

Interoperability between EU border and security information systems

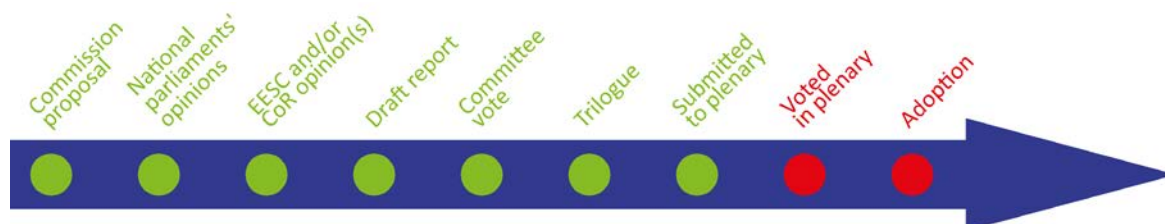
OVERVIEW

To enhance EU external border management and internal security, the European Commission has made several proposals to upgrade and expand European border and security information systems. As part of a broader process to maximise their use, the Commission presented legislative proposals for two regulations in December 2017 (amended in June 2018), establishing an interoperability framework between EU information systems on borders and visas, and on police and judicial cooperation, asylum and migration. The proposals, agreed by the co-legislators on 5 February 2019, are scheduled for plenary vote in March 2019. They aim to provide competent authorities with fast, efficient, systematic and controlled access to the information they need. The new rules would improve checks at the EU's external borders, allowing to better detect security threats and identity fraud, as well as help preventing and combating irregular migration.

A: Proposal for a regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226, Regulation (EU) 2018/1240, Regulation (EU) 2018/1861 and Regulation (EU) 2018/1726

B: Proposal for a regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) and amending [Regulation (EU) 2019/XX [the Eurodac Regulation], Regulation (EU) 2018/1862, Regulation (EU) 2019/XX [the ECRIS-TCN Regulation] and Regulation (EU) 2018/1726

<i>Committee responsible:</i>	Civil Liberties, Justice and Home Affairs (LIBE)	A: COM(2017) 793, 12.12.2017 amended by COM(2018) 478, 13.6.2018 2017/0351 (COD)
<i>Rapporteurs:</i>	A: Jeroen Lenaers (EPP, the Netherlands) B: Nuno Melo (EPP, Portugal)	B: COM(2017) 794, 12.12.2017 amended by COM(2018) 480, 13.6.2018 2017/0352 (COD)
<i>Next steps expected:</i>	First-reading votes in plenary	Ordinary legislative procedure (COD) (Parliament and Council on equal footing – formerly 'co-decision')



Introduction

As emphasised in the 2015 European agendas on [migration](#) and [security](#), addressing current EU migration and security challenges means strengthening the management of external borders, including by making better use of the opportunities information systems and technologies (IT) offer. Both the [Parliament](#) and [Council](#) have expressed the need to make better use of the European information systems in the fields of borders and security, and have called on the Commission to put forward proposals to improve these systems, not least by making them more interoperable. The [joint declaration](#) on the EU's legislative priorities for 2018-2019 identified enhancing EU information system interoperability as a key priority.

In its [2018 work programme](#), the Commission stated: 'we will reinforce our efforts to make the European Union a safer society, in full compliance with fundamental rights, with a proposal on the interoperability of information systems'. In its seventh [report](#) on progress towards an effective and genuine security union, of May 2017, the Commission stated that improving interoperability between information systems constituted a key dimension of its new approach to the management of data for border management and security.

'Interoperability means the ability of information systems to talk to each other. It is about a targeted and intelligent way of using existing data to best effect, without creating new databases or changing the access rights to existing information systems'.¹

To improve EU information systems in the area of borders and security, and to cover the existing information gaps, the Commission put forward a number of legislative proposals with regard to:

- extending the European Criminal Records Information System ([ECRIS](#)) to include third-country nationals and to create a centralised [ECRIS-TCN](#) database (agreement between the Parliament and the Council confirmed by plenary vote on 12 March 2019);
- establishing the entry/exit system ([EES](#)) (regulation entered into force in December 2017) – providing for the interconnection between the EES and the visa information system ([VIS](#)) (European Parliament first reading position adopted in plenary on 13 March 2019);
- reviewing the [Eurodac](#) Regulation for fingerprinting migrants to facilitate returns and help tackle irregular migration (provisional agreement between the Parliament and the Council reached on 19 June 2018 and expected to be voted in plenary in April 2019);
- developing the European travel information and authorisation system ([ETIAS](#)) (entered into force in October 2018);
- extending the use of the Schengen information system ([SIS II](#)) (entered into force in December 2018);
- extending the mandate of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice ([eu-LISA](#)) (adopted regulation entered into force on 11 December 2018).

