Fundamental rights review of EU data collection instruments and programmes

FINAL REPORT

FGB Fondazione Giacomo Brodolini

This report is the result of a Pilot Project requested by the European Parliament, managed by the Commission and carried out by a contractor (group of independent experts). The Commission selected the contractor on the basis of criteria defined by the European Parliament. The legislative scope is the one that existed on 1 December 2018. The report reflects the views and opinions only of the contractor, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Table of contents

1. Executive summary

Data protection law in the EU has advanced significantly in recent years and is widely recognised as providing one of the most advanced frameworks for the protection of personal data in the world, to the benefit of individuals, organisations and institutions (public and private alike). These changes have chiefly come from new secondary legislation (such as 2016's General Data Protection Regulation or GDPR[1] and 'Law Enforcement Directive' or LED[2]) and from important developments in the case law of the Court of Justice of the European Union.

This pilot project sought to assess whether existing EU legislation in the Area of Freedom, Security and Justice (AFSJ) meets these standards, with the aim of identifying shortcomings and suggesting possible remedies. It finds that while much of the relevant law is compliant with the standards and requirements of the EU's data protection framework and relevant jurisprudence, there are also shortcomings and issues that require further attention from the legislator and supervisory authorities. This is the case both in EU legislation itself and in national measures implementing that legislation. However, given sufficient time, resources and dedication from EU and national institutions, remedies for these problems are available and will further assist in ensuring that data protection and privacy underpin the processing of personal data in the AFSJ. This study and its accompanying reports identify these issues and set out some ways in which they might be resolved.

1.1 The project

The scope of the project was to establish and support an independent experts' group to carry out a fundamental rights review of existing EU legislation, instruments or agreements with third-parties that involve the collection, retention, storage or transfer of personal data. The methodology of the research reflects the two main general aims of the project: to provide a comprehensive catalogue and an independent expert analysis of existing EU legislation, instruments and agreements with third parties that authorises or allows the processing of personal data in relation to law enforcement and law enforcement agencies, on the basis of the EU Charter of Fundamental Rights (CFR) and the European Convention on Human Rights (ECHR). The project was organised into seven tasks to be implemented in 24-month. The legal instruments taken into consideration are those existing at the date of 1 December 2018.[3] Four workshops were held in Brussels attended by the leading partner, the Steering Group, the Experts Group and the Commission.

1 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), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

2 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, https://eur-lex.europa. eu/eli/dir/2016/680/oj

3 Task 1: Design and start of the activities of the Steering Committee; Task 2. Definition of the group of experts; Task 3. Setting of overall guidelines for each deliverable; Task 4. Creation of a catalogue; Task 5. Fundamental rights assessment; Task 6. Alignment with the LED; Task 7. Submission of the final report.

1.2 Building the catalogue and database

The first substantive task was to catalogue legislation, instruments or agreements in the Area of Freedom, Security and Justice that involve the processing of personal data. The cataloguing activity covered:

- EU legislation and any relevant related national transposition laws;
- law-enforcement instruments and cooperation, and
- third party agreements, including those with third countries and international organisations.

In all 77 instruments were identified and their content is detailed in the database (legal basis, material scope, personal scope, personal data to be processed, etc.). The 77 instruments were divided between five sub-groups, dealing with: borders; Passenger Name Record and finance instruments; EU agencies; Member States' legislation; and cross-border data collection and exchange instruments. This structure and the analysis of the legislation's content provided the basis for the following task of carrying out a fundamental rights assessment of the legislation.

1.3 Fundamental rights assessments

The instruments summarised in the database were subsequently analysed against the provisions of the CFR, the case law of the CJEU and (where relevant) the ECHR and relevant data protection law. The chosen structure adopts the test set out in Article 52(1) CFR: are limitations on fundamental rights provided by law; do they respect the essence of the rights; do they concern an objective of general interest; and are they necessary and proportionate? Given the aims of the project, the review focused on the assessment of safeguards for the fundamental rights to privacy and data protection, following a structure based on the necessity and proportionality test set out in the Article 52(1) CFR and elaborated upon by CJEU case law. Potential interferences with further rights were also examined as necessary: to freedom of expression and information; to a fair trial; to an effective remedy; to non-discrimination; and to liberty and security.

The analyses show that despite changes to the EU's data protection framework introduced in recent years by new legislation and case law, many of the instruments in question – even those that predate that legislation and case law – are largely compliant with current standards. On the other hand, there are also a number of instances where EU law (or member states' implementing legislation) does not meet those standards, and action by the legislator should be considered in order to remedy these shortcomings. In this report, these issues are raised with regard to individual instruments, while a thematic analysis is also provided to draw out some of the overarching issues present across different groups of instruments.

In the context of privacy and data protection, the thematic analysis highlights seven areas for consideration. The first of these concerns the legal basis of certain instruments – PNR agreements with third countries and certain working arrangements and agreements between EU agencies require a reference to Article 16 TFEU as their legal basis[4]. Secondly, it highlights a need to give consideration to more-clearly defining certain terms (such as "security risk" or "threat to public policy") and more strictly limiting the scope of certain instruments (in particular in various agency

4 Article 16

1. Everyone has the right to the protection of personal data concerning them.
2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.

Requirements and other safeguards on the legitimate access to and use of data are met.

agreements) in order to ensure that purpose limitation

The third issue highlighted in the thematic analysis concerns the possibility of personal data being processed for reasons beyond those originally legislated for (i.e. in breach of the purpose limitation principle) and without sufficient safeguards. For example, the Frontex Regulation[5] does not clearly establish limits on the purposes for which personal data may be processed. The same problem affects the measures providing Europol with access to SIS II and VIS, and Eurojust's national members with access to SIS II. The finance instruments examined do not set out the competent authorities that can access and use the data that must be retained. A particular example is law enforcement access to Eurodac. This is governed by law and access is subject to certain conditions and safeguards (i.e. it must be for investigating cases of serious crime and terrorism and after fulfilling certain procedural requirements). Access to the data stored in the system after the relevant legislation entered into force remains a controversial topic, but can be seen as justified. However, providing law enforcement access to the entire database violated the purpose limitation principle with regard to the personal data that was stored in the system prior to the introduction of the legislation governing law enforcement access, the potential uses of which were extended by the new rules.

A related issue highlighted by the thematic analysis concerns the rules governing law enforcement access to non-policing databases. The conditions governing law enforcement access to databases primarily established to assist in the implementation of EU asylum, visa, migration and border management policy (Eurodac, VIS and the forthcoming EES and ETIAS) are not uniform. Depending on the degree of interference and the assessment of proportionality different safeguards could be justified or could result in offering different levels of protection to individuals. At the same time, the procedure for authorising such access may not meet the relevant standards for independent authorisation. The central access points responsible for approving or denying requests for access can be part of the same organisation that is seeking access. Future evaluations of these instruments must examine whether, in practice, this meets the requirements of EU law and CJEU jurisprudence.

The expansion of existing centralised EU databases (Eurodac, SIS II, VIS) and the recent establishment of new systems (EES, ETIAS, ECRIS-TCN) also raises questions concerning necessity and proportionality. All these systems were the subject of legislative procedures whilst the project was ongoing, and so agreed texts were not yet available at the time this report was written. This meant that significant focus was given to the proposals presented by the Commission, where a number of shortcomings were identified. Although this is not a legal obligation, particular concern is that no impact assessment accompanied the legal proposal of ETIAS, despite the significant social and economic impact of the proposal, in terms of who it affects and how. The justifications offered for certain measures lack a strong evidence base or compelling arguments.

A number of these systems (EES, ETIAS, Eurodac and VIS) also raised concerns with regard to their data retention periods, an issue highlighted in relation to a number of instruments. National data retention laws – which, as they exercise an exemption set out in the e-Privacy Directive, come within the scope of EU law – in five different member states (Finland, Germany, Hungary, Poland and Spain) indiscriminately retain telecommunications metadata and, in all those countries but Germany, the retention period for that data has not been sufficiently justified. The approach of the Europol Regulation to data retention periods is not favoured by the project team, and stipulations on data retention are missing from all the inter-agency agreements and agreements between Europol, Eurojust and third states examined as part of this project. Equally, in the project team's view the PNR agreements analysed fail to provide proportionate data retention periods.

Finally, with regard to data protection and privacy, the thematic analysis highlights the lack of information duties in certain instruments – for example, regarding the requirement to provide notification to the data subject when their information is processed in one way or another. Such notifications are a prerequisite for individuals to exercise their right to an effective remedy. At the national level, the data retention laws analysed in Hungary, Spain and Poland and the Belgian PNR

5 This study examined the 2016 Frontex Regulation, which will shortly be replaced by a new Regulation.

law do not provide for any such notification when an individual's data is processed by law enforcement agencies (even when such a notification could no longer jeopardise an investigation). At EU level, no notification is provided in the context of the transfer of personal data between EU agencies, nor when Europol accesses data held in SIS II or VIS. The Frontex Regulation also lacks relevant notification requirements.

Further thematic issues have been raised in relation to a number of other rights. The national data retention legislation examined as part of this project raises concerns regarding the right to freedom of expression and information. The right to non-discrimination is negatively affected by the decision to include both non-EU nationals and dual nationals in the ECRIS-TCN database, while the profiling functions included in the PNR Directive, the ETIAS and proposal for the VIS will require detailed supervision and evaluation in order to assess their effects on the right to non-discrimination. Concerns are also raised regarding the potential for indirect discrimination based on gender, ethnicity or nationality with regard to the PNR agreements with the USA and Australia.

Certain instruments also bring the rights of the child into play. It has been proposed to lower the fingerprinting age for both Eurodac and VIS to six years old, with one cited aim being to better protect children. Both proposals put forward additional precautions for collecting children's biometric data, but the purposes for which that data can be used is not limited to when this is in the best interests of the child. At the same time, child protection is not listed as an aim of either instrument. Concerns over the impact of certain instruments on the rights to an effective remedy and a fair trial; to seek asylum; and on the prohibition of inhumane or degrading treatment are also raised.

These thematic issues, identified across different groups of instruments, are accompanied by more specific findings within each group (borders; Passenger Name Record and finance; EU agencies; Member States' legislation; cross-border data collection and exchange). Each group report follows the same structure and synthesises the findings of the individual assessments to provide an overview of the key issues raised by each set of instruments. For more detail, the reader is invited to access the individual assessments for each instrument.

1.4 Compliance with the Law Enforcement Directive (LED)

A subsequent phase of the project required an assessment of certain instruments with the LED. Under Article 62(6) of that Directive, the European Commission is obliged to review Union acts which regulate the processing of personal data by the competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Assessments of 32 instruments were carried out for this project in order to contribute to that review.

The range of problems identified primarily stem from the age and diverse nature of the instruments in question. In some, there is no reference to the EU data protection framework in this field, as it did not exist prior to the adoption of Framework Decision 977/2008/ JHA.[6] There are other instruments that cite that Framework Decision but nevertheless require specific amendments. Other instruments have complex data protection regimes due to their multiple possible uses (e.g. migration and border management databases that are also accessible, under certain conditions, to law enforcement agencies) and the consequent need for differing data protection regimes (i.e. application of both the GDPR and LED). The relationship between an instrument's specific data protection framework (lex specialis) and the rules of the LED (lex generalis) are sometimes unclear. It is further emphasised that the conformity of national laws transposing the LED is a crucial issue for ensuring compliance. The assessment concludes with an overview of the options available for reforming or amending those instruments for which it is necessary.

6 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters,
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008F0977

1.5 Considerations and recommendations

The variety and diversity of issues highlighted in this report can be explained most simply by the fact that the extensive array of data processing instruments and measures in the AFSJ have evolved largely independently of one other. It is thus clear that fundamental rights safeguards need to be more consistently considered and applied in the AFSJ. The transposition of the LED, the GDPR and the Regulation on data protection in EU institutions and agencies are important steps in that direction but require improved management and enforcement capabilities at both EU and Member State level to deliver on their promise.

The final section of the report draws on observations made in the fundamental rights assessments and the thematic analysis to highlight five broad issues for further consideration: ambiguous definitions and open terms; law enforcement access to migration databases; the expansion of centralised databases; data retention periods; and information rights and duties. These conclusions are intended to complement, rather than distract from, the many issues identified in relation to individual instruments and groups of instruments.

1.5.1 Ambiguous definitions and open terms

- Using either definitions or guidance, key legal terms in Union law must be clarified in order to understand, assess and satisfy the purpose limitation principle and the necessity and proportionality of interferences with the fundamental rights to the protection of privacy and personal data. This is as much the case for preparatory work (e.g. impact assessments and evaluations) as it is for legislation itself.
- A certain measure of clarification can be achieved in the course of the Commission's review of Union legal acts predating Directive (EU) 2016/680 (LED). Union law should always require Member States to explain how key terms of a Union instrument are used in practice in Member States' criminal (procedural) laws.
- Member States, where they implement EU law, are under an obligation to carry out data protection impact assessments pursuant to the LED. Generic definitions or guidance on how key legal terms of EU legal instruments should be interpreted and applied are imperative for this process.

1.5.2 Law enforcement access to migration databases

- Forthcoming evaluations of the EES, ETIAS, Eurodac and the VIS must be taken as a genuine opportunity to consider all aspects of law enforcement access to personal data gathered primarily for the purposes of migration policy, taking into account the substantive and procedural aspects of that access, including whether the designated central access points meet independence and impartiality requirements, and key related issues such as non-discrimination and the purpose limitation principle.
- Law enforcement access to non-policing databases (Eurodac, VIS, EES and ETIAS) should be provided on a uniform procedural basis that applies equally high standards to all relevant instruments.
- Union law should only provide law enforcement authorities access to non-law enforcement data when a sufficient evidence base relevant to the issue is available, and such access has been fully considered in light of its necessity, proportionality and appropriateness.
- Where the Union operates and manages migration databases there is a responsibility to collect and publish detailed statistical data about law enforcement's access requests to migration databases and facilitate the independent supervision of the legality of law enforcement access to non-policing databases, through both the carrying out of evaluations and the provision of sufficient resources to the responsible data protection authorities.

1.5.3 Expansion of centralised databases

- The Commission should strengthen its capacity to conduct meaningfully granular impact assessments that take into account all relevant fundamental rights issues, and no further centralised databases or large-scale information systems should be developed or extended without such an impact assessment.
- The Commission should continue to allow for sufficient consultation with Union bodies such as the European Data Protection Supervisor, the Fundamental Rights Agency, for public deliberation and seek independent advice in order to ascertain the necessity and proportionality of each and every intended measure.
- It must be ensured that the reviews foreseen in legislation establishing EU databases and information systems that make use of profiling functions include in-depth investigation and evaluation of the procedural and substantive aspects of those functions; no further profiling functions should be included in EU-level systems until those reviews have taken place and confirmed the compatibility of the practice with fundamental rights standards.
- Inject a fundamental rights and non-discrimination clause in the governing instrument of each Union centralised database analogous to Article 14 of the ETIAS Regulation.

1.5.4 Data retention periods

- The Commission should strengthen its capacity to assess data retention periods in a granular and differentiated manner taking into account the necessity of the personal data to achieve the purposes pursued and the fundamental rights of the individuals concerned.
- The project team is in favour of Union legislation in the AFSJ providing a maximum data retention period in the case of any personal data processing. If relevant legislation does not establish a maximum retention period, it should be amended.
- Sharing of and access to personal data between Member States' competent authorities in the AFSJ should not leave personal data in a legal limbo as to which legal framework applies and which retention periods should prevail to the personal data. Union legislation has to provide for unambiguous rules for ascertaining retention periods in situation when personal data is accessed and used by various EU agencies and national competent authorities.
- The proportionality of the proposed 10-year retention period for children's fingerprints in the recast Eurodac proposal remains questionable in the project team's view, particularly given that the study serving as justification for the measure is not fully conclusive.

1.5.5 Information duties

- The obligation to conform with information duties needs clear recognition in all Union instruments providing for the processing of personal data, and standard rights and duties should be complemented by more specific provisions, where appropriate.
- In order to effectively monitor EU bodies and Member States' competent authorities' compliance with information duties more closely, it must be ensured that EU and national data protection authorities are provided with sufficient resources to carry out their tasks effectively.

This project has provided an in-depth analysis of EU law in the Area of Freedom, Security and Justice that requires the processing of personal data. Despite the significant breadth of the project, its timeframe made it impossible to take into account certain developments, such as progress in certain legislative negotiations and proposals such as the interoperability Regulations, which introduce significant changes to the functioning and operation of EU databases and information systems. Developments such as this demonstrate the importance of the new EU data protection framework and the continued scrutiny of the CJEU in this area. This project has highlighted the shortcomings in existing law in relation to these new standards and it is clear that as the legal and policy framework evolves, spurred on by new technological and social developments, many new challenges will arise. At the same time, it is clear that, if provided with sufficient time and resources for supervision and implementation, the EU and its member states now have the legal framework, policy tools and oversight bodies in place to ensure that privacy and data protection serve as the foundation of the AFSJ as it further develops.

2. The project

2.1 Aim and Purpose, Overview of the activities carried out

The scope of the project was to establish and support an independent experts' group (whose composition is reported in detail in annex I of this report) to carry out a fundamental rights review of existing EU legislation in the Area of Freedom, Security and Justice (AFSJ) , instruments and agreements with third parties that involve the processing of personal data.[7] The methodology of the research (described in section 3.1) reflects the two main aims of the project: to provide (1) a comprehensive catalogue and (2) an independent expert analysis of existing EU legislation, instruments and/or agreements with third parties that authorise or allow the processing of personal data in relation to law enforcement and law enforcement agencies, on the basis of the EU Charter of Fundamental Rights and the European Convention on Human Rights (ECHR).

After the entry into force of the Lisbon Treaty, the CFR became binding upon the EU institutions when adopting new measures, as well as for Member States during the implementation of those measures. Although the ECHR is not EU law, Article 6 of the Treaty on European Union (TEU) confirms its prominent value as a reference point and source of inspiration for the Union and its standard of rights protection. This is also reflected in some of the horizontal provisions of the Charter, namely Articles 52(3) and 53, which urge a coherent interpretation of the rights enshrined in the Charter itself in light of the case law of the European Court of Human Rights. In relation to Article 8 CFR, the explanations attached to the Charter confirm that the protection of personal data in the EU legal order builds on – inter alia – Article 8 ECHR.

The catalogue of relevant EU legislation, instruments and agreements provided the basis for the subsequent fundamental rights reviews of relevant EU acts. Particular attention was given to the principles of necessity, proportionality and the adequacy of existing safeguards for privacy and data protection and of guarantees for fairness and lawfulness in criminal investigations and prosecutions by EU law enforcement agencies.

The project also reviewed several EU acts in order to assess the need to align them with Directive (EU) 2016/680 (the law enforcement and criminal justice Directive or LED).[8] This review served as the basis for proposals to ensure a consistent approach on the protection of personal data within the scope of the LED.

The questions raised in relation to the processing of personal data by law enforcement authorities aims to support the Commission's review of EU acts containing data protection rules that concern law enforcement and criminal justice authorities.

In order to carry out the analysis and assessment of existing EU legislation, instruments and agreements involving the processing of personal data and their impact on fundamental rights, the following activities were implemented by the group of experts:

7 "Processing" is defined in Article 4(2) of the General Data Protection Regulation as: "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." 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, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

8 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, https://eur-lex.europa. eu/eli/dir/2016/680/oj

- cataloguing ("mapping") existing EU legislation (and any relevant related national transposition laws) and agreements with third parties (including both third countries and international organisations) involving the processing of personal data, in particular those Union legal acts referred to in Article 60 of the LED;
- a legal analysis and fundamental rights review in the light of the most recent EU case law in the field of privacy and the protection of personal data and in the light of the new EU data protection legal instruments (GDPR and LED);
- analysing and assessing compound effects of existing EU data collection programmes, with a view to identifying potential fundamental rights loopholes and interferences with those rights;
- drawing up specific policy recommendations for each identified and reviewed element, including technical and procedural safeguards as well as general guidelines for EU data collection instruments and mechanisms and concrete proposals on aligning EU legal acts which regulate data processing by police and criminal justice authorities with the LED.

The project was divided into seven tasks (the present report representing the seventh task) which were implemented as scheduled during the 24 months of the project. Periodic monthly calls were organised between the experts representing the working groups described below and with the Commission to monitor the state of play of the research; to deal with issues emerging during the process; and to plan the implementation of the subsequent activities of the research project.

Task 1. Design and start of the activities of the Steering Committee: the steering committee, whose composition and functions are described in section 3 of this report, was established and began its activities.

Task 2. Definition of the group of experts: the group of experts was created and the management method to organise and coordinate the activities of its members was established and tested.

Task 3. Setting of overall guidelines for each deliverable: the starting point for the effective implementation of the project was the setting of overall guidelines for each deliverable, including an internal peer-review system and the identification of roles and responsibilities of each member of the expert groups. This guidance was provided by the Steering Committee in the first stages of the project and was subject to updates in the course of the project.

Task 4. Creation of a catalogue: this activity represents, together with tasks 5 and 6, the core of the research project. It involved the creation of a catalogue of existing EU legislation and agreements concluded with third parties entailing the processing of personal data. This task also involved the creation of a repository of the most relevant national transposition laws. The catalogue aims to provide a general, comprehensive and exhaustive overview of these instruments (its methodology, functionalities and key features are described into details in section 4 of this report) and was a crucial point of departure for the subsequent fundamental rights review.

A one-day workshop in Brussels involving the experts and the Commission was organised in May 2017 to foster exchanges of views and impressions and to fine-tune the implementation of the research.

Task 5. Fundamental rights assessment: under this task, experts carried out an in-depth analysis of the fundamental rights aspects of EU legislation related to the processing of personal data. This analysis, whose methodology and results are set out in section 5, provided the basis for policy recommendations to address shortcomings that were detected. A crucial part of this analysis was the need to take into consideration the "proportionality test", which is at the core of EU legislation when analysing norms that interfere with fundamental rights and freedoms as recognised in the Charter. The goal of this proportionality test was to examine, with regard to Article 52(1) CFR,[9] whether such

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

interferences were justified. The outcome of this task is a thematic analysis of the fundamental rights aspects of EU legislation highlighting the key shortcomings that were detected.

A one-day workshop in Brussels involving the experts and the Commission was organised in December 2017 to foster exchanges of views and impressions and to fine-tune the implementation of the research.

Task 6. Alignment with the LED: one of the major achievements of the LED is that it seeks to create a harmonised data protection regime for the processing of personal data by law enforcement and criminal justice authorities. In this task the experts assessed whether relevant instruments that now fall within the scope of the LED require alignment with its rules. Where such an alignment was deemed necessary, proposals for amendments have been provided with the aim of achieving a consistent and comprehensive approach to personal data protection..

A one-day workshop in Brussels involving the experts and the Commission was organised in March 2018 to foster exchanges of views and impressions and to fine-tune the implementation of the research.

Task 7. Submission of the final report. The present report is the comprehensive and thorough result of the research carried out during the 24 months of the project. It represents a standalone document meant to be accessible to a wider audience (including, but not limited to, experts and researchers in the privacy and data protection fields) interested in the results of the research. It is the outcome of the cooperation and networking of all the experts involved in the research process. Its finalisation was also subject to a one-day workshop in Brussels.

As a final remark, it is worth stressing that the bulk of the analysis was finalised in June 2018 and therefore refers to legislation in force at that time. Where possible, some elements of the analysis have been updated to include information on proposals that were approved up to December 2018, but these updates are not exhaustive (e.g. the research team was unable to update the ECRIS-TC analysis, and the assessment is therefore based on the proposal).

2.2 The team of experts and the Steering Committee

2.2.1 The leading partner

The research was coordinated by Fondazione Giacomo Brodolini (FGB), an Italian independent and non-profit research organisation that since 1971 has dealt with labour, economics, development and culture in Europe. Moreover, in the last 10 years, FGB has become a European player in terms of research from a gender perspective, also through a Masters programme which is taught by diversity management and gender experts; as well as through an online magazine – launched by FGB in 2009 – www.ingenere.it, the first of its kind in Italy. FGB's Management Board consists of prominent figures from the main Italian Universities. FGB offers support in policy development, implementation and impact evaluation to institutions at all levels – from local to European – in issues such as: labour market participation, immigration, gender issues, population ageing, job insecurity and development, industrial relations, social inclusion and fundamental rights.

Since 2008 the FGB has gained extensive expertise in managing EU-level academic experts' networks: these include the European Commission's employment and gender equality network (EGGE) between 2008 and 2011 and the Gender equality, social inclusion, health and long-term care network (EGGSI). Since 2011 FGB coordinates, on behalf of DG Justice, the European Network of Experts in the Field of Gender Equality (ENEGE), which provides external expertise to the European Commission in the field of gender equality policy.

In order to carry out complex, multi-country studies that require detailed knowledge of specific national policy contexts, FGB can count on the collaboration and expertise of an extended network of approximately 230 researchers.

In addition, FGB has acquired considerable experience in the setting up of large, multi-country online databases/repositories of documents and datasets containing information from different data sources. Two services – "Analysis of the outcome of the negotiations concerning the partnership agreements and ESF Operational Programmes for the programming period 2014-2020" on behalf of DG EMPL and the ESF 2014-2020 Synthesis and thematic reports, always for DG EMPL – are of particular relevance in this respect.

Eventually, in view of the implementation of this research project, FGB has reinforced its EU network with academics, civil society organisations, and practitioners, such as Access Now Europe, European Digital Rights (EDRi) and Mitopics, involved as subcontractors.

2.2.2 The Steering Committee (SC)

A steering Committee for the pilot project was created, identifying and mobilising qualified experts and designing an effective and efficient organisational model.

It included the following members: Professor Franziska Boehm, Professor Fernando Galindo, Silvia Sansonetti PhD and Marta Capesciotti PhD. Short profiles are contained in Annex 1.

The aim of the SC is to provide scientific supervision of the Experts Group. This supervision mission included the definition of the content and structure of each deliverable, the methodological approach to be followed for their preparation and the identification of the most suitable expertise to implement them. The SC also ensured that all members of the Experts Group (including the observers) were regularly consulted and that their feedback was duly considered. Its members chaired and oversaw the implementation of the workshops and liaised with the Commission on scientific and methodological issues.

During the implementation of its functions the SC was supported by the management team, which ensured the timely submission of the deliverables, coordinated the activities of the SC and the expert groups and acted as a liaison with the Commission. The management team also cooperated with the SC in the identification of the specific tasks to be carried out by each expert for the finalisation of the deliverables, in collecting contributions and submitting them to the attention of the SC. Based on that information, the SC prepared the documents for the workshops and the questions to consult and discuss with the expert group.

2.2.3 The Experts Group (EG)

In selecting the members of the EG (the aim of Task 2) the management team took into account relevant professional background including research field, publications, public speaking engagements, institutional affiliation, years of experience, reputation, professional network, availability and other factors. Each expert was attributed a specific role based on the aforementioned selection criteria and the roles were linked to the thematic working groups.

Considering that the project was highly sensitive in human rights terms, not just in terms of the specific instruments to be analysed, our expert group entailed a unique combination of expertise in not only the fundamental rights to privacy and data protection but also in a broader human rights perspective, including fairness and lawfulness in criminal investigations and trials, with a special regard to the proportionality principle; and in public international law and treaties relating to such matters, including the Council of Europe cybercrime and data protection conventions as well as relevant EU instruments.

Experts came from different EU countries and either had an academic background or were practitioners or representatives from civil society. However, these categories are not necessarily mutually exclusive as some experts actually fell in one or more of the above groups. The management team built the EG specifically on people (academics and lawyers as well as civil society activists) with direct expertise in the matters to be addressed, with special emphasis on the fundamental rights to privacy and data protection, and human rights more broadly.

Annex 1 presents a list of the experts explaining their specific role.

2.2.4 The relationship between the Steering Committee and the Experts Group

All members of the SC are also part of the EG. The SC members were frequently in touch with one another and with the project coordinators by email or phone. In addition, they also took part in the kick-off meeting and chaired and steered the internal inception meeting with the remaining members of the EG and the management team.

To sum up, the SC provided quality assurance of contents and methodology. It is an integral part of the EG. Its members ensured a balanced representation of different affiliations and backgrounds, provided key strategic advice and were charged with the drafting of the deliverables.

Monthly calls among the experts and with the Commission were established to fine-tune the methodology and consider the most relevant findings emerging from implementation of the research.

3. Building the catalogue and the database

3.1 Methodology

The execution of this task was achieved on the basis of thorough and comprehensive desk research. This cataloguing activity was crucial as both Task 5 (Deliverable 2) and Task 6 (Deliverable 3) were based on its results.

The scope and aims of the pilot project determined that one of the key perspectives from which the legal analysis was carried out was to ensure the consistent approach on the protection of personal data throughout EU legislation and its national transposition, where applicable. The fundamental rights review included, but was not limited to, the assessment of safeguards for the fundamental rights to privacy and data protection.

The cataloguing process focused on legislation, instruments and agreements that involve the processing of personal data and subsequently have an impact on rights protected by the CFR and ECHR such as the right to privacy, the protection of personal data, non-discrimination, the presumption of innocence and the rule of law.

The cataloguing activity covered: 1) existing EU legislation; 2) law enforcement instruments and cooperation, and 3) agreements with third parties (third countries and international organisations) involving the processing of personal data, such as mutual legal assistance agreements (MLAs), Passenger Name Record (PNR) agreements, and the Terrorist Finance Tracking Programme (TFTP). Relevant national transposition laws were included as well, requiring local contributors both from a language and a legal context perspective.

3.2 The experts' sub-groups

The methodology adopted divided the stock-taking and cataloguing into five areas, which were covered by five different working groups. For each area, a lead expert supervised the activities carried out by junior researchers in their respective working groups.

More specifically, five thematic working groups were active throughout the whole project:

1. Borders instruments: this sub-group was created to examine EU legislation and instruments concerning the activities of border control authorities, migration authorities or the implementation of any other measure affecting third-country nationals that require or permit the processing of personal data;
2. Passenger Name Record (PNR) and finances instruments: Measures concerning Passenger Name Records (PNR) and finances instruments were mapped into one sub-group because – despite appearing unrelated at first glance – after the preliminary mapping the experts found an overlap in the main goal of both PNR and Finances instruments, that is the fight against terrorism and major criminal offences, including money laundering or fraud;
3. EU agencies instruments: this subgroup selected relevant legislation of EU agencies in the Area of Freedom, Security and Justice (AFSJ), in particular in the framework of police and judicial cooperation as well as border management, asylum and migration, and counter-terrorism, focusing on the AFSJ agencies Europol, Eurojust and Frontex. The selection of these agencies was based on the scope of the study;

4. Member States' legislation: The selection of instruments in this sub-group working on the national instruments for data collection was based on two main criteria: (1) the relevance of the instrument in the national legislative and policy framework as well as in the EU, and (2) the expertise and language skills of the members of the expert group. In this respect, experts selected the legislative national instruments that could be representative of the nature of the data processing taking place in a large number of EU member states, as well as those instruments that would be particularly relevant to the project. The sub-group also tried to select those legislative instruments considered by the experts as potential models for the other EU member states, thus pointing out "lead" countries in specific matters covered by the research;
5. Cross-border collection instruments, including Mutual Legal Assistance Treaties (MLATs): this sub-group was created to analyse the most important EU cross-border exchange instruments. In this respect, experts selected those instruments which, because of their nature, may have a significant impact on the amount of data exchanged between the law enforcement authorities of the Member States. The sub-group also included relevant Mutual Legal Assistance Treaties (MLATs) in place in the EU to map, analyse and compare different type of instruments used for police and judicial cooperation.

The analysis of experts leading each working group in certain deliverables was complemented by the other experts from either the academic, practitioner, or civil society 'arm'.

3.2 The cataloguing activity: the "fiche method"

The key issues to be tackled when devising the methodological approach for the conceptualisation and operationalisation of the catalogue were the following:

- ensuring comprehensiveness and exhaustiveness;
- including a basic level of analysis to prepare the fundamental rights review;
- indicating the key points of each instrument based on the preliminary review and make them searchable; and
- to include references to the GDPR and the LED in case of interactions, overlaps or inconsistencies.

The cataloguing primarily required a thorough desk research carried out by junior researchers under the supervision of the academic experts. Moreover, the consortium included as experts, representatives of Statewatch who have a world-leading experience in such cataloguing processes from a human rights perspective. These subgroups collected the respective information in each section of the repository and the observers in the expert group confirmed the comprehensiveness of the catalogue.

The desk research included online research on relevant legislation, published decisions, opinions and annual reports, previous studies, seeking information on news with regard to relevant data protection issues, and contact with data protection authorities, local NGOs, local academic institutions, creating surveys and conducting interviews. It was crucial that the three working groups used the same criteria and methodology for both the cataloguing and the initial evaluation.

The catalogue included – for each instrument analysed in its implementation – the following items:

- Name of the instrument itself (for instance SIS II).
- Legal basis of the instrument.
- Links
- Tags
- Purpose (e.g. Border control, exchange of information, justice and security cooperation)
- Measures
- Personal scope
- Material scope
- Geographical scope
- Types of data collected
- Merging of databases (if applicable)
- Interoperability measures (if applicable)
- Rules on data security (juridical norms)
- Rules on data security (technical rules)
- Access to data (who has access)
- Access safeguards
- Review mechanisms (e.g. actors, when, mandatory/ad hoc, legal force of the review)
- Data retention periods
- International transfers (e.g. transfers to third countries, possibility of "onward transfers", authorisation to transfer to third parties)
- References to relevant data protection framework(s) (e.g. list of specific instruments plus the article(s) or paragraph in the instrument which refer to other data protection frameworks)
- Dependence on another EU instrument
- Impact on another EU instrument (e.g. Directive or Regulation impacted by instrument under review, for instance, what EU PNR means for Schengen Code, how the PNR agreements relate to the Umbrella Agreement, etc.)
- The instrument impacts on this/these article(s) of the EU Charter of Fundamental Rights (e.g. Art. 7, 8, 11, 47, 52 etc.)
- The instrument contradicts this/these relevant Court of Justice of the European Union case/cases
- The instrument impacts on article(s) of the European Convention on Human Rights
- The instrument contradicts relevant European Court of Human Rights case/cases
- The instrument bears features relevant to regulation(s) of the Council of Europe (e.g. Convention 108, Recommendations e.g. R(85)15)
- Institutional fundamental rights assessments in relation with the instrument (e.g. by the Article 29 Working Party, European Data Protection Supervisor (EDPS), European Network Information and Security Agency (ENISA), the EU Fundamental Rights Agency (FRA), Commission impact assessments or studies, the legal services of the EU institutions)
- Non-compliance of the instrument with other EU instruments (e.g. inner institutional contradictions).

Each instrument in the database[10] was associated with one or several tag(s), matching the corresponding subgroup. The instruments in the database can be searched using a selection of tags listed in alphabetical order. Using the code associated to the instrument, the name of the instrument or the tag(s), database users can have access to information collected by the experts for each considered instrument as well as a preliminary analysis of the instrument's impact on fundamental rights, as explained above.

Experts were asked to consider not only to the content of the GDPR and other related legislation, but also the impact of the so-called e-Privacy Directive,[11] for instance. The practical consequence of this is that any time the group catalogued and analysis existing EU legal instruments, they considered the fundamental rights to both data protection and to privacy. After the conclusion of the EU data protection reform process that resulted in the adoption of the GDPR and the LED, the Commission turned its attention to a review of the e-Privacy Directive. The e-Privacy Directive is the only piece of secondary legislation on EU level that protects the fundamental right to privacy in relation to the confidentiality of electronic communications. The anticipated timeframe of the review of the e-Privacy Directive coincided with the timeframe of this pilot project. Therefore, the expert group payed special attention to this issue.

With regard to cataloguing national implementing legislation, the composition of the EG – with its members having diverse backgrounds and being well-embedded in the NGO and academic community across Europe – made it possible to reach out to local experts' groups or researchers to have a better understanding of the relevance of the specific legal instruments and its impact. The EG also relied on the use of the websites, opinions and reports of national data protection authorities. Besides publicly available information, interviews were conducted to collect more information, especially on national transposition laws.

10 The database is accessible at the following link: http://brodolini.mbs.it/

11 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058

3.3 The analysed instruments by subgroups

Below the list of instruments analysed by each of the research sub-groups.

