants for a travel authorisation should receive an email notification with information related to their application. That email notification should include weblinks to applicable Union and national legislation.

(51) Precise rules should be laid down as regards the responsibilities of eu-LISA for the design, development and technical management of the ETIAS Information System. Rules should also be laid down governing the responsibilities of the European Border and Coast Guard Agency, the responsibilities of the Member States and the responsibilities of Europol as regards ETIAS. eu-LISA should pay particular attention to the risk of cost increases and ensure sufficient monitoring of contractors.

(52) Regulation (EC) No 45/2001 of the European Parliament and of the Council[(14)] applies to the activities of eu-LISA and the European Border and Coast Guard Agency when carrying out the tasks entrusted to them in this Regulation.

(53) Regulation (EU) 2016/679 applies to the processing of personal data by the Member States in application of this Regulation.

(54) Where the processing of personal data by Member States for the purpose of assessing applications is carried out by the competent authorities for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences, Directive (EU) 2016/680 of the European Parliament and of the Council[(15)] applies.

(55) Directive (EU) 2016/680 applies to the processing of personal data by the designated authorities of the Member States for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences pursuant to this Regulation.

(56) The independent supervisory authorities established in accordance with Regulation (EU) 2016/679 should monitor the lawfulness of the processing of personal data by Member States, whilst the European Data Protection Supervisor established by Regulation (EC) No 45/2001 should monitor the activities of the Union institutions and bodies in relation to the processing of personal data. The European Data Protection Supervisor and the supervisory authorities should cooperate with each other in monitoring ETIAS.

(57) Strict access rules to the ETIAS Central System and the necessary safeguards should be established. It is also necessary to provide for individuals' rights of access, rectification, restriction, completion, erasure and redress in relation to personal data, in particular the right to a judicial remedy and the supervision of processing operations by public independent authorities.

(58) In order to assess the security, illegal immigration or high epidemic risks which could be posed by a traveller, interoperability between the ETIAS Information System and other EU information systems should be established. Interoperability should be established in full compliance with the Union *acquis* concerning fundamental rights. If a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons is established at Union level, ETIAS should be able to query it.

(59) This Regulation should contain clear provisions on liability and the right to compensation for the unlawful processing of personal data and for any other act incompatible with this Regulation. Such provisions should be without prejudice to the right to compensation from, and liability of the controller or processor under Regulation (EU) 2016/679, Directive (EU) 2016/680 and Regulation (EC) No 45/2001. eu-LISA should be responsible for any damage it causes in its capacity as a data processor where it has not complied with the obligations specifically imposed on it by this Regulation, or where it has acted outside or contrary to lawful instructions of the Member State which is the data controller.

(60) The effective monitoring of the application of this Regulation requires evaluation at regular intervals. Member States should lay down rules on the penalties applicable to infringements of this Regulation and ensure that they are implemented.

(61) In order to establish the technical measures needed for the application of this Regulation, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission:

— to define the requirements of the secure account service,

— to lay down the predetermined list of job groups used in the application form,

— to specify the content and format of questions to applicants relating to convictions for criminal offences, stays in war or conflict zones and decisions to leave the territory or return decisions,

— to specify the content and format of additional questions to applicants who reply affirmatively to one of the questions relating to convictions for criminal offences, stays in war or conflict zones and decisions to leave the territory or return decisions, and to set out a predetermined list of answers,

— to lay down the payment methods and process for collecting the travel authorisation fee and any changes to the amount of that fee to reflect any increase in the costs of ETIAS,

— to lay down the content and format of a predetermined list of options for applicants requested to provide additional information or documentation,

— to further define the verification tool,

— to further define the security, illegal immigration or high epidemic risks to be used to establish the specific risk indicators,

— to define the type of additional information related to flags that may be added in the ETIAS application file, its formats, language and the reasons for the flags,

— to establish adequate safeguards by providing rules and procedures to avoid conflicts with alerts in other information systems and to define the conditions, the criteria and the duration of the flagging,

— to further define the tool to be used by applicants to give and withdraw their consent,

— to extend the duration of the transitional period during which no travel authorisation is required and the duration of the grace period during

which border guards will allow third-country nationals requiring a travel authorisation but not in possession of one exceptionally to enter subject to certain conditions,

— to define the financial support for Member States for expenses they incur to customise and automate border checks when implementing ETIAS.