In December 2017, the Commission announced an interoperability package, including a [proposal](#) on establishing a framework for interoperability between EU information systems on borders and visa and a second [proposal](#) on interoperability in the area of police and judicial cooperation, asylum and migration. The two proposals have many provisions in common but had to be kept separate, owing to the differing legal bases for cooperation in each field.² As stated in the proposals, the Commission aims to achieve interoperability by the end of 2023. To align the future regulations with the recently adopted legal instruments – ETIAS, SIS II, eu-LISA and ECRIS-TCN, two amending proposals were published by the Commission in June 2018. The new proposals did not include amendments relating to Eurodac, as its current architecture is not suitable for interoperability.

Existing situation

In its [communication](#) on stronger and smarter information systems for borders and security, of 6 April 2016, the Commission identified a series of key shortcomings in the existing information systems in the area of borders and security: partial utilisation of the existing information systems; suboptimal functionalities and technical limitations; gaps in the EU informational architecture; a complex legal and policy landscape; overall fragmentation of EU data management architecture and limited interoperability between information systems. On the same occasion, the Commission announced that it would start working, together with eu-LISA, towards establishing a single-search interface allowing simultaneous searches in all relevant systems without changing access rights.

The [impact assessment](#) accompanying the interoperability proposals identified two major problems relating to: (1) the type and quality of information provided by the EU information systems, which is not always complete, accurate and reliable and thus makes it difficult to detect multiple identities and to combat identity fraud; and (2) the legal and technical barriers to end-users accessing the systems, meaning that some authorities do not have fast and systematic access to all the information they need in order to perform their tasks.

The study identified four drivers of these problems: (1) inadequate organisation of access to information systems; (2) an imbalance between law enforcement access safeguards and operational needs; (3) restrictive interpretation of the purpose of border management systems; and (4) repeat and separate storage of personal data in different systems.

Parliament's starting position

The European Parliament has repeatedly called for more efficient and effective use of information systems for borders and security, provided that appropriate safeguards on data protection and privacy are maintained.

In its [resolution](#) of 17 December 2014 on renewing the EU's internal security strategy, the Parliament urged Member States to make better use of valuable existing instruments, including through 'more expeditious and efficient sharing of relevant data and information, subject to the appropriate data protection and privacy safeguards'.

In its [resolution](#) of 11 February 2015 on anti-terrorism measures, the Parliament expressed 'the need to improve, intensify and accelerate global law enforcement information sharing', adding that 'all data collection and sharing, including by EU agencies such as Europol, should be compliant with EU and national law and based on a coherent data protection framework'.

In its [resolution](#) of 6 July 2016 on the strategic priorities for the Commission work programme 2017, the Parliament called on the Commission to present 'proposals to improve and develop existing information systems, address information gaps and move towards interoperability' accompanied by necessary data protection safeguards.

In July 2017, the Parliament established a special committee on terrorism ([TERR](#)) to work inter alia on 'addressing the deficiencies and gaps in cooperation and information exchange between national law enforcement authorities, as well as the interoperability of European information sharing databases'. In its final [report](#), adopted in November 2018, the TERR committee called among other things for the full implementation of relevant databases, for working towards interoperability and for the introduction of biometric checks so as to contribute to the fight against identity fraud.

Council and European Council starting position

In its [strategic guidelines for freedom, security, and justice](#) of June 2014, the **European Council** called for the link between the EU's internal and external policies to be improved by 'intensifying operational cooperation while using the potential of information and communication technologies' innovations, enhancing the role of the different EU agencies and ensuring the strategic use of

EU funds'. In its [conclusions](#) of 15 December 2016, the European Council called for 'continued delivery on the interoperability of information systems and databases'. The European Council [conclusions](#) of 22-23 June 2017 emphasised that 'swift and targeted exchanges of information between law enforcement authorities' and improved interoperability between databases are essential for enhancing internal security and invited the Commission to prepare draft legislation on interoperability as soon as possible.

In its [conclusions](#) on the renewed European Union internal security strategy of 10 June 2015, the **Council** called for action to improve 'information exchange and accessibility, especially by ensuring the interoperability of different information systems'. In June 2016, the Council put forward a [roadmap](#) to enhance information exchange and information management, including interoperability solutions in the area of justice and home affairs. The roadmap emphasised the need to fully implement and use the existing information exchange instruments and to ensure the effective interconnectivity of European initiatives with national processes. It envisaged an enhanced role for eu-LISA, in particular in developing a central monitoring capacity for data quality, pursuing interoperability solutions, and ensuring compliance with data protection and data security standards.