Borders instruments:

- Biometric passports[12]
- Customs Information System (CIS)[13]
- Entry/Exit System (EES)[14]
- Eurodac (including the revision proposal)[15]
- European Travel Information and Authorisation System (ETIAS)[16]
- European Border Surveillance System (Eurosur)[17]
- SIS II (including the revision proposals regarding border checks and return of third-country nationals)[18]
- Visa Information System (VIS, including the revision proposal)[19]

12 Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, https://eur-lex.europa.eu/legal-content/ EN/ALL/?uri=CELEX:32004R2252; Regulation (EC) No 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, https://eur-lex.europa.eu/legal-content/EN/ TXT/?uri=celex:32009R0444

13 Council Regulation No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs or agricultural matters, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:019 97R0515-20160901; Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009D0917

14 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, https://eur-lex.europa.eu/legal-content/EN/ TXT/?uri=CELEX:32017R2226

15 Regulation (EU) 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32013R0604; Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless persons], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0272(01)

16 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, https://eur-lex.europa.eu/legal-content/ EN/TXT/?uri=CELEX:32018R1240

17 Regulation (EU) No 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur), https://eur-lex.europa.eu/legal-content/EN/ TXT/?uri=CELEX:32013R1052

18 Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second-generation Schengen Information System (SIS II), https:// eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006R1987; Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006, https://eur-lex.europa.eu/legal-content/AUTO/?uri=CELEX:32018R1861; Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals, https://eur-lex.europa.eu/legal-content/AUTO/?uri=CELEX:32018R1860

19 Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS), https://eur-lex. europa.eu/legal-content/EN/TXT/?uri=CELEX:32004D0512; Regulation (EC) 767/2008 of the European Parliament and of the

PNR and finances instruments:

Instruments examined in relation to Passenger Name Record (PNR)

- API Directive[20]
- PNR Directive[21]
- Belgium PNR[22]
- Denmark PNR[23]
- France PNR[24]
- EU-Australia PNR Agreement[25]
- EU-USA PNR Agreement[26]
- UK E-Borders Programme[27]

Instruments examined in relation to finances:

- Terrorist Finance Tracking Programme Agreement[28]
- Council Decision on Asset Recovery Offices[29]

Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008R0767; Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, https://eur-lex.europa.eu/legal-content/ EN/TXT/?uri=CELEX%3A32008D0633; Regulation (EC) 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code), https://eur-lex.europa.eu/legal-content/EN/ ALL/?uri=CELEX:32009R0810; Regulation (EC) 390/2009 of the European Parliament and of the Council of 23 April 2009 amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organisation of the reception and processing of visa applications, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009R0390; Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA, https://eur-lex.europa.eu/ legal-content/EN/TXT/?uri=CELEX:52018PC0302

20 Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004L0082

21 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, https://eur-lex.europa.eu/eli/dir/2016/681/oj

22 Loi relative au traitement des données des passagers, 25 December 2016, http://www.ejustice.just.fgov.be/eli/loi/2016/12/25/2017010166/moniteur

23 The Danish PNR framework consists of several measures across the following Danish laws: Customs Act, Section 17; Danish Security and Intelligence Service Act, Section 5; Danish Defence Intelligence Service Act, Section 3; Aliens Act, Section 38, and Law amending the Defense Intelligence Service Act (FE) and the Customs Act.

24 Article L. 232-7 in the Code for Interior Security as modified by the Law reinforcing the interior security and the fight against terrorism, LOI n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme

25 Council Decision of 13 December 2011 on the conclusion of the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012D0381

26 Council Decision of 26 April 2012 on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012D0472

27 Section 36-7, Immigration, Asylum and Nationality Act of 2016, http://www.legislation.gov.uk/ukpga/2006/13/ contents; Home Office and HM Revenue & Customs, Code of Practice on the management of information shared by the Border and Immigration Agency, http://www.statewatch.org/news/2008/may/uk-cop-data-share-borders.pdf

28 Council Decision of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX:32010D0412

29 Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of

- 4th Anti-Money Laundering Directive[30]
- Regulation on information on the transfer of funds[31]

EU Agencies instruments:

Agencies' founding legislation:

- Eurojust Council Decision[32]
- Europol Regulation[33]
- Frontex Regulation[34]

Access to databases and information systems:

- Eurojust access to SIS II[35]
- Europol access to Eurodac and 2016 proposal[36]
- Europol access to SIS II[37]
- Europol access to VIS[38]

---

the Member States in the field of tracing and identification of proceeds from, or other property related to, crime, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32007D0845

30 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, https://eur-lex.europa.eu/legal-content/ EN/TXT/?uri=CELEX-:32015L0849

31 Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006, https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX:32015R0847

32 Eurojust: Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, https://eur-lex. europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009D0426

33 Europol: 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, https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A32016R0794

34 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, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R1624

35 Eurojust access to SIS II, Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), http://eur-lex.europa.eu/legal-content/EN/ ALL/?uri=CELEX:32007D0533

36 Europol access to Eurodac: Regulation No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013R0603; Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] , for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast), https://eur-lex.europa.eu/legal-content/EN/ TXT/?uri=CELEX:52016PC0272(01)

37 Europol access to SIS II: Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), http://eur-lex.europa.eu/legal-content/EN/ ALL/?uri=CELEX:32007D0533

38 Europol access to the Visa Information System: Council Decision 2008/633/JHA of 23 June 2008 concerning access

Agreements with third states and international organisations:

- Eurojust: Iceland, Liechtenstein, Macedonia, Moldova, Montenegro, Norway, Switzerland, Ukraine, USA[39]
- Europol: Albania, Australia, Canada, Colombia, Iceland, Interpol, Liechtenstein, Macedonia, Moldova, Monaco, Montenegro, Norway, Serbia, Switzerland, USA[40]

Inter-agency agreements:

- Eurojust-OLAF[41]
- Europol-Eurojust[42]
- Europol-Frontex[43]
- Europol-OLAF[44]

Member States data collection instruments:

- Danish administration of justice act[45]
- Finnish telecommunications data retention law[46]
- German data retention law[47]
- Hungarian data retention law[48]
- Polish antiterrorist act[49]

---

for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008D0633

39 Eurojust agreements with third states: http://www.eurojust.europa.eu/about/legal-framework/Pages/eurojustlegal-framework.aspx#partners

40 Europol agreements with third states and international organisations: https://www.europol.europa.eu/partners-agreements/operational-agreements

41 Eurojust-OLAF agreement: http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/agreements/Practical%20Agreement%20on%20arrangements%20of%20cooperation%20between%20Eurojust%20and%20 OLAF%20(2008)/Eurojust-OLAF-2008-09-24-EN.pdf

42 Europol-Eurojust agreement: https://www.europol.europa.eu/sites/default/files/documents/Agreement_between_Eurojust_and_Europol.pdf

43 Europol-Frontex agreement: https://www.europol.europa.eu/sites/default/files/documents/Agreement_on_Operational_Cooperation_between_the_European_Police_Office_Europol_and_the_European_Agency_for_the_Management_of_Operational_Cooperation_at_the_External_Borders_of_the_Member_States_of_the_European_Union_Frontex.pdf

44 Europol-OLAF agreement: https://www.europol.europa.eu/partners-agreements/strategic-agreements

45 Denmark: Administration of Justice Act (Retsplejeloven), Data Retention Administrative Order (Logningsbekendtgørelsen)

46 Finland: Data Retention law (Tietoyhteiskuntakaari), sections 157–159 (statute 917/2014; Information Society Code)

47 Germany: Law on the introduction of an obligation to store and a maximum period to retain traffic data (Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten), 10 December 2015

48 Hungary: Act C of 2003 on Electronic Communications (2003. evi C. torveny az elektronikus hirkozlesrol)

49 Law Amending the Act on Police and Other Acts (Ustawa o zmianie ustawy o policji i innych ustaw), 15 January 2016, Journal of Laws 2016/147. The 'Surveillance Act' modified several laws regulating activities of different law-enforcement and intelligence agencies:

The Act of 6 April 1990 on Police;
The Act of 12 October 1990 on the Border Guard;
The Act of 28 September 1991 on Fiscal Controls;
The Act of 21 August 1997 on the Military Court System;
The Act of 27 July 2001 on the Common Court System;
The Act of 24 August 2001 on the Military Police and Military Law Enforcement Units;
The Act of 24 May 2002 on the Internal Security Agency and the Intelligence Agency;
The Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service;9) The Act of 9 June 2006 on the Central Anti-Corruption Bureau; 10) The Act of 27 August 2009 on the Customs Office.

- Spanish data retention law[50]

Cross-border collection instruments, including Mutual Legal Assistance Treaties (MLATs):

- Directive on the exchange of information on road traffic offences[51]
- EU-Iceland and Norway mutual legal assistance agreement[52]
- EU-Japan mutual legal assistance agreement[53]
- EU-USA mutual legal assistance agreement[54]
- European Arrest Warrant (EAW)[55]
- European Criminal Records Information System (ECRIS) and European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN)[56]
- European Investigation Order (EIO)[57]
- European Protection Order (EPO)[58]
- Prüm Decisions[59]

The Surveillance Act also modified other acts such as:

1) The Act of 18 July 2002 on the provision of services supplied by electronic means; 2) The Telecommunications Act of 16 July 2004.

The English translation of the Act is available here on the website of the Venice Commission, http://www.venice.coe. int/webforms/documents/?pdf=CDL-REF(2016)036-e.

50 Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones

51 Directive (EU) 2015/413 of the European Parliament and of the Council of 11 March 2015 facilitating crossborder exchange of information on road-safety-related traffic offences, https://eur-lex.europa.eu/legal-content/EN/ TXT/?uri=CELEX:32015L0413

52 Agreement between the European Union and the Republic of Iceland and the Kingdom of Norway on the application of certain provisions of the Convention of 29 may 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union and the 2001 Protocol thereto, https://eur-lex.europa.eu/legal-content/ EN/TXT/?uri=CELEX:22004A0129(01)

53 Agreement between the European Union and Japan on mutual legal assistance in criminal matters, https://eurlex.europa.eu/legal-content/EN/TXT/?qid=1557746113867&uri=CELEX:22010A0212(01)

54 Agreement on mutual legal assistance between the European Union and the United States of America, https:// eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX:22003A0719(02)

55 Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002F0584

56 Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, https://eur-lex.europa.eu/ legal-content/EN/TXT/?uri=celex:32009F0315; Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA, https://eur-lex.europa.eu/eli/dec/2009/316/oj; Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA, https://eur-lex.europa.eu/legal-content/EN/ TXT/?uri=CELEX:52016PC0007; Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011, https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX:52017PC0344

57 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32014L0041

58 Directive 2011/99/EU of the European Parliament and of the Council of 13 December 2011 on the European protection order, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0099

59 Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008D0615; Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, https://eur-lex.europa. eu/le-

- Swedish Framework Decision[60]
- SIS II and 2016 proposal (police and judicial cooperation in criminal matters)[61]

The database developed for the project allows the experts to retrieve the data on each of the instruments through the following means: 1) Code: the code assigned to each instrument; 2) Name: the name assigned to each instrument; and 3) Tag or tags: keywords assigned to each instrument, based on the selection made by the expert that has analysed/mapped the instrument.

The principal shortcoming of the database lies in the limited objective behind its construction. This was basically aimed at providing an output for the mapping exercise that was easy to access and user-friendly and was decided upon following the initial proposal of using spreadsheets. It was decided that an online repository/database would be a preferable solution, at least for collecting and organising the selected instruments.

gal-content/EN/TXT/?uri=celex:32008D0616

60 Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, https://eur-lex. europa.eu/legal-content/en/TXT/?uri=CELEX:32006F0960

61 Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32007D0533; Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0883

4. Fundamental rights assessment

4.1 Presentation of the methodology

Based on the mapping and review of existing legal acts at EU level and of selected Member States' legislation, the core part of the project consisted of a fundamental rights analysis of selected pieces of legislation. This analysis was planned to take place from July to December 2017 but was eventually extended until March 2018.

The analysis was carried out in light of the CFR, the case law of the Court of Justice of the European Union (CJEU), the ECHR and its respective case law as well as the provisions of the GDPR and, where applicable, regulations of the Council of Europe (CoE). At a later stage, a compliance check with Directive 2016/680 was carried out.

Due to the principal role of personal data processing in the instruments analysed, the review focused on the assessment of safeguards for the fundamental rights to privacy and data protection. Based on the necessity and proportionality test set out in the Article 52(1) CFR and elaborated upon by CJEU case law, the instruments were analysed to see how they interfere with these two rights and how the legislator acted to mitigate these interferences. Further, as some of the instruments also touch upon the fundamental rights to free expression and information, to a fair trial, to respect for private and family life, to an effective remedy, to non-discrimination and to access to documents, these rights are assessed where relevant and necessary, but in a less comprehensive way.

Interference with these rights is permitted under certain conditions. Article 52(1) CFR states:

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

Once a measure satisfies the conditions for being provided by law and respects the essence of the fundamental rights upon which it impinges, it needs to comply with a proportionality test. Proportionality comprised of several stages: the measure should pursue a legitimate aim; it needs to pass a means/ends assessment (meaning that there are no other less intrusive means available that can effectively achieve the aim); and the measure needs to be necessary in a democratic society (meaning that the advantages of introducing a certain legal measure should not exceed any possible disadvantages from a fundamental rights point of view, balancing stricto sensu). Each legal instrument was assessed on the basis of each of these prongs of the test. Therefore, each report was structured as follows:

- provided by law (satisfying conditions of foreseeability)
- respect for the essence of the rights
- legitimate aim
- necessity and proportionality

4.1.1 Three step approach

To carry out the fundamental rights analysis, a three step methodological approach was adopted. It consists of:

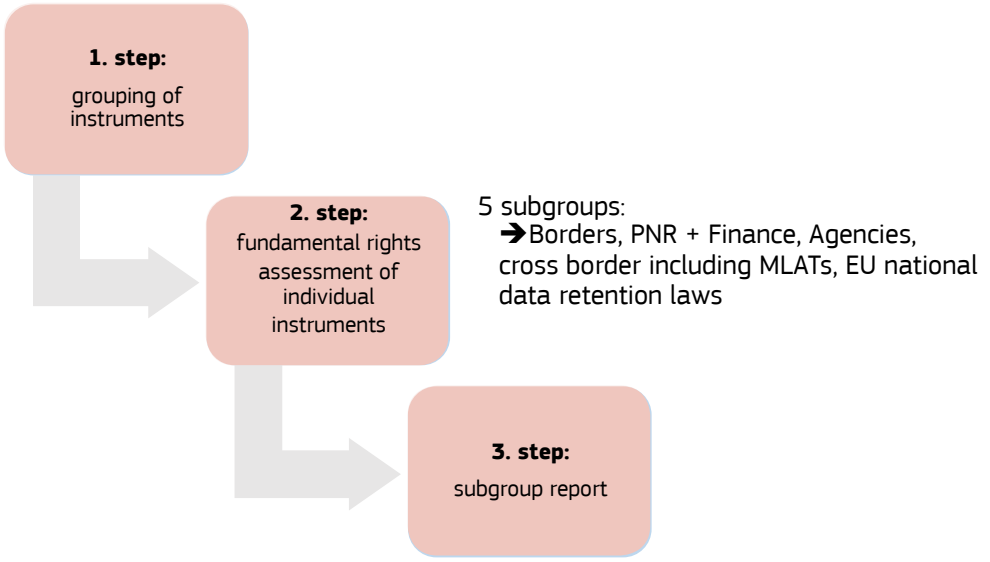

Chart 1: Overview of the adopted methodology

First step: grouping of instruments

Five (sub)groups were chosen, following on from those adopted in Task 4: borders, PNR and finance, agencies, cross-border instrument and national laws. In total, the experts analysed 78 instruments, distributed as follows: the border groups analysed nine instruments, the PNR and finance group 13, the agencies group 34, the cross-border the group 11 and the national laws group 11. Links to each piece of legislation are provided in section 3.4 and the assessments can be found in a database produced as part of the project is accessible on Brodolini website and available at the following link http://brodolini.mbs.it

Second step: fundamental rights assessment of individual instruments

In a second step, the experts carried out an instrument-by-instrument fundamental rights assessment, based on the scope and methodology set out in section 4.1. Existing EU fundamental rights assessments and analyses carried out by EU institutions, agencies and bodies were helpful in this context – for instance those of the Article 29 Working Party, the EDPS, ENISA, the FRA, the Commission and/or the EU institutions' legal services. The information mapped under Task 4 of this project served as background information. Further, a document containing case law relevant for this project was prepared and distributed to all experts.

For reasons of comprehensibility, all reports share a common structure, largely based on the proportionality test set out in Article 52(1) CFR (see section 4.1). Although some instruments share the same legal features (e.g. all agreements between Europol/ Eurojust and third states share essentially the same wording), it was agreed to include the results in separate reports instead of producing overall assessments for such instruments. The results of the individual reports were exchanged with the Commission in order to gather the views of relevant experts within different directorates. The process was finalised in March 2018.

Third step: subgroup reports

A report summarising the main findings of each subgroups' individual assesments was delivered to the Commission in November 2018. This document includes a brief overview of the assessments carried out in each subgroup and covers emerging challenges, fundamental rights infringements, the conclusions reached in each subgroup and an outline of the issues which are problematic from a fundamental rights perspective. The structure of the group reports reflects that used for the individual assessments. The group reports have been revised and are included in this section of the report; they served as one of the bases for the drafting of policy recommendations later on.

4.1.2 Challenges

During this phase of the project, specific challenges arose in assessing the current state of play of some instruments. A number of the instruments analysed were the subject of legislative proposals as well as policy debates, in particular those of the borders group. This situation necessitated an in-depth assessment of different stages of proposals, including (where possible) positions adopted by the Parliament and/or the Council at different stages of the negotiations. In cases of doubts regarding the current state of play, it was agreed with the Commission to focus on the most recently-available text or the text initially proposed by the Commission.

In addition, the contractor proposed a group assessment for instruments which share similar features, but at the request of the Commission this was ultimately changed to an individual assessment of each selected instrument. This made the process more complex and required additional efforts during both the assessment and revision process.

A summary of the main results of each group was carried out and is included in the following sections.

4.2 Borders group- report

4.2.1 Introduction

This report summarises the findings of the fundamental rights assessments of the eight instruments in the 'borders' group[62]. The instruments were placed under this heading as they require

62 Biometric passports: Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32004R2252; Regulation (EC) No 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, https://eur-lex.europa.eu/legal-content/EN/ TXT/?uri=celex:32009R0444

Customs Information System (CIS): Council Regulation No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs or agricultural matters, https://eur-lex.europa. eu/legal-content/EN/TXT/?uri=CELEX:01997R0515-20160901; Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes, https://eur-lex.europa.eu/legal-content/EN/ TXT/?uri=CELEX:32009D0917

Entry/Exit System (EES): 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, https://eur-lex.europa.eu/legal-content/EN/ TXT/?uri=CELEX:32017R2226

European Travel Information and Authorisation System (ETIAS): 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, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1240

Eurodac: Regulation (EU) 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person, https://eurlex.europa.eu/legal-content/en/TXT/?uri=CELEX:32013R0604; Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a thirdcountry national or a stateless persons], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0272(01)

European Border Surveillance System (Eurosur): Regulation (EU) No 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur), https://eur-lex. europa.eu/legal-content/EN/TXT/?uri=CELEX:32013R1052

Schengen Information System (SIS II, with regard to its use for border checks and return): Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second-generation Schengen Information System (SIS II), https://eur-lex.europa.eu/legal-content/ EN/TXT/?uri=CELEX:32006R1987; Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006, https://eur-lex.europa.eu/legal-content/AUTO/?uri=CELEX:32018R1861; Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals, https://eur-lex.europa.eu/legalcontent/AUTO/?uri=CELEX:32018R1860

Visa Information System (VIS): Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004D0512; Regulation (EC) 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas, https://eur-lex.europa.eu/legal-content/EN/ TXT/?uri=CELEX:32008R0767; Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, https:// eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-%3A32008D0633; Regulation (EC) 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code), https://eur-lex. europa.eu/legal-content/EN/ALL/?uri=CELEX:32009R0810; Regulation (EC) 390/2009 of the European Parliament and of the Council of 23 April 2009 amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organisation of the reception and processing of visa applications, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009R0390; Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EC)

No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA, https://eur-lex.

the collection and processing of personal data in relation to the crossing of borders or to migration policy. The initial collection of personal data may take place at the borders of the EU or in some other location (for example, national consulates dealing with visa applications or asylum application processing centres).

The instruments are varied in nature and range from large-scale centralised databases that are already in existence (CIS, Eurodac, SIS II, VIS) or were proposed more recently (EES, ETIAS), to networked information systems (Eurosur) and data collection measures (the Regulations governing biometric passports).

A particular difficulty that arose when assessing these instruments was that half of them was subject to ongoing legislative proposals (namely ETIAS, Eurodac, SIS II and VIS) as part of ongoing legal and policy changes as part of the 'Security Union' initiative. This required assessments of what can best be described as a 'moving target', as the proposals were subject to – or were going to be subject to – ongoing changes as part of the legislative process. Where possible, positions adopted by the Parliament and/or the Council during the negotiations (e.g. first reading positions, partial general approaches, general approach) were taken into account. Elsewhere, the analysis was based on the text initially proposed by the Commission. In either case, this is noted in the text of the individual assessments. Where relevant, the content in this summary report has been updated to take into account final texts adopted.

4.2.2 Fundamental rights assessment

While the instruments in question have all been grouped under the heading of 'borders', they have diverse aims. Equally, the personal data processed for each system varies significantly in scale and in scope. There is thus an array of impacts on a variety of different fundamental rights.

A common theme amongst the aims of the instruments is the prevention of irregular or undesired entry to or stay in the EU, along with the enforcement of return decisions. These are the primary purposes of the EES (through the system's ability to identify 'overstayers', whether visa-holders or visa-exempt), the ETIAS (to assess whether travellers are a security, irregular migration or public health risk and, if so, to deny them entry to the Schengen area), Eurosur (for the surveillance of external borders and the "pre-frontier area" in order to assess the need for 'interception' of irregular migrants) and the VIS (to facilitate enforcement of the rules on short-stay visas and denying ineligible persons entry to the Schengen area).

Rules on biometric passports were introduced with similar ends in mind – the inclusion of biometrics is intended to make the production and use of false documents more difficult, thus making irregular entry harder. The SIS II contains alerts on persons to be refused entry at the external borders of the EU. Following a 2016 proposal, in 2018 the legislation governing the SIS II was amended to underpin a more systematic role in enforcing returns (for example, through the mandatory inclusion of return decisions in the system). A proposal published in the same year on Eurodac "extends its scope for the purposes of identifying illegally staying third-country nationals and those who have entered the European Union irregularly at the external borders, with a view to using this information to assist a Member State to re-document a third-country national for return purposes,"[63] although the proposal has not yet been adopted. Currently, Eurodac has the primary purpose of supporting the implementation of the 'Dublin' system through assisting in determining the Member State responsible for an asylum application. The Customs Information System, meanwhile, functions primarily at the borders of EU Member States and allows the processing of data on possible infringements of customs and agricultural legislation.

A number of databases primarily developed for migration purposes have been or will be made available to law enforcement authorities, with access generally restricted in relation to serious crime and terrorism. This is already the case for Eurodac and VIS. National law enforcement au-

europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0302

63 European Commission, COM(2016) 272 final, 4 May 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0272(01)

thorities and Europol will also be given access to the EES and ETIAS. One of the aims of EUROSUR is to assist in exchange of information and cooperation to improve situational awareness and to increase reaction capability at the external borders for the purpose of detecting, preventing and combating illegal immigration and cross-border crime. The SIS II is primarily a law enforcement and border control database but, as noted, is being adapted to better assist with the implementation of return decisions.

As regards personal data, a common theme across many of the instruments is the collection, processing and/or storage of biometric data, which is required for five of the eight instruments (all apart from the CIS, ETIAS and Eurosur). The biometric data gathered ranges from two fingerprints and a facial image (biometric passports) to a full set of ten fingerprints and a facial image (Eurodac, under the 2016 proposal; and the VIS). The EES will require the collection of four fingerprints and a facial image from all visa-exempt travellers, and a facial image from visa-obliged travellers (10 fingerprints from this category of individual are already stored in the VIS). Following the approval of legislation in 2018, palm prints and DNA may also be included in the SIS under certain conditions.[64]

The scale of other types of personal data processed varies from instrument to instrument. The inclusion of biographical data is a mandatory feature of almost all instruments, with the exception of Eurodac (although this will change under the 2016 proposals) and Eurosur, which is something of an outlier in this group of instruments in that, formally, it permits only the inclusion of an extremely limited type of personal data (ship identification numbers). Other personal data that can be included in the systems concerns information on individuals' family and employment (VIS, ETIAS), intended destinations in the EU and by whom an invitation has been issued (VIS), data on presence in a region facing outbreaks of epidemic disease and criminal convictions, if any (ETIAS), date and time of border crossings (EES) and information on asylum claims (Eurodac). Furthermore, the legal basis of the CIS (Council Regulation No 515/97 of 13 March 1997) establishes the possibility for authorities to undertake discreet surveillance of individuals. This is also the case for the SIS II but only as regards its legal basis for police cooperation, which was beyond the scope of these assessments (SIS is examined here with regard to the legal bases for border control and return).

4.2.3 Rights to privacy and data protection

Provided for by law/legal basis

Regarding the need for interferences with individual rights to be provided for by law, problems were identified with five of the instruments.

ETIAS will check all applicants seeking permission to enter the EU to establish whether they are a potential security, health or irregular migration risk. The provisions in the proposal concerning health contained a cross-reference to relevant provisions of the Schengen Borders Code, but there were no definitions setting out what may constitute a "security" or "irregular migration" risk. This has been somewhat remedied in the final text,[65] although the definition of who may con-

64 Up to two palm prints in alerts on third-country nationals subject to a return decision and from whom the collection of fingerprints is impossible or whom are subject to a criminal law sanction (Article 4(3)(b) and (c), Regulation 2018/1860); in alerts on refusal of entry and stay on third-country nationals, (Article 20(2)(x), Regulation 2018/1861); and in alerts on persons wanted for arrest for surrender or extradition, missing or vulnerable people who need to be prevented from travelling, persons sought to assist with a judicial procedure, persons for discreet, inquiry or specific checks, on unknown wanted persons (Article 20(3)(y), Regulation 2018/1862). DNA may only be included in alerts on missing persons who need to be placed under protection, and may be profiles of that persons or of their "direct ascendants, descendants or siblings" (Article 42(3), Regulation 2018/1862).

65 "Public health risk" has become "high epidemic risk" and is defined as "any disease with epidemic potential as defined by the International Health Regulations of the World Health Organization (WHO) or the European Centre for Disease Prevention and Control (ECDC) and other infectious diseases or contagious parasitic diseases if they are the subject of protection provisions applying to nationals of the Member States" (Article 3(8)). "Illegal immigration risk" is now defined as "the risk of a third-country national not fulfilling the conditions of entry and stay set out in Article 6 of Regulation (EU) 2016/399" (Article 3(7)).

stitute a "security risk" is still rather loose: "the risk of a threat to public policy, internal security or international relations for any of the Member States" (Article 3(6)).

The question of legal certainty is also a concern regarding the 2013 Regulation on Eurodac, insofar as it does not contain a definition of "in connection with the crossing of the external border." This broad wording makes it in principle possible to enter into Eurodac data on persons irregularly present in EU territory potentially a significant time after they have crossed the border and without requiring the establishment of a clear link with that crossing. The 2016 proposal does not remedy this problem as it contains no definition of the phrase in question and broadens the scope of data storage to include persons irregularly present in the territory, rather than just applicants for international protection.

Changes to the Eurodac system in 2013 that defined the conditions for giving access to the system to law enforcement agencies also raise concerns. The project team's opinion is that these changes violated the purpose limitation principle, insofar as access is provided to personal data held in the system prior to the entry into force of the 2013 Regulation, which changed the purposes for which data held in Eurodac could be used. Regarding SIS II, the national criteria for inserting alerts on third-country nationals are available in national legislation which makes it more difficult for individuals to know under what circumstances their data may be collected, stored and further processed than if the criteria were published in a single location. A harmonisation of national criteria would assist in resolving this issue, although rights for the individual to access and, if necessary, correct or delete data held in the system are provided for. Finally as regards the CIS, there is no obligation to publish the specific list of authorities with access to the system (although they all have to have a role in the enforcement of customs legislation), making it difficult for individuals to know which authorities are able to access and process their personal data.

Respect for the essence of the rights

Only one instrument assessed here has raised concerns regarding respect for the essence of rights. It would conceivably be possible for use of the Eurosur system to breach the right to seek asylum, were it to be used to assist in preventing individuals seeking international protection from reaching EU territory. It should be noted that these concerns remain hypothetical and depend on the future deployment and use of the system. The concerns raised should be taken into account when any possible changes to the composition and use of the system are considered.

Legitimate aim

The assessments did not identify any problems regarding the legitimacy of the aims of the instruments examined. This concern the prevention of illegal entry to the EU (biometric passports, EES, ETIAS, Eurosur, SIS II, VIS); combating serious crime and terrorism (EES, ETIAS, Eurodac, Eurosur, SIS II, VIS); the development and implementation of a common asylum policy (Eurodac); preventing, investigating and prosecuting breaches of agricultural and customs legislation (CIS); and improving the exchange of information in order to ensure a high level of security within the EU (SIS II). These aims have either been confirmed as legitimate by the Court of Justice or can be considered legitimate on a prima facie basis.

Necessity and proportionality

Based on the assessment of a number of the measures, the authors of the report consider that taken as a whole, the foreseen intrusions on the rights to privacy and data protection have not been sufficiently justified in terms of necessity and proportionality. These concerns have been grouped under the headings that follow.

a) Centralised databases

A number of issues were identified with the centralised databases of the EES, the ETIAS and Eurodac.

The authors consider that the Impact Assessment of the EES proposal issued in 2013[66] does not demonstrate the necessity and proportionality of establishing a centralised database for the EES. It is the author's view that border checks could be sped up without the centralised storage and processing of personal data. In the case of visa-exempt travellers, it would be possible to use the photographs and/or fingerprints contained in e-passports to verify individuals' identity, as is done for EU citizens.[67] The identity of travellers subject to a visa requirement can be verified against the information contained in the Visa Information System, as currently done. These alternatives are clearly less restrictive of fundamental rights than the situation foreseen by the EES. The strongest argument made for a centralised database in relation to border checks is that "a traveller may change identity, legitimately (e.g. name change after marriage) or illegitimately, or in the worst case may maliciously use different passports to hide his/her identity." No evidence has been provided to demonstrate more precisely the practical significance of the alleged "significant minority" that holds two passports. While such a situation may present a genuine problem, the number of individuals concerned is likely to be minimal in relation to the total number of people in question, providing a very weak justification for such a large-scale data collection and processing scheme.[68]

The second policy objective relates to identifying people who overstay the length of time they are permitted to remain in the Schengen area (whether they are obliged to hold a visa or not). There is a profound lack of statistical information about the scale of overstaying in the EU. Although, amongst other objectives, the EES in itself is intended to close this gap, there have been no ad-hoc surveys or partial collections of statistics undertaken to estimate the magnitude of the problem. The intrusions upon Articles 7 and 8 of the Charter required by the EES in the name of dealing with overstaying cannot be justified in the absence of data that goes some way towards genuinely demonstrating the scale of the problem. In this respect it cannot be said that the measures foreseen can be shown to address a "pressing social need", a prerequisite for an interference with fundamental rights to be considered necessary.[69]

The authors of the report also consider that ETIAS lacks sufficient justification of its necessity and proportionality. An assessment of the efficiency of existing data processing systems that serve, or could serve, similar purposes to the ETIAS (for example, API and PNR) has not been carried out.[70] The proposal was not accompanied by a genuine impact assessment, meaning that the data processing foreseen by the system has never been justified in detail.[71] Furthermore, there is no evidence that visa-exempt travellers (with whom the system is concerned) are, as a group, particularly likely to present security, public health or irregular migration risks.

The assessment of Eurodac also questioned the necessity and proportionality of its centralised database, keeping in mind that the database's primary purpose is the implementation of the Dublin system. If the Dublin system itself is not functioning properly – as has been widely recognised – the legitimacy of the centralised data storage has to be called into question. In this respect, the

66 There has been an EES proposal in 2013 and a new one in 2016 at the same time as the previous one was withdrawn. The impact assessment done for the 2013 proposal reviews the options for building the EES. This impact assessment can be found under https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=SWD:2013:0047:FIN

67 Nationals of visa-exempt countries must hold a valid biometric passport to be able to undertake visa-free travel. The verification of EU nationals' identity is currently undertaken primarily by using the facial image stored in the passport.

68 European Commission, SWD(2016) 115 final, https://eur-lex.europa.eu/legal-content/EN/ TXT/?uri=CELEX-:52016SC0115

69 ECtHR, Case of S. and Marper v. the United Kingdom (Application nos. 30562/04 and 30566/04), 4 December 2008, para. 101, http://hudoc.echr.coe.int/eng?i=001-90051

70 These systems currently only concern passengers arriving by air, and their scope is thus not as wide as the ETIAS. Nevertheless, the risk of partial duplication of other databases which are not fully implemented yet seems to impose a high sacrifice of data protection rights with unclear benefits. To avoid redundancy an assessment of the already-existing systems should be carried out.

71 The system was the subject of a feasibility study carried out for the European Commission by PwC. This examined the usefulness and relevance of different data elements for the system, outlined their potential impact on privacy and looked at possible data protection safeguards. However, this cannot be considered as equivalent to an in-depth assessment of the necessity and proportionality of the data collection proposed for the system undertaken against the requirements of the Charter of Fundamental Rights and relevant case law.

2016 proposal that would extend the scope of Eurodac to play a role in the implementation of return policy was not accompanied by an impact assessment. As a consequence, the assessment of the necessity and proportionality of the proposed extension and the suggestion of possible alternative policy options could not be carried out. For this reason, the proposed extension has not, to date, been sufficiently justified.

b) Biometric data

A number of the instruments assessed require the processing of biometric data, considered a special category of data under the GDPR and LED and thus meriting specific justifications for its collection and specific protections when it is processed. As far as the GDPR is concerned, the collection of biometric data merits specific grounds for derogating from the prohibition principle enshrined in the GDPR.

Under EU rules first established in 2004 and updated in 2009, all passports issued by Member States (bar Ireland and the UK) require the inclusion of biometric identifiers: a facial image and two fingerprints, with the aim of preventing the fraudulent production, acquisition and use of passports and travel documents. With regard to protecting against fraudulent acquisition and fraudulent use, the inclusion of fingerprints could have a positive effect. However, the gathering of fingerprints is only necessary to the extent that the checking of fingerprints is enacted. Based on the limited evidence available, it appears that such checking is in practice extremely limited. This suggests that the storage of fingerprint data goes beyond what is necessary to achieve the aims pursued. At the very least it must be observed that gathering the data and storing it within passports, without using it for the aims foreseen, does not meet the requirements that personal data processing be limited to that data which is adequate, relevant and not excessive.

The EES will require the collection of four fingerprints and a facial image from all visa exempt travellers, and a facial image from visa-obliged travellers (this latter category also has ten fingerprints and a facial image stored in the central database of the VIS). The intention is to facilitate border management (by enabling the automation of border checks) and to make it easier to establish and to identify individuals who have 'overstayed' (an ancillary objective is the possibility, under certain conditions, for law enforcement agencies to access data held in the system). However, the only compelling justification for including biometric data in the system's centralised database concerns what is likely to be a very small minority of third-country nationals – specifically, those who overstay their visa and do not retain any travel or identification documents.[72] Given this, the need to gather and process biometric data from every individual covered by the scope of the system has not been sufficiently justified.

With regard to Eurodac, the authors of the report consider that there has never been a detailed assessment of the need to collect the full set of 10 fingerprints from the individuals covered by the scope of the system. The 2016 proposal adds a further biometric - a facial image - without any substantial justification – as noted above, there was no impact assessment to accompany the proposal. Equally, it is unclear why there is a need to gather 10 fingerprints from visa-obliged travellers when their inclusion in the VIS is mainly used for the verification of identity and, for this purpose, fewer fingerprints would suffice.

A related issue concerns the possibility of false fingerprint matches in Eurodac, an issue that although highly infrequent does not appear from the available information sources to have been

72 There would be a need for a centralised database holding biometric data in the case of individuals who overstay their entry permission and, when apprehended by the authorities, do not own any identification documents. However, there is no meaningful data on the number of people overstaying their entry permission in general; nor are there statistics on this particular subset of overstayers. This makes it impossible to establish whether the establishment of the system is a proportionate response to the stated problem. The Commission's impact assessment for the EES cites an estimate that "1,9 to 3,8 million persons are irregular migrants," which "is assumed to increase by another 250,000 persons on a yearly basis." The estimate of up to 3.8 million people was described as "low quality" and "not very reliable" by the project that produced it in 2009 and was accompanied by a warning that "we should not put too much trust in the estimates at the present stage." The Commission itself states in the impact assessment that the figures are both "conservative and by now outdated," and that "accurate figures or estimates are not available." See: CLANDESTINO Project, 'Final Report', 23 November 2009, p.106, http://clandestino.eliamep. gr/wp-content/uploads/2010/03/clandestino-final-report_-november-2009.pdf.

given sufficient attention given the particularly serious consequences it may have for those included in the system. One such case was highlighted in a 2018 report by the Fundamental Rights Agency and indicates a potential need for improved access to remedies for those affected.[73]

The processing of biometric identifiers (fingerprints and facial images) was fully implemented in SIS II by March 2018, to enable both the verification and identification of individuals for whom biometrics are available. The 2016 proposals would extend the biometric capabilities of the system by making it possible to include DNA and palm prints in the system for certain purposes (which are very limited in the case of DNA); they also abolish the former prohibition on including sensitive data in the system.[74] However, in general, the processing of biometric identifiers in the SIS II does not take into consideration the age of the individuals, nor the different categories of persons against whom alerts are inserted (e.g. criminals, suspects, irregular migrants). The authors of the report consider that irregular migrants who are the subject of a return decision should not receive the same treatment with regard to their identification at borders or within the territory as third-country nationals or EU nationals who have been convicted of a criminal offence. Notwithstanding the usefulness of biometrics for the verification of individuals' identity which is considered by the Commission as the justification for their use, there is a qualitative difference between the perpetration of a criminal offence and the violation of immigration laws, which may be punishable by a fine only. An analogy can be drawn with national criminal justice systems, in which only offences of a certain gravity or particular categories may merit the retention of biometric identifiers.