(62) It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making[16]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(63) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to adopt detailed rules on:

— a form allowing the reporting of abuses by commercial intermediaries authorised by applicants to submit applications on their behalf,

— the conditions for operation of the public website and the app for mobile devices, and detailed rules on data protection and security applicable to the public website and the app for mobile devices,

— the requirements governing the format of the personal data to be inserted in the application form and the parameters and verifications to be implemented for ensuring the completeness of the application and the coherence of these data,

— the requirements, testing and operation of the means of audio and video communication relied on for applicant interviews, and detailed rules on data protection, security and confidentiality applicable to such communication,

— the security, illegal immigration and high epidemic risks on which specific risk indicators are to be based,

— the technical specifications of the ETIAS watchlist and of the assessment tool to be used to assess the potential impact of entering data into the ETIAS watchlist on the proportion of applications that are manually processed,

— a form for refusal, annulment or revocation of a travel authorisation,

— the conditions for ensuring secure access to the ETIAS Information System by carriers, and the data protection and security rules applicable to this access,

— an authentication scheme for access to the ETIAS Information System for duly authorised members of carrier staff,

— the fall-back procedures to be followed in the case of a technical impossibility for carriers to query the ETIAS Information System,

— model contingency plans in the case of a technical impossibility for border authorities to consult the ETIAS Central System or in case of a failure of ETIAS,

— a model security plan and a model business continuity and disaster recovery plan concerning the security of processing of personal data,
— access to the data in the ETIAS Information System,
— amendment, erasure and advance erasure of data,
— the keeping of logs and access to them,
— performance requirements,
— specifications for technical solutions to connect central access points to the ETIAS Central System,
— a mechanism, procedures and interpretations of data quality compliance for the data contained in the ETIAS Central System,
— common leaflets to inform travellers of the requirement to be in possession of a valid travel authorisation,
— the operation of a central repository containing data solely for the purpose of reporting and statistics, and the data protection and security rules applicable to the repository, and
— the specifications of a technical solution for the purpose of facilitating the collection of statistical data necessary to report on the effectiveness of access to data stored in the ETIAS Central System for law enforcement purposes.

Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[17].

(64) Since the objectives of this Regulation, namely, the establishment of a European Travel Information and Authorisation System and the creation of common obligations, conditions and procedures for use of the data stored in it 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.

(65) The operational and maintenance costs of the ETIAS Information System, of the ETIAS Central Unit and of the ETIAS National Units should be covered entirely by the revenues generated by the travel authorisation fees. The fee should therefore be adjusted as necessary in light of the costs incurred.

(66) The revenue generated by the payment of travel authorisation fees should be assigned to cover the recurring operational and maintenance costs of the ETIAS Information System, of the ETIAS Central Unit and of the ETIAS National Units. In view of the specific character of the system, it is appropriate to treat the revenue as internal assigned revenue. Any revenue remaining after covering these costs should be assigned to the Union budget.

(67) This Regulation is without prejudice to the application of Directive 2004/38/EC.

(68) This Regulation respects fundamental rights and observes the principles recognised by the Charter of Fundamental Rights of the European Union.

(69) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the TEU and to the TFEU, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. Given that this Regulation builds upon the Schengen *acquis*, Denmark shall, in accordance with Article 4 of that Protocol, decide within a period of six months after the Council has decided on this Regulation whether it will implement it in its national law.

(70) This Regulation constitutes a development of the provisions of the Schengen *acquis* in which the United Kingdom does not take part, in accordance with Council Decision 2000/365/EC[(18)]; the United Kingdom is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(71) This Regulation constitutes a development of the provisions of the Schengen *acquis* in which Ireland does not take part, in accordance with Council Decision 2002/192/EC[(19)]; Ireland is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(72) As regards Iceland and Norway, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latters' association with the implementation, application and development of the Schengen *acquis*[(20)] which fall within the area referred to in Article 1, point A of Council Decision 1999/437/EC[(21)].

(73) As regards Switzerland, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*[(22)] which fall within the area referred to in Article 1, point A of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/146/EC[(23)] and with Article 3 of Council Decision 2008/149/JHA[(24)].