Preparation of the proposals

Increasing the exchange of information in the areas of borders and security was highlighted as a priority measure in the European Council's [strategic guidelines for freedom, security, and justice](#) and in the [European agenda on security](#). The Commission [communication](#) on stronger and smarter information systems for borders and security of 6 April 2016, identified a number of key shortcomings of EU's information systems and explored ways that existing and future information systems could enhance external border management and internal security.

In June 2016, the Commission established a High-Level Expert Group on Information Systems and Interoperability ([HLEG](#)) to address the legal, technical and operational challenges posed by different interoperability options. In its [final report](#) of May 2017, the HLEG recommended focusing on three interoperability solutions: (1) a European search portal; (2) a shared biometric matching service; and (3) a common identity repository.

In its May 2017 seventh progress [report](#) towards an effective and genuine security union, the Commission set out a new approach to the management of data for borders and security. This approach is built on three pillars: maximising the benefits of existing information systems by making full use of these systems; developing new systems and complementary actions to address gaps in the EU's data management structure; and improving the interoperability of information systems.

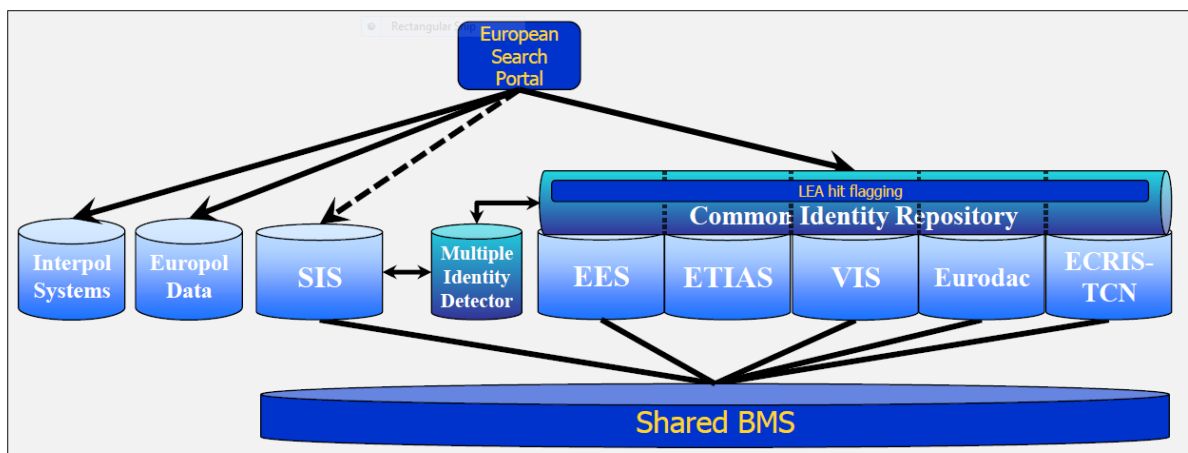
In June 2017, the Commission presented a [proposal](#) to revise the eu-LISA mandate. The proposal aims to expand the agency's mandate to enable it to secure the centralised operational management of existing and future information systems and to develop technical means to achieve interoperability between these systems.

In July 2017, the Commission launched an [inception impact assessment](#) on interoperability, seeking to inform and receive feedback from stakeholders and citizens. A [public consultation](#) on the Commission's proposed approach gathered [18 responses](#). The interoperability proposals, presented in December 2017, were accompanied by an [impact assessment](#) study and three feasibility studies on the issues of the [European search portal](#), the shared [biometric matching service](#), and the [common identity repository](#). The Commission also organised a series of stakeholder workshops with representatives of Member States and Schengen associated countries, the EU counter-terrorism coordinator, the European Data Protection Supervisor (EDPS), relevant EU agencies, the General Secretariat of the Council and the secretariat and advisors to the LIBE Committee, as well as various Commission departments. A tripartite technical meeting between the Commission, the Parliament and the Council was held in November 2017. EPRS completed an [initial appraisal](#) of the Commission's impact assessment in February 2018.

The changes the proposals would bring

The two interoperability proposals concern the three existing centralised EU information systems for borders and security ([SIS](#), [VIS](#), and [Eurodac](#)), and other centralised systems that have been proposed or are under development (the [EES](#), [ETIAS](#), and [ECRIS-TCN](#)). They also concern Interpol's stolen and lost travel document ([SLTD](#)) database, Interpol's travel documents associated with notices ([TDAWN](#)) database and [Europol](#) data, as far as the latter are relevant for the functioning of the ETIAS. The scope of the [proposal](#) on establishing a framework for interoperability between EU information systems for borders and visa is limited to VIS, SIS, the new EES and ETIAS, whereas the [proposal](#) on police and judicial cooperation, asylum and migration applies to Eurodac, SIS and the future ECRIS-TCN, as well as to Europol data.