Proposals published in May 2018 to reform the VIS foresee the existing biometric data collected by national authorities being included from applicants for other visas than the short-stay visas. In particular, there would be a new obligation for the storage of existing biometric data (namely photographs and fingerprints) that would have been collected by national authorities during the processes that are not harmonised at EU level, like from long-stay visa holders.[75] The proposals also foresee inclusion in the system of fingerprints from children the age of six and up.[76]

Regarding the inclusion of the facial images and fingerprints from long-stay visa holders in a centralised database, the impact assessment considered that "it would be technically feasible" to meet new policy demands "only with facial image" when only identity verification is needed and facial images are sufficiently recent, while other biometrics "could be considered after a period

73 "A provider of legal assistance in Sweden explained a case whereby an asylum seeker was transferred to another Member State, in accordance with the Dublin procedures. However, the transfer was based upon a false biometric match. In the other Member State, the fingerprints were taken again and there was no match, which proved that the asylum seeker was indeed right in objecting to his transfer. Nonetheless, the asylum seeker continued to be met with distrust. The processing of the case was delayed by 6 months to 1 year. He was detained in Belgium and had no access to legal representation, even after the mistake was discovered. As a consequence, the applicant suffered mental health issues. The provider of legal assistance representing the asylum seeker in Sweden could not legally challenge the claims and statements made by the Swedish Migration Agency. The provider of legal assistance has no opportunity to undertake a biometric test to prove that the client was right. Although conducting such a test should be possible in theory, it would be difficult in practice. Furthermore, the legal assistance did not have access to all relevant information and documents regarding the events that had taken place in Belgium. Regardless of the arguments or evidence the legal assistance presented, the authorities appeared to have already decided on the case. Later on, the provider of legal assistance had troubles getting in contact with the client. The provider of legal assistance found it close to impossible to understand who was responsible for the mistake and if there were any legal possibilities to claim compensation. In any case, such a claim would have had to be pursued pro bono." Fundamental Rights Agency, 'Under watchful eyes: biometrics, EU IT systems and fundamental rights', March 2018, p.76-77,

https://fra.europa.eu/en/publication/2018/biometrics-rights-protection

74 These provisions remain in the new rules as adopted. DNA data may only be entered on missing persons, children at risk of abduction, children who need to be prevented from travelling abroad, and vulnerable adults who need to be prevented from travelling (Article 32(1), Regulation 1862/2018). Furthermore, DNA data can only be entered when photographs, facial images or fingerprint data are not available (Article 42(3)). Palm prints are considered as complementary or alternative to fingerprint data.

75 Articles 22c(f) and (g), Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0302

76 Article 3(2)(c) of Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0302

of assessment."[77] The proposal itself ignores this suggestion and proposes the inclusion of facial images and fingerprints, yet there has been no assessment of the necessity and proportionality of doing so. However, such an assessment is necessary for two reasons: firstly, the format of long-stay visas remains a national competence and the inclusion in EU legislation of a requirement for two fingerprints appears to be a case of minimum harmonisation without it being declared as such. Secondly, as biometrics, fingerprints are one of the "special categories of data" recognised by Article 9 of the GDPR and merit special consideration and protection.

With regard to lowering the minimum fingerprinting age to six years old, the proposal concerns the sensitive data (fingerprints) of a vulnerable group (children) and the threshold for justifying such an intrusion of fundamental rights should thus be set extremely high. The principal reason for lowering the fingerprinting age is stated in the proposal to be the protection[78] yet this is not included as one of the purposes of the VIS.[7980] Furthermore, the feasibility study accompanying the proposal does not contain any meaningful data on the number of children travelling to the Schengen area with a visa that are trafficked, go missing or are abducted that would justify the introduction of the fingerprinting measure on child protection grounds.81 Neither are there any specific safeguards surrounding the protection of children's fingerprint data. As published, the authors consider that the proposals cannot be said to meet the requirements of necessity and proportionality for processing this type of personal data.

A final issue regarding fingerprint data in the VIS concerns the apparent abolition of quality requirements for storage in the central system.[81] The authors of the report fear that this increases the risk of misidentification for any individual with their fingerprints stored in the VIS (requiring the carrying out of more lengthy identification procedures) and may particularly effect children due to the changing nature of their fingerprints, although studies point to that this does not affect the accuracy of identity verifications[82]

c) Alphanumeric and other data

All the instruments in question mandate the processing of alphanumeric personal data, to varying extents, with the exception of Eurosur and Eurodac. However, alphanumeric data would also be included in Eurodac the basis of a proposal published in 2016.

The 2016 Eurodac proposal foresees an expansion of the types of data to be stored in the system (with biographical data to be included alongside biometric data and the limited set of alphanumeric data that is currently collected[83]), as well as an expansion of the categories of person covered by the system (irregular migrants will also have their data recorded, alongside applicants for international protection). The justification offered for the collection of alphanumeric data is that it will "allow immigration and asylum authorities to easily identify an individual, without the need

77 Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-:52018SC0195

78 Explanatory memorandum of the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0302

79 Article 1(2), Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0302

80 Ecorys, 'Feasibility and implications of lowering the fingerprinting age for children and on storing a scanned copy of the visa applicants' travel document in the Visa Information System (VIS)', March 2018, pp. 89-94, https://publications.europa.eu/en/publication-detail/-/publication/e96fb1d8-79b6-11e8-ac6a-01aa75ed71a1/language-en

81 Eu-Lisa, 'VIS Report', July 2016, p.10, https://www.eulisa.europa.eu/Publications/Reports/VIS%20Reports%20 on%20the%20technical%20functioning%202015.pdf

82 Jrc Technical report Automatic fingerprint recognition: from children to elderly, 2018, http://publications.jrc.ec.europa.eu/repository/bitstream/JRC110173/jrc_fingerprint_children_elderly_study_v.final.pdf

83 Fingerprint data; Member State of origin, place and date of the apprehension; sex (i.e. gender); reference number used by the Member State of origin; date on which the fingerprints were taken; date on which the data were transmitted to the Central System; operator user ID.

to request this information directly from another Member State."[84]

The proposal for the EES sought to justify each data element individually. Unfortunately, that approach was not taken with regard to the Eurodac proposal and, notwithstanding the fact that the proposed changes build on an existing system rather than introduce a new one, there has been no such examination of the necessity and proportionality of each particular data element. It appears that the additional data has more to do with the migration control aspects of the proposal than those concerned with implementation of the Dublin Regulation. This is particularly so given that no operational issues have been reported regarding the current Dublin system that would require additional data.

The rules governing the CIS were put in place over 20 years ago and in this regard are lacking the specificity of many subsequent instruments that require the processing of personal data. In the 1997 Regulation, there is a need for clarification of the meaning of the phrases "reasonable grounds" and "grounds to suspect" in relation to undertaking "special watches" to ascertain possible breaches of the law. Likewise, rules permitting Member States to transmit "all relevant information" and "all information in their possession" to another Member State and provisions allowing data held by the Commission to be "indexed" and "enriched" also require clarification.[85]

As noted above, the ETIAS proposal was not accompanied by a genuine necessity and proportionality assessment. Some categories of data proposed for inclusion in the system were highly questionable. This was particularly so for health data, which was to be gathered based on self-declaration and so may well have been inaccurate. The foreseen retention period (five years) may also have led to accurate information becoming outdated. A more specific definition has been included in the final text and self-declarative questions concerning applicants' health have been removed from the application form.

The ETIAS proposal also foresaw collecting data on criminal convictions, in particular on whether the travel applicant "has ever been convicted of any criminal offence in any country," raising obvious problems with regard to the potential negative effects (denial of travel) based on convictions from untrustworthy judicial systems, or convictions for acts that are not criminal offences in the EU. The assessment carried out for this project highlighted the need to consider setting thresholds regarding the gravity of offences concerned or providing a list of comparable offences in EU law which are relevant. The final text improves upon the proposal by including a list of relevant offences and time periods within which they must have been committed to be taken into consideration for the purposes of an ETIAS application. These changes regarding data on health and criminal convictions should be illustrative for any future proposals concerning the collection and processing of personal data.

With regard to Eurosur, the Regulation is not specific enough regarding the types of data that can be processed as part of the system. The personal data processed by Member States as part of the system is governed by national law, but the non-exhaustive set of data sources for National Coordination Centres, set out in the Regulation, could clearly permit the gathering of significant amounts of detailed personal data.[86] Were a National Coordination Centre established in order to

84 Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013, https://eur-lex.europa.eu/legal-content/AUTO/?uri=CELEX:52016PC0272(01)

85 Council Regulation No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs or agricultural matters, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:019 97R0515-20160901

86 The numbered and lettered points carry the text from the Regulation (Article 9), those in square brackets carry the text from the Eurosur handbook:

2. The national situational picture shall be composed of information collected from the following sources:

a. the national border surveillance system in accordance with national law; [land, maritime and air border surveillance systems]

b. stationary and mobile sensors operated by national authorities with a responsibility for external border surveillance; [radar: position course, speed, time, size of target; cameras: pictures, videos, time, direction, image-processed data; active range gated cameras: target distance, ship identification; radio frequency sensors/direction systems: position,

meet the requirements of the Eurosur Regulation, it could be questioned whether that legislation contains "clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data."[87] Furthermore, the inclusion of images and video in the system may include personal data, an issue which does not appear to have been given sufficient consideration in either the Regulation or the Eurosur handbook. Neither is the text clear on whether, under Article 12, personal data may be processed outside of the scope of that regulated by Article 13, which only permits Frontex to process personal data concerning ship identification numbers.[88] Finally, it would be welcome for the text to explicitly reference the applicable data protection regime.

Regarding SIS II, one problem raised by the assessment undertaken for this project concerned the lack of harmonised rules governing the inclusion of entry bans in the database. This is likely to be remedied by the 2018 Regulation, which will make the inclusion of such bans mandatory.[89] However, under the Return Directive, Member States are granted wide discretion on the nature of entry bans and SIS II alerts will thus be registered solely because of the issuance of a return decision.[90] Return decisions will also be included in alerts in the system under the 2018 SIS legis-

operating frequency, radio type; hydrophone systems: ship movement data, ship identification]

c. patrols on border surveillance and other monitoring missions; [sea, land and air border surveillance missions; military assets assisting a law enforcement mission; search and rescue missions; customs/fishery control missions; maritime safety missions (e.g. oil spill detection)]

d. local, regional and other coordination centres; [local and regional coordination centres; maritime rescue coordination centres]

e. other relevant national authorities and systems, including liaison officers, operational centres and contact points; [national contact points for the prevention of illegal immigration/drug smuggling; operational centres for cross-border cooperation; national centres for fishery control/maritime safety; contact points between neighbouring Member States (e.g. for false documents, borders, customs, or tackling cross-border vehicle crime); embassies, consulates and liaison officers in third countries]

f. the Agency; [EUROSUR Fusion Services including information from the common application of surveillance tools (e.g. vessel detection service, satellite imagery, terrain information, weather forecast); analytical products developed by the Agency's risk analysis unit (e.g. impact levels allocated to the border sections); joint operation information, including event reports sent through the joint operations reporting application (JORA); information on the Agency's own assets]

g. national coordination centres in other Member States; [Neighbouring border sections: incidents, tactical risk analysis reports and, possibly, patrols; regional networks; European patrols network (EPN)]

h. authorities of third countries, on the basis of bilateral or multilateral agreements and regional networks as referred to in Article 20; [regional networks; bilateral cooperation]

i. ship reporting systems in accordance with their respective legal bases; [Automatic identification system (AIS); Vessel monitoring system (VMS); Union Maritime Information and Exchange System, including SafeSeaNet (SSN) and the Long-range identification and tracking system (LRIT)]

j. other relevant European and international organisations;

k. other sources.

87 CJEU, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland, 8 April 2014, para. 54, https://eur-lex. europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0293

88 According to Article 13, personal data to be gathered by or provided to Frontex is strictly limited to ship identification numbers and must be processed in line with Frontex's founding legislation. These appear to rule out Frontex itself storing personal data gathered under Article 12 (on the "common application of surveillance tools"), but this does not seem to be the case for personal data gathered under Article 12 that may be provided by Frontex to a Member State or to a third country. Article 20 appears to imply that such gathering and provision of personal data is possible, by referring explicitly to legislation concerning the protection of personal data: "Any exchange of information with third countries acquired via the common application of surveillance tools shall be subject to the laws and rules governing those tools as well as to the relevant provisions of Directive 95/46/EC, Regulation (EC) No 45/2001 and Framework Decision 2008/977/JHA." In this respect there would appear to be a gap in the data protection provisions of the Regulation.

89 Article 24(1)(b), Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1861

90 An evaluation of the implementation of the Return Directive found that although provisions on procedural safeguards had largely been implemented into law by the Member States, their practical application was far more problematic. European Commission – Directorate-General Home Affairs, 'Evaluation on the application of the Return Directive (2008/115/EC)', 22 October 2013, pp.115-128, http://ec.europa.eu/smart-regulation/evaluation/search/ download.

lation and will be systematically deleted after an individual's departure, according to provisions in Article 6 and Articles 8 to 12. However, in certain cases that would occur in exceptional circumstances, the burden for ensuring that such an alert is deleted may lie with the individual who has been returned, who under Article 14 has to "demonstrate that he or she has left the territory of the Member States in compliance with the respective return decision."[91] Thus, it is essential that such individuals are notified about the alerts and effective procedures are established to ensure that deletion is properly monitored.

d) Retention periods

Article 33 of the Regulation governing the CIS states that data "may not be stored for more than five years with an additional period of two years if justified." It is not clear whether this additional two-year period is, or can be, recurring and for how long it may recur. However, the relevant Decision does require that there be a review "at least annually" by the supplying Member State as to whether information should be retained within the system.

National laws govern the retention of data held in the accompanying FIDE (Customs Files Identification Database), although upper limits are set by the Regulation (six years for data on offences identified but as yet unpunished and ten years for data on investigation files that have led to a conviction or fine). The legislation does not offer "objective criteria in order to ensure that it [the data retention period] is limited to what is strictly necessary."[92] In relation to offences identified but as yet unpunished, the retention period may exceed statutes of limitations established by national law and thus cease to serve a purpose in relation to punishing the offence identified. On the other hand, if data on offences identified but as yet unpunished does not include personal data, such a retention period could be justified; the same can be said for data on investigation files that have led to a conviction or fine.

The assessment of the EES proposal raised concerns over the lengthy retention periods foreseen – particularly in comparison to the 2013 proposal[93] – and suggested that some element of consent could be introduced into the procedure regarding the retention of data on travellers who comply with entry and exit requirements; it should be up to the individual in question whether they wish to have their data retained or not. With regard to the retention of data for the purpose of risk analysis, it is not clear why there is a need to retain every data element in records concerning travellers who comply with the obligations placed upon them; a record of their entry and exit time should be sufficient, if it is required at all. The same can be said regarding the retention of information for visa issuance. As it stands, the system appears more intrusive upon the fundamental rights of 'bona fide' travellers than it need be. The legislators eventually settled on a general retention period of three years for law-abiding travellers, and a five-year retention period for alerts on overstayers. The authors of the report still consider this latter period excessive.

The blanket retention period for all types of entry refusals in the EES (three years) is also disproportionate – data on an individual refused entry for not having a valid travel document should not be treated in the same way as an individual considered a threat to public policy, internal security, public health or international relations. However, the related data elements within individual records have been differentiated for different types of refusal in the final Regulation.

---

do?documentId=10737855

91 Article 14, Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1860

92 Joined Cases C-293/12 and C-594/12, Digital Rights Ireland, 8 April 2014, para. 60, https://eur-lex.europa.eu/ legal-content/EN/TXT/?uri=CELEX:62012CJ0293

93 The law provides for a retention period of three years and a day for files and records on those registered as exiting the Schengen area within the permitted time period of their stay, three years on those refused entries to the Schengen area, and five years on those on whom there is no exit record registered. Whilst improving upon the 2016 proposal (which foresaw a blanket retention period of five years), it is significantly more restrictive than the 2013 proposal, which foresaw retention of entry/exit records for a maximum of 181 days where an exit was recorded, and five years when no exit was recorded.

Regarding the ETIAS, the assessment of the proposal undertaken for this project considered that the retention periods foreseen[94] could not be considered necessary or proportionate, as no detailed analysis or justification was offered and no alternative, less intrusive, options were suggested as comparative policy options. The CJEU has made clear that measures concerning data retention must make a "distinction… between the categories of data… on the basis of their possible usefulness for the purposes of the objectives pursued." The authors of the report consider that intrusions upon fundamental rights foreseen were not "precisely circumscribed by provisions to ensure that [they are] actually limited to what is strictly necessary," and thus could not be said to meet the tests of necessity and proportionality.

There are improvements in the agreed text, although the retention period remains five years following the last decision to refuse, annul or revoke a travel authorisation. Regarding approved applications, the application file is to be stored for the period of the travel authorisation – reduced to three (from five) years or until the expiry of the travel document the authorisation is attached to, whichever is sooner[95] – unless the applicant gives their explicit consent for it to be further stored. This latter period may not exceed three years following the end of the authorisation's validity period.[96]

With regard to Eurodac, the 10-year retention period of asylum seekers' fingerprints has never been properly justified, although during negotiations on the Regulation there was an attempt to reduce the period to five years.[97] The "marking" and retention of the data held on individuals for a further three years after they have been granted international protection for potential law enforcement purposes has never been sufficiently explained, and treats an ancillary purpose of the system (law enforcement access) as a reason for extended data retention.[98] The authors of the report consider the storage period for data on irregular border crossers (18 months) disproportionate as it does not correspond to the Dublin rules on cessation of responsibility for asylum claims (12 months after the date on which an irregular border crossing took place). This will be increased to five years under the 2016 proposal.[99] That proposal will also permit the storage of data on persons for return purposes, but taking into account the maximum length of detention for the purposes of return to the country of origin (18 months under the current Return Directive), the five year retention period seems unreasonably long. This retention period is the same as that for data on overstayers stored in the EES, for storing information on a visa in the VIS and the maximum duration of an entry ban under the Return Directive. If a connection with the length of the entry ban exists, it should be explicitly mentioned and the length of the retention period should be adapted to the length of the particular entry ban, which is often less than five years.

The retention period established by the VIS Regulation is based on a 'catch-all' approach without

94 According to Article 47 of the proposal, each application file for the system would have been stored for the period of validity of travel authorisation (five years or until the expiry of the travel document registered during the application); five years from the last entry record of the applicant stored in the EES (with which the ETIAS is to be "interoperable"); or five years from the last decision to refuse, revoke or annul the travel authorisation.

95 Article 36(5), Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1240

96 Article 54(2), 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, https://eur-lex.europa.eu/ legal-content/EN/TXT/?uri=CELEX:32018R1240

97 The Parliament did suggest reducing the retention period to five years but the amendment was ignored by the Council. See: Jonathan Aus, 'Eurodac: A Solution Looking for a Problem?', European Integration Online Papers, 2006 (10)

98 Pursuant to Article 18 of the recast Regulation, the data of beneficiaries of international protection are marked by the Member State which granted protection and retained for a further three years for potential law enforcement use. This is a novelty of the Regulation, since under the former regime when an asylum seeker was granted international protection, their data were immediately blocked and no further use of the data could take place. Hence, the marking of data is an intermediate stage between the full use of the data of beneficiaries of international protection and the complete blocking of use of this data, which takes place only after the expiration of the three-year period. As such, an ancillary purpose of the system (law enforcement access) extends the storage period of data.

99 Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac', https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0272(01)

any selective criteria requiring differentiated retention periods. It thus fails to take into account the different situations that may arise and the different types of visas that come within the scope of the VIS. In particular, cases where a visa applicant has been detected making duplicate or fraudulent visa applications may justify a longer retention period than in cases involving individuals whose visas have been issued without any problems. The authors of the report also consider that there is also a need to re-evaluate the retention period for visa applications that have been discontinued, as the individuals in question have only a very indirect relation with the EU and should not be put on the same footing as 'risky' travellers whose application has been rejected. Differentiated treatment is also necessary regarding refusal of visas, depending on the reason for refusal.

e) Access by law enforcement agencies

The threshold for law enforcement access to data in the ETIAS is lower than that set out for other comparable systems, requiring only that there be "reasonable grounds… to consider that the consultation of the data stored in the ETIAS Central System may substantially contribute to the prevention, detection or investigation of any of the criminal offences in question." For the VIS and for Eurodac, there must be reasonable grounds to believe that law enforcement access "will substantially contribute". The difference between the two, then, rests on the distinction between the possibility and the certainty (or at least a very high likelihood) that access to data will contribute to a specific case.

While it is clear from systems currently in use (VIS and Eurodac) that law enforcement access is relatively limited, it would be preferable for law enforcement access to non-policing databases to be provided on the basis of equally high standards for all the relevant instruments, taking into account principle of proportionality. In this regard, it must be highlighted that there is clearly the possibility of introducing more stringent access requirements, for example by requiring "clear indications" as a basis for reasonable grounds, as was raised within the Council during discussions on the VIS Council Decision.[100] At the same time, assessments of how data contained in those systems has been used by law enforcement authorities and with what effect would assist in evaluating whether that access is genuinely necessary.

With regard to Eurodac, the extension of purpose provided for in the 2013 proposal and its continuation on the basis of new rules does not comply with the purpose limitation principle, at least with regard to data accessible under these provisions that was inserted in the system before they came into force. It is unfortunate that an impact assessment concerning the extension of access to law enforcement agencies was never undertaken, as it could have offered a meaningful exploration of the policy options available and the justifications underpinning them.

The same point can be made regarding the VIS – law enforcement access should have been properly assessed in terms of its necessity and proportionality in the fight against terrorism and other serious crimes. While there are clear conditions regulating access by law enforcement agencies, the simple fact that a 'first pillar' database was opened up to those agencies introduces in the opinion of the authors of this report a generalised suspicion that third-country nationals subject to a visa requirement may be potential terrorists or criminal offenders, and this group is under a greater risk of being exposed to law enforcement measures or covert surveillance than those whose data is not held in the VIS. The VIS was designed with a view to supporting the administration of visa policy and not as a police cooperation tool, which the CJEU judgment in UK v Council[101] made clear.

100 Whilst consultation of VIS data by law enforcement authorities cannot take place on a routine basis, the current wording of Article 5(1) of the VIS Decision on the conditions of access leaves wide discretion over access by police authorities. The threshold for allowing access could have been set higher by requiring the existence of factual indications as a basis for reasonable grounds (Council document 5456/1/07). Although it was then submitted that this condition could de facto make it impossible to access the VIS for the prevention of criminal offences, the substitution of "factual indications" with "clear indications" would have been a more balanced approach (Council document 11062/06, https://data.consilium.europa.eu/doc/document/ST-11062-2006-INIT/en/pdf). Such an approach has been endorsed by the ECtHR in *Zakharov v Russia (Application no. 14881/03), 5 October 2006,* http:// hudoc.echr.coe.int/eng?i=001-77266

101 CJEU, Case C-482/08, United Kingdom of Great Britain and Northern Ireland v Council of the European Union, 26 October 2010, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62008CJ0482

The verification process by which competent authorities may gain access to Eurodac, the EES, the ETIAS and the VIS also raises some questions. For all four systems, the process works in essentially the same way – the nomination of a central access point for verifying requests for access to data by law enforcement authorities. These central access points can be part of the same organisation as the authority seeking access. While the legislation requires that they act independently, future evaluations should examine whether they meet the requirements of EU law and CJEU jurisprudence for "prior review carried out by a court or by an independent administrative body."[102]

National security and intelligence agencies (understood here as agencies responsible for national security that fall under the sole competence of the Member States, as provided for in the treaties) are explicitly excluded from access to Eurodac. However, given that the EU has no competence with regard to national security, it is not clear how this could be enforced. Meanwhile the competent authorities with access to SIS and VIS include security and intelligence agencies, but it is hard to see how EU legislation might address any problems arising from this access.

f) Purpose limitation

The Regulation on CIS permits partners of the system, including Europol and Eurojust, to use data "for administrative or other purposes"[103] which diverge from those set out in the rules (although such use must be within the context of the enforcement of agricultural and customs legislation),[104][105] if authorised by the CIS partner that introduced the data into the system or the Commission. The introducing partner or the Commission may set out conditions on that use, which must also be in line with the laws and regulations of the Member State making use of the data, although "other purposes" is undefined. The term would benefit from clarification or the addition of a list of what those other purposes may be.

The SIS II Decision allows the further processing of data on certain categories of persons under certain conditions.105 This can be done when it is "linked with a specific case and justified by the need to prevent an imminent serious threat to public policy and public security, on serious grounds of national security or for the purposes of preventing a serious criminal offence."[106][107] In the author's view, the lack of clear definitions on what constitutes an "imminent serious threat to public policy and public security" or "preventing a serious criminal offence" causes problems with foreseeability, although reaching agreement on such terms is undoubtedly complicated107 (this issue is also reflected in the ETIAS legal basis, which seeks to define "security risk" in relation to a series of other non-concrete factors[108]). Furthermore, in the author's view the legislation does not make clear that only those authorities foreseen in the Decision may access the data. Finally, it is not indicated in which cases the Member State which entered the alert may give the required prior authorisation for the further use of the data.

102 CJEU, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland, 8 April 2014, para. 62, https://eur-lex. europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0293

103 Article 30(1), Council Regulation (EC) No 515/97, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:01997R0515-20160901

104 Article 23(2), Council Regulation (EC) No 515/97, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:01997R0515-20160901

105 Alerts on persons wanted for arrest or extradition (Article 26); on missing persons (Article 32); on persons sought to assist with a judicial procedure (Article 34); on persons and objects who should be subject to discreet or specific checks (Article 36); on objects for seizure or use as evidence in criminal proceedings (Article 38).

106 Article 46(5), Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), https://eur-lex.europa.eu/legal-content/EN/ ALL/?uri=CELEX-:32007D0533.

107 CCBE, 'Recommendations on the protection of fundamental rights in the context of national security', April 2019, https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Guides_recommendations/EN_SVL_20190329_CCBE-Recommendations-on-the-protection-of-fundamental-rights-in-the-context-of-national-security.pdf

108 Article 3 of the ETIAS Regulation: "'security risk' means the risk of a threat to public policy, internal security or international relations for any of the Member States." The lack of clear definitions of these terms is clearly problematic.

4.2.4 Interference with other rights

Right to non-discrimination

The Regulation governing the EES lacks specific provisions that would ensure the implementation of the non-discrimination safeguards foreseen in Article 10(2). According to the agreed text, national authorities are required to "ensure that the use of the EES, including the capturing of biometric data," is in accordance with numerous human rights obligations.[109] However, with no advice on exactly what those obligations mean in practice it is likely that Member States will adopt divergent practices. While this matter may be best left to implementing legislation or guidelines, there is no requirement in the Regulation to adopt any such texts and thus is remains unclear how these safeguards will be put into practice in a uniform or harmonised way.

The proposal on ETIAS was not been accompanied by a specific assessment of the compliance of the new profiling functionality (formally referred to as "screening rules") with the right to non-discrimination. The foreseen screening rules raise issues because they could lead to discrimination, despite the inclusion in the text of safeguards[110] – apparently neutral criteria may hide or lead to information that would qualify as prohibited grounds for discrimination. For example, nationality may be a proxy for race, ethnic origin, or religion; differences of treatment on grounds of nationality can turn into discrimination on prohibited grounds. Data mining based on apparently neutral factors can also lead to indirect discrimination. For example, the combination of information on occupation, education level and criminal convictions could single out people from a specific trade union group, due to the specific policy of a single state on demonstrations or on access to occupation and education.[111] In this respect the authors of this report consider that it is extremely unfortunate that the ETIAS Fundamental Rights Guidance Board is not given a direct, binding role in overseeing the establishment and review of the screening rules.[112]

Concerning the VIS, the proposal for a Regulation published in May 2018 also introduces an element of profiling and the impact assessment stated that this functionality is based on "the exact same conditions as those applied in ETIAS." The same problems as outlined above thus apply. The authors of this report consider that it is premature to introduce the same profiling functions in another system before the initial ETIAS function has been put into use and adequately assessed.

Finally, the routine processing of personal data on persons inviting or sponsoring visa-holders may raise issues. This data may be relevant, but unless there is a justified need, the processing of these data in the course of routine implementation of the visa policy is disproportionate. It could even amount to indirect discrimination, as lawful residents who are third-country nationals are more likely to have to offer invitations to their family members than EU citizens and will thus have their data stored in the VIS far more frequently.

109 European Convention for the Protection of Human Rights and Fundamental Freedoms, in the Charter of Fundamental Rights of the European Union and in the United Nations Convention on the Rights of the Child.

110 Article 33(5), ETIAS Regulation: "The specific risk indicators shall be targeted and proportionate. They shall in no circumstances be based solely on a person's sex or age. They shall 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."

111 Fundamental Rights Agency, 'The impact on fundamental rights of the proposed Regulation on the European Travel Information and Authorisation System (ETIAS)', 30 June 2017, pp.27-30, https://fra.europa.eu/en/ opinion/2017/etias-impact

112 The ETIAS Fundamental Rights Guidance Board is able to "perform regular appraisals and issue recommendations to the ETIAS Screening Board on the impact on fundamental rights of the processing of applications and of the implementation of Article 33 ['The ETIAS Screening Rules'], in particular with regard to privacy, personal data protection and non-discrimination." Under Article 33(6), the ETIAS Screening Board will be consulted on the definition, establishment, assessment, implementation, evaluation, revision and deletion of the "specific risk indicators" which are to inform the screening rules. Given that the Fundamental Rights Guidance Board ultimately has "an advisory and appraisal function" (Article 10(1)), the need to takes its recommendations into account appears to be minimal.

Right to an effective remedy

The Regulation and Decision on CIS allow for the rights to access, correction, erasure and blocking, although it is not stated in either text that individuals should have access to an effective judicial remedy, with the type of procedure left to be determined by national law. A guide has been produced by the CIS Supervision Coordination Group to assist individuals in exercising their rights.

The proposal on ETIAS foresees all the relevant rights for individuals, although there are no provisions setting out the possibility of accessing, or mentioning the potential need to access, legal aid or assistance (thought such right cold be provided under the national legislation). The basis of remedial procedures in national law may lead to significant divergences in practice; on the other hand, this depends on the compliance of the Member States with the EU's data protection legislation. The minimal information to be offered to applicants as to the grounds for refusal, annulment or revocation may limit their ability to appeal effectively. According to the final text, individuals whose application has been refused shall be provided with various types of information. This includes "a statement of the grounds for refusal of the travel authorisation indicating the applicable grounds from those listed in Article 37(1) and (2) enabling the applicant to lodge an appeal,"[113] but this may simply be a statement that the applicant "poses a security risk" or "poses an illegal immigration risk". This may not provide sufficient explanation in order to make a reasoned appeal.

Regarding Eurodac and VIS, the extremely low use by data subjects of their rights to access data suggests that practical implementation of those rights is an issue that merits further attention. For example, with regard to Eurodac, 0.0017%, 0.0009%, 0.0002% and 0.0003% of data subjects made requests in the years 2013 to 2017 respectively, with the majority of requests in one Member State.[114] As remarked by the European Commission in its evaluation of VIS, such low numbers of requests "could be explained by Member States' good performance on the protection of personal data. However, it could also in part be due to data subjects being unaware of their data protection rights and not knowing how to exercise them."[115] Regarding SIS II, standard information regarding remedies is limited, as these are primarily dealt with by national courts. The 2018 legislation goes some way towards rectifying this situation by introducing a "standardised statistical system for reporting annually" on subject access requests, requests for rectification and cases heard before national courts.

Rights of the child

The 2016 proposal on Eurodac and the 2018 proposal on the VIS would lower the minimum age for fingerprinting to six years old. However, it has not been established that doing so will actually assist in protecting children, despite the claims in the proposals' explanatory memorandum. The study[116] used to justify lowering the age to six was based on fingerprint datasets taken from individuals at five-year intervals (at most). It concluded that the results did not contradict previous assumptions of "an almost isotropic growth model" (i.e. uniform growth in all directions) and that

113 Article 38(2)(c), Regulation of the European Parliament and of the Council establishing a European travel information and authorisation system (ETIAS), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R2226

114 This means 48, 26, 89 and 156 people across the four years out of 2,738,008, 2,707,339, 4,076,408 and 5,095,191 fingerprints inserted. Data are available in EU-Lisa, Annual report on the 2015 activities of the central system of Eurodac, including its technical functioning and security pursuant to Article 40(1) of Regulation (EU) No 603/2013, November 2016, https://www.eulisa.europa.eu/Publications/Reports/Eurodac%202015%20 Annual%20Report.pdf; EU-Lisa, Annual report on the 2014 activities of the Central System of Eurodac pursuant to Article 24(1) of Regulation (EC) No 2725/2000, June 2015, https://www.eulisa.europa.eu/Publications/Reports/ Eurodac%202014%20Annual%20Report.pdf; EU-Lisa, Annual report on the 2013 activities of the Central Unit of Eurodac pursuant to Article 24(1) of Regulation (EC) No 2725/2000, https://www.eulisa.europa.eu/Publications/ Reports/eulisa_report_eurodac_en.pdf

115 European Commission, Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EC) 787/2008, COM(2016) 655 final, 14 October 2016, p.12, https://ec.europa.eu/ home-affairs/sites/homeaffairs/files/what-we-do/policies/borders-and-visas/visa-policy/docs/report_to_the_european_parliament_and_council_on_implementation_of_vis_en.pdf

116 Joint Research Center of the European Commission (JRC), Institute for the Protection and security of the citizen, '2013 Study on fingerprint Recognition for children', September 2013, http://publications.jrc.ec.europa.eu/ repository/bitstream/JRC85145/fingerprint%20recognition%20for%20children%20final%20report%20(pdf).pdf.

"it is desirable to draw conclusions for time windows (beyond 5 years) in order to give a clear message to developers of fingerprint recognition systems." At the same time, it observed that the dataset used was limited and "does not allow for seamless conclusions from birth to adulthood." In this regard, and given the lack of inclusion of child protection as a purpose of the two systems, a lower age limit of six and a retention period of ten years seems disproportionate for the authors of this report.

The proposal on ETIAS required that particular attention be given to children, as well as to the elderly and to persons with a disability (included in the final Regulation in Article 14). However, as stated above, no more detailed provisions set out how this will be ensured. No age limits regarding data collection are set out in the ETIAS proposal.[117] While data on children may be necessary for the purposes of dealing with criminal offences (e.g. child trafficking), no specific safeguards are included that would limit law enforcement access to such cases.

Right to asylum

Article 38 of the proposed Regulation on Eurodac allow Member States to share personal data stored in Eurodac with third countries whenever necessary to prove the identity of third-country nationals for the purpose of return. While the proposal includes safeguards,[118]their practical implementation could be challenging and should be closely monitored.

The ETIAS proposal would introduce new requirements beyond those that already exist for transport providers to check the eligibility of individuals for travel. Currently, those to whom the ETIAS would apply (visa-exempt third-country nationals) are only required to be in possession of a valid biometric passport to travel, but under the ETIAS anyone falling within this category and seeking international protection would require a valid travel authorisation. The existence of visa obligations does not ultimately prevent people seeking asylum – but it is a major factor that leads to people travelling to the EU for that purpose via dangerous, irregular routes. The need for a travel authorisation could in theory lead to people making equally dangerous choices. The proposal included the possibility to apply to an individual Member State for a limited humanitarian travel authorisation, which remains in the final text[119] This is welcome, but it must both be well-publicised and closely-monitored to establish how it is used in practice.

The relationship between the Eurosur Regulation and the right to asylum is problematic. In carrying out tasks related to "detecting, preventing and combating illegal immigration" both Member States and Frontex are permitted to gather and compile information that can be passed to third states. Should Member State authorities observe, via their monitoring of third country ports or the "pre-frontier area", an individual or group of individuals who appear to be heading towards EU territory, they may alert the authorities of a neighbouring state or states about the situation, leading to their interception by those authorities. It is difficult to imagine how, in such a situation, the authorities would ensure "that people seeking international protection are identified". Thus, despite the formal protections afforded to the right to seek asylum in the Eurosur legislation, in practice it seems entirely feasible that they may not be respected, depending on any future extension, territorial configuration and use of the Eurosur system. Any such denial of access to formal asylum proceedings would breach the essence of the right to seek asylum.

Inhumane or degrading treatment; the right to liberty and security

In the Schwarz decision, the CJEU found that the collection of two fingerprints for the purposes of issuing an EU passport is proportionate, taking into account that it does not "cause any particular physical or mental discomfort to the person affected any more than when the person's facial im-

117 Data is to be collected on minors and adults, with minor defined in Article 3(19) as "a third-country national or a stateless person below the age of 18 years."

