

Interoperability between EU border and security information systems

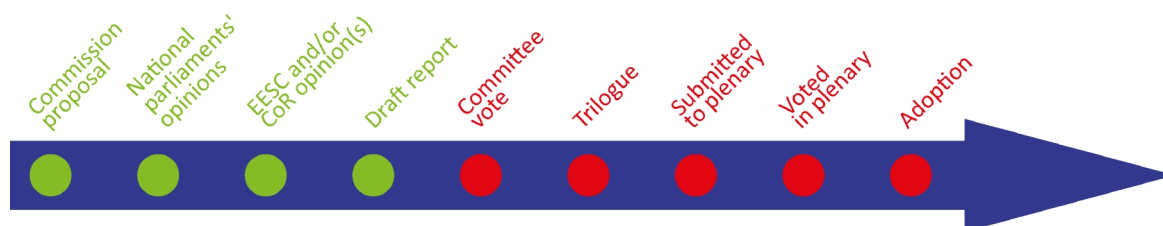
OVERVIEW

To strengthen EU external border management and enhance 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 seek effective and efficient information exchange and data sharing between EU information systems, by providing fast, seamless, efficient, systematic and controlled access to all the data authorities need to accomplish their tasks.

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/XX [the Regulation on SIS in the field of border checks] and Regulation (EU) 2018/XX [the eu-LISA Regulation]

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) 2018/XX [the Eurodac Regulation], Regulation (EU) 2018/XX [the Regulation on SIS in the field of law enforcement], Regulation (EU) 2018/XX [the ECRIS-TCN Regulation] and Regulation (EU) 2018/XX [the eu-LISA Regulation]

<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>	Committee votes	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.

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 (ongoing negotiations);
- establishing the entry/exit system ([EES](#)) – providing for the interconnection between the EES and the visa information system (VIS) (EES Regulation adopted in November 2017);
- 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);
- developing the European travel information and authorisation system ([ETIAS](#)) (Regulations – including the necessary amendments to the [Europol Regulation](#) – adopted in September 2018);
- extending the use of the Schengen information system ([SIS II](#)) (European Parliament first-reading vote, following agreement on the text in trilogue, planned for October 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](#)) (agreed text adopted at first reading by the European Parliament in July 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 establishing a framework for interoperability between EU information systems on 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.¹ 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 or agreed legal instruments (namely, ETIAS, SIS II and eu-LISA) and the [provisional text](#) of ECRIS-TCN, two amending proposals were published by the Commission (one for each of the initial proposals) in June 2018. The new proposals do not include amendments relating to Eurodac, as its current architecture is not suitable for interoperability.

¹Interoperability is the ability of information systems to exchange data and enable sharing of information. It improves the efficiency and effectiveness of Europe-wide information-sharing tools, by ensuring the technical processes, standards and tools that allow EU information systems to work better together'.²

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'.

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 interoperability of information systems for borders and security was highlighted as a priority measure 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.

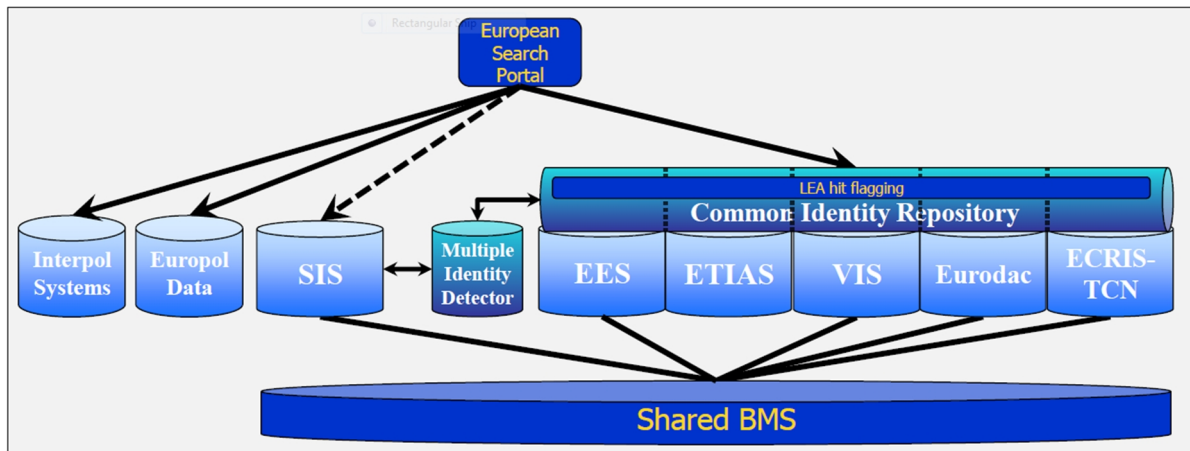
In its May 2017 seventh progress [report](#) towards an effective and genuine security union, the Commission set out a new approach to the management of data for borders and security. This approach is built on three pillars: maximising the benefits of existing information systems by making full use of 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

Figure 1 – Proposed technical components (both interoperability proposals)



Source: [European Commission](#).