Figure 1 – Proposed technical components (both interoperability proposals)



Source: [European Commission](#).

The proposals introduce new elements to make more intelligent and targeted use of the information available in the existing and future systems, which will allow the relevant authorities to carry out effective checks, detect multiple identities and counter identity fraud. The Commission has proposed four technical components to achieve interoperability (see figure 1):

- a **European search portal (ESP)** that would allow simultaneous searches of all relevant information systems to obtain the results of all checks on a single computer screen; the portal would not store or process any new data and would not change users' access rights;
- a **shared biometric matching service (BMS)** that would enable the querying and comparison of biometric data (fingerprints and facial images) from several central systems, in particular, SIS, Eurodac, VIS, the new EES and the future ECRIS-TCN;
- a **common identity repository (CIR)** that would store basic biographical (such as names and dates of birth) and biometric information on third-country nationals recorded in Eurodac, VIS, the EES, ETIAS and the future ECRIS-TCN, to enable effective identity checks of these persons on the territory of a Member State;
- a **multiple-identity detector (MID)** that would enable the correct identification of persons and the discovery of identity fraud and multiple identities; it would cover the systems that store data in the common identity repository, as well as SIS.

The proposals define a **two-step approach** to granting law enforcement authorities access to the information systems that have only a secondary law enforcement objective (the EES, VIS, ETIAS and Eurodac), linked to searches related to preventing, investigating, detecting or prosecuting serious crime or terrorism. Initially, searches would be carried out on a 'hit/no hit' basis. Subsequently, if a

'hit' were generated, law enforcement authorities would be able to request access to the information needed, in line with the respective rules and safeguards.

The proposals also provide for the establishment of a central repository for reporting and statistics (CRRS), to enable the creation and sharing of reports with anonymous statistical data. Moreover, the proposals include provisions for the development of a universal message format (UMF) as an EU standard for structured cross-border information exchange between information systems, authorities and/or organisations in the field of justice and home affairs. Such a standard would guarantee easier integration and interoperability with systems, in particular for Member States needing to build interfaces to communicate with these new systems. The proposals furthermore introduce the concepts of automated data quality control mechanisms and common quality indicators, and the need for Member States to ensure the highest level of data quality when feeding and using the systems.

With regard to fundamental rights, the proposals state that 'the proposed interoperability solutions are complementary components to existing systems' and 'as such, they do not alter the balance already ensured by each of the existing central systems as regards their positive impact on fundamental rights'. The Commission acknowledges that interoperability has the potential to have an 'indirect impact on a number of fundamental rights', such as on the right to respect for private life, the right to dignity and the right to the protection of personal data. However, it also highlights several positive impacts on fundamental rights, such as on preventing identity confusion, detecting missing children, and supporting the implementation of the right to asylum. The proposals are also 'based on the principles of data protection by design and by default' and include 'provisions limiting data processing to what is necessary for the specific purpose' and granting data access only to those entities that 'need to know'.

Budget

The initial proposal was based on the assumption that the co-legislators would adopt the legal framework by the end of 2018. In that case, the development period for the different interoperability components would run from 2019 to 2023 inclusive, followed by full-scale operations. In the [financial statement](#) attached to the revised proposals from June 2018, the Commission estimates the financial impact of the initiative over the 2019-2027 period. The total budget required amounts to €461 million over nine years and covers the following costs:

- €261.3 million for eu-LISA;
- €136.3 million for Member States;
- €48.9 million for Europol;
- €4.8 million for the European Border and Coast Guard Agency (Frontex);
- €2 million for the European Union Agency for Law Enforcement Training (CEPOL);
- €7.7 million for the European Commission's Directorate-General for Migration and Home Affairs (DG HOME).

Advisory committees

The European Economic and Social Committee (EESC) adopted its [opinion](#) on the two proposals on [23 May 2018](#). The EESC considers interoperability between EU information systems for borders and visas and for police and judicial cooperation, asylum and migration to be 'a strategic objective for the EU'. The Committee, however, fears that the proposed measures do not fully safeguard the fundamental and data protection rights of the people concerned, and that they might create new barriers to the normal flow of passengers and freights. It therefore calls for the procedures and guarantees regarding the use of data for law enforcement purposes to provide for the application of the EU General Data Protection Regulation (GDPR), recommends more training opportunities for supervisory authorities throughout the EU and pleads for an annual reporting exercise on the security of the interoperability components and a biannual reporting exercise on the impact of the

measures on fundamental rights. The EESC also expressed concerns about the funding for the new system and recommends a follow-up to the planning in order to ensure budget compliance. Should abuse of the system threaten freedom and fundamental rights, the Committee considers that the possibility to halt the project should be included. The European [Committee of the Regions](#) decided not to adopt an opinion on the proposals.