118 Articles 37(2) and 38(1), Proposal for a Regulation on the establishment of 'Eurodac', https://eur-lex.europa. eu/legal-content/EN/TXT/?uri=CELEX:52016PC0272(01)

119 Article 44 of the Regulation of the European Parliament and of the Council establishing a European travel information and authorisation system (ETIAS), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1240

age is taken."[120] In the case of Eurodac, the taking of fingerprints primarily concerns a vulnerable group of individuals[121] who have often fled their country of origin to escape war or persecution and may have experienced significant hardships in their journey to EU territory. They may not feel comfortable in registering their fingerprints whether it is to avoid the coercive Dublin rules[122], because they have had bad experiences with fingerprinting and state authorities, or because they fear the fingerprints may be shared with their country of origin that could endanger family members.[123]

A lack of cooperation in fingerprinting can lead, in certain Member States, to the deprivation of liberty through detention, and even physical or psychological coercion, to overcome resistance as a means to force people to register their fingerprints,[124] which could lead to a risk of re-establishing feelings of trauma and victimisation.[125] This practice is confirmed in the 2016 proposal[126] and may entail the risk of inhuman or degrading treatment or punishment or breaching the right to liberty. It is unfortunate that, in the proposal, the requirement for national measures governing the taking of fingerprints by force to comply with the Commission's "best practice" guidelines and the Charter of Fundamental Rights is not included in the operative part of the text, but only in the recitals.[127]

4.2.5 Conclusions

This overview has summarised the findings of fundamental rights assessments of eight different instruments, concerning: biometric passports; the Customs Information System (CIS); the Entry/Exit System (EES); the European Travel Information and Authorisation System (ETIAS); Eurodac; the European Border Surveillance System (EUROSUR); the Schengen Information System (SIS II); and the Visa Information System (VIS). It has highlighted a number of problematic provisions in existing and proposed legislation, focusing on the rights to privacy and data protection but also taking into account the rights to non-discrimination; to an effective remedy; of the child; to asylum; to not be subjected to inhumane or degrading treatment; and to liberty and security.

One instrument (EUROSUR) raises concerns regarding respect for the essence of the right to asylum – depending on the configuration and use of the system, it could be used to direct the "interception" of persons outside of EU territory who may wish to request international protection, with no way of assessing whether those persons have a legitimate claim or not. This issue must be taken into account in subsequent policy-making and the further development of EUROSUR.

The opinion of the authors of this report are that there are issues with the necessity and pro-

120 CJEU, Michael Schwarz v Stadt Bochum, Case C-291/12, 17 October 2013, para. 48, https://eur-lex.europa.eu/ legal-content/EN/TXT/?uri=CELEX:62012CJ0291

121 ECtHR, M.S.S. v Belgium and Greece (Application no. 30696/09), para. 233, http://hudoc.echr.coe.int/ eng?i=001-103050

122 Elspeth Guild and others, 'New approaches, alternative avenues and means of access to asylum procedures for persons seeking international protection', *European Parliament, PE509.989, October 2014, p.57,* https://www. europarl.europa.eu/RegData/etudes/STUD/2014/509989/IPOL_STU(2014)509989_EN.pdf

123 FRA, 'Fundamental Rights Implications of the Obligation to provide Fingerprints for Eurodac', 2015, p.4, https:// fra.europa.eu/en/publication/2015/fundamental-rights-implications-obligation-provide-fingerprints-eurodac; FRA, 'Under watchful eyes: biometrics, EU IT systems and fundamental rights', 2018, https://fra.europa.eu/sites/default/ files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf

124 European Commission, 'Staff Working Document - Implementation of the Eurodac Regulation as regards the obligation to take fingerprints' COM(2015) 150 final, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/elibrary/documents/policies/asylum/general/docs/guidelines_on_the_implementation_of_eu_rules_on_the_obligation_to_take_fingerprints_en.pdf

125 FRA, 'The impact of the proposal for a revised Eurodac regulation on fundamental rights', 2016, p. 7, available at: https://fra.europa.eu/en/opinion/2017/impact-proposal-revised-eurodac-regulation-fundamental-rights.

126 Article 2(3), Proposal for a Regulation on the establishment of 'Eurodac', https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX:52016PC0272(01)

127 Recital 30, Proposal for a Regulation on the establishment of 'Eurodac', https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0272(01)

portionality of some aspects of all the instruments examined – for example in relation to what the authors considered as the lack of sufficient justification of the centralised databases (EES, ETIAS, Eurodac); the unnecessary, excessive or insufficient justification of processing biometric and alphanumeric data (biometric passports, EES, Eurodac, SIS, VIS); excessive retention periods (CIS, EES, ETIAS, Eurodac, VIS); insufficient justification of access by law enforcement authorities or retention periods justified on the grounds of the ancillary purpose of law enforcement access (CIS, ETIAS, Eurodac, VIS) and purpose limitation (CIS, ETIAS, SIS II).

Regarding the right to non-discrimination, concerns have been raised over a lack of specific provisions that would allow the uniform implementation of non-discrimination safeguards (EES) and the possibility of prohibited discriminatory profiling techniques being used on individuals (ETIAS and VIS).

Individuals may have trouble exercising the right to an effective remedy in relation to ETIAS, in particular because the information to be supplied to individuals whose applications are rejected may not be sufficient to conduct a meaningful appeal. With regard to Eurodac and VIS, it is noted that there are extremely low numbers of persons who exercise their rights to access their data within the systems, may require more vigorous awareness-raising regarding those rights.

Concerns over the rights of the child have been raised in relation to the retention period of ten years for fingerprints taken from children as young as six (Eurodac and VIS), due to the conservative conclusions of the study used to justify the change and the fact that neither of the systems has child protection as a purpose. As regards the right to non-discrimination, while the ETIAS proposal included a requirement for "particular attention" to be given to the best interests of the child, there is a requirement for the introduction of specific provisions that would ensure uniform implementation of this requirement. Finally, the ETIAS text does not set out any age limits for data collection; nor is law enforcement access to data limited solely to data on children that may be necessary in specific types of cases (e.g. concerning child trafficking).

ETIAS also raises issues in relation to the right to asylum, as the need for a travel authorisation may lead to individuals taking risky journeys in order to reach EU territory. The possibility to apply to an individual Member State for a limited humanitarian travel authorisation is welcome, but it must both well-publicised and closely-monitored to establish how it is used in practice. The proposal on Eurodac includes the possibility for member states to share personal data with third countries when necessary for return purposes; yet the foreseen safeguards may be very challenging to properly implement. The relationship between EUROSUR and the right to asylum is potentially problematic.

Finally, the possibility of using force to obtain asylum-seekers' fingerprints (already in place in practice and confirmed in the 2016 proposal) entails the risk of inhumane or degrading treatment or punishment or breaching the right to liberty. While "best practice" guidelines drafted by the Commission are welcome, it is unfortunate that the Eurodac proposal only mentions them in the recitals rather than the operative part of the text.

In sum, there are a range of issues, of varying levels of seriousness, affecting the instruments that have been examined. Many of them could be resolved through recast legislation, although this is perhaps unlikely for many of the instruments, in particular those that have only just been approved or which are currently the subject of negotiations between the co-legislators. Nevertheless, the findings of the assessments carried out as part of this project can provide some useful guidance for future proposals.

In particular, the need to systematically justify each and every limitation of fundamental rights must be taken into account. Many of the instruments examined here were not accompanied by an impact assessment for a variety of reasons, While they cannot be seen as a substitute for political debate, the impact assessments are crucial in laying out the policy options available, their different implications, and for justifying those options that are considered most desirable. Although they are not legally required, according to the Commission's own 'Better Regulation

Guidelines'[128], "an impact assessment is required for Commission initiatives that are likely to have significant economic, environmental or social impacts".

It cannot be denied that the establishment of large-scale, centralised databases that process sensitive personal data and are designed to control or delimit individuals' movements is an act with a significant social impact. The lack of such assessments merely gives the impression that certain approaches are taken for granted and do not require any explanation or justification. Such an approach does not meet the requirements of either the Better Regulation Guidelines or, perhaps more importantly, the Charter of Fundamental Rights.[129]

A second key issue common to the majority of the instruments examined here concerns the processing of biometric data. The establishment of the EES involved a clear attempt to limit the biometric data to be gathered and to justify the necessity and proportionality of that collection. However, it is also the case that for the authors of this report the collection of biometric data in itself appears disproportionate for this instrument, as less intrusive alternatives are realistically available for achieving the same ends – for example, by simply using the data contained in e-passports to verify individuals' identity. Yet the limited gathering of biometric data for the purposes of the EES (four fingerprints) or biometric passports (two fingerprints) calls into question the more extensive gathering of such data in other systems – in particular, the VIS and Eurodac, both of which require a 'full take' of ten fingerprints alongside a facial image (already in place for the VIS, and included in the Eurodac proposal currently under discussion). In the case of Eurodac the need to take all 10 fingerprints has never been formally justified, and given that the primary purpose of the fingerprints collected for the VIS is the verification of identity, it is unclear why the collection of 10 fingerprints is necessary. The rules on biometric passports and the EES both mandate the processing of biometrics, primarily for identity verification, and a far lower amount of personal data suffices.

Biometric data is classified as a 'special category' of personal data in EU data protection law for a good reason, and the use of such data needs specific and strong precautions. While strong safeguards do govern the collection and use of biometric data in EU databases and information systems, they can be improved upon according to the authors of the report. For example, higher thresholds for law enforcement access setting out uniform conditions across different systems, could be considered. A re-assessment of the collection of biometric data in EU databases and computer systems could also be undertaken to ensure that each system only requires collection of the absolute minimum necessary for its purposes.

Finally, the procedure by which law enforcement agencies are provided with access to the EES, ETIAS, Eurodac and VIS requires further attention. The bodies nominated to process law enforcement authorities' requests for access can be part of the same organisation as the authority seeking access. While the legislation requires that they act independently, future evaluations should examine whether they meet the requirements of EU law and CJEU jurisprudence for "prior review carried out by a court or by an independent administrative body."[130]

128 European Commission, 'Better Regulation "Toolbox"', http://ec.europa.eu/smart-regulation/guidelines/docs/ br_ toolbox_en.pdf.

129 Article 52(1) CFR: "Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others." It is difficult to argue that limitations are "necessary and genuinely meet objectives of general interest" when there has been no attempt to provide detailed arguments in their favour.

130 CJEU, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland, 8 April 2014, para. 62, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0293

4.3 Agencies sub-group report

4.3.1 Introduction

This is a summary of the main outcomes of the fundamental rights review carried out by the agencies subgroup.[131] It comprises a short thematic overview of the assessment of the legal bases of the EU agencies Europol, Eurojust and Frontex, the agreements between those agencies and third states and the inter-agency agreements between Europol and Eurojust, Europol and Frontex and Europol and the European Anti-Fraud Office (OLAF). Europol's access to the VIS and SIS II and Eurojust´s access to SIS II were also analysed. In total, the agencies group analysed 35 instruments, the bulk of which were agreements between Europol or Eurojust and third states. However, those agreements do not have any major structural or substantial differences, leading to very similar outcomes in terms of analysis.

4.3.2 Right to privacy and data protection

All of the instruments analysed impact the fundamental rights to privacy and data protection, sometimes without respecting the necessity and proportionality limitations required by Article

131 **Europol:** 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, https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A32016R0794

Europol agreements with third states and inter-agency agreements: Europol-Albania agreement, EuropolAustralia agreement, Europol-Canada agreement, Europol-Colombia agreement, Europol-Macedonia agreement, Europol-Iceland agreement, Europol-Lichtenstein agreement, Europol-Moldova agreement, Europol-Monaco agreement, Europol-Montenegro agreement, Europol-Norway agreement, Europol-Serbia agreement, Europol-Switzerland agreement, Europol-USA supplemental agreement, Europol-Interpol agreement, Europol-Eurojust agreement, Europol-Frontex agreement: available at: https://www.europol.europa.eu/partners-agreements/operational-agreements **Europol-OLAF agreement:** available at: https://www.europol.europa.eu/partners-agreements/strategic-agreements **Europol access to the Visa Information System:** Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008D0633

Europol access to SIS II: Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), http://eur-lex.europa.eu/legal-content/EN/ ALL/?uri=CELEX:32007D0533

Europol access to Eurodac: Regulation No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of Eurodac for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013R0603

Eurojust: Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, https://eur-lex. europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009D0426

Eurojust agreements with third states: Eurojust-Iceland agreement, Eurojust-USA agreement, Eurojust-Liechtenstein agreement, Eurojust-Switzerland agreement, Eurojust-Moldova agreement, Eurojust-Ukraine agreement, Eurojust-Norway agreement, Eurojust-Macedonia agreement, Eurojust-Montenegro agreement: available at: http:// www.eurojust.europa.eu/about/legal-framework/Pages/eurojust-legal-framework.aspx#partners

Eurojust access to SIS II, Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II)**,** http://eur-lex.europa.eu/legal-content/EN/ ALL/?uri=CELEX:32007D0533

Eurojust-OLAF agreement: available at: http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/agreements/Practical%20Agreement%20on%20arrangements%20of%20cooperation%20between%20Eurojust%20 and%20OLAF%20(2008)/Eurojust-OLAF-2008-09-24-EN.pdf

European Border and Coast Guard Agency (Frontex): 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, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R1624

52 CFR. None of the analysed instruments violate the essence of those rights. However, there are major differences in terms of the seriousness of interferences and the negative fundamental rights impacts of the instruments assessed. These are examined in the following sections.

Provided for by law/legal basis

The majority of instruments do not contain any shortcomings regarding the requirement that interferences with fundamental rights must be provided for by law. However, all of the inter-agency agreements, which provide for the exchange of personal data between the agencies and thus interfere with the right to privacy and data protection, need further specification. Both the agreements themselves and the legal acts of the agencies provide for information exchange. Often they provide, different rules regarding the scope of access,.[132] Further, Eurojust's legal basis does not contain a provision that provides the possibility for Eurojust's national members or assistants to consult the SIS II.[133]

Respect for the essence of rights

The fundamental rights assessments did not reveal any shortcomings regarding respect for the essence of the rights to privacy and data protection.

Legitimate aim

All of the instruments in question pursue legitimate aims. However, it would be desirable to specify in the SIS II Regulation the purposes for which Europol and the national members and assistants of Eurojust may access the system. This specification is currently missing.[134]

Necessity and proportionality

A number of shortcomings are evident regarding the necessity and proportionality of measures in the instruments in question that impinge upon fundamental rights.

a) Lack of legal clarity

Some of the analysed instruments lack legal clarity due to their vague scope. The CJEU held in the Schrems case as well as in the Digital Rights Ireland case that "EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question".[135] ECtHR case law requires a similar clarity.[136] In relation to the purpose of crime prevention and in particular the prevention of terrorism, the concrete offences must be specified and defined "in a clear and precise manner," setting out "both the activities covered by that term and the persons, groups and organisations liable." This should ideally be listed in the agreement or an annex thereto.[137]

---

132 For more details, please refer to the report on the inter-agency agreement Europol-Eurojust and EuropolOLAF, Europol-Frontex.

133 For more details, please refer to the report on Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second-generation Schengen Information System (SIS II).

134 For more details, please refer to the report on Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second-generation Schengen Information System (SIS II).

135 CJEU, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, 8 April 2014, para. 54, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0293; CJEU, Case C-362/14, Maximillian

Schrems v Data Protection Commissioner, 6 October 2015, para. 91, https://eur-lex.europa.eu/legal-content/EN/ TXT/?uri=CELEX:62014CJ0362

136 ECtHR, Case of M.M. v the United Kingdom (Application no. 24029/07), 13 November 2012, para. 206, http:// hudoc.echr.coe.int/eng?i=001-114517

137 CJEU, Opinion of Advocate-General Mengozzi, Draft agreement between Canada and the European Union — Transfer of Passenger Name Record data from the European Union to Canada, 8 September 2016, para. 328, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62015CC0001; CJEU, Opinion of the Court (Grand Chamber), Draft agreement between Canada and the European Union - Transfer of Passenger Name Record data from the European Union

The scope of the both the Europol-Frontex and Europol-OLAF agreements are formulated rather broadly.[138] For instance, it is not clear on which legal ground OLAF is permitted to transfer and receive personal data from Europol.[138] Furthermore, the Europol-Frontex Agreement does not itself precisely define the areas of crime to which it relates, but refers to the Europol mandate. Article 3(1) lists "other cross– border activities". The Europol Regulation specifies this term by adding a list of all relevant crimes (Annex I), but the Frontex Regulation does not include such a list. It merely defines "cross-border crimes" as crimes with a cross-border dimension committed at or along, or which is related to, the external border. This definition does not provide sufficient precision over the crimes to which it refers. Therefore, a definition of "other cross–border activities" for which data can be processed is necessary.

Furthermore, all of the agreements between Europol or Eurojust and third states provide for a broad scope of data processing and transfer; they fail to identify the detailed personal scope of subjects targeted by the agreement, but refer to Europol's mandate, which is itself very broad and covers a wide range of subjects possibly concerned.

b) Lack of explicit list of categories of personal data allowed for processing

Some of the instruments lack essential data protection requirements, such as precise specification of the data to be collected. The Frontex Regulation, for instance, does not specify the exact categories of personal data that can be processed by the Agency. Some more detailed rules concerning the categories of data allowed for processing have been developed in the 'Implementation Measures' with respect to the processing of personal data collected during joint operations, pilot projects and/or rapid interventions.[139] However, this Decision only lists "examples of data categories" that may be processed (Article 8) and other unspecified categories of data may thus also be processed.[140]

c) Purpose limitation principle

Some of the instruments assessed raise doubts concerning compliance with the purpose limitation principle. The latter is considered a very important factor when assessing the proportionality of data processing. Purpose specification/limitation as well as the concept of compatible use of data contribute to transparency, legal certainty and predictability of data processing. The purpose limitation principle aims to protect the data subject by setting limits on how controllers are able to use their data and reinforce the fairness of the processing. The limitation principle prevents the use of individuals' personal data in a way (or for further purposes) that they might find unexpected, inappropriate or otherwise objectionable.[141] The purpose limitation principle is recognised in both Article 5(1b) and recital 50 of the GDPR and Article 4(1b) and recital 29 of the LED.

Provisions of the Frontex Regulation, for instance, raise the risk of further processing of personal data that is incompatible with the original purpose of its collection, thus possibly breaching the purpose limitation principle[142], as recommended also by the EDPS, it would be desirable to implement a mechanism obliging to verify the compatibility between the purposes of original and further processing listed in 46(1)[143].

---

to Canada, 26 July 2017, para. 174 et. seq., https://eur-lex.europa.eu/legal-content/EN/ TXT/?uri=CELEX:62015CG0001; CJEU, Digital Rights Ireland, op. cit., para. 61 138 For details, please refer to the inter-agency assessment reports.

138 For details, please refer to the Europol-OLAF assessment report.

139 Management Board Decision No 58/2015 of 18 December 2015, http://frontex.europa.eu/assets/About_ Frontex/Data_Protection/MB_Decision_58_2015.pdf

140 For details, please refer to the Frontex assessment report.

141 Article 29 Data Protection Working Party, 'Opinion 03/2013 on purpose limitation', 2 April 2013, p. 11, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

142 For details, please refer to the Frontex assessment report.

143 See EDPS' recommendations on the proposed European Border and Coast Guard Regulation (...), op. cit., p. 12-13.

The Europol-Eurojust Agreement allows for further processing of received data for the purposes for which the data was communicated, which is not the same thing as the purpose for which the information was collected.

Regarding access to SIS II by Europol and Eurojust, it should be noted that both agencies may, under certain conditions, have access to the data contained in certain categories of alerts in SIS II. Access by both agencies must be "within its mandate" (i.e. their mandates), but in the author's view the access conditions do not seem sufficiently detailed and rigid, an issue raised by the EDPS in their opinion on the SIS II proposals.[144] The EDPS urged the Commission to define restrictively the tasks for the performance of which access by Europol and Eurojust would be justified.[145] It should be also noted in this context that the scope of the Europol's and Eurojust's mandates and their tasks are defined in separate legal acts (the Europol Regulation[146] and the Eurojust Decision[147]) and can be subject to modifications, including broadening, at any time (subject to the relevant legislative procedure).[148] For example, in January 2010 the Europol Convention was replaced by the Europol Decision[149] which altered Europol's legal framework and considerably enlarged its tasks.[150] Furthermore, Council Decision 2007/533/JHA contains no explicit statement concerning the need for Europol or for Eurojust's national members or assistants to access SIS II. The Decision does not include a requirement to demonstrate the need for access to SIS II data, namely that there are reasonable grounds to believe that such access would substantially contribute to the exercise of the agencies' tasks, as well as to demonstrate that there is no possibility to obtain the data by other less intrusive means.[151]

Another aspect of the SIS II Decision which may raise concerns over purpose limitation, in the context of access to SIS II data by Europol or Eurojust's national members or assistants, is the question of the subsequent use of that data accessed. No link is established between the purpose of the access and the later use of the data in a law enforcement database. Providing Europol with access to the extent that is necessary "for the performance of its tasks,"[152] without restricting subsequent use, is too far-reaching and should be clarified by specifying the purpose of access and

144 European Data Protection Supervisor, 'Opinion of the EDPS – on the Proposal for a Council Decision on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) (COM(2005) 230 final); - the Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) (COM(2005) 236 final), and – the Proposal for a Regulation of the European Parliament and of the Council regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM(2005) 237 final)', 2006 C/91/11, 19 October 2005, https://edps.europa.eu/sites/edp/files/publication/05-10-19_sisii_en.pdf

145 European Data Protection Supervisor, 'Opinion 7/2017 on the new legal basis of the Schengen Information System', 2 May 2017, https://edps.europa.eu/sites/edp/files/publication/17-05-02_sis_ii_opinion_en.pdf. In its opinion on the proposal to revise the SIS legal basis from 2017, the EDPS opinion remained silent on this issue.

146 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, https://eur-lex.europa.eu/legal-content/EN/ TXT/?uri=CELEX%3A32016R0794

147 Council Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002D0187:en:HTML; repealed by Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA, https://eur-lex. europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1727

148 F. Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-Level*, Springer, 2012, p. 345; F. Boehm, *Information Sharing in the Area of Freedom, Security and Justice—Towards a Common Standard for Data Exchange Between Agencies and EU Information Systems* in S. Gutwirth et al. (eds.), 'European Data Protection: In Good Health?', Springer, 2012, p. 162

149 Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol), https://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009D0371

150 F. Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice,* op. cit., p. 351

151 European Data Protection Supervisor, Opinion 2006 C/91/11, op. cit., para 4.2.2.2, https://edps.europa.eu/sites/ edp/files/publication/05-10-19_sisii_en.pdf

152 Article 17, Regulation 2016/794, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0794

linking it to the purpose of any subsequent use of the data. A failure to provide such clarification may interfere with the purpose limitation principle.[153]

d) Disproportionate data retention period

One of the main shortcomings observed in the instruments in question relates to what the author considers to be potentially unlimited data retention periods. CJEU and ECtHR case law requires a maximum data retention period – indefinite storage is not permitted.[154] Furthermore, the length of time for which data may be stored must be based on objective criteria in order to ensure that storage and retention are limited to what is strictly necessary. [155]

- The Europol Regulation has no maximum period for the retention of data. The three-year deadline set out in the Regulation can be extended provided the EDPS is informed. This is also the case for sensitive data, violating the proportionality principle by introducing an indefinite retention period for sensitive data.[156] It is also remarkable that there is no maximum retention period for: data at Eurojust, in cases where the original data retention period is exceptionally extended; for data transferred under all of the interagency agreements (Europol-Eurojust; Europol-Frontex; Europol-OLAF);[157] nor in any of the agreements concluded between Europol or Eurojust and third states. Considering the lack of a maximum data retention period in Europol's legal basis, this aspect should be regulated when reviewing both the inter-agency agreements and the Europol Regulation.
- Furthermore, Europol's access to SIS II gives rise to a potentially extensive data retention period. According to Article 41(1) of the SIS II Decision, the agency may have access to and search directly data entered into SIS II in accordance with Articles 26, 36 and 38 of that Decision. Europol may use that data subject to the consent of the Member State concerned (Article 41 (3)). If consent is granted, the handling thereof shall be governed by the Europol Convention (today the Europol Regulation). Once this happens, it becomes subject to the provisions of the Europol Regulation, which has no maximum storage period. As a result, it may 'extend' the retention of data which were initially in SIS (for three years), and now are retained by EUROPOL in particular in cases in which the data are transferred shortly before the original time limit expires.[158]

e) Unspecified access conditions

Some of the instruments in question include unspecified conditions for access to data. According to CJEU case law, objective criteria that clarify the limits of access to data and their subsequent use are needed to comply with Articles 7 and 8 of the Charter.[159] Furthermore, objective criteria are required, "by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued."[160] No such criteria are set out in the agreements between Europol or Eurojust and third states. In

153 F. Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-Level*, Springer 2012, op. cit., p. 369.

154 Digital Rights Ireland, op. cit., para. 64, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0293; ECtHR, Case of M.K. v. France (Application no. 19522/09), 18 April 2013, para. 45, http://hudoc.echr.coe.int/ eng?i=001-119075; ECtHR, Case of S. and Marper v. the United Kingdom (Application nos. 30562/04 and 30566/04), 4 December 2008, para. 118 et. seq., http://hudoc.echr.coe.int/eng?i=001-90051

155 Digital Rights Ireland, op. cit., para. 64

156 Europol assessment report, p. 7 and 8

157 Inter-agency assessment reports: Europol-Eurojust Agreement report, p. 7; Europol-Frontex, p. 6 and Europol-OLAF, p. 5 and 6

158 F. Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-Level*, op. cit., p. 172

159 Digital Rights Ireland, op. cit., para 60; Schrems, op. cit., para 93

160 Digital Rights Ireland, op. cit., para 62

the case of Europol's access to the VIS, neither the access procedure nor the prior verification of requests for access are specified in the Decision.[161] The only condition that must be fulfilled for Europol to process data is obtaining consent from the Member State that entered the data into the system. Regarding Europol's access to SIS II, it would be desirable to consider adding additional restrictions such as those recommended by the Joint Supervisory Authority Schengen and the EDPS that would limit the agencies' access to SIS II only to data about individuals whose name already appear in their files, so that only alerts relevant for these individuals are consulted.[162] Furthermore, the transfer of data from OLAF to Europol is unregulated, that is to say, there are no provisions in this regard. This serious shortcoming should be considered when revising OLAF's legal framework.

The Europol-Eurojust Agreement also has some shortcomings in this area. The agreement simply states that access to data shall be granted to a "duly authorised" person until the data has been included in the files of the agency receiving the data. It is questionable whether the term "duly authorised" contains an objective criterion. It is, for instance, unclear under which condition a person is duly authorised to access data of the other agency. Reference to the establishing acts of the agencies does not provide further clarification over this term. A more concrete definition of persons "duly authorised" to access the data of the other agency should set out objective criteria for deciding upon duly authorised persons and clarify access limits.

f) Transparency

The instruments must also be assessed in the context of the principle of transparency of data processing, which is a precondition to ensure that data protection rights can be effectively exercised. Some of the instruments reveal shortcomings in this regard.

For instance, a number of detailed provisions that are important from the fundamental rights perspective are not included in the text of the Frontex Regulation, but instead appear in the Implementation Measures.[163] This may impair both transparency of data processing but also the accessibility of data protection rules, given that the Implementation Measures are not an official legislative act. They are therefore not subject to official publication and available only in English. The question of limited accessibility of internal documents in the national context was noted by the CJEU in the case Smaranda Bara and Others,[164] where the Court was dissatisfied that certain detailed arrangements concerning the transfer personal data were laid down not in a legislative measure, but in a protocol agreed between two state agencies which was not published in the country's official journal.

Furthermore, the Frontex Regulation does not contain any specific rules, beyond relying on general rules of Regulation (EU) 2018/1725, on informing data subjects of the processing of their data.[165] Taking into consideration that the activities of Frontex and data processing under the Frontex Regulation may affect the protection of fundamental rights of vulnerable groups of people such as migrants and refugees in need of international protection, including minors, unfamil-

161 High-level expert group on information systems and interoperability, Final report, May 2017, Ares(2017)2412067, 11 May 2017, p. 13, http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail. groupDetailDoc&id=32600&-no=1

162 Schengen Joint Supervisory Authority, 'Opinion on the proposed legal basis for SIS II', 27 September 2005, http://www.statewatch.org/news/2005/oct/JSA-SIS.pdf; European Data Protection Supervisor, Opinion 2006 C/91/11, op. cit., point 4.2.3

163 Management Board Decision No 58/2015 of 18 December 2015, https://frontex.europa.eu/assets/Key_Documents/MB_Decision/2015/MB_Decision_58_2015_on__adopting_implementing_measures_for_processing_personal_data_collected_during_joint_operations_pilot_projects_and_rapid_interventions.pdf.

164 CJEU, Case C-201/14, Smaranda Bara and Others v Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală (ANAF),1 October 2015, para. 40, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0201

165 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32018R1725

iar with a European legal system, it is important to develop specific rules ensuring an effective access of those persons to such information. It is important that the information is provided in an age-appropriate manner and adapted to the particular needs of these data subjects. Merely including a reference to application of the general rules contained in Article 45(1) of Regulation (EU) 2018/1725 seems insufficient in this respect.

In addition to the Frontex Regulation, the VIS Decision on law enforcement access and the SIS II Decision do not contain a specific requirement for Europol to notify the data subject that their data included in VIS were transferred to Europol for law enforcement purposes.[166] Neither is there a duty to notify the person once the police activities with regard to them have been terminated. This may have a negative impact on the correct application of the principle of transparency of personal data processing, which is essential for uncovering unlawful processing and enabling data subjects to effectively exercise their rights.[167]

g) Supervision

Although transfers of data between different actors should be accompanied by additional safeguards[168] (e.g. information and/or notification duties) and some form of external supervision,[169] the rules regarding this topic in the instruments in question are not clear and supervisory mechanisms differ from actor to actor, which may complicate an overall overview and a comprehensive data protection compliance checks of all data transfers. The Europol-Eurojust Agreement, for instance, has no rules on external review, but there are such rules in the legislation establishing the agencies. The general approach in the context of the Agreement is self-monitoring on the question whether storage of transmitted data is still necessary, combined with general supervision of the agencies (including of transfers based on this agreement). The supervision of Eurojust, however, is on a different level to that of Europol – Europol has to report to the EDPS and to a data protection officer upon request, while Eurojust is supervised by the JSB (although these concerns will disappear with the entry into force in December 2019 of the new Eurojust Regulation, which introduces supervision by the EDPS[170]). As things stand, problems regarding the accountability of processing and supervision might arise. The EDPS, in its opinion[171] on the amendment of the Eurojust Decision, rightly points to the questions of "who will be the processor?" and "who will be the controller?" within this collaboration. Details to these questions are unfortunately not provided in the Europol-Eurojust Agreement. It provides for mutual association, but neither clarifies questions of supervision in cases where Eurojust participates in Europol's analysis work files, nor regarding the transmission of personal data.

Furthermore, none of the agreements between Europol or Eurojust and third states address the issue of external review of the processing and sharing of data. The respective agencies may request data on their own initiative, with no prior review. The EDPS and the JSB supervise these agencies in general, but don't have the right to object to transfers of data to third states based on the agreements in force. Every transfer of data between different actors, in particular those with

166 For details, please refer to the VIS access decision assessment report (Council Decision 2008/633/JHA).

167 For details, please refer to the VIS access decision assessment report (Council Decision 2008/633/JHA).

168 See Boehm, F, de Hert, P 'Notification, an important safeguard against the improper use of surveillance - finally recognized in case law and EU law', European Journal of Law and Technology, Vol. 3, No. 3, 2012.

169 With regard to law enforcement access to retained data: CJEU, Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others., para 120, 123, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62015CJ0203; ECtHR, M.M. v. the United Kingdom, op. cit., para 206; ECtHR, Szabó and Vissy v. Hungary (Application no. 37138/14), 12 January 2016, para 78, http://hudoc.echr.coe.int/eng?i=001-160020; ECtHR, Weber and Saravia v. Germany (Application no. 54934/00), admissibility decision 29th June 2006, paras. 127-8, http://hudoc.echr.coe.int/eng?i=001-76586

170 Chapter IV – Processing of information, Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA, https://eur-lex.europa.eu/legal-content/EN/ ALL/?uri=CELEX:32018R1727

171 European Data Protection Supervisor, 'Opinion on the Initiative with a view to adopting a Council Decision concerning the strenghtening of Eurojust and amending Decision 2002/187/JHA', 25 April 2008, para 34, https:// edps.europa.eu/data-protection/our-work/publications/opinions/eurojust_en

third states, should be accompanied by additional safeguards and some form of external supervision.[172] Thus, the role of the supervisory bodies with regard to data sharing agreements with third states should be clarified.

Interference with other rights

Regarding compliance with the right to an effective remedy, measures that do not provide for the deletion of retained data once a case is concluded (e.g. the Eurojust Decision, the inter-agency and the third states agreements) can have an impact on Article 47 CFR (and likewise Articles 7 and 13 ECHR), if those measures hinder access to an effective remedy.

The fundamental rights assessment of the instruments in question did not reveal any shortcomings regarding the rights to respect for family life, freedom of expression and information, non-discrimination, access to documents or to a fair trial. However, these latter checks were carried out only on a brief and superficial basis due to the focus of this report.

4.3.3 Conclusion

The analysed instruments cover a wide range of the agencies' work and include structurally different actors. The results of the fundamental rights analyses therefore vary to some extent. In addition to structural differences, the founding legislation of the agencies in question, as well as the data exchange agreements analysed, were in some cases put in place over a decade ago (a number of the third states agreements, OLAF), giving rise to more compliance issues then those instruments agreed or renewed recently (e.g. the Europol Regulation). However, even in the latter case, there are a number of concerns that need to be addressed to ensure compliance with CJEU case law.

There is a lack of legal clarity regarding "clear and precise rules governing the scope and application of the measure in question"[173] in some of the instruments, mainly in the interagency agreements as well as in the agreements between Europol or Eurojust and third states. Furthermore, the Frontex Regulation lacks an explicit list of categories of personal data which may be processed.

In the Frontex and Europol Regulations, the Europol-Eurojust Agreement, the instrument providing access to SIS II for Europol and Eurojust's national members or assistants and the instrument providing Europol with access to the VIS, the purposes for which data can be processed are very broad, raising compliance issues with the purpose limitation principle.

Lengthy and sometimes disproportionate data retention periods can be observed in the Europol Regulation (no maximum data retention period), the Eurojust Decision (in cases where the original data retention period is exceptionally extended), the inter-agency agreements (Europol-Eurojust; Europol-Frontex; Europol-OLAF), as well as in all of the third states agreements concluded by Europol and Eurojust (there is no mentioning of a maximum time limit for the retention of transferred data within the agreements).

Some instruments, such as access by Europol to the VIS, by Europol and Eurojust's national members or its assistants to SIS II, transfer of data from OLAF to Europol, the Europol - Eurojust Agreement and all the agreements between Europol or Eurojust and third states require further specifications regarding conditions for accessing data. It should be made clear whether there is a hit/no-hit procedure and/or any further access conditions.

Furthermore, the Eurojust Decision lacks a review procedure for the implementation of the Decision and contains several unclear principles for sharing personal data with national authorities. Regarding the transparency of data processing and notification duties, the conditions set out in

172 CJEU, Tele2 Sverige, op. cit., paras. 120, 123, with regard to law enforcement access to retained data; ECtHR, M.M. v. the United Kingdom, op. cit., para. 206; ECtHR, Szabó and Vissy v. Hungary, op. cit., para. 78; ECtHR, Weber and Saravia v. Germany, op. cit., paras 127-8

173 CJEU, Digital Rights Ireland, op. cit., para 54; CJEU, Schrems, op. cit., para. 91

the Frontex Regulation, access by Europol to the VIS and access by Europol and Eurojust's national members and assistants to SIS II could be improved to allow individuals to be informed when their data is processed and/or transferred, especially since access is possible to, inter alia, biometric data). In all of the instruments assessed, with the exception of Eurojust Decision, the right of the individual concerned to information in cases of data processing and/or data transfer should be improved to meet the ECtHR requirements stipulated in Weber and Saravia v. Germany[174] and in Principle 2.2 of Council of Europe Recommendation R (87) 15,[175] which relate to a right to be informed when the provision of such information no longer prejudices police activities and/or no longer hinders ongoing investigations.

The Frontex Regulation in particular has shortcomings in terms of transparency, as important data protection provisions are mainly included in 'Implementation Measures' rather than the legal basis itself, complicating the possibility for individuals concerned to exercise their data protection rights. Finally, the supervision of data transfers, in particular between Europol and Eurojust and between Europol or Eurojust and the third states with which they have agreements, could be improved upon by clarifying responsibilities when data are exchanged between different parties or when Eurojust participates in Europol's analysis work files.

The major concerns arising from these assessments relate to disproportionate data retention periods and/or the possibility to extend given data retention periods for an uncertain amount of time. This arises in the cases of Europol and Eurojust, in the agreements that those two agencies have with third states, and in the three inter-agency agreements analysed. There is a need for a clear and precise description of the categories of data to be processed, clear purpose specifications and improved data protection rights in the legislation governing Frontex. Some instruments, such as access by Europol to VIS, access by Europol and Eurojust's national members or assistants access to SIS II, data transfers from OLAF to Europol and the Europol-Eurojust Agreement urgently require further specifications regarding the mutual access conditions in place.