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 proposed 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 the future ETIAS, whereas the proposal on police and judicial cooperation, asylum and migration applies to Eurodac, SIS and the proposed ECRIS-TCN, as well as to Europol data.

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 proposed 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 proposed 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, 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

On the assumption that the co-legislators will adopt the legal framework by the end of 2018, 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.

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'.

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 – the standing committee of experts on international migration, 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'.

The Article 29 Data Protection Working Party (WP29) – an independent European advisory body on data protection and privacy, 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.

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.

Academic views

In an April 2018 [study](#) carried out at the request of the LIBE committee, the authors concluded that the proposals 'do not propose a framework for interoperability, but instead propose technical solutions' and thus called for 'much greater clarity' regarding the definition of interoperability. They also stated that the proposals 'lack supporting evidence' to explain the needs for interoperability and 'lacks clarity' on the objectives of the proposals and the design of the proposed solutions. The study highlights the implications for fundamental rights, such as privacy and data protection, but also the rights of the child or the right of non-discrimination, as well as the potential risks for data security.

Another [research paper](#), examining the interoperability proposals against the background of the CJEU's case law on data retention, concluded that the proposed system of interoperable databases raises a fundamental concern in terms of data protection, namely the circumvention of the [purpose limitation principle](#). As the 'interoperability will fundamentally change the current architecture of EU large-scale IT-systems and introduce a shift from separated silos to an interconnected framework', there might be an increased risk of 'function creep', i.e. a widening of the purpose for which data processing is undertaken. Another risk to mitigate is 'discriminatory profiling', in order to avoid creating different standards for EU and third-country nationals. For interoperability to comply with the legal framework and the requirements of the CJEU, 'non-discrimination standards, the security and integrity of personal data, oversight mechanisms, transparency requirements and rights for data subjects' must be respected.

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 during a joint debate held on [11 June 2018](#). Updated versions of the draft reports, taking into account the June 2018 amended proposals, were published on 24 July 2018. In their draft texts, the rapporteurs aimed to strike a balance between the need to enhance security and protect borders

and the need to limit interference with fundamental rights to what is strictly necessary and proportional. They introduced a number of amendments aimed at avoiding cumbersome procedures at borders and facilitating the work of border guards, ensuring the smooth functioning of the interoperability components and creating proper back-up systems, clarifying the access rights and procedure for law enforcement officers and introducing stronger monitoring and evaluation clauses.

By 23 July 2018, no less than 1 012 amendments had been tabled for the borders and visa file, and 926 amendments for the file on the area of police and judicial cooperation, asylum and migration. The consideration of amendments took place during a joint debate in 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 vote on the two draft reports on the interoperability proposals is planned for October 2018.

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. During the meetings held in April and May, [discussions](#) continued on issues such as whether there is a need to make substantial changes to the Entry-Exit System in relation to interoperability, the data retention periods, the necessity to add data to SIS in case a link between information systems is established, the obligation to keep logs of all data-processing operations and what information on end-users should be available at what level. 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 are mostly of a technical nature and aim to correct some errors or oversights. The Council aims to reach an agreement with the European Parliament by the end of 2018.

EP SUPPORTING ANALYSIS

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.

Atanassov N. and Radjenovic A., [EU asylum, borders and external cooperation on migration: Recent developments](#), EPRS, European Parliament, September 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.

Scherrer A. [Revision of the Visa Code \(Regulation 810/2009\) and Visa Information System \(Regulation 767/2008\)](#), Implementation Appraisal, EPRS, 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.

Dumbrava C., [European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice \(eu-LISA\)](#), EPRS, European Parliament, January 2018.

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

Voronova S., [Combating terrorism](#), EU legislation in progress, EPRS, European Parliament, September 2017.

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.

[European travel information and authorisation system \(ETIAS\): border management, fundamental rights and data protection](#), Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, April 2017.

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

[The European Union's policies on counter-terrorism – Relevance, coherence and effectiveness](#), Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, January 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 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).
- ² [Interoperability of EU information systems for security, border and migration management](#), press release, European Commission, 12 December 2017.
- 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, 2018.

eprs@ep.europa.eu (contact)

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

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

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



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