National parliaments

The deadline for the submission of reasoned opinions on the grounds of subsidiarity was set for 16 April 2018 for the initial proposals on [borders](#) and on [law enforcement and migration](#) respectively. In the first period, no Member State expressed concerns regarding the subsidiarity principle. [Contributions](#) to both proposals were received from the Portuguese Parliament, the Spanish Congress of Deputies, the Romanian Senate and the Czech Republic's Senate and Chamber of Deputies. The latter recalled the importance of reaching a balance between the effectiveness of the system and the level of personal data protection, whereas the Czech Senate called for effective financial planning and spending during the implementation period, as well as for sufficient time to be allowed for the adaptation of national systems. Following the publication of amended proposals in June 2018, a new deadline was fixed for 12 October 2018. [France, Spain and Ireland](#) were the only three countries to send in contributions on that occasion. France expressed hopes that the interoperability will be operational by 2020-2021. Ireland, in a reasoned opinion, said that the proposals did not comply with the principle of proportionality.

Stakeholders' views³

In its statement [annexed](#) to the HLEG's final report on information systems and interoperability, the **European Data Protection Supervisor (EDPS)** maintained that it 'is not in a position to endorse all the conclusions referred to by the high-level expert group in its final report' because 'full compliance with data protection requirements can ... only be assessed having a comprehensive and further detailed picture of the measures and solutions envisaged by the group'. The EDPS endorsed the idea of establishing a central single search interface 'as long as this solution fully complies with purpose limitation and access rights', but warned that 'a common (and centralised) identity repository raised serious issues in terms of data protection'. In its [reflection paper](#) on the interoperability of information systems, presented in November 2017, the EDPS stated that as 'introducing interoperability is likely to imply new (or changed) personal data processing, such changes would require a clear basis in legislation in full compliance with the EU Charter of Fundamental Rights' and that any 'new or modified data processing would need to be clearly defined in the relevant legal instrument and be equally necessary and proportionate in relation to its clearly stated objectives'. In its [opinion](#) of 16 April 2018, the EDPS added that the decision to make large scale IT systems interoperable 'is not primarily a technical choice' but 'a political choice' that would mark 'a point of no return'. The proposals would namely 'introduce new possibilities to access and use the data stored in the various systems in order to combat identity fraud, facilitate identity checks, as well as streamline access to non-law information systems⁴ by law enforcement authorities'. They would also create a new centralised database, with a risk to harm 'a potentially very large number of individuals' in case of a data breach. According to the EDPS, it 'would not be acceptable' that genuine fundamental rights safeguards be removed to speed up the procedure. Given the complexity of the proposed system both in legal and technical terms and the potential implications for the rights and freedoms in the EU, the EDPS calls for a wider debate on the future of EU information exchange, its governance and the ways to safeguard fundamental rights in this context.

In its [statement](#) annexed to the HLEG's final report, the **European Union Agency for Fundamental Rights (FRA)** stated that 'interoperability should not lead to the processing of more – biometric or alphanumeric – data than necessary for the existing purposes under the individual legal instruments'. Given that data stored in information systems may not always be accurate, there is an important need to uphold the right to effective remedies. While enhanced interoperability may help with identifying missing children, detecting identity fraud, while also reducing the risk of the

apprehension, detention or return of persons in need of international protection, interoperability may have a disproportionate impact on certain persons, such as irregular migrants, and increase the risk of discriminatory profiling. In July 2017, FRA published a [report](#) on fundamental rights and the interoperability of EU information systems, which highlights the key fundamental rights issues and discusses ways to address them. Another [report](#) on the findings of the FRA research project on the processing of biometric data in large-scale information technology systems established in the EU to manage asylum and migration was published in March 2018. Following a request from the European Parliament of 28 March 2018, FRA adopted an [opinion](#) on the fundamental rights implications of the two interoperability proposals on 11 April 2018, to be read together with the opinion of the EDPS. The opinion focuses in particular on the CIR and MID because these components were not yet fully conceptualised at the time of the Agency's July 2017 report. FRA questions the starting point of the proposals, namely that interoperability does not affect access rights to the data held in the underlying IT systems and calls for 'careful analysis to assess whether or not it can be justified to make these additional data visible to authorities who would otherwise not have access to these (data) in light of the principle of purpose limitation enshrined in Article 8 of the Charter of Fundamental Rights of the EU'. The agency also highlights several fundamental rights set out in the Charter that are affected or given 'little visibility' in the proposals, such as the rights to respect for private and family life (Article 7), to protection of personal data (Article 8), to asylum (Article 18), to an effective remedy and to fair trial (Article 47), as well as to protection in the event of removal, expulsion or extradition (Article 19) and the rights of the child (Article 24). FRA furthermore states that there are 'possible longer-term implications of interoperability', since the proposals are meant to serve as the basis for future developments. This would 'raise very serious and new necessity and proportionality questions'. Given that several of the affected IT systems are under preparation or revision, the agency finally calls for 'strong ex-post evaluations'.