174 Weber and Saravia v. Germany (Application no. 54934/00), admissibility decision 29th June 2006, http://hudoc.echr.coe.int/eng?i=001-76586

175 Recommendation No. R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector, 17 September 1987, https://polis.osce.org/node/4656

4.4 Cross-border group report

4.4.1 Introduction

This document summarizes the main outcomes of the fundamental rights review undertaken of ten instruments under the "cross-border" sub-group.[176] This sub-group consists of a varied group of instruments, which poses a limit to drawing general conclusions and recommendations regarding their compliance with fundamental rights requirements as set out by EU and international human rights law, including the jurisprudence of the European Court of Human Rights (ECHR) and the Court of Justice of the European Union (CJEU). In addition, there is a difference in the geographical scope of some of the instruments as the mutual legal assistance agreements are between the EU and third countries, while the other instruments are relevant for EU member states alone.

Furthermore, some of the intra-EU instruments form part of the former third-pillar acquis, whereas others date from after the entry into force of the Lisbon Treaty that abolished the pillar structure. The European Commission has the power to launch infringement proceedings against Member States that have not correctly transposed these instruments in their national law or where the implementation of such instruments show important shortcomings , including the former third pillar instruments. The analysis of the instruments in this group has shown differences in their im-

176 EU - Japan MLAT: Agreement between the European Union and Japan on mutual legal assistance in criminal matters, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1557746113867&uri=CELEX:22010A0212(01)

EU – Iceland, Norway MLAT: Agreement between the European Union and the Republic of Iceland and the Kingdom of Norway on the application of certain provisions of the Convention of 29 [M]ay 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union and the 2001 Protocol thereto OJEU L 26/3, 29 January 2004, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:22004A0129(01)

EU – USA MLAT: Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009D0820; Agreement on mutual legal assistance between the European Union and the United States of America, https://eur-lex.europa.eu/legal-content/EN/ TXT/?uri=CELEX:22003A0719(02)

European Arrest Warrant: 2002/584/JHA: Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, https://eur-lex.europa.eu/legal-content/EN/ ALL/?uri=CELEX-%3A32002F0584

European Investigation Order: Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, https://eur-lex.europa.eu/legal-content/EN/ TXT/?uri=celex:32014L0041

European Protection Order: Directive 2011/99/EU of the European Parliament and of the Council of 13 December 2011 on the European protection order, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0099

Exchange of information on road traffic offenses: Directive 2015/413/EU of the European Parliament and of the Council of 11 March 2015 facilitating the cross-border exchange of information on road safety related traffic offences, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L0413

Prüm Decisions: Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, https://eur-lex.europa.eu/legal-content/EN/ TXT/?uri=celex-:32008D0615; Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008D0616

ECRIS and ECRIS-TCN: Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, https://eurlex.europa.eu/legal-content/EN/TXT/?uri=celex:32009F0315; Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA, https://eur-lex.europa.eu/eli/dec/2009/316/oj; Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA, https://eur-lex.europa.eu/legal-content/EN/ TXT/?uri=CELEX:52016PC0007; Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011, https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX:52017PC0344

Swedish Framework Decision: Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the

European Union, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32006F0960

plementation, particularly with regard to member state practices and commitments to cooperate or to use specific instruments.

Finally, legal instruments do not exist in a vacuum. Ongoing legislative processes will greatly impact some instruments in this group, both directly and indirectly. These ongoing processes, however, do not impact the fundamental rights review of the current instruments; therefore, the study analyses them.

The instruments in the cross-border subgroup aim to improve different types of cooperation in the area of freedom, security and justice, in particular in the area of criminal investigations. There are however some differences in the material, personal and geographical scope of the instruments, such as the range of measures they cover and to which authorities they are applicable. For instance, the three MLA agreements have very similar purposes, relating to the improvement of judicial cooperation between EU member states and third countries in criminal matters. The aim of the Prüm Decisions is "to step up cross-border cooperation particularly the exchange of information between authorities responsible for the prevention and investigation of criminal offences," primarily by establishing a system based on the networking of Member States' databases containing DNA profiles, fingerprint data and vehicle registration data. The 'Swedish Framework Decision' establishes the rules under which Member States' law enforcement authorities may exchange existing information and intelligence effectively and expeditiously for the purpose of conducting criminal investigations or criminal intelligence operations.

Other instruments in this group have rather different purposes. The European Protection Order aims to "enable a competent authority in another Member State to continue the protection of victims of crime in the territory of that other Member State, following criminal conduct, or alleged criminal conduct, in accordance with the national law of the issuing State". This instrument also aims at improving cross-border collaboration, but in the context of protecting victims as opposed to advancing criminal investigations through information sharing. Finally, Framework Decision 2002/584/JHA on the European Arrest Warrant (EAW) sets out the rules concerning the execution by one Member State of a judicial decision issued by a Member State, with a view to surrender a requested person for criminal prosecution or for the execution of a custodial sentence or detention order. As clarified by the Framework Decision and repeatedly confirmed by the Court of Justice (CJEU), the EAW was meant to abolish the traditional system of extradition between Member States and to replace it with a simplified, quick and effective mechanism of surrender, to facilitate and accelerate judicial cooperation.

The fundamental rights assessment here follows that set out in Article 52(1) CFR. Relevant references to ECHR case law are also included. The analysis primarily focuses on the rights to privacy and data protection (Article 8 CFR, Articles 7 and 8 ECHR), but other relevant rights are also taken into account:

- the right to respect for private and family life protected under Article 7 of the Charter and 8 of the ECHR jointly with the right to personal data protected under Article 8 of the Charter;
- the right(s) to an effective remedy and fair trial recognised under Article 47 of the Charter and Articles 6 and 13 of the ECHR;
- the right to non-discrimination protected under Article 21 of the Charter and Article 1 of the ECHR;
- the protection of human dignity (Article 4 of the Charter and Article 3 of the ECHR); and
- the right to good administration according to Article 41 of the Charter.[177]

4.4.2 Fundamental rights assessment

Instruments in the mutual recognition framework are based on the default principle that a decision of a member state should be recognised and enforced in another member state. As a consequence, these instruments include a limited list of grounds for non-execution that the requested

177 This is included in the analysis of the European Arrest Warrant.

member state may or shall take into account and invoke as necessary. One overarching issue that was raised in a number of the individual assessments and which concerned both intra-EU and EU-third country arrangements (European Arrest Warrant, EU Japan MLAT, EU-U.S. MLAT, European Investigation Order, the Swedish Framework Decision) is whether, firstly, fundamental rights considerations constitute a ground for refusal/withholding information; and secondly, if the grounds for refusal are optional or mandatory. From a fundamental rights perspective, the possibility to refuse on broad grounds related to fundamental rights would provide a stronger safeguard. However, broadening refusal grounds would conflict with the principle, purpose and efficiency of mutual recognition instruments.

One important difference between the instruments analysed is that, due to their nature, the exchange/disclosure/sharing requirement is not always accompanied by a data collection obligation. For example, the Swedish Framework Decision does not contain an obligation to collect data but only focuses on making data available that law enforcement authorities in a given Member State already have in their possession. While the instruments in question have all been grouped under the heading of 'cross borders', they have diverse aims or purposes as discussed above.

4.4.3 Rights to privacy and data protection

Provided for by law

The analysed instruments did not reveal serious shortcomings regarding the criterion that interferences with rights must be provided for by law.

Respect for the essence of rights

None of the instruments analysed violates the essence of fundamental rights. However, there are major differences between the instruments in terms of the seriousness of interferences and negative impacts on fundamental rights.

Legitimate aim

All of the instruments analysed pursue legitimate aims. Following the EDPS opinion, this issue also had to be considered in relation to the Directive on facilitating the cross-border exchange of information on road safety related traffic offenses,182[178] in order to assess whether "the measures envisaged constitute an appropriate tool with regard to this objective of reducing road fatalities" and the material scope of the Directive (i.e. the offences covered by it). In a 2008 opinion, the EDPS raised the issue of legitimacy and necessity by stressing that "it is not questionable that reducing the number of road fatalities is a legitimate purpose that could qualify as a public interest task. The question is rather whether the measures envisaged constitute an appropriate tool with regard to this objective of reducing road fatalities." The EDPS concluded that "the elements given in the explanatory memorandum and in the preamble of the proposal are sufficiently detailed and founded to support the legitimacy of the proposal and the necessity of the foreseen exchange of data." Statistics will prove relevant for assessing whether this assumption continues to support the appropriateness of the data exchange measures set out by the Directive.

Necessity and proportionality

Every instrument analysed under the cross-border group has been found to create at least one interference with the test of necessity and proportionality. The seriousness of the interferences varies between instruments, depending on the level of clarity and precision in the measures in question and the amount of personal data processed.

178 European Data Protection Supervisor, 'EDPS comments on a proposal for a Directive of the European Parliament and of the Council facilitating cross-border exchange of information on road safety related traffic offences', 3 October 2014, https://edps.europa.eu/sites/edp/files/publication/14-10-03_road_safety_en.pdf; 'Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council facilitating cross-border enforcement in the field of road safety', 8 May 2008, https://edps.europa.eu/sites/edp/files/_publication/08-05-08_road_safety_en.pdf

Certain instruments lack legal clarity due to their broad scope (either material or personal). The CJEU reasserted previous jurisprudence in Schrems, when it ruled that "EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question".[179] ECHR case law requires a similar clarity.[180]

The scope of the European Investigation Order (EIO), for instance, is formulated rather broadly. EIO does not aim to harmonise investigative measure across the EU. The investigative measures are not defined in the Directive; judicial authorities are able to request a wide range of investigative measures that could be ordered under the same conditions in a similar domestic case. The Member States measures would inevitably vary in terms of the degree of intrusiveness and, thereby, their application poses different risks and levels of interference with individual rights.

Article 6 sets out the conditions for issuing and transmitting an EIO which includes the condition that the "issuing of the EIO is necessary and proportionate for the purpose of the proceedings referred to in Article 4 [types of proceeding] taking into account the rights of the suspected or accused person." The conditions should be assessed by the issuing authority in each case to ensure that the chosen investigative measure(s) are necessary and proportionate in the particular criminal case. Under the EIO scheme it is for the issuing authority to decide on the most suitable investigative measure for obtaining evidence. According to Recital 11, part of this assessment is "whether the investigative measure chosen is necessary and proportionate for the gathering of the evidence concerned".

This specific element of the assessment leaves a wide margin of discretion to the issuing authorities and might give raise to concern based on the practices of specific national authorities, in particular because this component is not repeated by Article 6 and therefore only set out by a recital. After this assessment, the executing authority is bound to execute it unless it can rely on one of the grounds for non-recognition or non-execution. The executing authority is thus in principle deprived of the possibility to assess or question the suitability or the proportionality of the requested investigative measure beyond the limitations detailed in the individual report on EIO.[181]

The issue of processing sensitive data is most prevalent with regard to ECRIS and the ECRIS-TCN proposal. The assessment argues that the necessity and proportionality of including fingerprints (for searching the system) and facial images (for confirmation of identity) in the centralised ECRIS-TCN database is not evident. With this in mind, the interference with the right to non-discrimination foreseen in the proposals cannot be justified either.

Similar issues were identified in the analysis of the Prüm decisions. The assessment concluded that the hit/no hit procedure related to searches with reference to DNA profiles creates an unjustified interference with the rights to privacy and data protection. The return of a 'hit' in response to a search, even though it does not reveal any further data, makes clear that information on an un-identified individual exists in the database in question, even where there may be no legal requirement for further data on that individual to be given to the searching Member State.

Some of the assessed instruments reveal doubts as to their compliance with the purpose limitation principle,[182] for example in the EU-US MLAT. Even though the Agreement includes a provision (Article 9) that sets limitations on data processing to protect personal and other data, the purpose

179 CJEU, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland, 8 April 2014, para. 54,* https://eur-lex. europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0293; Case C-498/16, *Schrems, 25 January 2018, para. 91,* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62016CJ0498

180 ECtHR, *M.M. v. the United Kingdom (application no. 24029/07), 9 April 2013,* http://hudoc.echr.coe.int/ eng?i=001-114517

181 For details, please refer to the EIO report.

182 The purpose limitation principle is considered a very important factor for the assessment of the proportionality of data processing. Purpose specification as well as the concept of compatible use of data contribute to transparency, legal certainty and predictability of data processing. The purpose limitation principle aims to protect the data subject by setting limits on how controllers are able to use their data and reinforce the fairness of the processing. The limitation prevents the use of individuals' personal data in a way (or for further purposes) that they might find unexpected, inappropriate or otherwise objectionable. The purpose limitation principle is recognised both in Article 5(1b) and recital 50 of the GDPR and in Article 4(1b) and recital 29 of the LED.

of the use of information obtained is set out in such broad terms that it is questionable whether it meets the fundamental EU data protection principle of purpose

limitation.[183, 184]

It is a structural flaw that many instruments in this group lack detailed safeguards regarding access, data security, data retention periods despite the existence of different data protection frameworks on the EU level prior to the adoption of the analysed instruments. However, the significance of the full enforcement of the Umbrella Agreement, the GDPR and the implementation of the LED will be of paramount importance to ensure compliance with fundamental rights.

The lack of specified safeguards or the dependence of safeguards on third countries' legal instruments or national practices also leads to a transparency issue. The instruments have to be also assessed in the context of the principle of transparency of data processing, which is a precondition to ensure that data protection rights can be effectively exercised. Some instruments reveal shortcomings in this regard. Regarding the MLAs, foreign law and the applicable data protection and procedural standards are not easily accessible or foreseeable for individuals.

On a separate consideration for foreseeability, the question of limited accessibility of internal protocol in the national context was noted by the CJEU in the case Smaranda Bara and Others[185], where the Court was dissatisfied that certain detailed arrangement concerning transferring personal data were laid down not in a legislative measure but in the protocol agreed between two state agencies which were not published in the official journal of laws, and that the data subject didn't have adequate information of the data transfer. The data processing takes place under public laws in the assessed instruments.

The best example from this group in terms of fundamental rights standards is the European Protection Order. Compared to other instruments implementing the principle of mutual recognition in criminal matters, the European Protection Order minimizes the use of personal data and the subsequent impact on the right to privacy and data protection. The rules on the scope of the data to be processed and their transfer is specific and precise, and the purpose limitation is adequate to pursue the sole objective of facilitating the rapid and correct identification and localisation of the persons concerned, with a view to ensure the effective functioning of the EPO system. On the practical side, however, the EPO cannot serve as an example due to the fact that it is heavily underused and thus fails to achieve its objectives. According to the an evaluation report, to date only seven EPOs have been identified compared to the approximately 100,000 women residing in the EU who were covered by protection measures related to gender-based violence since 2010.[186]

183 Center for European Policy Studies, 'Access to Electronic Data by Third-Country Law Enforcement Authorities Challenges to EU Rule of Law and Fundamental Rights', 8 July 2015, https://www.ceps.eu/ceps-publications/accesselectronic-data-third-country-law-enforcement-authorities-challenges-eu-rule-law/

184 Details of purpose limitation should be assessed on the basis on the Umbrella Agreement. See further details in the individual report.

185 CJEU, Case C-201/14, *Smaranda Bara and Others v Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală (ANAF)*, 1 October 2015, para, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0201

186 "To date, only seven EPOs have been identified. The very limited use of this instrument is striking given the number of victims who are benefiting from protection measures in criminal matters at the level of Member States – many of whom probably travel/move/commute across the EU on a regular and/or occasional basis. By way of illustration, it has been estimated that in 2010 over 100 000 women residing in the EU were covered by protection measures related to gender-based violence." European Parliament 'European Protection Order Directive 2011/99/EU European Implementation Assessment', September 2017, https://www.europarl.europa.eu/RegData/ etudes/STUD/2017/603272/EPRS_STU(2017)603272_EN.pdf

4.4.4 Interference with other rights[187]

The right to non-discrimination

Compliance with the right to non-discrimination has been analysed in relation to the ECRIS and ECRIS-TCN, the European Arrest Warrant and the European Protection Order. Of these, the analysis of the ECRIS argues that the ECRIS-TCN proposal violate the essence of the right to non-discrimination. With regard to the European Arrest Warrant and the European Protection Order, the review concluded that non-discrimination concerns can be dismissed as follows.

With regard to the European Arrest Warrant (EAW), the issue of potential violation of the right to non-discrimination was settled by the CJEU in Advocaten voor de Wereld.[188] The arguments by Advocaten voor de Wereld were that the abolition of the double criminality requirement for only some offences listed in Article 2(2) of the European Arrest Warrant (whilst being maintained for the others) infringed the principle of equality and non-discrimination. The same consequence was attached to the "absence of a clear and precise definition of the offences referred to in that provision", which was considered capable of leading to "a disparate application of [national laws of implementation] by the various authorities responsible for the enforcement of a European arrest warrant." The CJEU dismissed these arguments. The principle of equality and non-discrimination requires that comparable situations must not be treated differently and that different situations must not be treated in the same way unless such treatment is objectively justified. Consequently, a varied approach to different categories of offences is objectively justified. With regard to the risk of diversified implementation at the national level, the CJEU noted that the European Arrest Warrant does not aim to harmonise domestic legal orders and that nothing in its legal bases makes the application of the EAW conditional on harmonisation of national substantive criminal law.

With regard to the European Protection Order, the review touched on the issue that the EPO system could lead to de facto discrimination, in terms of differential treatment of victims, depending on the Member States involved in the judicial cooperation procedure. In fact, the Directive does not harmonise national legislation concerning protection measures, such as their duration or the criteria for their enforcement. Consequently, there is a significant variety of approaches at the national level. The fragmentation of domestic legislation can lead to similar situations having very different outcomes, for instance in terms of nature, duration, intensity, modification in itinere and the termination of protection measures. However, this situation is due to the current limits imposed on EU powers in this field, on the basis of the principle of conferral of competences. Indeed, the differing implications of the links between EU harmonisation and often diverging national legal orders is a recurring and inherent feature of judicial cooperation procedures. Even though there is no violation of the right to non-discrimination, making efforts towards further coordination – where not approximation – of national legal orders could be a promising policy.

The fundamental rights review of ECRIS and ECRIS-TCN was much more complex. ECRIS is an information exchange network that allows the transfer of information extracted from criminal records between the Member States of the EU. The system is aimed at assisting in the implementation of the obligation to take into account, in new criminal proceedings, a conviction or convictions handed down in another Member State or States. ECRIS is currently under revision and the analysis considered both the proposal for Directive (ECRIS) and for Regulation (ECRIS-TCN).

Information on convictions can be used in criminal proceedings, in which the provision of information is mandatory; or for "purposes other than criminal proceedings" (which can be considered unlimited given the lack of specificity and clarity of the scope) in accordance with the national law of both the Member State seeking information and the one providing it. Available statistics indicate a set of purposes for which ECRIS was used so far but that does not address the broad

187 Within the other rights listed, the right to human dignity and the right to good administration were also analysed relation to one specific instrument, the European Arrest Warrant. Due to the fact that it was only an issue in the case of one instrument, we will not cover these issues in this report, details are contained in the individual assessment.

188 CJEU, Case C-303/05, *Advocaten voor de Wereld, 3 May 2007,* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62005CJ0303

nature of the provision at the time of analysis.[189]

As non-EU states do not participate in ECRIS, information on the criminal records of third-country nationals is not systematically available to Member States apart from the possibility to use "blanket requests" to all other Member States, in order to see whether they hold such information. To remedy this issue, the proposed Directive would have established an obligation for any Member State that convicts a non-EU national to ensure the storage of a set of personal data in pseudonymised form in an "index-filter", which would have been available in a decentralised manner for all other Member States to search (Article 4a). A "hit" would have consisted of a notice telling the searching Member State to contact one or more Member States holding information on the individual they were looking for. This element of the proposed Directive was subsequently discarded on technical and cost grounds, and a proposal for a Regulation instead foresees the establishment of a centralised database of convicted third-country nationals' identity data (alphanumeric data, fingerprints and optional photos). Like the proposed "index-filter" it replaces, a "hit" in the centralised database would inform the searching Member State which other Member State(s) to contact for more information on the sought third-country national.

Two different regimes of data collection are foreseen by each proposal, one for EU nationals and one for non-EU nationals (which is also foreseen to include dual nationals, those who hold the citizenship of both an EU and non-EU state) raising issues regarding the right to non-discrimination on grounds of nationality (Article 21 CFR, Article 18 TFEU). The analysis concludes that the proposal for a Regulation would have breached the essence of the right to non-discrimination (Article 21 CFR) and treaty provisions on citizenship (Article 20 TFEU) in relation to dual nationals who hold an EU and a non-EU state's nationality, but notes that this issue may be resolved through the legislative process.

The analysis concluded that this interference with the non-discrimination principle could not be justified under the necessity and proportionality test. Due to the particular position of non-EU nationals who don't have a "state of nationality" to serve as a central register for any convictions received, the changes proposed by the Directive and the Regulation would establish systems of differential treatment for EU and non-EU citizens in order to achieve the same end – to give effect to the obligation to take into account, in new criminal proceedings, a conviction or convictions handed down in another Member State or States. In doing so, the proposals interfere with the right to non-discrimination in an unjustifiable way. This interference relates to the mandatory inclusion of third-country nationals' fingerprints in the central database, the hit/no-hit function[190] and the definition of dual nationals according to the proposals, which would breach Article 20 TFEU on citizenship.

The rights to an effective remedy and a fair trial

The fundamental rights review covered the rights to fair trial and effective remedy with regard to two instruments – the European Arrest Warrant and the European Protection Order.

Soon after its adoption the European Arrest Warrant raised serious concerns in relation to the right to a fair trial, stemming from the consideration that the instrument is primarily focused on strengthening judicial cooperation in criminal matters and far less on enhancing the concerned person's procedural rights. The entry into force of the Treaty of Lisbon and the following package of EU rules on procedural rights for persons accused or suspected of crime changed this land-

189 Since April 2012, statistics for the monitoring the functioning of the ECRIS system show the purposes for which it has been used. See: Report from the Commission to the European Parliament and of the Council concerning the exchange through the European Criminal Records Information System (ECRIS) of information extracted from criminal records between the Member States, COM(2017) 341 final, 29 June 2017, https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX:52017DC0341 and the accompanying document: SWD(2017) 242 final, https://eur-lex. europa.eu/legal-content/EN/TXT/?uri=CELEX:52017SC0242

190 Under the current system, requests for information for any purpose other than criminal proceedings do not have to be responded to by Member States, thus allowing them to meet the requirement of not disclosing information unless the procedure meets the legal requirements of both the requesting and the requested state. Under the proposed Regulation (Article 7), Member States querying the central system would receive a "hit" if information was found, even if their request was for purposes other than criminal proceedings.

scape. Concrete measures (such as right to interpretation and translation, the right to information, the right to access to a lawyer, and the procedural guarantees for children who are suspects or accused persons in criminal proceedings) were put in place in the attempt to address the main loopholes in procedural rights. More specifically, Article 10 of Directive 2013/48/EU expressly provides for the right to access to a lawyer in EAW proceedings, which should be guaranteed in both the executing and issuing Member States. In practice, additional issues may arise in national legal orders, due, for instance, to the lack of or poor implementation of relevant EU law or to the specific circumstances of a case (e.g. delayed access to a lawyer, poor quality of interpretation or translation services).

The CJEU has provided further clarification, considering potential violations of the right to a fair trial. The CJEU stated that Article 47 does not grant absolute protection. Instead, its scope must be balanced with the need for effective judicial cooperation procedures. The well-known preliminary rulings in Melloni and Radu[191] are highly instructive, in particular in relation to the accused person's right to participate in the proceedings and the right to be heard. In conclusion, provided that - pursuant to the Melloni doctrine - the executing authority could be required to balance the absolute protection of the right to an effective remedy and of its corollaries with the principle of effectiveness of EU law, the EAW does not raise compelling issues under this heading.

The European Protection Order is largely compliant with the right to a fair trial and an effective remedy, but there are some specific obligations that must be borne in mind to ensure that these rights are respected. These includes the obligation for national authorities to ensure that the pre-EPO phase fully complies with fair trial rights, details for the issuing state on how to inform the protected person, and also additional procedural rights that must be ensured by the executing state. The right to an effective remedy of the person causing danger, in both the issuing and the executing State, must be considered. The Directive per se does not raise concerns under Article 47 of the Charter, but it is up to the Member States, through their implementing legislation and/or their general regimes on legal remedies, to ensure effective and equivalent protection.

4.4.5 Conclusion

The fundamental rights assessment conducted under Task 5 has led to the identification of a series of justified and unjustified interferences with rights protected under the ECFR and the ECHR, and in particular the rights to data protection and to private life. Overall, we detected improvement from a fundamental rights perspective in the quality and clarity of the laws as time progressed, in particular after the entry into application of the Lisbon Treaty and the applicability of the CFR. The reports on instruments have suggested concrete areas for improvement detailed in the assessment. In conclusion, the assessment of the instruments in the cross-border group pointed out issues with the necessity and proportionality requirements but did not find a breach to the essence of the analysed rights. One exception to that – as reported above – is the ECRIS-TCN proposal with regard to the right to non -discrimination[192].

191 CJEU, Case C-399/11, *Melloni and Radu v. Ministerio Fiscal, 26 February 2013,* https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX:62011CJ0399

192 As per the individual report at the time of analysis of the ECRIS-TCN which was the subject of negotiations during the completion of this study.

4.5 PNR and finances group report

4.5.1 Introduction

This report summarises the findings of the fundamental rights assessments of the 12 instruments belonging to the Passenger Name Record (PNR) and finances group.[193]

The PNR instruments in question are the 2016 EU PNR Directive and the PNR agreements that the EU has concluded with third states (currently the US and Australia). The purpose

of these instruments is the prevention, detection, investigation and prosecution of terrorist offences and serious crime. The API Directive, a border management instrument, was also analysed under this group given the link between API and PNR data, at least in the context of the EU PNR Directive.

In addition, four EU member states' PNR systems were assessed:

- Belgium, one of the first countries to implement the EU PNR Directive. The Belgian PNR law is particularly relevant as it extends the scope of processing of PNR data to other means of transport beyond air carriers;
- Denmark, as the country put in place a PNR framework despite its opt-out from the EU PNR Directive. The analysis helps assess possible differences in the approach adopted compared the measures provided for under the EU PNR Directive and EU member states' implementation;
- France, one of the countries that requested the EU PNR Directive and which had a PNR system

193 EU Passenger Name Record Directive: Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, https://eur-lex.europa.eu/eli/dir/2016/681/oj Advance Passenger Information Directive: Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004L0082

Belgium PNR law: Loi relative au traitement des données des passagers, 25 December 2016, http://www.ejustice. just.fgov.be/eli/loi/2016/12/25/2017010166/moniteur

France PNR law: Article L. 232-7 in the Code for Interior Security as modified by the Law reinforcing the interior security and the fight against terrorism, LOI n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme UK PNR system: Section 36-7, Immigration, Asylum and Nationality Act of 2016, http://www.legislation.gov.uk/ukpga/2006/13/contents; Home Office and HM Revenue & Customs, Code of Practice on the management of information shared by the Border and Immigration Agency, http://www.statewatch.org/news/2008/may/uk-cop-data-shareborders.pdf

Danish PNR system: The Danish PNR framework consists of several measures across the following Danish laws: Customs Act, Section 17; Danish Security and Intelligence Service Act, Section 5; Danish Defence Intelligence Service Act, Section 3; Aliens Act, Section 38, and Law amending the Defense Intelligence Service Act (FE) and the Customs Act. EU-USA PNR Agreement: Council Decision of 26 April 2012 on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012D0472 EU-Australia PNR Agreement: Council Decision of 13 December 2011 on the conclusion of the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, https://eur-lex.europa.eu/legal-content/EN/ TXT/?uri=CELEX:32012D0381

4th Anti Money Laundering Directive: Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/ EC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L0849

Council Decision on Asset Recovery Offices: Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32007D0845 Regulation on information on the transfer of funds: Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015R0847

Terrorist Finance Tracking Programme: Council Decision of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32010D0412

in place well before EU legislation was approved; and

- the UK, as recommended by Commission representatives during the study, considering that the UK was the first EU country to develop a PNR framework.

Regarding finances, the most recent and important measures concerning the fight against fraud, money laundering and terrorist financing were analysed.

Fourteen PNR and finances instruments were initially identified, although eventually only 12 of them were analysed. The Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record (known as the EU-Canada PNR Agreement) and the Delegated Regulation on high risk third countries were discarded, the former due to the ongoing negotiations between the EU and Canada following the Opinion of the European Court of Justice of 26 July 2017[194] and the latter because of its nature and content.

The envisaged EU-Canada PNR Agreement has been under discussion since 2013. A proposed text was signed by the Council of the EU and Canada, but in December 2014 the European Parliament referred the text to the CJEU to test its compliance with the CFR (the Parliament must consent to the text before the Agreement can be ratified by the EU). The pilot project of which these assessments are a component began in January 2017. On 26 July 2017, the CJEU issued opinion A-1/15, in which it found that the proposed Agreement is not compatible with Article 52(1) of the Charter nor with the fundamental rights to privacy (Article 7), data protection (Article 8) and non-discrimination (Article 21), insofar as it does not preclude the transfer of sensitive data from the EU to Canada and the use and retention of that data. The CJEU's opinion sets out the conditions that must be met by the envisaged Agreement, in the form of safeguards and modifications, for it to comply with the requirements of the CFR. In the author's view, given the findings of the Court, the need for another fundamental rights assessment of the proposed agreement under this pilot project become superfluous.

Regarding the Commission Delegated Regulation on high-risk third countries, the document is comprised of a list of third countries which have strategic deficiencies in their legislation to counter money laundering and terrorist financing, which may pose significant threats to the financial system of the EU. It does not provide for any form of data processing and therefore falls outside the scope of this pilot project.

Finally, the scope of analysis of the 4th Anti Money-Laundering Directive (4AMLD) was slightly altered in the course of this project. After the pilot project began in January 2017, the EU legislators reached political agreement on a Commission proposal amending that Directive. We therefore took into consideration relevant measures under the 4AMLD and the newly concluded proposal.

4.5.2 Fundamental rights assessment

A number of instruments include measures that create unjustified and/or disproportionate interferences with specific rights. In addition, some measures were found to be in contradiction with provisions of the EU data protection framework, including the GDPR. In both cases, recommendations were provided to ensure that the measures and instruments respect the Charter and the Convention and comply with the EU data protection framework. Finally, for the analysis of agreements between the European Union and the United States, the analysis took into consideration the 2016 Umbrella Agreement which puts in place a data protection framework between the EU and the US for criminal law enforcement cooperation.

Besides the assessment of the compatibility with fundamental rights, the analysis of the twelve instruments under this Task revealed a few issues regarding the choice of legal basis for certain measures under the API Directive, the EU-US and EU-Australia PNR Agreements.

As regards the API Directive, the measures under this law are set for the objective of migration and

194 CJEU, Opinion of the Court (Grand Chamber), Draft agreement between Canada and the European Union - Transfer of Passenger Name Record data from the European Union to Canada, 26 July 2017, para. 174 et. seq., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62015CG0001

border management. As a result, the API Directive is based on former Article 62 (2) (a) and Article 63 (3)(b) of the Treaty establishing the European Community which are now, respectively, Article 77 and 79 of the TFEU. These articles refer to border management and immigration purposes only. However, paragraph 5 of Article 6 (1) of the Directive indicates that the API data may be used for law enforcement purposes, even though the Directive is not based on a legal basis in EU law which would authorise the use of API data for law enforcement purposes.

Concerning the EU-US and EU-Australia PNR, it is unclear if the legal basis provided for in these instruments for transfer of data is appropriate. Both agreements have the dual purposes of ensuring the security and safety of the public while ensuring the protection of the PNR data transferred. Specifically to the transfer of PNR data to third countries, the Court indicates in its opinion in the EU Canada PNR Agreement that while PNR agreements cannot be treated as "equivalent to an adequacy decision", they intend to reconcile the dual objectives of protection of public safety and protection of PNR data. As a result of these two objectives which are "inseparably linked", the Court recommend to base such agreements on the first subparagraph of Article 16(2) TFEU.[195]

Following the jurisprudence of the Court, to ensure that PNR data can lawfully be transferred between the EU and a third-country, PNR Agreements should be based on Articles 16(2) and 87 of the Treaty of the Functioning of the European Union (TFEU). However, neither the EUUS nor the EU-Australia PNR Agreements refers to this Article as a legal basis; they, instead, only refer to articles of the EU Treaties on cooperation between judicial and police authorities.[196] The legal basis of these two PNR Agreements are relevant to one of the goal of the acts but insufficient to fulfil the second linked objective to protect the transferred data .

This procedural issue is relevant in the context of the fundamental rights review as any interference with the rights to privacy and data protection regarding the retention and the use of PNR data is directly linked to the original transfer of these data between the EU and the third-country and the processing of data in this third-country.

The detailed group report below will provide an overview of the nature and scope of identified interferences with each right through the fundamental right assessment conducted, as well as some information regarding the similarities or differences of the interferences between the instruments.

As regards the 12 instruments under the PNR/Finance group, experts have analysed the impact of the data processing measures of the instruments on the following rights:

- the right to respect for private and family life protected under Article 7 of the CFR; and 8 of the ECHR jointly with the right to personal data protected under Article 8 of the CFR;
- the right to an effective remedy and a fair trial recognised under Article 47 of the CFR and Article 6 of the ECHR;
- the right to non-discrimination protected under Article 21 of the CFR and Article 1 of the ECHR;
- the right to liberty and security protected under Article 6 of the CFR and Article 5 of the ECHR; and
- the right to property recognised under Article 17 of the CFR and Article 1 of the Protocol on the ECHR.

While conducting the analysis, experts found that specific measures from the 12 instruments created interferences with most of the above-mentioned rights, with the exception of the right to liberty and security.

195 CJEU, Opinion of the Court (Grand Chamber) of 26 July 2017, op. cit., paras. 93 and 96

196 CJEU, Opinion of the Court (Grand Chamber) of 26 July 2017, op. cit., paras. 95-7

4.5.3 Rights to privacy and data protection

Compliance with the right to privacy and the right to data protection were analysed jointly given the close relationship between these two distinct rights. Every instrument analysed by the PNR and finances group is considered to cause at least one interference with these rights. Indeed, the jurisprudence of the CJEU establishes that the mere processing of any personal data may constitute a "threat" to the rights to respect for private life and the protection of personal data recognised by Articles 7 and 8 CFR and Article 8 ECHR, as well as Article 16 of the TFEU.[197] The seriousness of the identified interferences, however, varies depending on the instrument, the nature of the measure, the level of clarity and precision in the measures and the amount of personal data processed.

Overall, most of the identified interferences were found to be unjustified for failing to meet the requirements of the principles of necessity and proportionality. These unjustified interferences mainly resulted from the following measures:

- Broad data retention mandates, either in terms of retention duration, and/or scope of data subject covered;
- Vague measures on access to retained data that often lack appropriate safeguards on data security or limitation on authorities authorised to access the data;
- Authorisation to process sensitive data, or failure to adequately prevent such processing, even though the processing of special categories of data goes beyond what is necessary for the identified aim of the instrument.

Finally, one measure was found to create an unjustified interference with the rights to privacy and data protection for not passing the test of being "provided for by law".

Provided for by law

Following the ECtHR's case-law, for an interference to be "provided for by law" within the meaning of Article 8 (2) of the ECHR, it requires not only that the measure should have some basis in legislation, but it also refers to the quality of the law in question. The legal basis for the interference has to be sufficiently precise and accessible to the person concerned, who has, moreover, to be able to foresee its consequences for him/her (Kruslin v. France; Rotaru v. Romania; M.M. v. United Kingdom).[198] The CJEU has also established that the expression "provided for by law" requires, in essence, for the interference to be in line with the "accessibility" and "foreseeability" criteria.

Of the twelve assessed instruments, only the Belgian PNR law was found to not meet the criteria of being "provided for by law". The particular measure concerns the collection and processing of PNR data of all passengers to all trains, buses and boats travelling to and from Belgium. The collection and processing of all PNR data of all flights' passengers travelling to and from Belgium is mandated by the EU PNR Directive. Belgium has, however, decided to increase the scope of application to other means of transport.

In the context of communications data, the CJEU has held that "the fact that data are retained and subsequently used without the [...] user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance."[199] Some member states argued before the CJEU that such a conclusion cannot be drawn in the case

197 CJEU, Michael Schwarz v Stadt Bochum, Case C-291/12, 17 October 2013, para. 48, https://eur-lex.europa.eu/ legal-content/EN/TXT/?uri=CELEX:62012CJ0291

198 ECtHR, Case of Kruslin v. France (Application no. 11801/85), 24 April 1990, http://hudoc.echr.coe.int/ eng?i=001-57626; ECtHR, Case of Rotaru v. Romania (Application no. 28341/95), 4 May 2000, http://hudoc.echr. coe.int/eng?i=001-58586; ECtHR, Case of M.M. v the United Kingdom (Application no. 24029/07), 13 November 2012, http://hudoc.echr.coe.int/eng?i=001-114517

199 CJEU, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, 8 April 2014, para. 37, https://eur-lex. europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0293

of PNR data, as less data would be processed and fewer persons would be concerned than with regard to telecommunications data retention measures. In fact, the collection of all PNR data from all passengers on (at least) all flights to and from the EU involves the processing of a large amount of personal data with the aim to assess the risk presented by air passengers. Such data, by default, also includes data of bona fide travellers that has no link with the terrorism and serious transnational crimes. The results from the risk analysis show that the vast majority of air passengers can be considered bona fide travellers.