(74) As regards Liechtenstein, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*[(25)] which fall within the area referred to in Article 1, point A of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/350/EU[(26)] and with Article 3 of Council Decision 2011/349/EU[(27)].

(75) In order to determine the modalities relating to the financial contribution of third countries associated with the implementation, application and development of the Schengen *acquis*, further arrangements should be concluded between the Union and those countries under the relevant provisions of their association agreements. Such arrangements should constitute international agreements within the meaning of Article 218 TFEU.

(76) In order to integrate this Regulation into the existing legal framework and to reflect the necessary operational changes for eu-LISA and the European Border and Coast Guard Agency, Regulations (EU) No 1077/2011[(28)], (EU) No 515/2014[(29)], (EU) 2016/399, (EU) 2016/1624[(30)] and (EU) 2017/2226[(31)] of the European Parliament and of the Council should be amended.

(77) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 6 March 2017[(32)],

HAVE ADOPTED THIS REGULATION:

(**1**) OJ C 246, 28.7.2017, p. 28.

(**2**) Position of the European Parliament of 5 July 2018 (not yet published in the Official Journal) and decision of the Council of 5 September 2018.

(**3**) Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC (OJ L 158, 30.4.2004, p. 77).

(**4**) Council Regulation (EC) No 1030/2002 of 13 June 2002 laying down a uniform format for residence permits for third-country nationals (OJ L 157, 15.6.2002, p. 1).

(**5**) Judgment of the Court of Justice of 31 January 2006, *Commission v Spain*, C-503/03, ECLI:EU:C:2006:74.

(**6**) Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 205, 7.8.2007, p. 63).

(**7**) Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53).

(**8**) OJ L 239, 22.9.2000, p. 19.

(**9**) Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ L 77, 23.3.2016, p. 1).

(**10**) 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).

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

(**12**) Judgment of the Court of Justice (Grand Chamber) of 8 April 2014, Digital Rights Ireland Ltd, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238.

(**13**) 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) (OJ L 119, 4.5.2016, p. 1).

(**14**) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

(**15**) 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 purposes of 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).

(**16**) OJ L 123, 12.5.2016, p. 1.

(**17**) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

(**18**) Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen *acquis* (OJ L 131, 1.6.2000, p. 43).

(**19**) Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen *acquis* (OJ L 64, 7.3.2002, p. 20).

(**20**) OJ L 176, 10.7.1999, p. 36.

(**21**) Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen *acquis* (OJ L 176, 10.7.1999, p. 31).

(**22**) OJ L 53, 27.2.2008, p. 52.

(**23**) Council Decision 2008/146/EC of 28 January 2008 on the conclusion, on behalf of the European Community, of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* (OJ L 53, 27.2.2008, p. 1).

(**24**) Council Decision 2008/149/JHA of 28 January 2008 on the conclusion on behalf of the European Union of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* (OJ L 53, 27.2.2008, p. 50).

(**25**) OJ L 160, 18.6.2011, p. 21.

(**26**) Council Decision 2011/350/EU of 7 March 2011 on the conclusion, on behalf of the European Union, of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*, relating to the abolition of checks at internal borders and movement of persons (OJ L 160, 18.6.2011, p. 19).

(**27**) Council Decision 2011/349/EU of 7 March 2011 on the conclusion on behalf of the European Union of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* relating in particular to judicial cooperation in criminal matters and police cooperation (OJ L 160, 18.6.2011, p. 1).

(**28**) Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (OJ L 286, 1.11.2011, p. 1).

(**29**) Regulation (EU) No 515/2014 of the European Parliament and of the Council of 16 April 2014 establishing, as part of the Internal Security Fund, the instrument for financial support for external borders and visa and repealing Decision No 574/2007/EC (OJ L 150, 20.5.2014, p. 143).

(**30**) Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC (OJ L 251, 16.9.2016, p. 1).

(**31**) 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 (OJ L 327, 9.12.2017, p. 20).

(**32**) OJ C 162, 23.5.2017, p. 9.

Changes to legislation:
There are currently no known outstanding effects for the Regulation (EU) 2018/1240 of the European Parliament and of the Council, Introductory Text.