In October 2017, the **European Border and Coast Guard Agency (Frontex)** presented a [non-paper](#) on the agency's access to EU information systems for borders and security, in which it asked for greater access to databases under the upcoming interoperability proposals.

The Article 29 Data Protection Working Party (WP29) – an advisory body on data protection and privacy that was composed of a representative from the data protection authority of each EU Member State, a representative from the European Data Protection Supervisor and from the European Commission, and replaced by the European Data Protection Board (EDPB) from 25 May 2018 – agreed with several of the points raised by other stakeholders. In its [opinion](#) of 11 April 2018, WP29 calls for 'an analysis of less intrusive means to reach the goals set in these proposals ... to justify the choices made and ensure the respect of the purpose, necessity and proportionality principles'. WP29 also asks for 'stronger data protection safeguards' and 'enhanced legal certainty' as to the functioning of the new databases.

On 22 June 2018, the Data Protection Authorities (DPAs) supervising SIS II, VIS and Eurodac issued an [opinion](#) on the two interoperability proposals, pointing to the misleading nature of the term 'interoperability' and warning against the serious impact the interconnection of information systems can have from a data protection perspective. The DPAs also focus on the 'likely impact' on the legal frameworks of the IT systems that are currently under preparation or revision: 'Systems will be adjusted to accommodate for the interconnection, instead of being considered based on their own real purpose'. In order to 'allow a consistent, effective and independent supervision', they call for more financial and human resources.

The Meijers Committee – group of experts on international immigration, refugee and criminal law – takes a similar view in a [comment](#) published on 19 February 2018 on the proposal for interoperability between EU information systems on police and judicial cooperation, asylum and migration, stating that 'the proposal adds another difficult and technically very complicated supervision task to the long list of tasks' of the DPAs. The committee also raises questions with regards to the 'necessity and proportionality of the differential treatment between ... EU citizens and ... third country nationals' and warns against 'the risk of discrimination of third country nationals and

of persons of racial or ethnic origin'. In line with the subsequent FRA opinion of 11 April 2018, the Meijers Committee calls for an assessment of the principle of proportionality of access, because 'on the basis of the proposal, every designated authority of Member States will be able, via the European Search Portal, to learn about the fact that information on a third-country national is stored in one of the EU databases. ... Even if access to the personal file in this database is not allowed because of lack of authorisation, the authority will have gained knowledge of the existence of the file ... which in itself can be an interference with the right to data protection'.

Legislative process

The two interoperability proposals ([COM\(2017\) 793](#) and [COM\(2017\) 794](#)) were published on 12 December 2017. On 13 June 2018, the European Commission issued two amending proposals, [COM\(2018\) 478](#) and [COM\(2018\)480](#), to insert the necessary amendments for recently adopted or agreed legal instruments (ETIAS, SIS, eu-LISA) and for the text, as it stood on 31 May 2018, for ECRIS-TCN. Amendments to Eurodac were not included, in the absence of agreement on the 2016 proposal and due to the technical incompatibility of the current system. The Commission intends to present additional amendments related to the interoperability proposals once the co-legislators reach a formal agreement on an upgraded Eurodac database.

Within the European Parliament, the proposals on establishing a framework for interoperability between EU information systems (and the corresponding amending proposals) have been assigned to the LIBE committee, with Jeroen Lenaers (EPP, the Netherlands) rapporteur on the borders and visa proposal, and Nuno Melo (EPP, Portugal) rapporteur for the police and judicial cooperation, asylum and migration proposal. Two committees were asked to submit their opinion: the Committee on Foreign Affairs (AFET) and the Committee on Budgets (BUDG). The AFET committee decided not to give an opinion on either proposal. The BUDG committee (rapporteur: Bernd Kölmel (ECR, Germany)) issued its opinions on 20 June 2018. It welcomed the two proposals on interoperability as well as the fact that there were no overlaps with the budget requests under other recent legislative proposals in this area, and considered the estimated cost to the EU budget to be justified and proportionate.