While these measures may impact fewer people than in the context of telecommunications data retention and the quantity of data processed may arguably be smaller, it does not necessarily mean that the measures laid down in the PNR instrument do not amount to surveillance of travellers. Profiles and patterns of travel can be established and thus provide detailed insight into people's private lives. For instance, while passengers may understand that they have been flagged for further scrutiny following a first series of questions upon arrival at the airport, despite the fact that the national and EU PNR instruments have been published in national and EU official journals, the author takes the view that they are not necessarily aware of the fact that information about them will be stored for several years and that these data could be shared with other authorities.

Regarding the Belgian law, the collection of PNR data of passengers on all flights, trains, buses and boats to and from Belgium involves the processing of an excessive amount of personal information which, by the same reasoning set out above, by default includes data that is not necessary for the purpose of the fight against terrorism and serious transnational crime. Despite this serious interference with the right to privacy and data protection, the Belgian PNR law does not provide for any obligation to inform passengers of the specific processing of their PNR data. However, a quick internet search reveals that such information can be found on the website of the Belgium Federal Department of the Interior. Yet, some passengers may not necessarily be aware that information about them will be stored for several years and that this data can be shared with other authorities. In that sense, passengers whose data will be collected, assessed, retained and accessed under the PNR law will not be able to foresee the consequences of these processing for them.

As a result, in the authors view, the Belgian PNR law does not provide adequate safeguards to ensure that passengers will be aware of the measure. It therefore does not meet the "foreseeability" criteria, which, as noted above, is a necessary requirement for an interference with fundamental rights to be considered clear and precise enough to be "provided for by law".

Respect for the essence of the rights

The 12 instruments assessed have been found to respect the essence of the rights to privacy and data protection. Despite the existence of interferences, all instruments acknowledge, in more or less detail, the importance and relevance of privacy and data protection rights. In addition, most instruments include explicit reference to relevant data protection frameworks.

Legitimate aim

All the instruments analysed have been found to satisfy the criteria of meeting an objective of general interest, or legitimate aim. The instruments covered under the PNR and Finances group pursue one or more of the following objectives:

- fight against crime, organised crime, and cross-border crime;
- migration and border management;
- fight against terrorism;
- combating money-laundering and the financing of terrorism; and
- prevention, detection, investigation and prosecution of terrorist offences and serious crimes

Each of these purposes are recognised as objectives of general interest by the EU through Article 52 CFR, the Treaties or the jurisprudence of the CJEU. These objectives also constitute legitimate aims in the sense of the ECHR, based on the jurisprudence of the ECtHR and/or conventions of the Council of Europe.

Necessity and proportionality

Provisions in each of the 12 instruments analysed were found to create unjustified interference with the rights to privacy and data protection, for failing to meet the requirements of the principles of necessity and proportionality.

a) Data retention

A common issue identified concerns data retention mandates that go beyond what is necessary and proportionate. The jurisprudence of the CJEU in Digital Rights Ireland and in the opinion on the Canada PNR Agreement has established that an instrument introducing data retention measures must include rules governing the scope and application of these measures in a clear and precise manner, and provide for sufficient guarantees to effectively protect personal data against the risk of abuse and against any unlawful access to and use of retained data.[200]

Several data retention mandates in the instruments analysed under this group go beyond what is necessary for the defined objective of the instrument, by, for instance, not requiring a link between the information retained and the purpose of the instrument.[201] For instance, the envisage PNR agreement does not require any relationship between the person whose data is being collected and retained and the existence of a threat to public security once the person has arrived in Canada and up to her or his departure from the country. Instead, this was considered unjustified by the Court : "as regards air passengers in respect of whom no [such] risk has been identified on their arrival in Canada and up to their departure from that non-member country, there would not appear to be, once they have left, a connection — even a merely indirect connection — between their PNR data and the objective pursued by the envisaged agreement which would justify that data being retained. The considerations put forward before the Court, inter alia, by the Council and the Commission regarding the average lifespan of international serious crime networks and the duration and complexity of investigations relating to those networks, do not justify the continued storage of the PNR data of all air passengers after their departure from Canada for the purposes of possibly accessing that data, regardless of whether there is any link with combating terrorism and serious transnational crime".[202]

b) Data security and access to data by third parties

A number of instruments lack appropriate data security and integrity safeguards which would help mitigate risks of abuse and unlawful access to the retained data. For instance, instruments such as the AROs Decision and the 4AMLD do not include any provisions concerning data security. Ensuring data security is a key component of EU data protection framework and data security requirements stemming from these laws have been further refined by the CJEU in the Digital Rights Ireland case in the area of communications data. Further interferences were highlighted with regard to some of the finances instruments and their rules on access to data, as some of those instruments do not specify which authorities will be able to access and use the retained data.

c) Sensitive data

A small number of provisions in the instruments analysed fail to meet the requirements of necessity and proportionality as they either allow or do not adequately prevent the collection of sensitive data in cases where the processing such information goes beyond what is necessary for the aim of the instruments.[203] Specifically, with regard to the PNR legislation examined, we recommend that the legislator be more precise in the language used to ensure that there will be no processing of sensitive personal data in this context. In its opinion on the EU-Canada PNR

200 CJEU, Digital Rights Ireland, op. cit., para. 54; CJEU, Opinion of the Court (Grand Chamber) 1/15 of 26 July 2017, op. cit., para. 54

201 See, for instance, CJEU, Opinion of the Court (Grand Chamber) 1/15 of 26 July 2017, op. cit., para. 205

202 CJEU, Opinion of the Court (Grand Chamber) 1/15 of 26 July 2017, op. cit., para. 205

203 See, for instance, CJEU, Opinion of the Court (Grand Chamber) 1/15 of 26 July 2017, op. cit., para. 167

Agreement, the CJEU indicated that the processing of sensitive data would be incompatible with Articles 7 and 8 and Article 52(1) of the Charter and therefore recommended that such data be excluded from the scope of the agreement.[204] We do however note an improvement of this language over time. As a result, the language provided for under the EU-US and EU-Australia PNR agreements would require significant amendments to be brought into line with the necessity and proportionality principles, while the language of the EU PNR Directive shows more consideration, although further improvement is still possible according to the authors (as detailed in the individual assessments) despite the fact that the Directive contains a prohibition to collect and use sensitive data.

Overall, there has been an improvement in the quality and clarity of the PNR and finances legal frameworks over the years, in particular after the entry into application of the Lisbon Treaty and the applicability of the Charter. The EU PNR Directive, for instance, contains some flawed provisions and would have to be amended to fully comply with Articles 7 and 8 CFR; however, it is significantly clearer and provides for more safeguards than the EU-US and EU-Australia PNR agreements.

4.5.4 Interference with other rights

The right to non-discrimination

Compliance with the right to non-discrimination was analysed considering specific measures enshrined by the following instruments:

- the Belgian PNR law;
- the EU PNR Directive;
- the EU-Australia PNR Agreement; and
- the EU-US PNR Agreement.

As highlighted by the Fundamental Rights Agency, the processing of PNR data against various databases may lead to an interference with the right to non-discrimination protected under Article 21 CFR.[205] It was therefore necessary to conduct a preliminary analysis to determine whether any data processing measures under these frameworks created such an interference.

As for the EU PNR Directive and the Belgian PNR law, the assessments concluded that the measures under these frameworks are satisfactory to mitigate the risk of direct discrimination. In particular, the measures prohibiting the processing of sensitive data and requiring that the assessment of passengers' data be carried out in a non-discriminatory manner with pre-established models and criteria which are specific and reliable, significantly contribute to mitigating the risks of direct discrimination and discriminatory profiling.

As for the EU-Australia and EU-US PNR agreements, the measures on automated processing of PNR data are not clear, precise and limited enough to justify the interference established with the rights to privacy and data protection, when read in conjunction with the right to non-discrimination. An additional unjustified interference was identified in the EU-US PNR Agreement, which includes measures contradicting the jurisprudence of the CJEU by authorising the transfer of sensitive data to third countries' authorities. In this respect, the EU Court of Justice have pointed the risks of such data being processed in a way that leads to discrimination: "the transfer of sensitive data to Canada requires a precise and particularly solid justification, based on grounds other than the protection of public security against terrorism and serious transnational crime. In this

204 Ibid.

205 'Opinion of the European Union Agency for Fundamental Rights on the proposal for a Directive on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011) 32 final)', 15 June 2011, https://fra.europa.eu/en/opinion/2011/fra-opinionproposal-passenger-name-record-pnr-directive.

instance, however, there is no such justification". [206] Therefore, the EU Court of Justice establishes that Articles 7 and 8 of the Charter, read in conjunction with Article 21 of the Charter preclude the transfer of sensitive data to third-countries authorities[207].

Finally, it was noted that for every instrument, beyond potential risks of direct discrimination, a risk of indirect discrimination may exist. Research conducted by the FRA pointed out that several passengers felt they were being checked unfairly because of their ethnic or national background.[208] Other passengers felt they were discriminated against on the basis of their gender.[209] In the context of PNR; the research did not find systematic discriminatory patterns of profiling, but some incidents of possible discriminatory treatment were observed.

It is important to note that some of the PNR legislation examined, such as the EU PNR Directive, includes safeguards to prohibit discrimination (for example, on the basis of ethnic origin or gender). However, it is very difficult in practice to ensure that all border agents will implement these safeguards as some agents may have conscious or subconscious biases. In fact, border agents may interpret PNR data in a discriminatory manner, despite existing safeguards. While this risk is not the result of measures introduced by the PNR frameworks or due to the processing of PNR data in itself, FRA stressed that the addition of specific provisions requiring statistics on border controls could help detect discriminatory patterns and trends in the application of specific rules, criterion or practices which can then help mitigate the risk of indirect discrimination.[210] While this latter point falls outside the scope of the Pilot Project sticto sensu as it is not linked to a violation of a right resulting from data processing measures, the individual assessments provided recommendations aimed at reducing the risks of indirect discrimination, as they can contribute to improving the overall quality of the law and its implementation.

The right to an effective remedy and a fair trial

Compliance with the right to an effective remedy and a fair trial was analysed in relation to the 4AMLD. This instrument includes measures requiring specific categories of subjects whose activities are covered by professional secrecy (including lawyers) to report to competent authorities potential money-laundering perpetrated by their clients, when they become aware of such facts (e.g. when advising them on tax or financial matters). This obligation may create tension with the protection of professional secrecy, confidentiality and privacy in the lawyer-client relationship which is essential to ensure a proper representation in judicial proceedings.

Following the line of reasoning set out in the CJEU ruling on the Second Anti Money Laundering Directive, it can be concluded that the obligation to report clients required by the 4AMLD does not unjustly infringe on the right to a fair trial protected by Article 47 CFR.[211] The obligations under the 4AMLD do not apply in the context of judicial proceedings but when lawyers advise their clients on financial or tax matters. Consequently, those activities fall outside the scope of the right to a fair trial.

206 See, for instance, CJEU, Opinion of the Court (Grand Chamber) 1/15 of 26 July 2017, op. cit., para. 165.

207 See, for instance, CJEU, Opinion of the Court (Grand Chamber) 1/15 of 26 July 2017, op. cit., para. 165-167

208 Fundamental Rights Agency, 'Fundamental rights at airports: border checks at five international airports in the European Union', November 2014, p. 47, https://fra.europa.eu/en/publication/2014/fundamental-rights-airportsborder-checks-five-international-airports-european

209 Ibid.. p.47

210 'Opinion of the European Union Agency for Fundamental Rights on the proposal for a Directive on the use of Passenger Name Record (PNR) data', op. cit., p.21

211 CJEU, Case C-305/05, Case C-305/05, *Ordre des barreaux francophones et Germanophone*, para. 33, 26 June 2007, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62005CJ0305

The right to liberty and security

None of the instruments or specific measures on data processing in this group were analysed in relation to their compliance with the right to liberty and security. However, it should be noted that a large number of the instruments analysed under the PNR and finances group pursue objectives of general interest recognised by the EU and, because of their nature, may contribute to safeguarding the right to liberty and security.

The right to property

Compliance with the right to property was analysed in relation to two instruments: the 4AMLD and the Asset Recovery Offices (AROs) Decision. Both instruments include measures that either refer to or may lead to the freezing, seizure or confiscation of assets.

The freezing, seizure or confiscation of assets may occur in operations related to the implementation or linked to the 4AMLD and the more recently-agreed amending legislation, but none of the actions are likely to result from the processing of information under the Directive. As a result, even if an interference with the right to property were found, such interference would fall outside the scope of this Pilot Project. No further analysis was therefore conducted.

Regarding the AROs Decision, the Decision's measures permitting the freezing, seizure or confiscation of assets (for example, through the processing of information for tracing and identification of proceeds of crime and other crime related property) constitute an interference with the right to property. In Kadi, the CJEU ruled that for the interference with the right to property to be justified, there must be a reasonable relationship of proportionality between the means employed and the aim sought to be realised.[212] The AROs Decision aims to contribute to the fight against crime, organised crime, and cross-border crime. Assets can only be frozen, seized or confiscated pursuant to a judicial order and persons affected by such decisions must be able to exercise their right to a remedy guaranteed under the EU legal order in case of abuse. Thus, the interference to the fundamental right to property in the AROs decision is, in principle, justified, as the measures in question pursue a clearly defined objective of general interest and the instrument provides for adequate safeguards which ensure compliance with the principles of necessity and proportionality.

4.5.5 Conclusions

The fundamental rights assessment of the 12 instruments in the PNR and finances group identified a series of justified and unjustified interferences with rights protected under the CFR and ECHR. In general terms, improvements emerged in the quality and clarity of the laws over the years, in particular after the entry into application of the Lisbon Treaty and the applicability of the Charter.

Overall, we found that all the instruments in question respect the essences of the fundamental rights to privacy, data protection, property and judicial remedy. All the instruments pursue objectives of general interest and a large number of them contribute to the protection of the right to liberty and security. One instrument – the Belgian PNR law – was found to lack sufficient clarify to meet the criteria of quality of law to be considered "provided for by law".

At least one provision of every measure assessed is incompatible with the rights to privacy and data protection, for failing to meet the requirements of the principles of necessity and proportionality. These interferences concern overly-broad data retention mandates, a lack of appropriate data security measures, inadequate or insufficient safeguards on access to data by third parties and provisions allowing or not adequately preventing the collection of sensitive data.

212 CJEU, Joined Cases C-402/05 P and C-415/05 P, Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities, 3 September 2008, para. 360, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62005CJ0402

Regarding the right to non-discrimination, unjustified interferences can be found in provisions of the EU-Australia and EU-US PNR agreements that are not sufficiently clear and precise. The EU-US PNR Agreement also includes measures contradicting the jurisprudence of the CJEU, as it permits the transfer of sensitive data to third countries' authorities. In contrast, the EU PNR Directive and the Belgian PNR law set out measures that are satisfactory to mitigate the risk of direct discrimination. In particular, the measures prohibiting the processing of sensitive data and requiring that the assessment of passengers be carried out in a non-discriminatory manner with pre-established models and criteria which are specific and reliable, greatly contributes to mitigating the risks of direct discrimination and discriminatory profiling.

Measures in the 4AMLD and AROs Decision that infringe upon the right to property through provisions permitting the freezing, seizure or confiscation of assets either fall outside the scope of this project (4AMLD) or are justified (AROs Decision). The analysed measures under the AROs decision pursue a clearly defined objective of general interest and the instrument provides for adequate safeguards which ensure compliance with the principles of necessity and proportionality.

In sum, there are a range of interferences, of varying levels of seriousness, affecting the instruments that have been analysed. Many of the identified issues could be resolved through recast legislation. The findings of the assessments can provide some useful guidance for future proposals, as well as for amendments to existing proposals, where possible. In particular, greater attention should be paid to the development of data retention mandates and rules on access to personal data by authorities and third parties to ensure compatibility with the principles of necessity and proportionality. The CJEU provided useful guidance on these matters over the last few years in the rulings in Digital Rights Ireland and Tele2, as well as in its opinion on the EU-Canada PNR Agreement.

4.6 Data retention laws group report

4.6.1 Introduction

This report summarises the findings of the fundamental rights assessments of data retention legislation introduced by five Member States (Denmark, Finland, Germany, Hungary, and Spain).[213] These measures permit the processing of personal data concerning electronic communications for the purposes of preventing, investigating, detecting and prosecuting criminal offences.[214] More specifically, they require electronic communications providers to collect communications metadata so that it may be accessed by competent national law enforcement and/or intelligence authorities and security agencies.[215]

The instruments within this group fall within the scope of the EU law and therefore must comply with the requirements set out in the CFR (in particular Article 52(1)).[216] This conclusion has been drawn considering the jurisprudence of the CJEU, which in the Tele2 case decided that an analogous legislative measure introduced in Sweden fell within the scope of the e-Privacy Directive.[217] The CJEU ruled that the scope of the e-Privacy Directive extends both to a legislative measure that requires electronic communications providers to retain traffic and location data, as well as to legislation regulating access to that data by the national authorities.[218] Such measures can be adopted on a national level in accordance with Article 15(1) of the e-Privacy Directive, which enables the Member States to introduce exceptions to the principle of confidentiality of communications laid down in Article 5(1) of the same Directive. If follows, therefore, that national laws in any Member State that provide for the collection and retention of metadata by electronic communications providers and for access to that metadata by competent national authorities, also fall within the scope of the EU law and the CFR.

213 **Denmark:** Administration of Justice Act *(Retsplejeloven)*, Data Retention Administrative Order *(Logningsbekendtgørelsen)*

Finland: Data Retention law *(Tietoyhteiskuntakaari)*, sections 157–159 *(statute 917/2014; Information Society Code)*

Germany: Law on the introduction of an obligation to store and a maximum period to retain traffic data (*Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten)* from 10 December 2015

Hungary: Act C of 2003 on Electronic Communications (*2003. evi C. torveny az elektronikus hirkozlesrol*)

Spain: Data Retention law (*Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*).

214 An overview of the status of data retention laws in the EU and their adequacy in relation to CJEU case law is available in: Privacy International, 'A Concerning State of Play for the Right to Privacy in Europe: National Data Retention Laws since the CJEU's Tele-2/Watson Judgment', September 2017, https://privacyinternational.org/sites/default/files/Data%20Retention_2017.pdf

215 The term "metadata" refers in this report to data revealing that a given electronic communications activity took place but not the content of that communication. Metadata may include, for example, phone billing information, mobile phone location data, visited website addresses, personal settings or web-logs (the exact types of metadata collected under each of the national laws analysed are indicated in the reports assessing each specific instrument). The recitals of the Data Retention Directive, which was annulled by the CJEU in the *Digital Rights Ireland* case, explained that retention of metadata, as demonstrated by the research and practical experience of several Member States, has proved to be a necessary and effective investigative tool for law enforcement authorities, in particular as far as serious matters such as organised crime and terrorism are concerned. See: Recitals 9 and 11, Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006L0024

216 Details are provided in the individual assessments.

217 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058

218 CJEU, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, 21 December 2016, paras. 74-79, https://eur-lex.europa.eu/ legal-content/EN/TXT/?uri=CELEX:62015CJ0203

Recent years have seen significant legal developments regarding data retention in Europe. In 2014 the CJEU judgment in Digital Rights Ireland[219] annulled the EU Data Retention Directive. This was followed by key judgments in theTele2 and Ministerio Fiscal[220] cases (2016 and 2018 respectively). However, in some of the states examined as part of this project (such as Spain), the pre-Digital Rights Ireland regime transposing the invalidated Data Retention Directive is still in place. In others (such as Denmark and Hungary), laws are still in force that precede the Directive, but which were amended in order to implement it. In other states (Germany, Poland, and Finland), legislative changes were introduced following the CJEU judgments.

In Germany a new law was adopted in 2015, aimed at adjusting the national data retention law to the Digital Rights Ireland judgment and a 2010 German Constitutional Court judgment. However, following a 2017 judgment of the Higher Administrative Court of North Rhine-Westphalia (OVG NRW)[221] delivered in the interim proceedings, the German Federal Network Agency (Bundesnetzagentur, a higher federal authority that regulates the telecommunications sector) decided to temporarily suspend the data retention obligations under the new regime for all providers, pending a final ruling in the main proceedings.[222] It also should be noted that the current data retention legislation in Germany is being challenged before the German Constitutional Court (there are several constitutional complaints pending[223]). Requests for interim decisions in relation to some of these complaints have been denied in July 2016 and in April 2017.

In Finland, some changes to national legislation were introduced in 2015 in response to the

Digital Rights Ireland ruling.[224] However, these amendments have not made the German or Finnish legislation fully compliant with the standards laid down by the CJEU. In Denmark, Hungary and Spain, meanwhile, the invalidation of the Data Retention Directive by the CJEU has not been followed by legislative changes at the domestic level. In Denmark, this is despite the fact that the authorities have explicitly admitted that the national law does not meet the standards for data retention regimes set out by the CJEU.[225]

219 CJEU, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland, 8 April 2014, https://eur-lex.europa.eu/ legal-content/EN/TXT/?uri=CELEX:62012CJ0293

220 CJEU, Case C-207/16, *Ministerio Fiscal*, 2 October 2018, https://eur-lex.europa.eu/legal-content/EN/ TXT/?uri=CELEX:62016CA0207

221 *Higher* Administrative *Cour*t of *North Rhine-Westphalia* (OVG NRW), 22 June 2017 (13 B 238/17). The OVG NRW held in an application for an interim order that the plaintiff in the case, a telecommunications provider, need not comply with the data retention obligation until the court has reached a final judgment because, according to the court, it was doubtful whether the German data retention provisions were compatible with the requirements for national data retention laws as formulated by the CJEU.

222 C. Etteldorf, 'Higher Administrative Court of Northrhine Westphalia Declares German Data Retention Law Violates EU Law', European Data Protection Law Review, 3/2017, pp. 394-398. Until the final judgment in the main proceedings, the application of the data retention laws is suspended which means that no sanctioning procedures would be initiated against providers and even if the final decision would be against the applicants they would not be fined retroactively.

223 See cases nos: 1 BvR 3156/15; 1 BvR 2845/16; 1 BvR 141/16; 1 BvR 229/16; 1 BvR 2023/16 ; 1 BvR 2683/16.

224 It should be noted that during the parliamentary process on the Information Society Code in 2014, the Constitutional Law Committee of the Finnish Parliament gave a statement on the constitutional aspects of the bill, including data retention and reflecting upon *Digital Rights Ireland* case. In the Constitutional Law Committee's view, the proposed changes were sufficient to bring the law into line with the EU Charter and the CJEU judgement. After the *Tele2* judgment, the Ministry of Transport and Communications instituted a working group to assess the legislation. The conclusion of the report is that the Finnish law is proportionate enough and no changes are needed at the moment. Ministry of Transport and Communications, 'Selvitys sähköisen viestinnän välitystietojen säilytysvelvollisuudesta', Raportit ja selvitykset 9/2017, https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80111/ Raportit%20ja%20selvitykset%209-2017.pdf

225 Two months after the *Tele2* judgment the Danish Minister of Justice told the Legal Affairs Committee of the Danish Parliament that the data retention framework did not meet the requirements of EU law because of the indiscriminate nature of data retention; thus, the Minister said, the law needed to be amended accordingly. However, no changes were adopted following the *Tele2* judgment. In June 2018, the Ministry of Justice claimed it is waiting for the guidance from the European Commission before a new data retention law is proposed to the Danish Parliament. In June 2018, the Association Against Illegal Surveillance filed a lawsuit with a national court against the Minister of Justice demanding the immediate annulment of the data retention provision. EDRi, 'Litigation against the Danish government over data retention', 13 June 2018, https://edri.org/litigation-against-the-danish-government-over-data-retention

The relevant national legislation is examined here in line with the test set out in Article 52(1) CFR and relevant case law of the CJEU. Furthermore, whenever relevant, references to the European Convention of Human Rights (ECHR) and the case law of the European Court of Human Rights (ECtHR) are included, in order to ground the assessment in a more comprehensive fundamental rights context. Article 6(3) TEU confirms that fundamental rights recognised by the ECHR constitute general principles of EU law. Furthermore, in principle there should be consistency between the CFR and the ECHR insofar as the rights in the CFR correspond to rights guaranteed by the ECHR, as regards the meaning and scope of those rights, including authorised limitations (Article 52(3) of the ECHR). At the same time, it should be noted that landmark judgments of the ECtHR referred to in this report have mostly involved competent authorities' activities in the area of national security (which as such falls outside the scope of EU law) and mainly concern the interception of the content of communications. While this differs to the retention and further processing of communications metadata, these rulings nevertheless provide precious insights and guidance which can be applied, by analogy, to other forms of access to individuals' data by competent domestic authorities. They should therefore be taken into consideration in the course of analysis of the national laws in question.[226]

The following overview outlines the extent to which instruments in question comply with these standards and points out those aspects that raise the most serious fundamental rights concerns and should therefore be addressed by domestic legislators in the future. More detailed descriptions of the instruments are presented in the individual reports.

4.6.2 Fundamental rights assessment

The instruments analysed interfere with several fundamental rights, primarily the rights to privacy and data protection, but also with the rights to an effective remedy and to freedom of expression.

The rights to privacy and data protection are the most severely compromised, as has been confirmed by the two aforementioned CJEU cases (Digital Rights Ireland and Tele2). The right to an effective remedy is also relevant, because of the potential impact on the possibility for affected individuals to challenge the application of data retention measures and their right to seek redress. The impact on the right to freedom of expression has been considered, as data retention measures may lead to 'self-censorship' by individuals who feel "that their private lives are the subject of constant surveillance."[227] Moreover, data retention regimes may pose a threat to the protection of journalistic secrecy, which forms an essential element of freedom of expression[228]

4.6.3 Rights to privacy and data protection

Both the CJEU and the ECtHR have developed jurisprudence concerning the rights to privacy and data protection as well as justified limitations to these rights in the context of data retention regimes.

According to the ECtHR, the rights to private and family life cannot be understood in a narrow sense, as the notion of private life is broad and does not lend itself to exhaustive definition. Thus, private life, in the Court's view, includes a person's physical and mental integrity. The guarantee afforded by Article 8 of the ECHR is primarily intended to ensure the development, without outside interference, of the personality of each individual in his/her relations with other human beings. In the case Liberty and others v. UK, the ECtHR explicitly stated that:

226 In both *Digital Rights Ireland (paras. 35, 47, 54, 55) and Tele2 (paras. 119-120), the CJEU has referred by analogy to the standards developed by the ECtHR in 'classical' surveillance cases.*

227 CJEU, Digital Rights Ireland, para. 37

228 ECtHR, Goodwin v. United Kingdom (application no. 28957/95), 11 July 2002, para. 39, http://hudoc.echr.coe. int/eng?i=001-57974

> "the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them."[229]

Moreover, the ECtHR has emphasised on several occasions that interferences with the right to privacy result not only from monitoring of the content of communications, but also from monitoring of the metadata.[230] At the same time, the ECtHR has also repeatedly reaffirmed that the right to privacy is not an absolute one.[231]

As for EU law, the CJEU clarified in Digital Rights Ireland that:

> "the retention of data for the purpose of possible access to them by the competent national authorities (…) directly and specifically affects private life and, consequently, the rights guaranteed by Article 7 of the Charter. Furthermore, such a retention of data also falls under Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, therefore, necessarily has to satisfy the data protection requirements arising from that article."[232]

The CJEU also stated that:

> "the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance."[233]

Furthermore, interferences with the right to privacy and data protection caused by data retention regimes should be seen as particularly far-reaching. Even though access to retained metadata does not reveal the content of communications, it involves the processing of personal data and may, in the era of the Internet, smart phones and other mobile devices, disclose considerable information about a person's private life such as social connections, behavioural patterns, preferences or interests. This is especially so given that large volumes and different types of metadata can be easily combined and systematically tracked over a certain period of time. Thus, even though the collection of and access to metadata has in the past generally been perceived as less privacy-intrusive than, for example, wire-tapping,[234] contemporary perceptions have changed. In certain situations, metadata, taken as a whole, is not necessarily considered less sensitive than

229 ECtHR, Liberty and Others v. the United Kingdom (application no. 58243/00), 1 July 2008, para. 56, http:// hudoc.echr.coe.int/eng?i=001-87207

230 ECtHR, Copland v. United Kingdom (application no. 62617/00), 3 April 2007, paras. 43-44, http://hudoc.echr. coe.int/eng?i=001-79996; Malone v. the United Kingdom (application no. 8691/79) 2 August 1984, para. 84, http:// hudoc.echr.coe.int/eng?i=001-57533; Barbulescu v. Romania, 12 January 2016, paras. 36-37, http://hudoc.echr.coe. int/eng?i=001-177082

231 ECtHR, Weber and Saravia v. Germany, 29 June 2006, 54934/00, para. 94, https://www.bailii.org/eu/cases/ECHR/2006/1173.html; Liberty and Others v. the United Kingdom, para. 62; Klass and Others v. Germany (application no. 5029/71), 6 September 1978, paras. 49-50, http://hudoc.echr.coe.int/eng?i=001-57510

232 The judgment refers here to Joined Cases C92/09 and C93/09, *Volker und Markus Schecke and Eifert, 9 November 2010, para. 47,* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62009CJ0092

233 CJEU, Digital Rights Ireland, para. 37

234 ECtHR, Malone v. the United Kingdom (application no. 9691/79), para. 84, http://hudoc.echr.coe.int/ eng?i=001-57533. The ECtHR underlined that the two types of surveillance should be distinguished and that accessing the metadata is less intrusive. One should not forget however, that the judgement was issued more than 30 yeas age in a very different technological environment.

data directly revealing the content of communications. In the Tele 2 judgment[235] the CJEU held that metadata analysis can allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained:

> "in particular, that data provides the means, as observed by the Advocate General in points 253, 254 and 257 to 259 of his Opinion, of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications."

According to the UN High Commissioner for Human Rights,[236] access to metadata may even in some cases give an insight into an individual's private life that goes beyond what is conveyed by accessing the content of a private communications. This particularly severe interference has to be compensated for with strong safeguards for data protection and privacy rights.

In the following sections, interferences with the rights to privacy and data protection caused by the data retention instruments in question are assessed according to the test laid down in Article 52(1) CFR.

Provided for by law

Under the ECtHR's case-law, for an interference to be "in accordance with the law" within the meaning of Article 8(2) ECHR requires not only that the measure have some basis in a legal act, but that the law be of sufficient quality. The law must be sufficiently precise, foreseeable and accessible to the person concerned, who must, moreover, be able to foresee its consequences for them.[237]

Two of the instruments examined here (the Hungarian and Spanish laws) do not meet the criterion of being "provided for by law". Their provisions dealing with the access of the competent national authorities to data have not been drafted with sufficient precision to meet the "foreseeability" requirement as defined in the ECtHR's jurisprudence. This is mainly because, by analogy to Iordachi and Others v. Moldova,[238] the instruments provide the competent authorities with wide discretion when it comes to accessing data, inter alia by allowing access in a very large spectrum of criminal investigations and by failing to narrow down the application of the measures to clearly-defined categories of persons. Hence, the scope of the limitations of fundamental rights in these instruments is not sufficiently clear.[239]

As regards the Danish, Finnish and German instruments, they comply with the criterion of "provided for by law". While they provide for the targeting of a broad and, in practice, indiscriminate spectrum of individuals, they provide at the same time a number of important safeguards clarifying and restricting the scope of data retention activities and the further use of data (these are discussed in more detail below).

235 CJEU, Tele2, para. 99

236 Report of the UN High Commissioner for Human Rights on the right to privacy in the digital age from 30 June 2014, A/HRC/27/37, para. 19, www.ohchr.org/EN/Issues/DigitalAge/Pages/ReportDigitalAge.aspx

237 See, for example: ECtHR, Kruslin v. France (application no. 11801/85), 24 April 1990, para. 27, http://hudoc. echr.coe.int/eng?i=001-57626; Rotaru v. Romania (application no. 28341/95), 4 May 2000, para. 57, http://hudoc. echr.coe.int/eng?i=001-58586; M.M. v. United Kingdom (application no. 24029/07), 9 April 2013, para. 193, http:// hudoc.echr.coe.int/eng?i=001-114517

238 ECtHR, Iordachi and Others v. Moldova (application no. 25198/02), 14 September 2009, http://hudoc.echr.coe. int/eng?i=001-91245

239 Such a conclusion is in line with the view expressed by the Venice Commission with regard to the Polish data retention law adopted in 2016, which in this respect resembles the Spanish and Hungarian laws. In its legal analysis of the Polish law, the Venice Commission highlighted that it may not satisfy the requirement of foreseeability of law under Article 8(2) ECHR. See: European Commission for Democracy Through Law (Venice Commission), 'Poland – Opinion on the Act of 15 January 2016 amending the Police Act and certain other Acts', 10 June 2016, pp.15-16, https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)012-e

Respect for the essence of rights

As already noted, merely permitting the retention of electronic communications data implies a restriction of individuals' rights to privacy and data protection of individuals. This restriction must respect the essence of those rights. In the Digital Rights Ireland judgement, the CJEU held that even though the Data Retention Directive constituted a serious interference with those rights, it would not directly affect their essence. Article 1(2) of the Directive made clear that it did not permit the collection or analysis of the content of the electronic communications.[240] Moreover, in the Tele2 judgement, even though the CJEU stressed the sensitive nature of metadata, it confirmed that legislation requiring the retention of metadata of electronic communications would not directly affect the essence of the rights to privacy and data protection.[241] All of the instruments analysed here contain measures analogous to those assessed by the Court, and thus should be considered to respect the essence of data protection and privacy rights.

Legitimate aim

In Digital Rights Ireland, the CJEU ruled that data retention measures can serve a legitimate aim, given the increasing use of technologies in our societies. Furthermore, the retention of telecommunications data can be particularly useful in the fight against serious and organised crime, in which case the retention of data "genuinely satisfies an objective of general interest." The CJEU also recalled in this context that Article 6 CFR lays down the right of any person not only to liberty, but also to security.

All the instruments analysed regulate the retention of data related to electronic communications and public communications networks, in order to contribute to public safety and national security (in most cases to detect, investigate, and prosecute serious crimes). Thus, in light of the CJEU's jurisprudence, those instruments (even if their aims are sometimes rather broadly-formulated) pursue objectives of general interest recognised by the EU.

Necessity and proportionality

According to the CJEU judgment in the Schwarz case,[242] it must be ensured that limitations imposed on fundamental rights are necessary and proportionate to the aims pursued. The restrictive measures should be appropriate for attaining those aims and not go beyond what is necessary to achieve them. In the context of data retention mechanisms and access by law enforcement agencies to retained metadata, the CJEU has established a set of detailed criteria that assist in assessing the necessity and proportionality of such interferences. It should be underlined that, in order to ensure that these measures effectively respect necessity and proportionality, "safeguards must be put in place to ensure that the interference with fundamental rights is minimised at both the retention and the access stages."[243]

The level of safeguards differs in each of the instruments in question. Some of them (for example, the German or Finnish laws) include several relevant safeguards; while others (for example, the Polish and Hungarian laws) have very minimal guarantees protecting data subjects' rights against abuse. None of the analysed instruments, however, fully satisfies the standards for data retention laws outlined in the CJEU and ECtHR jurisprudence and they therefore raise concerns regarding their necessity and proportionality. The most important weaknesses identified are outlined below.

240 CJEU, Digital Rights Ireland, para. 39

241 CJEU, Tele2, para. 101

242 CJEU, Case C-291/12, Schwarz, 17 October 2013, para. 40, https://eur-lex.europa.eu/legal-content/EN/ TXT/?uri=CELEX:62012CJ0291

243 Privacy International, "A Concerning State of Play for the Right to Privacy in Europe", op. cit.

a) Broad, indiscriminate retention of metadata

One of the essential requirements set out by the CJEU in Digital Rights Ireland is the need to specify who can be targeted by a measure, in order to avoid indiscriminate, over-broad retention powers. The law needs to differentiate, limit and/or make exceptions "for persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime."[244] The Tele2 judgment confirmed that a general data retention obligation is impermissible under EU law: in light of Articles 7, 8, and 11 and Article 52(1) CFR, national legislation cannot mandate "general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication,"[245] and any such legislation must be restricted to the fight against serious crime. According to the CJEU, data retention obligations should also be restricted to a "particular time period, a geographical area or a group of persons." Competent national authorities should consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences.[246] Legislation which does not meet these requirements will most likely be considered by the CJEU to cause interferences to fundamental rights that exceed the limit of what is strictly necessary and proportionate.

None of the instruments analysed meets the criterion outlined above. The retention of telecommunications metadata in all five countries is indiscriminate: it applies equally to those whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious criminal offences; and regardless of the fact that any investigation will ever be carried out against the majority of individuals affected by the metadata collection. The laws in question require the undifferentiated collection and retention of telecommunications metadata without corresponding personal, geographical or time limits. Moreover, they do not provide for exceptions for persons whose communications are subject to professional secrecy, such as lawyers or journalists.[247]

Finland is the only one of the five countries in question where there have been certain restrictions introduced (in 2015) to limit the scope of data retention. In principle, the only providers obliged to retain data are those set out in a decision of the Ministry of the Interior. In practice, however, the obligation to retain data concerns providers who jointly hold a 90% market share in internet access services and 99% in mobile phone users.[248] In practice, this does not amount to a very effective restriction.

In light of the standards set by the CJEU for data retention measures, the instruments analysed here – which allow for indiscriminate data retention and at the same time allow for the retention of a wide range of metadata which may reveal a great deal of information about the data subject's private life – may be considered to exceed the limits of what is strictly necessary and proportionate. Such a conclusion is in line with the decision delivered in Germany by the OVG NRW which, in its ruling from June 2017, delivered in the interim proceedings, relieved one of the providers of its obligation to retain traffic data.[249] The court noted that general and indiscriminate blanket data retention in Germany violated EU law as it has been interpreted by the CJEU in the Digital Rights Ireland and Tele 2 cases and lacked appropriate fundamental rights safeguards. The view of the OVG NRV has been subsequently shared by the Administrative Court of Cologne (VG Köln) in its ruling delivered in the main proceedings[250]. The judgment is not final (the appeal is currently

244 CJEU, Digital Rights Ireland, para. 58

245 CJEU, Tele2, para. 112

246 CJEU, Tele2, para 111.

247 CJEU, Digital Rights Ireland, para. 58; Tele2, para. 105.; ECtHR, Big Brother Watch and Others v. UK, para. 495.

248 Ministry of Transport and Communications, 'Selvitys sähköisen viestinnän välitystietojen säilytysvelvollisuudesta', Raportit ja selvitykset 9/2017, https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80111/Raportit%20 ja%20selvitykset%209-2017.pdf

249 Higher Administrative Court of North Rhine-Westphalia, *paras. 34-36*

250 *Administrative Court of Cologne* (VG Köln), 20 April 2018 (9 K 3859/16).

pending before the German Federal Administrative Court - Bundesverwaltungsgericht)[251].

b) Questionable data retention periods

The data retention periods differ among countries. The shortest is in Germany. The data is to be retained for the following periods: 10 weeks for traffic data, four weeks for location data (with one week as a grace period for irreversible deletion). The law provides no possibilities for extending the retention periods. In the other four states the data retention periods are significantly longer: 12 months in Denmark and Spain (although in Spain the government, taking into account the costs of storage of the data and its value in relation to the investigation of serious crimes, is able to vary the retention term for specific types of data to a maximum of 2 years and a minimum of 6 months); and from six to 12 months in Hungary and Finland, depending on the types of data.

According to the CJEU, the retention period should be justified by the aims of the law.[252] Such an explanation should be provided by the domestic legislator. The Danish and Spanish laws do not make any distinction between different categories of data, for example on the basis of their potential usefulness for law enforcement purposes. In Spain, no clear justification has been offered for the retention period, while in Denmark the government provided a only general explanation, without recourse to research or well-grounded statistical information.[253] In Finland and Hungary, the laws make some distinction between different categories of data, but in Hungary the national legislator has not provided a comprehensive justification for the respective retention periods either (only in Finland establishing data retention periods for particular categories of data has been backed up by a more thorough analysis of their necessity and proportionality[254]). Because of the lack of sufficient, evidence-based justification in Spain, Denmark and Hungary, the proportionality of the retention periods chosen in those jurisdictions cannot be clearly established.

c) Requirements for data localisation

Another requirement laid down in the Digital Rights Ireland and Tele 2 judgments is that the data should be retained within the EU. According to the Digital Rights Ireland judgment, this is a prerequisite in order to guarantee control by an independent authority of compliance with data protection and security requirements (as explicitly required by Article 8(3) CFR). Such control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data.[255] In Tele2, the CJEU focused on the data security context. It held that providers of electronic communication services must take appropriate technical and organisational measures to ensure the effective protection of retained data against risks of misuse and against any unlawful access to that data. In order to guarantee that, national legislation must, inter alia, make provision for the data to be retained within the European Union.[256]

Only in Germany and Hungary is this requirement fulfilled. The Danish, Finish and Spanish laws does not impose a "data residence" requirement and therefore do not comply with the relevant CJEU standards.

251 Case no. BVerwG - 6 C 12.18. Another corresponding complaint has been filed by another Internet Access Provider (Telekom Deutschland GmbH). It was parallel ruled by the Administrative Court Cologne. The appeal against this decision is pending at the Federal Administrative Court as well.

252 CJEU, Digital Rights Ireland, para. 64.

253 In 2014 Danish Ministry of Justice, to explain the 12-months data retention period, cited preparatory works for the 2002 data retention law. In these, the one-year retention period was justified on grounds that the planning for terrorist attacks such as 9/11 often takes more than six months, so a retention period of one year would be appropriate. See: 'Denmark: data retention is here to stay despite the CJEU ruling', *EDRi, 4 June 2014,* https://edri. org/denmark-data-retention-stay-despite-cjeu-ruling.

254 Report 10/2014 of the Committee on Transport and Communications (LiVM 10/2014 vp).

255 CJEU, Digital Rights Ireland, para. 64

256 CJEU, Tele2, para. 122

d) Access to retained data – the 'serious crime' threshold

As noted, the CJEU requires safeguards concerning both the collection of data and access to that data. As regards the latter, access to the retained data by competent national authorities needs to be clearly defined and limited by appropriate safeguards to minimise the risk of abuse.[257] One of those safeguards is that access to data must be limited to investigations for serious criminal offences. In Tele2, the CJEU ruled that national legislation governing access of the competent national authorities to metadata – where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime – should be in principle precluded.[258] At the same time, as the CJEU ruled in the 2018 Ministero Fiscal case, access to data does not have to be restricted solely to the objective of fighting serious crime, in situations where that access does not constitute a serious interference with fundamental rights. This includes situations when access is limited to obtaining a telephone number and its owner identity such as surname, forename and, if need be, address.[259]

According to current CJEU jurisprudence, then, serious interferences (i.e. when access to retained data, taken as a whole, allows precise conclusions to be drawn concerning the private lives of the persons whose data is concerned) can be justified only by the objective of fighting serious crime. By contrast, when the interference is not serious (i.e. when access to retained data is only requested for the purpose of determining the identity of a subscriber), that access may be justified by the objective of preventing, investigating, detecting and prosecuting criminal offences more generally.[260]

The serious crime threshold is fulfilled only under the German and Finnish laws, and to some extent the Danish law. The Hungarian and Spanish laws allow the competent national authorities to request access to data in connection with preventing or investigating all (or broad) types of crimes set out in national legislation (in neither law is there a specific, exhaustive catalogue of particular crimes that might justify access to retained data). At the same time, these laws allow for access to different types of retained data and do not preclude crossreferencing them, thus allowing precise conclusions to be drawn concerning the private lives of the persons concerned (and resulting therefore in serious interferences with fundamental rights).

In the case of the Danish law, the "serious crime requirement" is met with regards to most kinds of data but does not apply to assigned IP addresses and mobile location data. In the latter case, access to data is permitted in the context of investigations targeting all types of criminal offences (chapter 74 of the Administration of Justice Act). This limitation seems insufficient in light of the CJEU jurisprudence, given that in Ministerio Fiscal the CJEU implied that cross-referencing data concerning the identity of the owner of a SIM card with data pertaining to the communications with that SIM card or its location equates to a serious interference with fundamental rights.[261]

e) Access to retained data - lack of effective oversight mechanism

The necessity for effective, independent oversight of access to retained data by competent national authorities has been emphasised by the CJEU.[262] It has been also stressed by the EU Agency for Fundamental Rights.[263] According to the CJEU, access by competent national law enforcement authorities to retained data:

257 CJEU, Tele2, paras. 118-125

258 CJEU, Tele2, para 125

259 CJEU, Ministerio Fiscal, paras. 59-61,

260 CJEU, Ministerio Fiscal, paras. 55-57,

261 CJEU, Ministerio Fiscal, para. 59

262 CJEU, Digital Rights Ireland, para. 62; Tele2, para. 120

263 Fundamental Rights Agency, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update', Fundamental Rights Agency, November 2017, p.135, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf

> has to be made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued".

Such a prior review should be a general rule, subject to exception only in cases of validly established urgency.[264]

Such an oversight mechanism (in principle, ex-ante judicial review) exists in Denmark, Germany, Finland and Spain, while this condition is not met by the Hungarian legislation. The Hungarian law does not provide for any independent prior authorisation (such as a judicial warrant) to collect the data. Police and the National Tax and Customs Office require the prosecutor's authorisation; the prosecutor and national security agencies may access such data without a court order.

For certain instruments, there are additional oversight mechanisms provided by national regulators for the electronic communications sector (in Denmark) or the competent Data Protection Authority (in Spain).

f) Access to retained data - lack of subsequent notification

The obligation to provide ex-post or subsequent notification to the data subject when it is no longer liable to jeopardise ongoing investigations was emphasised by the CJEU in Tele 2. The obligation is only met by the German and Finnish legislation; it does not exist in Hungary or Spain. In Denmark, the obligation is limited. Under chapter 71 of the Administration of Justice Act, the affected person is only notified of certain types of access. Access to mobile location data and IP addresses, which can be used to construct a complete profile of a person's movements, are not covered by the notification requirement in Danish law. There is no justification for limiting it to cases concerning access to only certain types of data and excluding it with respect to access to other types of data, particularly when the latter also interferes with privacy and data protection rights.[265] In sum, the subsequent notification criteria is not satisfied in three of the five measures in question.

To conclude the necessity and proportionality assessment, since the analysed instruments target indiscriminately a large group of individuals (basically all users of publicly available electronic communications networks whose data is retained) and, at the same time, allow for retention of a wide range of metadata which may reveal a great deal of information about the data subjects' private lives, the interference they cause in the data protection and privacy rights cannot be considered necessary and proportionate. This conclusion applies in particular to those instruments mentioned above which, in addition, do not provide appropriate access safeguards (in particular Spanish and Hungarian laws; in Germany, Finland and in most aspects in Denmark appropriate access safeguards are in place). For these reasons, the analysed laws do not satisfy the last prong of the fundamental rights test.

4.6.4 Interference with other rights

Right to an effective remedy

The ECtHR has ruled that when analysing the right to an effective remedy, it must be assessed whether the law foresees the creation of a domestic remedy allowing the competent national authority both to deal with the substance of the relevant complaint and to grant appropriate relief, although states are afforded some discretion regarding how they conform to these obligations.[266]

264 CJEU, Tele2, para 120

265 CJEU, Ministerio Fiscal, para. 59

266 ECtHR, Rotaru v. Romania, para. 67

The remedy must be effective in practice as well as in law.[267] In the CJEU, the Tele2 judgment held that the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities. That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy.[271] Moreover, in Schrems, the CJEU held that legislation must provide effective oversight and redress mechanisms in the context of processing of personal data. Failing to provide an effective remedy violates Article 47 of the Charter.

A number of the data retention laws analysed here do not contain appropriate guarantees to protect the right to an effective remedy. As explained in the previous section, some instruments (the Hungarian and Spanish laws and to some extent also Danish law) only provide data subjects with limited possibilities for being informed that their metadata has been acquired by the competent authorities. There is no general requirement of a notification to the person whose data has been acquired, even when proceedings have been completed and are no longer at risk of being undermined or jeopardised. Data subjects therefore have very limited possibilities to challenge the application of the measures in question (especially when, as in Hungary, there are no provisions ensuring effective judicial oversight). Only the Finnish and German data retention laws properly secure data subjects' right to access an effective remedy in order to challenge the application of the measures in question.

Right to freedom of expression and information

The instruments analysed have an indirect impact on the right to freedom of expression and information. As noted, blanket data retention regimes may result in data subjects feeling they are under constant surveillance, which can lead those individuals to censor themselves (the so-called "chilling effect"). This negative consequence of data retention regimes has been recognised by the CJEU in both Digital Rights Ireland and Tele2.[268] Furthermore, as previously highlighted, the instruments analysed do not provide for any exceptions regarding professional secrecy. They therefore pose a risk for the protection of journalistic sources of information, which is also crucial in the context of freedom of expression (see Goodwin v. United Kingdom,[269] Big Brother Watch and Others v. UK[270]). The indiscriminate nature of the data retention measures, affecting all persons using electronic communication services with no specific safeguards for journalistic or other professional secrecy requirements raises concerns as to whether they meet the necessity and proportionality criteria when assessed in light of Article 11 CFR.

4.6.5 Conclusion

This overview has summarised the findings of fundamental rights assessments of data retention regimes in five EU Member States: Denmark, Finland, Germany, Hungary, and Spain. It should be noted that, even if these instruments 'only' allow for the retention of and access to metadata, without revealing the content of communications, it does not mean that their measures are necessarily less intrusive. Since it may be possible to obtain a person's entire 'social graph' and other behavioural patterns from such metadata, it can reveal a great deal of information about various aspects of the targeted individuals' private lives. The overview has highlighted a number of problematic provisions in existing legislation, focusing on the rights to privacy and data protection but

267 ECtHR, Wille v. Liechtenstein (application no. 28396/95), para. 75, http://hudoc.echr.coe.int/eng?i=001-58338 271 CJEU, Tele2, para. 121

268 CJEU, Tele2, paras. 92 and 101. Para. 92 reads: "In that regard, it must be emphasised that the obligation imposed on providers of electronic communications services, by national legislation such as that at issue in the main proceedings, to retain traffic data in order, when necessary, to make that data available to the competent national authorities, raises questions relating to compatibility not only with Articles 7 and 8 of the Charter, which are expressly referred to in the questions referred for a preliminary ruling, but also with the freedom of expression guaranteed in Article 11 of the Charter (see, by analogy, in relation to Directive 2006/24, the *Digital Rights judgment, paragraphs 25 and 70)*."

269 ECtHR, Goodwin v. United Kingdom, para. 39

270 ECtHR, Big Brother Watch and Others v. UK, para. 495

also taking into account the rights to an effective remedy and freedom of expression.

Concerning the rights to privacy and data protection, the Hungarian and Spanish laws raise concerns when considering whether the measures are provided for by law, as they lack sufficient quality in terms of their foreseeability. However, even if this criterion of the fundamental rights assessment were satisfied, none of the analysed data retention regimes fully pass the necessity and proportionality test. They all provide for the indiscriminate retention of data, essentially covering all users of publicly available communications networks and services, including those with respect to whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious criminal offences. They allow the undifferentiated storage of metadata and do not provide exceptions for persons whose communications are subject to professional secrecy requirements. In addition, some of the instruments do not meet the 'data residence' requirement (Denmark, Finland, Spain) and do not contain adequate access safeguards. In particular, they do not provide for independent external oversight; ex-post notification to data subjects; and they do not limit access to data on the basis of an exhaustive list of serious criminal offences (this is the case in Hungary, to some extent in Spain and in some aspects also in Denmark).

At the same time, all the legislation in question contains some safeguards for data protection and privacy rights, but the quality of those safeguards varies. Some (for example, in the German and Finnish laws) are well-developed, while others (for example, the Hungarian laws) offer minimal guarantees protecting data subjects' rights against abuse. Regarding the other fundamental rights examined here, only in Finland and Germany do data subjects have the full possibility to access an effective remedy allowing them to question the application of the measures introduced by domestic data retention laws. At the same time, none of the legislation contains appropriate safeguards protecting freedom of expression.

The findings of the assessments carried out in this report demonstrate that while some national legislation has stronger fundamental rights safeguards, none of the analysed data retention regimes fully meet all the standards established in the relevant ECtHR case law, or the more demanding standards set out in CJEU case law, in particular the substantive requirements set out in Digital Rights Ireland and Tele2. There is therefore a need to adjust those national data retention regimes to the European standards.

5. Thematic analysis to identify the main unjustified interference with fundamental rights

5.1 Introduction

The thematic analysis provides an aggregated overview of fundamental rights issues arising from the review of instruments in the areas of police and criminal justice as well as migration and home affairs. The thematic analysis is based on the six group reports that have already reviewed similar instruments in section 5.2. The thematic analysis looks for structural, systemic and/or horizontal issues that affect fundamental rights because of the reoccurrence of the same issue within the same or more groups of instruments.

The thematic analysis can help flag particular issues at an aggregate level; it ties in with the group reports which in turn bundle the reviews of selected individual instruments. As a consequence, the information presented is not as granular as the individual reviews and the group reports which can be consulted for complementary details. Already the group reports have signalled that the instruments from the individual instruments that are grouped together can be very diverse in their objectives and in substance. The same caveat necessarily persists at the level of abstraction that a thematic analysis commands. Last but not least, some of the legal instruments which have been analysed in this report are subject to legislative change which means that the assessment of compliance with fundamental rights has to continue for each legislative change. However, the high level of analysis in the report may actually be an advantage for discovering structural and horizontal issues within existing legal instruments that can inform legislative craftsmanship in the areas of police and criminal justice as well as migration and home affairs.

It is not the objective of this thematic analysis to replace possible issues with fundamental rights that have been identified in the review of individual instruments and the group reports. Rather, the thematic analysis should be seen as complementary. As an illustration, the EU law instruments involving the processing of personal data typically employ one of the following cooperation mechanisms: mutual recognition, mutual assistance or mutual access. With the help of the thematic analysis it would be possible to discern fundamental rights issues that typically follow from a given cooperation mechanism.

The thematic report is structured preserving the logic of a fundamental rights review following European constitutional law that draws from two sources: the European Convention on Human Rights (ECHR) and its application by the European Court of Human Rights (ECtHR) on the one hand, and, on the other hand, the Charter of Fundamental Rights of the European Union (Charter) and its interpretation by the Court of Justice of the European Union (CJEU). It will in the first place present some horizontal observations. Second, it conducts a vertical assessment in relation to each fundamental right touched upon in the group reports.

Starting with the rights to privacy and data protection, the report turns to freedom of expression and to receive information, the right to non-discrimination, the rights of the child, the right to an effective remedy and to a fair trial as well as and the right to seek asylum. The assessment will highlight issues that interfere with fundamental rights in one or several group reports and explain the impact on fundamental rights, suggesting modifications. Each right consists of differ-

ent aspects that might be violated. Only rights for which the analysed instruments may present unjustified interferences with certain aspects of the right are discussed in the report. For each possibly unjustified interference of an aspect of a fundamental right we give examples based on the group reports; however, the examples are not to be considered exhaustive.

5.2 Horizontal observations

To begin with, a few horizontal observations are in order to help set the scene. In EU law, the police and justice area and the migration and home affairs area are characterised by a great variety of self-standing instruments that operate independently of each other with little shared procedural or substantive guarantees. This means that for each legal instrument there are specific provisions to safeguard fundamental rights with a distinct wording. This can have the advantage that the provisions correspond better with a particular instrument but from the perspective of preserving fundamental rights this can contribute to diverging legal standards for similar safeguards in different legal instruments.

EU primary law does as much as furnishing the competences, legal bases and attendant legislative procedures complemented by the Charter's fundamental rights guarantees which are binding since the entry into force of the Lisbon Treaty in 2009. In the view of the authors, negotiating the considerable tension between fundamental rights and the two EU competences, i.e. police and justice and migration and home affairs, is pursuant to Art. 19(1) TEU ultimately left to the jurisprudence of the CJEU. The CJEU in its decision-making will take the Charter's fundamental rights into account and over some time its binding interpretations of EU law will have an effect on the legal instruments of the police and justice area and the migration and home affairs area. If however there is very little shared substance between each legal instrument's provisions to safeguard fundamental rights, the authors take the view that the effect of obtaining a binding precedent from Europe's highest court remains limited to the very instrument under consideration.

Besides, EU institutions and agencies (e.g. Frontex, Europol) have also no shared administrative (procedural) law that could confer a set of horizontally streamlined guarantees on procedural fairness, redress, etc. for individuals and organisations.[271] This does not mean that there are no guarantees at all but that we are relying on a combination of 'general principles of European Union law', [272] often developed by the courts, and instrument-specific guarantees and safeguards. In that sense, Directive 2016/680/EU shows progress in terms of providing for horizontal data protection rules in the field of law enforcement, which however does not generally extend to the instruments in migration and home affairs.[273]

The piecemeal composition of a significant area of EU law comes at the cost of internal policy consistency. The area of freedom, security and justice, for example, is characterised by a great number of self-standing legal instruments which taken together form a in the details diverse and complex system of processing activities involving individuals' personal data.[274] This does not only pose a challenge for the interoperability between legacy databases of the EU and member states as is recognised by EU institutions and Member States.[275] Also in situations in which data is

271 European Parliament resolution of 15 January 2013 with recommendations to the Commission on a Law of Administrative Procedure of the European Union (2012/2024(INL)), Annex, Recommendation 3.

272 See Diana-Urania Galetta, et al. (2015), The General Principles of EU Administrative Procedural Law, In-depth analysis requested by the JURI Committee of the European Parliament (Brussels: European Union), available at: www.europarl.europa.eu/RegData/etudes/IDAN/2015/519224/IPOL_IDA(2015)519224_EN.pdf.

273 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.

274 See for a graphical impression Council of Europe, Overview of the information exchange environment in the justice and home affairs area, 6253/17, Brussels, 15 February 2017, available at: http://data.consilium.europa.eu/ doc/document/ST-6253-2017-INIT/en/pdf

275 *Ibid.*

handed over between EU and Member States' databases and/ or authorities, such a transaction involving individuals' personal data can have repercussions for the consistent approach to the protection of fundamental rights, where the protocol on the legal guarantees, responsibilities and rights for such transactions does not retain high fundamental rights standards. The Commission initiative to improve the interoperability and further development of Union databases should go hand-in-hand with streamlining personal data protection and security capacity. The founding legislation of the Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) which currently manages Eurodac, SIS II and VIS provides an example for addressing also the responsibility for personal data protection and data security.

Considering next multilevel governance in the EU, Member States, either when they are implementing EU law or cooperating in the modes of mutual recognition, mutual assistance or mutual access, act in conformity with their respective domestic criminal and/ or administrative laws. Among Member States procedural and substantive rules and practices necessarily vary which can have an adverse effect for individuals' fundamental rights in the event of a cross-border cooperation between member states. Quite illustrative to that point is the ruling of the CJEU which authorises an EU Member to refrain from giving effect to the European arrest warrant issued by another Member State if there is "a real risk of breach of the fundamental right to a fair trial" in the country issuing the arrest warrant.[276] This is of course only further exasperated in the case of cooperation with third countries. (e.g. as shown by the cases of Schrems and Canada PNR). Another related issue is the limited EU competence in criminal investigations, which results in divergences in the Member States with possible detrimental effects on human rights.

5.2.1 Right to privacy and to the protection of personal data

Much of the thematic analysis will focus on the inherent tensions between the data collection and processing instruments and individuals' right to privacy and data protection. CJEU jurisprudence attaches much value to highly formalized and granular legislative provisions about purposes of the data processing and the safeguards on access and use by competent authorities. This in turn creates a high threshold for the legislative quality, which, however, is important for legal certainty and in light of individuals' fundamental rights. In the following sections seven horizontal issues have been selected which have surfaced from one or several group reports as reoccurring and possibly affecting legislative quality detrimental to the high standards in personal data protection law and jurisprudence.

Legal basis

The Lisbon treaty which entered into force in 2009 introduced the new competence on the protection of personal data in Art. 16 TFEU. Following a recent clarification by the CJEU on the PNR agreement with Canada,[277], there appear to be quite a few instances in which data collection and exchange instruments in EU justice and home affairs were passed with an incomplete legal basis. The PNR agreements with Australia and US, but also third-county agreements in force with Europol and inter-agency agreements like Europol-Eurojust and Europol-OLAF, as well as Europol-Frontex and OLAF's data transfer to Europol should be based on Article 16 TFEU.

Ambiguous definitions and open terms

Ambiguous definitions and open terms have been flagged as a source of legal uncertainty that undermines the purpose limitation and other safeguards on the legitimate access and use of personal data. Following established CJEU jurisprudence in relation to the processing of personal data, EU legislation must be clear and precise with regards to the scope and application of the

276 CJEU, judgment of 25 July 2018, case C-216/18 PPU (*Minister for Justice and Equality v LM*).

277 CJEU, PNR Canada Opinion 1/15, judgment of 26 of July 2017, ECLI:EU:C:2017:592, para. 118.

measures.[278] The overbroad scope of measures, the overbroad definitions or even their absence can be the cause for excessive or simply unjustified data processing. Examples include the unclear definition of "security risk" under ETIAS, the term "purposes other than criminal proceedings" in the ECRIS and ECRIS TCN legislative proposals, the lack of definition of "in connection with the crossing of the external border" in the 2013 Regulation on Eurodac as well as in the 2016 Eurodac proposal. Yet another example is the lack of specification on personal data to be processed in Eurosur or the lack of a definition of "other purposes" for sharing of data collected under CIS with among others, Europol and Eurojust. The SIS II Decision allows further processing of data in cases of "imminent serious threat to public policy and public security" or "preventing a serious criminal offence" without defining the terms. The Europol-Eurojust Agreement gives an overbroad definition for "duly authorized persons" that can have access to the data and in the case of CIS the competent authorities in the member states are not enumerated. Where the scope of a legislation has found to be overly broad the legislation at hand fails to comply with the CJEU's requirement to be clear and precise with regards to the scope. Problematic is the broad scope of the Europol-OLAF data exchange, the Europol-Frontex Agreement and the Frontex Regulation, and in particular the overbroad definition of "cross-border crimes". Europol's and Eurojust's third-state agreements have been flagged for their broad scope that fails to delineate and limit the legitimate purposes of the data exchange.

Law enforcement access to migration and border control databases

Moreover, the context collapse between migration and law enforcement and/or violation of the purpose limitation principle can result in excessive processing of personal data. In the field of data protection law, a collapse of context exists when an individual's personal data is mandatorily collected in one context, such as migration, but this personal data is then further processed for a different and unrelated purpose. Examples include access for member states' and Europol law enforcement to data collected in the context of migration (Eurodac, VIS, EES and ETIAS, EUROSUR, SIS II). Another example is CIS that permits further sharing with national and international/regional organizations without requirements for equivalent data protection standards. Generally, law enforcement access to non-policing databases is not premised on keeping up with high data protection standards. The Prüm decisions reveal the existence of information on an unidentified individual in law enforcement databases, even where there is no legal requirement for further data on that individual to be given to the searching Member State. The EU-US MLAT similarly presents issues with purpose limitation because the agreement itself does not carry clear and precise provisions on the subsequent use of the personal data. Purpose limitation is not observed in the Frontex Regulation, access by Europol and Eurojust to SIS II or by Europol to VIS and in the analysed finance instruments which do not provide information on the competent authorities that can access and use the data, thus again endangering purpose limitation.

Centralized databases' expansion

Centralized databases show a certain proneness for expansion of personal data processing which is not consistently justified as necessary and proportionate. Impact assessments which can aid the assessment of necessity and proportionality are not required in the field of migration and border control instruments and have only recently been introduced by Directive (EU) 2016/680 with regards to data processing systems in the member states but not for passing EU instruments involving the collection of personal data. It must be contented that while they are not mandatory, impact assessments are the only methodology to granularly argue the necessity and proportionality of any new or expanded data processing activity. However, prior impact assessment, where they are conducted at all, do not always have a fine granularity and tend to be uncritical about expanding personal data categories. Examples include EES and ETIAS where there is first no sufficient evidence that visa over-staying presents a major problem that cannot be tackled with less restrictive means for the right to privacy and data protection than storing personal data in a centralized system or second, that visa exempt travellers can present security, public health or irregular migration problems that necessitate storing their personal data in a centralized database. Similar considerations exist for the Eurodac system, which expanded in the types of data

278 CJEU, C – 293/12 and C-594/12, Digital Rights Ireland, para 54 and CJEU, C362/14, Schrems, para 91.

stored and the persons covered, and for the proposal on establishing an ECRIS-TCN system that holds facial images and fingerprints. Certain elements of collection of biometrical data in the field of migration and home affairs are not consistently justified. Examples include the inclusion of biometric data collection in SIS II and VIS without impact assessments to justify the need for that. The collection of ever new categories of data such as alphanumeric and other data (e.g. health data, data on criminal convictions) constitutes another area of excessive data processing: examples include Eurodac and CIS. Another concrete example is the ETIAS proposal that lacks the necessary assessment of proportionality.

Disproportionate data retention periods

Following the group reports disproportionate data retention periods or blanket data retention constitutes another type of excessive data processing. Examples include CIS, EES, the ETIAS proposal, Eurodac and VIS. Indiscriminate data retention both ratione personae and ratione materiae is mandated also by the national data retention laws of all analysed Member States (, Finland, Germany, Hungary, Poland and Spain) whereas no sufficient justification is given for the chosen on national level retention periods in all of the above countries but Germany. Alternatively, the data retention period is also not explicit but re-assessed on a regular basis under the Europol Regulation and inter-agency agreements as well as in all third- state agreements concluded by Europol and Eurojust. Extended data retention results from Europol's access to SIS II and disproportionate data retention periods are also present under all the analysed PNR agreements.

Independent oversight and data localisation

Lacking independent oversight and data security can result in unjustified breach of the rights to data protection and privacy. As was argued in the agencies' group report the rules on supervision are not clear and supervisory mechanisms differ between the EU agencies. The arrangements of Eurosur, in the Europol-Eurojust Agreement and Europol and Eurojust's third-state agreements do not meet the requirement of supervision by an independent authority in Article 8(3) of the Charter. In spite of a clear requirement stipulated in CJEU caselaw the national Danish, Finnish and Spanish data retention laws lack requirements that would ensure that the data are to be retained within the EU in order to ensure review by an independent authority.

Information duties

The non-compliance with the right to be notified of personal data held about an individual can lead to unjustified breaches of the right to privacy and personal data protection. No notification is provided in the context of intra-EU agencies' transfers of data from one database to another and the same is true for the Frontex Regulation and Europol's access to VIS and SIS II. No notification is provided about information gathered on individuals also under the Belgian PNR law. In data retention laws in Hungary, Spain and Poland no notifications, even ex post, is foreseen. There is a strong interrelation between data protection law's information duties and the right to an effective remedy and to a fair trial. .

No information or difficulty in accessing information by individuals on the data collected on them may equally constitute an unjustified violation of the rights to data protection and privacy. There is, for example, no public information available on the authorities with access to the CIS. Likewise, the Frontex Regulation does not include information about data subject rights which are instead inserted in its Implementation Measures. Whether this satisfies EU law or obstructs data subjects' rights has yet to be asserted.

5.2.2 Right to freedom of expression and to receive information

The CJEU has confirmed for metadata retention cases its complementary reading of such measures as interfering with the rights to privacy and data protection as well as with the right to freedom of expression.[279] Thus, remaining national data retention instruments in the EU, namely

279 Tele2 Sverige AB and Watson, para 92f.

the Finnish, German, Polish, Hungarian, Spanish and Danish Data Retention Laws, insofar as they provide for the indiscriminate collection and retention of metadata of an entire population would contradict the CJEU's interpretation of what is necessary and proportionate in the light of fighting serious crime. The lack of protection of journalistic sources in the six analysed national data retention laws is problematic because the CJEU asks for qualified protection of professional secrecy and privileges.

5.2.3 Right to non-discrimination

The right to non-discrimination in Article 21 of the Charter prohibits direct and indirect discrimination. In principle, this requires that comparable situations must not be treated differently and that different situations must not be treated in the same way unless such treatment is objectively justified. Within the scope of EU law also the discrimination on grounds of nationality are prohibited. The proposal for a ECRIS-TCN Regulation has been flagged for its likely breach of the essence of the right to non-discrimination (and EU citizenship in Article 20 TFEU) in relation to dual nationals who hold an EU and a non-EU state's nationality. The group reports identified two instances that risk direct discrimination. Firstly, in the EES Regulation there is a general requirement that member states use the EES in a non-discriminatory manner, but there are no specific provisions setting out how this may be done (for example through a requirement to draft a handbook or guidelines). Secondly, the listing of nationality as one of the search keys for examining visa applications in the VIS may be used for establishing patterns of behaviour or travel routes on the basis of an applicant's country of origin, meaning that visa applicants may be subject to discriminatory decision-making practices.

EU non-discrimination law cannot remedy situations in which EU instruments do not aim to harmonise member states' laws. This can result in that comparable situations are being treated differently between member states. In its ruling Advocaten voor de Wereld, the CJEU sets out that EU instruments, which do not aim to harmonize member states' law, are not liable for differences that occur in the criminal laws of the member states.[280] It follows that EU instruments involving the processing of personal data which underpin cooperation between member states without the competence to harmonise member states laws do not protect against disparate treatment between member states. Nevertheless, the EU legislator can adopt legislation that harmonise the criteria for member states to enter an alert in the SIS II database on third country nationals. Presently, member states insert such alerts following to different criteria, but the database is operated by the EU.

There is an intrinsic link between the fundamental right to non-discrimination and the additional protection vested for special categories of personal data pursuant to Article 10 of Regulation 2016/680/EU. The special categories of personal data in EU data protection law have precisely been introduced because of the possibility to use such data in a manner that can violate EU non-discrimination rules. Authorities should refrain from using as proxies "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."

Several EU instruments that can be used for (group) profiling have been found susceptible to indirect discrimination because it is possible to circumvent existing safeguards in the legislation. Examples include the ETIAS profiling functionality or the inclusion of personal data in VIS of visa sponsors that may result in the over-processing of personal data of third-country nationals.[281] Other concerns about indirect discrimination based on gender, ethnicity or nationality (sensitive data) arose in relation with the implementation of the PNR agreement with the USA.

280 Advocaten voor de Wereld, para 59.

281 See FRA (2018), "Preventing unlawful profiling today and in the future: a guide", available at: https://fra.europa.eu/en/publication/2018/prevent-unlawful-profiling.

5.2.4 Rights of the child

In addition to children being protected by fundamental rights in general, the fundamental rights of a child are especially codified in Article 24 of the Charter. From the instruments reviewed in this report in particular the migration and home affairs instruments affect children, namely the 2016 proposal on amending Eurodac[282] and the 2018 proposals on reforming VIS.[283] Whereas the age for taking fingerprints is currently 12 and 14 years of age respectively, the VIS and Eurodac proposals foresee lowering the minimum age for fingerprinting to six years old. Acknowledging that children need special protection, both proposals put forward additional precautions for collecting children's biometric data. However, the purposes for which children's biometric data can be used are not limited to situations in which this is in the best interests of the child. For example, law enforcement access children's fingerprints in the Eurodac database on the same grounds as apply for adults. With respect to justifying the age at which it may be necessary and proportionate to collect children's fingerprints, the proposal for a ten year retention period in Eurodac is based on a scientific study that was based on a limited sample of data and drew only a limited set of conclusions.

5.2.5 Right to an effective remedy and to a fair trial

The successful exercise of the right to an effective remedy and to a fair trial hinges on access to information: first, that personal data about the individual is held and, second, when an authority has accessed, shared or used an individuals' personal data. Here the thematic analysis sees grave problems with informing individuals about the relevant facts and/or their rights. For SIS II there are no standard information on legal remedies available. In general, EU Justice and Home Affairs instruments must be streamlined to require information on assessing legal aid or assistance. Examples include information on refusal, annulment or revocation of travel authorisation applications (ETIAS) that may be insufficient to lodge an appeal. Another example is that member states can register in SIS II alerts that a return decision has been issued. The burden to ensure that such alert is deleted, however, lies with the individual who has to demonstrate that he or she left the territory of the member state. In order for individuals to exercise their right to delete alerts they need to know about the alert and their right to request deletion in the first place. The same applies to data retention laws in Hungary, Spain, Poland and Denmark that do not require individuals to be informed on personal data held on them and similarly make the exercise of the rights difficult.

In the context of migration and border control the issues for a right to an effective remedy and to a fair trial are aggravated for individuals who belong to vulnerable groups (children and minors), are in a vulnerable position (e.g. asylum seekers), inexperienced or simply not capable of the language in which the information is presented to them.

5.2.6 Right to seek asylum

The borders group report considered the relationship between the Eurosur Regulation and the right to asylum as problematic from the perspective of Article 18 of the EU Charter. Under the Eurosur regulation Member States and Frontex are authorised to gather information for the purpose of "detecting, preventing and combatting illegal immigration" and to be authorised to share such situational awareness with third countries. There is a risk of conflict with the right to asylum of third country nationals. The very essence of the right can be breached were the Eurosur system be used to assist in preventing individuals seeking international protection from reaching EU territory. In the context of the Common European Asylum System, the CJEU ruled that EU law precludes the application of a conclusive presumption that a responsible Member State observes

282 Proposed Articles 10, 13 and 14, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016PC0272&from=EN.

283 Proposed Article 3(2)©, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:0302:FIN.

the fundamental rights of the EU.[284] This means that national authorities and courts in the member states have to take into account whether systemic deficiencies in another member states interfere with an asylum seeker's fundamental rights. In a similar fashion this must apply to third countries' capacity to observe fundamental rights in the event that personal data is exchanged under the Eurosur mechanism.

5.2.7 Prohibition of inhumane or degrading treatment

Forcefully taking fingerprints from asylum seekers as foreseen by border instruments can breach the prohibition of inhumane and degrading treatment provided for in Article 4 of the Charter. The group report recommends that the Commission's best practice guidelines[285] and a reference to the Charter of Fundamental Rights, presently referred to in the recitals, are included in the operative part of Eurodac for example via a binding reference.