Following preparatory work within the LIBE committee, including a series of meetings with experts from eu-LISA, Europol, Frontex, FRA and the EDPS, the rapporteurs presented their draft reports on [11 June 2018](#). Updated versions of the draft reports, taking into account the June 2018 amended proposals, were published on 24 July 2018. Nearly 2 000 amendments were tabled for the two interoperability files and discussed during the LIBE committee meeting of [3 September 2018](#). Although most of the political groups in Parliament agreed that interoperability is a technical necessity, several expressed concerns with regard to the principle of proportionality when it comes to fundamental rights and data protection. Issues mainly concerned the common identity repository, the shared biometric matching service and the multiple-identity detector. Whereas most expressed understanding of the political urgency to finalise the legislative procedure before the European elections in May 2019, others warned against excessive haste.

The LIBE committee [adopted](#) the two reports on interoperability on 15 October 2018. The [report](#) on borders and visa was adopted by 45 votes to 10, with no abstentions, and the [report](#) on police and judicial cooperation, asylum and migration was adopted by 45 votes to 9, also without abstentions. The LIBE committee recommended that the Commission's proposals be amended so its main elements would: enhance the effectiveness and efficiency of border checks at the external borders; contribute to preventing and tackling irregular migration; contribute to the prevention, detection and investigation of terrorist offences or of other serious criminal offences; and aid in the identification of unknown persons who are unable to identify themselves or unidentified human remains in cases of natural disasters or terrorist attacks. LIBE Members called, among other things, for all data protection rules to be applicable to all information systems, and for data subjects to be provided with a single web service through which they can exercise their rights to access, as well as rectification, erasure and restriction of their personal data. Changes were also made so that the

identity of a person is first established on the basis of the identity or travel document, following the rules and procedures provided for in national law, before it is possible to launch a search in the common identity repository (CIR) using the biometric data of the person concerned. The CIR should furthermore only be consulted for the purpose of identifying a person if the person concerned is physically present during the check. The LIBE committee also called for the new regulations not to modify the rights of access as set out in the legal basis of each European information system. Moreover, amendments were introduced to provide for a transitional period including training programmes for end-users as well as for better monitoring and evaluation of the future system.

Within the Council, the working party on information exchange and data protection (DAPIX) began [examining](#) the proposals in January 2018. The main issues under discussion related to the functioning of each of the interoperability components, the expected data workflow and the overall interoperability architecture, as well as its roll-out, the implications of interoperability components for the current technical set-up at national level and for the response times at borders, and the practical functioning of user profiles and access rights. The Commission organised two technical workshops to discuss these issues on 14 February and 16 March 2018. Europol, Frontex and eu-LISA were invited to some of the Council working party meetings to answer specific operational questions. The [general approach](#) was [endorsed](#) by the Permanent Representatives Committee (Coreper), on behalf of the Council, on 14 June 2018, to serve as a mandate for negotiations with the European Parliament. The common position reached by the Member States approves the creation of the different interoperability components and adds a number of amendments related to the technical features of the system. It aims to ensure the smooth running of the system through business continuity solutions. The Council also made terminological changes, replacing references to third-country nationals with the more general term, 'persons', and those to law enforcement authorities with the wider term 'designated authorities', while the term 'fingerprints' is replaced by 'dactyloscopic data'. Several amendments concern Europol access to EU information systems. Following the publication of the amending proposals in June 2018, the Council adopted a [revised mandate](#) in September 2018. Further changes were mostly of a technical nature and aimed to correct some errors or oversights.

On 24 October, MEPs gave the green light to start trilogue negotiations with the Council. Trilogue meetings took place on 24 October 2018, 15 and 17 November 2018, 13 December 2018 and on 5 February 2019. The December trilogue meeting allowed the main political issues to be solved, such as the methods and procedure for accessing data in the common identity repository. A [provisional agreement](#) between the Council Presidency and the Parliament negotiators was reached during the final trilogue meeting in February, after the remaining disagreements – including on the system's entry into force – were solved. It was agreed not to set a strict deadline in order to give the Member States the time to implement the changes. More specifically, the provisions of the regulations related to the technical components (the ESP, the BMS, the CIR and the MID), the automated data quality control mechanisms and procedures, the common data quality indicators and the minimum quality standards, as well as to the central repository for reporting and statistics (CRRS) will apply from a date to be determined by the Commission, with a few exceptions, as described in Article 69. The final provisions furthermore establish transition periods for the use of the ESP, CIR and MID after entry into force of the regulations. The provisions relating to Eurodac will also apply only from the date the recast of its current regulation becomes applicable.

Several demands of Parliament in relation to data protection safeguards were incorporated, such as: not to change the access rights for each information system; to put in place a dedicated web service to facilitate the exercise of their rights by persons whose data are processed; and to provide end-users (staff authorised to process data) with a training programme about data security, data quality and data protection rules. It was moreover agreed that the Commission will have to keep the Parliament and Council informed, by means of an annual report, about the progress of the preparations for the full implementation of the regulations. The report will also have to include detailed information about the costs incurred and about any risks that may impact the overall costs.

Once the system becomes operational, the Commission will have the obligation to produce, based on eu-LISA reports, overall evaluations of the different interoperability components, assessing the validity of their underlying rationale and their security, the results achieved and the impact on fundamental rights, including on the right to non-discrimination.

The Permanent Representatives Committee ([Coreper](#)) confirmed the agreement on behalf of the Council on 13 February 2019. On the Parliament's side, the [LIBE committee](#) approved the provisional agreement on 19 February 2019, with 43 votes in favour, 11 against and no abstentions for the borders and visa file, and with 44 votes in favour, 10 against and no abstentions for the police, judicial cooperation, asylum and migration file. The agreed texts now need to be formally approved by the Parliament as a whole (the vote is scheduled for the March II plenary session) and by the Council. The regulations will enter into force 20 days after their publication in the Official Journal of the EU.

EP SUPPORTING ANALYSIS

Radjenovic A., [EU policies - Delivering for citizens: Protection of EU external borders](#), EPRS, European Parliament, December 2018.

Jurviste U., [European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice \(eu-LISA\)](#), EU Legislation in Progress briefing, EPRS, European Parliament, December 2018.

Atanassov N., [Revision of the Schengen Information System for law enforcement](#), EPRS, European Parliament, October 2018.

Atanassov N., [Revision of the Schengen Information System for border checks](#), EPRS, European Parliament, October 2018.

Atanassov N., [Use of the Schengen Information System for the return of illegally staying third-country nationals](#), EPRS, European Parliament, October 2018.

Radjenovic A., [European Travel Information and Authorisation System \(ETIAS\)](#), EPRS, European Parliament, October 2018.

Bakowski P. and Van Ballegooij W., [The fight against terrorism](#), EPRS Cost of Non-Europe Report, May 2018.

[Interoperability of Justice and Home Affairs Information Systems](#), Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, April 2018.

[The future of the Schengen area: latest developments and challenges in the Schengen governance framework since 2016](#), Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, March 2018.

Eisele K. [Interoperability between EU information systems for security, border and migration management](#), Initial Appraisal of a European Commission Impact Assessment, EPRS, European Parliament, February 2018.

Orav A. and D'Alfonso A., [Smart Borders: EU Entry/Exit System](#), EPRS, European Parliament, January 2018.

Dumbrava C., [Interoperability of European information systems for border management and security](#), European Parliament, June 2017.

Dumbrava C., [European information systems in the area of justice and home affairs: An overview](#), European Parliament, EPRS, May 2017.

Orav A., [Recast Eurodac Regulation](#), EU Legislation in Progress Briefing, EPRS, European Parliament, March 2017.

Dalli H., [Exchange of Information on Third Country Nationals – European Criminal Records Information System \(ECRIS\)](#), Initial Appraisal of a European Commission Impact Assessment, EPRS, European Parliament, March 2016.

OTHER SOURCES

[Interoperability between EU information systems \(borders and visa\)](#), European Parliament, Legislative Observatory (OEIL).

[Interoperability between EU information systems \(police and judicial cooperation, asylum and migration\)](#), European Parliament, Legislative Observatory (OEIL).

ENDNOTES

- ¹ [Security Union - Closing the information gap](#), Factsheet, European Commission, 5 February 2019.
- ² Even though both proposals have common legal bases (Articles 16(2) and 74 TFEU), their main legal bases differ according to the objectives pursued. The proposal on borders and visas is based on Article 77(2)(a) (b) (d) and (e), while that on police cooperation, asylum and migration is based on Article 78(2)(e), Article 79(2)(c), Article 82(1)(d), Article 85(1), Article 87(2)(a) and Article 88(2).
- ³ This section aims to provide a flavour of the debate and is not intended to be an exhaustive account of all different views on the proposal. Additional information can be found in related publications listed under 'EP supporting analysis'.
- ⁴ Databases containing information obtained by authorities for purposes other than law enforcement.

DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

© European Union, 2019.

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

<http://epthinktank.eu> (blog)



Second edition. The 'EU Legislation in Progress' briefings are updated at key stages throughout the legislative procedure.