284 CJEU, N. S. (C-411/10) v Secretary of State for the Home Department and M. E. and Others (C-493/10) v Refugee Applications Commissioner and Minister for Justice, Equality and Law Reform, ECLI:EU:C:2011:865.

285 European Commission, 'Staff Working Document - Implementation of the Eurodac Regulation as regards the obligation to take fingerprint' COM(2015) 150 final.

6. Compliance with Directive 680/2016

6.1 Presentation of the methodology

This activity required an assessment of the compliance of certain EU instruments with Directive 680/2016 (LED Directive). It should contribute to the Commission's obligation to review Union acts which regulate the processing of personal data by the competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties by 6 May 2019.[286] This review also includes Union acts that entered into force prior to the LED, i.e. on or before 6 May 2016.

6.1.1 Limitations to the scope of assessment

To conduct the compliance check and to find an appropriate methodology, first it was necessary to narrow down the scope of assessment and to adapt it to the scope of the LED.

The LED applies to Union acts which regulate the processing of personal data in the Member States "by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties." It does not cover activities related to national security or processing carried out by EU institutions and agencies. Some of the instruments analysed for this study are therefore excluded from this analysis, such as the instruments of the Agencies group or national laws of the Member States.

On the other hand, some instruments that were not included in the previous fundamental rights assessment were included in this activity (e.g. Council Framework Decision 2008/909/ JHA of 27 November 2008[287]) and several instruments have been added in mutual agreement with the Commission, such as the proposal for a regulation on mutual recognition of freezing and confiscation orders, Council Framework Decision of 13 June 2002 on joint investigation teams and Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences. A compliance check was not carried out for instruments due to be repealed. In total, 32 checks for compliance with the LED were conducted.

286 Article 62 (6), 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, https://eur-lex.europa.eu/eli/dir/2016/680/oj

287 Council Framework Decision 2008/909/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments in criminal matters imposing custodial sentences or measures involving deprivation of liberty for the purpose of their enforcement in the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008F0909

The relevant instruments are as follows:

1. Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on mutual assistance and cooperation between customs administrations Customs Information System (CIS), Decision 2009/917/JHA[288]
2. Entry/Exit System (EES),[289] including Regulation (EU) 2017/2225 of the European Parliament and of the Council of 30 November 2017 amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System[290] (measures on law enforcement access)
3. European Travel Information and Authorisation System (ETIAS)[291] (measures on law enforcement access)
4. Eurodac[292] (measures on law enforcement access)
5. Schengen Information System II (SIS II, Council Decision 2007/533/JHA[293])
6. Visa Information System (VIS, Council Decision 2008/633 JHA[294])
7. Advance Passenger Information (API) Directive[295]
8. Passenger Name Record (PNR) Directive[296]
9. Asset Recovery Offices Decision[297]
10. European Arrest Warrant[298]
11. Exchange of information on road traffic offences[299]

288 Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009D0917

289 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, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R2226

290 Regulation (EU) 2017/2225 of the European Parliament and of the Council of 30 November 2017 amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System, https://eur-lex.europa.eu/legal-content/EN/ TXT/?uri=CELEX%3A32017R2225

291 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, https://eur-lex.europa.eu/ legal-content/EN/TXT/?uri=CELEX:32018R1240

292 Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013R0603

293 Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32007D0533

294 Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, https://eur-lex.europa.eu/ legal-content/EN/TXT/?uri=CELEX%3A32008D0633

295 Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004L0082

296 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, https://eur-lex.europa.eu/eli/dir/2016/681/oj

297 Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32007D0845

298 Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32002F0584

299 Directive 2015/413/EU of the European Parliament and of the Council of 11 March 2015 facilitating the cross-border

12. European Protection Order[300]
13. European Investigation Order[301]
14. Swedish Framework Decision
15. Prüm Decisions (2008/615/JHA[302] and 2008/616/JHA[303])
16. Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with Interpol[304]
17. Council Framework Decision 2008/909/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments in criminal matters imposing custodial sentences or measures involving deprivation of liberty for the purpose of their enforcement in the European Union[305]
18. Council Framework Decision 2008/947/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments and probation decisions with a view to the supervision of probation measures and alternative sanctions[306]
19. Council Framework Decision 2009/829/JHA of 23 October 2009 on the application, between Member States of the European Union, of the principle of mutual recognition to decisions on supervision measures as an alternative to provisional detention[307]
20. Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings[308]
21. EU Mutual Legal Assistance Convention[309] (EU MLAT)
22. EU-USA Mutual Legal Assistance Agreement[310] (EU-USA MLAT)
23. EU-Iceland and Norway mutual legal assistance in criminal matters (EU-Iceland and Norway MLAT)[311]
24. EU-Japan MLAT[312]

---

exchange of information on road safety related traffic offences, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L0413

300 Directive 2011/99/EU of the European Parliament and of the Council of 13 December 2011 on the European protection order, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0099

301 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32014L0041

302 Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008D0615

303 Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, http://eur-lex. europa.eu/legal-content/EN/TXT/?uri=celex:32008D0616

304 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32005E0069

305 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008F0909

306 https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32008F0947

307 https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32009F0829

308 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009F0948

309 Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union, https://eur-lex.europa. eu/legal-content/EN/TXT/?uri=celex:42000A0712(01)

310 Agreement on mutual legal assistance between the European Union and the United States of America, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:22003A0719(02)

311 Agreement between the European Union and the Republic of Iceland and the Kingdom of Norway on the application of certain provisions of the Convention of 29 may 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union and the 2001 Protocol thereto, https://eur-lex.europa.eu/legal-content/ EN/TXT/?uri=CELEX:22004A0129(01)

312 Agreement between the European Union and Japan on mutual legal assistance in criminal matters, https:// eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A22010A0212(01)

25. ECRIS (Council Framework Decision 2009/315/JHA[313] and Council Decision 2009/316/ JHA[314])[315]
26. Council Framework Decision of 13 June 2002 on joint investigation teams[316]
27. Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences[317]
28. Council Framework Decision 2005/214/JHA of 24 February 2005 on the application of the principle of mutual recognition to financial penalties[318]
29. New Regulation on the mutual recognition of freezing and confiscation orders[319]
30. Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence [320]
31. Council Framework Decision 2006/783/JHA of 6 October 2006 on the application of the principle of mutual recognition to confiscation order[321].
32. Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information[322]

6.1.2 Methodological approach

The project team undertook an analysis of the compliance of each instrument with each article of the LED. In order to improve readability, the findings have been presented in a table, which offers an overview of the main compliance questions to be addressed in the Commission's review of Union acts. It does not relate to a fundamental rights assessment. However, the table includes suggested modifications.

Preliminary remarks illustrating the context of each instrument are included, highlighting any direct or indirect references to the application of the LED or its predecessor, Framework Decision 2008/977/JHA. The table subsequently shows:

- the relevant articles of the LED against which the instrument is to be checked, e.g. Article 4(1)

313 Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, https://eur-lex.europa.eu/ legal-content/EN/TXT/?uri=celex:32009F0315

314 Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA, https://eur-lex.europa.eu/eli/dec/2009/316/oj

315 After this assessment was carried out a new Directive emended the ECRIS legal framework.

316 Council Framework Decision of 13 June 2002 on joint investigation teams https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002F0465

317 Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32005D0671

318 Council Framework Decision 2005/214/JHA of 24 February 2005 on the application of the principle of mutual recognition to financial penalties https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32005F0214

319 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the mutual recognition of freezing and confiscation orders, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0819; the Regulation was agreed in November 2018: Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders, https://eur-lex. europa.eu/legal-content/EN/ALL/?uri=celex:32018R1805

320 Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003F0577

321 Council Framework Decision 2006/783/JHA of 6 October 2006 on the application of the principle of mutual recognition to confiscation orders, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32006F0783

322 Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX-%3A32000D0642

(a) (principles relating to processing of personal data, lawfulness and fairness);

- the relevant articles, recitals and annexes of the instrument that correspond to the analysed article of the LED.
- the expert's observations on whether the instrument is compliant, partially compliant or not compliant with the LED, together with explanations; and
- suggested modifications and proposals for amendments to specific articles of the instruments, for example with regard to the wording of the provision in question, proposals for specific additions, modifications, amendments or deletions and, in some cases, proposals for more general modifications.

32 individual compliance checks have been provided. The results of the individual tables were exchanged with the Commission for the provision of information and exchanges of views. This process was completed in December 2018.

A concrete example is the analysis of Article 5 of the LED in relation to Council Decision 2008/633/JHA on access to VIS by Member States' law enforcement authorities and Europol

Directive 2016/680 (the LED)	**Council Decision 2008/633/JHA**	**Remarks**	**Suggested modifications**
Art. 5, Time-limits for storage and review	Not mentioned in Council Decision 2008/633/JHA Article 13 - Keeping of VIS data in national files 1. Data retrieved from the VIS may be kept in national files only when necessary in an individual case in accordance with the purposes set out in this Decision and in accordance with the relevant legal provisions including those concerning data protection and for no longer than necessary in the individual case. Article 16 – Keeping of records 3. These records shall be protected by appropriate measures against unauthorised access and abuse and deleted after a period of one year after the retention period referred to in Article 23(1) of Regulation (EC) No 767/2008 has expired, unless they are required for monitoring procedures referred to in paragraph 2 of this Article which have already begun.	Not (yet) compliant since it does not provide for periodic reviews and permanent erasure of the data.	A sentence could be added to Article 16 (3) that after the monitoring has ended, the data should be permanently deleted. An obligation could be added to Article 13 (1) that the controller should periodically review the necessity for further storage of the data and its permanent deletion when the case for which the data were accessed has been closed. General comment: it could be assumed that the LED is lex generalis to data protection provisions of Council Decision 2008/633, which could in turn be seen as lex specialis. This would lead to the situation that the more specific and detailed data protection provisions of Council Decision 2008/633 are a specification of the more general provisions of the LED and thus in a way implement them for the context of law enforcement access to VIS. However, this should be clarified within Decision 2008/633/JHA. It would be recommendable that it is specified that the LED is applicable to the processing of personal data by the law enforcement authorities pursuant to the VIS Decision and all the provisions of the Directive apply to it (so that the Directive does not need to be copy-pasted into the VIS Decision). In consequence, the data protection provisions in the VIS Decision should be seen only as a specification to the Directive's provisions.

Chart 5: Example of analysis of Article 5 Directive 2016/680 in relation to Council Decision 2008/633/JHA: access to VIS Member States' law enforcement authorities and Europol.

6.1.3 Challenges

Similar challenges arose as in the previous activity of the project. The current state of play of some instruments was difficult to assess as they were or are subject to ongoing legislative proposals. Assessments took into account, where possible, positions adopted by the Parliament and/or the Council. Where this was not possible, it was agreed with the Commission to focus on the initial proposal. This required a constant exchange between experts and the Commission. Some of the identified shortcomings are already in the process of changed and/or remedied.

6.2 Analysis of the issues related to compliance with the LED

The problems identified are primarily related to the age and diverse nature of the instruments. In some instruments there is no reference to the EU data protection framework in this field, as it did not exist prior to the adoption of Framework Decision 977/2008/JHA. There are other instruments that cite that Framework Decision but nevertheless require specific amendments. Other instruments have complex data protection regimes due to their multiple possible uses (e.g. migration and border management databases that are also accessible, under certain conditions, to law enforcement agencies) and the consequent need for differing data protection regimes (i.e. application of both the GDPR and LED)

One general issue in terms of compliance is the sometimes-unclear relationship between an instrument's specific data protection framework (lex specialis) and the rules of the LED (lex generalis). Some instruments require references to and clarifications regarding the applicable framework. The project team recommends a consistent approach to this issue.

Another key issue is the compliance of Member States' implementing laws. Compliance with the LED could be enhanced through specific guidance to assist national authorities, for example in the form of a handbook underlining key points, pertinent CJEU jurisprudence and good practices.

A number of instruments require specific amendments to comply with Articles 4 (1)(b) and (c) of the LED, concerning respectively the requirements that data be collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes; and that it be adequate, relevant and not excessive in relation to the purposes for which it is processed. Requirements for time limits for storage and review (Article 5) and for distinctions to be made between personal data based on facts and on personal data based on subjective assessments (Article 7) are issues raised in relation to a number of instruments.

Furthermore, newer provisions –for instance, the prohibition on profiling that results in discrimination, or the rights of data subject including the information about follow up, are missing in a number of instruments. These should be explicitly included in the instruments, and there is a particular need to ensure verification and oversight of how profiling systems (as provided for in the ETIAS Regulation and the proposal for a new Regulation on the VIS) function in practice.

The table below contains an instrument-by-instrument overview with suggestions for articles that could be modified. "Highlight" refers to specific elements of some instruments. The detailed individual assessments of each instrument are included in the online database and include specific drafting suggestions. The instruments are numbered as in the list in section 1.1.1.

Instrument	Overview
Customs Information System (CIS), Decision 2009/917/JHA	Clear references to LED and GDPR required Suggested modifications: Article 1; Article 5; Article 8; Article 13; Article 21; Article 28; Article 30 Highlight: Joint Supervisory Authority is obsolete and should be replaced according to Article 62
Advance Passenger Information (API) Directive	Clear references to LED and GDPR required Suggested modifications: Article 3; Article 6
Passenger Name Record (PNR) Directive	Reference to Framework Decision 2008/977/ JHA needs to be replaced Clear references to LED and GDPR required Suggested modifications: Article 12; Article 13
Council Decision 2007/845/JHA on cooperation between EU countries' Asset Recovery Offices (AROs) in the field of tracing and identification of proceeds from, or other property related crimes	Clear references to LED required Suggested modifications: Article 3; Article 5
European Arrest Warrant	Clear references to LED required Suggested modifications: Article 8; Article 15; Annex with the certificate form
European Protection Order	Reference to Framework Decision 2008/977/ JHA needs to be replaced Suggested modifications: Article 7 Highlight: complementarity to Regulation 606/2013 needs to be considered
Exchange of information on road traffic offences	Clear references to LED and GDPR required Suggested modifications: Article 7 Highlight: Reference to Decision 2008/615/UE needs to be replaced
European Investigation Order	Clear references to LED and GDPR required Suggested modifications: Article 7; Article 13
Swedish Framework Decision (Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the EU)	Clear references to LED required Suggested modifications: Article 5; Article 6; Article 8; form in Annex A
Prüm Decisions (Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime)	Clear references to LED required Suggested modifications: several articles of both the Decisions need amendments

Council Framework Decision 2008/909/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments in criminal matters imposing custodial sentences or measures involving deprivation of liberty for the purpose of their enforcement in the European Union	Clear references to LED required Suggested modifications: Article 4; Article 23; Annex with the certificate form
Council Framework Decision 2008/947/ JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments and probation decisions with a view to the supervision of probation measures and alternative sanctions	Clear references to LED required Suggested modifications: Annex with the certificate form (as with Framework Decision 909/2008).
Council Framework Decision 2009/948/ JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings	Reference to Framework Decision 2008/977/ JHA needs to be replaced Clear references to LED required Suggested modifications: Article 8; Article 9(2)
ECRIS (Council Framework Decision 2009/315/JHA and Council Decision 2009/316/ JHA)[323]	Clear references to LED and GDPR required Suggested modifications: Article 7; Article 9; Article 11;
Council Framework Decision of 13 June 2002 on joint investigation teams	Clear references to LED required Suggested modifications: Article 1(10)
Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences	Clear references to LED required New articles could be added
Council Framework Decision 2005/214/ JHA of 24 February 2005 on the application of the principle of mutual recognition to financial penalties	Clear references to LED and GDPR required New articles could be added
Framework decision 2003/577/JHA on freezing orders	Clear references to LED required
Framework decision 2006/783/JHA on confiscation orders	Clear references to LED required

Chart 6: overview of the suggested modifications for each instrument. For details see the analysis of the single instruments

323 After this assessment was carried out a new Directive emended the ECRIS legal framework (see footnote no.39)

6.3 Possible options for alignment with the LED

To contribute to the Commission's obligation to review Union acts which regulate the processing of personal data by the competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, this section divides the instruments into five groups, depending on the types of potential amendments. This report also provides a 'cost-benefit' analysis, setting out the advantages and drawbacks of the procedures required to make those amendments.

The five groups consist of:

- instruments without any reference to the EU data protection framework;
- instruments with clear references to Framework Decision 977/2008/JHA that do not require major amendments;
- instruments with multiple data protection regimes that require more substantial amendments
- new or recently-amended instruments which can be considered compliant with the existing data protection framework but could be amended for greater clarification; and
- international and inter-EU agreements, the amendment of which would require international negotiations.

6.3.1 Instruments enacted prior to the negotiation and entry into force of Framework Decision 2008/977/JHA

- Council Framework Decision 2008/909/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments in criminal matters imposing custodial sentences or measures involving deprivation of liberty for the purpose of their enforcement in the European Union
- Council Framework Decision 2008/947/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments and probation decisions with a view to the supervision of probation measures and alternative sanctions
- European arrest warrant
- Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences
- Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence
- Council Framework Decision 2006/783/JHA of 6 October 2006 on the application of the principle of mutual recognition to confiscation order
- Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with Interpol
- Council Framework Decision of 13 June 2002 on joint investigation teams
- Council Decision 2007/845/JHA on cooperation between EU countries' Asset Recovery Offices (AROs) in the field of tracing and identification of proceeds from, or other property related crimes
- Swedish Framework Decision (Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the EU)
- Prüm Decisions (Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime and Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime)

According to Article 60 of the LED, the new data protection regime does not apply to existing, specific provisions in legislation concerning the processing of personal data by national authorities in the context of police and judicial cooperation in criminal matters. There is thus a need to amend these instruments with, at a minimum, an overarching reference to the LED. This appears the least-onerous way to provide sufficient legal clarity. Any such reference should be included in the operative part of the text.

Certain articles of these instruments could also be modified to better bring them into line with the LED. The specific amendments are provided in the individual assessments (available in the online database).

A number of the instruments in this group contain references in their recitals to the Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data. Notwithstanding the fact that the requirements of the LED encompass the provisions of both the 1981 Convention and Council of Europe Recommendation No. R(87) 15 regulating the use of personal data in the police sector, these references could be maintained in order to ensure coherence with the work of the Council of Europe.

Further comment is necessary with regard to the freezing and confiscation instruments. The two Framework Decisions[324] pre-date Framework Decision 977/2008/JHA and so do not include any specific data protection regime. These require the introduction of an overarching reference to the LED, taking into account that they still apply between Member States that are not bound by the new Directive, but also between Member States that are not bound by the new Directive and Member States that are.

6.3.2 Instruments with a reference to Framework Decision 2008/977/JHA that do not require major amendments

- Directive 2011/99/EU of the European Parliament and the Council of 13 December 2011 on the European Protection Order
- Council Framework Decision 2009/829/JHA of 23 October 2009 on the application, between Member States of the European Union, of the principle of mutual recognition to decisions on supervision measures as an alternative to provisional detention
- Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings

Under Article 59(2) of the LED, references to Framework Decision 2008/977/JHA in existing EU legislation are to be construed as reference to the LED (which repeals that Framework Decision). Given that these instruments contain such a reference, whether in the recitals or the operative part of the text, the least onerous solution for the EC is to consider this reference sufficient to oblige national authorities to comply with the LED.

6.3.3 Instruments with multiple data protection regimes that require more substantial amendments-

- Customs Information System (CIS) decision 2009/917/JHA
- Council Framework Decision 2005/214/JHA of 24 February 2005 on the application of the principle of mutual recognition to financial penalties
- EU PNR Directive
- API Directive
- European Investigation Order
- ECRIS (Council decisions 2009/315 and 2009/316)
- Exchange of information on road traffic offences

324 Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003F0577; Council Framework Decision 2006/783/JHA of 6 October 2006 on the application of the principle of mutual recognition to confiscation orders, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32006F0783

This group includes both instruments which do contain a reference to Framework Decision 2008/977/JHA (CIS Decision, EU PNR, EIO, ECRIS[325]) and instruments which dates back prior to the FD (Council FD on financial penalties, API Directive). All these instruments require an overarching reference to Directive 680/2016 and also specific references to the application of the Regulation 679/2018 (GDPR). The compliance with GDPR was out of the scope of this analysis, however it worth mentioning that there is a need to clarify the different area of application of LED and GDPR.

6.3.4 Instruments that are new, recently-amended or subject to ongoing legislative negotiations

- Entry/Exit System (EES), including Regulation (EU) 2017/2225 of the European Parliament and of the Council of 30 November 2017 amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System (only the law enforcement access)
- European Travel Information and Authorisation System (ETIAS) (only the law enforcement access aspects)
- Eurodac (only the law enforcement access aspects)
- Schengen Information System II (SIS II) (police and judicial cooperation aspects)
- Visa Information System (VIS) decision 2008/633 JHA (only the law enforcement access)
- New Regulation on mutual recognition of freezing and confiscation orders

The ETIAS Regulation,[326] the most recent of the border instruments, does contain a clear reference to the applicability of the LED (Article 49(2) and (3)). However, the assessment carried out for this phase of the project highlights issues with the applicability of the LED safeguards with regard the data processing activities provided for in ETIAS regulation, in particular the watch list.

Articles 49 and 58 of EES Regulation clearly affirm the applicability of LED.

The current Eurodac Regulation, which was approved in 2013, contains a reference to Framework Decision 977/2008/JHA and thus now refers to the LED (with regard to the provisions concerning law enforcement access). The recast proposal currently being negotiated does not contain an exhaustive data protection regime but, given that the new text is expected to give law enforcement agencies broader access to more categories of personal data, a clearly-defined, instrument-specific data protection framework is essential. Equally, the rules governing law enforcement access to the VIS will be substantially changed by the 2018 proposal.[327]

The three new Regulations establishing the SIS[328] clarify that both the GDPR and LED are applicable. The proposed Regulations on border checks and police and judicial cooperation in criminal matters clarify that both the GDPR and LED apply (Articles 46(2) and 64(2). They specify that the LED is applicable when the processing is carried out by the competent authorities for law enforcement purposes. The Regulation on returns provides in Article 13 that the applicable data protection regime is that set out in the Regulation on border checks. Recital 17 acknowledges that the national authorities processing data for return purposes may differ and could also include law enforcement and judicial authorities, especially if a return decision is the result of a criminal sanction, in which case the LED would apply.

325 After this assessment was carried out, ECRIS has been amended by the Directive which amends the Framework Decision 2009/315 and replaces the ECRIS Decision 2009/316. References to both, LED and GDPR have been included now and other modifications addressing data protection have been introduced to the text (e.g. Recital 12 of the Directive, new Art.11(4), new Art.11a(1) of the FD).

326 The assessment has been carried out on the draft compromise package of 25 April 2018.

327 Proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA, COM (2018) 302, 16 May 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1558346217835&uri=CELEX:52018PC0302

328 The assessment has been carried out on the compromise text of 14 June 2018.

One broader issue concerns the fact that the relationship between the specific data protection rules provided in the instruments and the general rules of the LED is not always clear. A handbook addressed to national law enforcement that clarifies the applicable provisions in each relevant instrument could be provided, in order to prevent differing interpretations of the lex generalis -lex specialis relationship.

Finally, the new Regulation on mutual recognition of freezing and confiscation orders was under negotiation during this phase of the project. The proposal did not include any reference to the LED or the preceding Framework Decision, nor to any other data protection standards, although the applicability of the LED to the activities conducted pursuant to the new Regulation is beyond doubt (freezing and confiscation orders are "measures imposed by a court following proceedings in relation to a criminal offence", according to Article 2 of the Regulation).

Article 1 of the Regulation includes a generic reference to fundamental rights, but this cannot be deemed sufficient to cover the provisions of the LED. At the same time, Article 23 stipulates that the law governing the execution of freezing and confiscation orders is the law of the executing state. It could be argued that this necessarily includes the national measures implementing the LED. From this perspective, it is could be sustained that an express reference to the applicability of the LED would be superfluous, thus avoiding the need to return a recently-agreed instrument to the legislative procedure.

6.3.5 International agreements

- Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on mutual assistance and cooperation between customs administrations
- EU MLAT 2000 Convention
- EU-USA MLAT[329]
- EU-Iceland and Norway MLAT
- EU-Japan MLAT

This group includes international agreements that require amendments through international negotiations.

329 The Umbrella Agreement supplements, where necessary, data protection safeguards, but it was not part of the assessment carried out in the previous phase of the project.

6.4 Assessment of the options

This section provides a brief 'cost-benefit' analysis of options available for reforming or amending the relevant instruments. The analysis is offered group-by-group, with the exception of groups four (new or recently-amended instruments that can be considered compliant with the existing data protection framework but could be amended for greater clarification) and five (international and interstate agreements, the amendment of which would require international negotiations).

It should also be considered the possibility that the European Commission does not reform or amend any instrument. It is well known that the actions to claim the responsibilities of EU institutions are difficult to activate due to their complexity and vagueness. However, it seems useful to underline the possible scenarios.

The first possible scenario is the activation of the action for failure to act (art. 265 TFEU) that is the remedy in case an EU institution does not properly fulfil its obligations under the EU legislation. The second scenario is the action for damages (art. 340 TFEU), which requires to prove certain, specific and quantifiable damage.

6.4.1 Instruments without any reference to the EU data protection framework

These twelve instruments are all former Third Pillar instruments that require a clear reference to the LED. Specific amendments to some articles are also necessary in order to ensure compliance with the LED (e.g. Article 4 of FD 2008/909; Articles 7, 8 and 15 of FD 2002/584). The first option is to introduce an overarching reference to LED and neglect any more specific amendments. The second option is to include an overarching reference and make specific amendments. The third option is to approve a recast version of the instruments to bring them clearly into line with the post-Lisbon and post-data protection reform legal regime.

Instruments without any reference to the EU data protection framework		
Option	*Costs*	*Benefits*
1. Reference to the LED in the text of the instrument	High cost for the EC because of the need to go through the legislative procedure MS would have to assess the changes introduced by the LED and modify the transposed legal acts accordingly	Clarity on the legal basis for Member States' law enforcement authorities (LEAs)
2. Reference to the LED in the instrument of specific of specific articles, maintaining the same legal basis	High cost for the EC because of the need to go through the legislative procedure Low cost for MS because horizontal legal rules will apply	Clarity on the legal basis for the text of MS LEAs and on the specific and modifications provisions that need to be applied
3. Recast legislation	High cost for EC because a legislative procedure needs to be open Reduced cost for MS	High legal clarity High benefits for MS LEAs cause the recast version will clarify the legal basis and applicable specific provisions.

Options 2 or 3 are the more preferable Option 1 will have a high degree of uncertainty and the cost of going through the legislative procedure will be the same.

6.4.2 Instruments with clear references to Framework Decision 2008/977/JHA that do not require major amendments

The three instruments in this group[330] contain a reference to Framework Decision 2008/977/ JHA, and thus to the LED, in the recitals. The first option is therefore to do nothing. However, due to the importance of the new legal framework for data protection, an alternative approach would be to replace the reference to Framework Decision 2008/977/JHA with a specific reference to the LED. The reference could be inserted in the operative part of the text rather than just the recitals. This scenario is more demanding, but provides more legal clarity.

A third option would be to issue a communication to the Member States that clarifies the changes introduced by the LED and outlines the key features of the LED in relation to the three instruments.

Instruments with clear references to Framework Decision 977/2008/JHA that do not require major amendments		
Option	*Costs*	*Benefits*
1. Do nothing	High cost for the EC because of the need to go through the legislative procedure MS would have to assess the changes introduced by the LED and modify the transposed legal acts accordingly	No specific benefit for MS
2. Insert a specific reference to the LED in the operative part of the text	High cost for the EC because of the need to go through the legislative procedure MS would have to assess the changes introduced by the LED and modify the transposed legal acts accordingly	Clarity on the legal basis for MS
3. Issue a communication to MS providing clarification	Medium cost for the EC – the drafting of a communication is a more feasible and MS to amend transposed less resource-consuming that legislation legislative amendments	More legal clarity Likely little or no need for

Option 3 seems to offer the best balance between costs and benefits.

330 Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009F0948 Directive 2011/99/EU of the European Parliament and of the Council of 13 December 2011 on the European protection order, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0099 Council Framework Decision 2009/829/JHA of 23 October 2009 on the application, between Member States of the European Union, of the principle of mutual recognition to decisions on supervision measures as an alternative to provisional detention, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32009F0829

6.4.3 Instruments with multiple data protection regimes that require more sub-stantial amendments

This group includes both instruments which do contain a reference to Framework Decision 2008/977/JHA[331] and instruments that predate that Framework Decision.[332] All these instruments require an overarching reference to the LED as well as specific references to the application of the GDPR. The compliance with GDPR was out of the scope of this analysis, however it worth mentioning that there is a need to clarify the different area of application of LED and GDPR.

Instruments with multiple data protection regimes that require more substantial amendments		
Option	*Costs*	*Benefits*
1. Replace references to previous data protection regimes	High cost for the EC because of the need to go through the GDPR/LED in the text of instruments Medium cost for MS because horizontal legal rules will apply	Clarity on the legal basis for MS reference to legislative procedure
2. Replace references to previous data protection regimes with references to GDPR/LED and amend specific articles, maintaining the same legal basis	High cost for the EC because of the need to go through the legislative procedure Low cost for MS because horizontal legal rules will apply	Clarity on the legal basis for MS and on the specific provisions that need to be applied in the text of instruments and tailor-made rules will be specified
3. Recast legislation	High cost for the EC because of the need to go through the legislative procedure Reduced cost for MS LEAs	High legal clarity High benefits for MS LEAs because the recast version will clarify the legal basis and the applicable specific provisions

Option 2 or 3 is preferable. Option 1 will have a high degree of uncertainty and the cost of opening a full legislative procedure will be the same.

331 Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009D0917

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, https://eur-lex.europa.eu/eli/dir/2016/681/o

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32014L0041

Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, https://eur-lex.europa.eu/legal-content/ EN/TXT/?uri=celex:32009F0315; Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/ JHA, https://eur-lex.europa.eu/eli/dec/2009/316/oj

332 Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004L0082

7. Elements to be considered in a possible adjustment of data protection instruments

This section concludes the fundamental rights review of existing EU legislation, instruments or agreements with third parties that involve the processing of personal data in the Area of Freedom, Security and Justice (AFSJ). The variety and diversity of issues highlighted in this report make clear that fundamental rights safeguards need to be more consistently considered and applied in the AFSJ. The transposition of the LED, the GDPR and the Regulation on data protection in EU institutions and agencies are important steps in that direction but require improved management and enforcement capabilities at both EU and Member State level to deliver on their promise.

Where the Union establishes instruments that require the processing of personal data it must maintain and build upon the high standards set by the new EU data protection framework. This section draws on observations made in the fundamental rights assessments and the thematic analysis to highlight five broad issues for further consideration: ambiguous definitions and open terms; law enforcement access to migration databases; the expansion of centralised databases; data retention periods; and information rights and duties. These conclusions are intended to complement, rather than distract from, the many issues identified in relation to individual instruments and groups of instruments.

The extensive array of data processing instruments and measures in the AFSJ have evolved largely independently of one another, which explains their diversity of design and treatment of personal data. Emphasis should now lie on the establishment of robust horizontal protections and safeguards for fundamental rights and corresponding data protection inspection and enforcement capabilities that can meet the requirements stemming from EU law and fundamental rights standards.

7.1 Ambiguous definitions and open terms

The instruments analysed as part of this project have highlighted a number of instances of undefined, poorly-defined or ambiguous terminology.[333] Potential remedies to this problem are more-or-less straightforward depending on the terminology in question. For example, the broad definition of "cross-border crime" in the Europol-Frontex Agreement and the Frontex Regulation can be addressed through the specification of which crimes are relevant; the broad definition of "duly authorised persons" in the Europol-Eurojust Agreement should be narrowed; while the "other purposes" for which Customs Information System data can be shared should be specified.

This issue becomes more complicated with the employment of terms such as "security risk", "security", "public security", "national security", "threats" and "public order", for example as used in the ETIAS Regulation, the Prüm Decisions and the SIS II legislation.[334] Precisely what "security" is and

333 For example: the term "security risk" in the ETIAS Regulation; "maintaining public security", "maintaining public order and security", "mass gatherings and similar major events, disasters and serious accidents" in the Prüm Decisions; "imminent serious threat to public policy and public security" and "preventing a serious criminal offence" in the SIS II Decision (now replaced by Regulation (EU) 2018/1862, which features similar wording).

334 The analysis undertaken for this project primarily examined the SIS II Decision, has now been replaced by Regulation (EU) 2018/1862. However, the same problem persists, with the extensive use of undefined terms such as "public order",

how it should be defined is rather a thorny issue. The same may be said for "public order". Current attempts to offer definitions are rather lacking in substance – for example, the ETIAS Regulation defines "security risk" as "the risk of a threat to public policy, internal security or international relations for any of the Member States," which offers very little clarity.[335]

Some of the instruments in question do contain limits, but these tend to be procedural rather than substantive in nature (for example in the SIS II legislation[336]). Elsewhere, alternative approaches have been adopted – for example, the guidelines on the 'Swedish Framework Decision' seeks to offer guidance "to help in determining what circumstances may be deemed as 'urgent', but [the guidance] is not to be regarded as definitive."[337] A similar approach could be considered in relation to terms that remain vaguely-defined or undefined in existing legislation. Such an approach also has obvious procedural advantages in that it does not require going through the legislative process – although any resulting guidance may of course not provide the necessary guarantees. It may also be more appropriate given that each Member State retains a significant margin of interpretation with regard to issues of security and public order.

Thus, while it is beyond the scope of this project to try to offer definitions, in the future consideration should be given to finding ways to introduce some limits or boundaries as to how the terms in question may be interpreted and understood.[338] Doing so will ensure that basic requirements of legal certainty and legal quality can be met. This will help to ensure compliance with the requirement for EU law infringing upon privacy and data protection rights to include "clear and precise rules governing the scope and application of the measure in question," and to include "objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use."[339]

7.1.1 Recommendations

- Using either definitions or guidance, key legal terms in Union law must be clarified in order to understand, assess and satisfy the purpose limitation principle and the necessity and proportionality of interferences with the fundamental rights to the protection of privacy and personal data. This is as much the case for preparatory work (e.g. impact assessments and evaluations) as it is for legislation itself.
- A certain measure of clarification can be achieved in the course of the Commission's review of Union legal acts predating Directive 680/2016 (LED). Whenever possible Union law "in the field of judicial cooperation in criminal matters and police cooperation, which regulate processing between Member States and the access of designated authorities of Member States to information systems" (Article 60 of the LED) should be amended to "ensure a consistent approach to the protection of personal data" (Article 63). Union law should always require Member States to explain how key terms of a Union instrument are used in practice in Member States' criminal (procedural) laws.

"public security" and "national security".

335 Article 6, ETIAS Regulation

336 "…any processing of information in SIS for purposes other than those for which it was entered into SIS has to be linked with a specific case and justified by the need to prevent an imminent and serious threat to public policy and to public security, on serious grounds of national security or for the purposes of preventing a serious crime. Prior authorisation from the issuing Member State shall be obtained for this purpose." Article 56(5), Regulation 2018/1862. This mirrors Article 46(5) of the now-repealed Decision 2007/533/JHA.

337 Guidelines on the implementation of Council Framework Decision 2006/960/JHA, 9512/10, 26 May 2010, p.7, available at: https://data.consilium.europa.eu/doc/document/ST-9512-2010-INIT/en/pdf. The manual replacing these guidelines unfortunately does not include this guidance on urgency. See Manual on Law Enforcement Information Exchange, 6261/17, 4 July 2017, available at: https://data.consilium.europa.eu/doc/document/ST-6261-2017-INIT/en/pdf.

338 See, Council of Bars & Law Societies of Europe, 'CCBE Recommendations on the protection of fundamental rights in the context of 'national security'', April 2019, pp.17-18, https://www.ccbe.eu/news/news-details/article/ccbe-makes-recommendations-on-the-protection-of-fundamental-rights-in-the-context-of-national-securi/

339 Digital Rights Ireland, paras 54 and 60.

- Member States, where they implement EU law, are under an obligation to carry out data protection impact assessments pursuant to the LED. An impact assessment involves "at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Directive" (Article 27(2)). Generic definitions or guidance on how key legal terms of EU legal instruments should be interpreted and applied are imperative for this process.

7.2 Law enforcement access to migration databases

The growing trend in recent years to provide access for Member States' law enforcement agencies, under certain conditions, to personal data primarily gathered for other purposes (in particular migration management or asylum policy) should, in the authors' view, be reconsidered, taking into account the concerns that have been expressed in this project and by many other experts over the years regarding the necessity and proportionality of such access.[340]

According to the authors of this report, a context collapse between migration and law enforcement purposes raises issues that are not limited to the protection of privacy and personal data but can affect other fundamental rights of EU citizens and third-country nationals, such as the right to a judicial remedy and a fair trial, non-discrimination, and the right to asylum, among others

Evaluations that will be undertaken in the coming years of the VIS (2020), Eurodac (2022), EES (2024) and ETIAS (2024) provide an opportunity to conduct in-depth, meaningful assessments of how access to the systems has affected the work of law enforcement authorities, the impact of that access on potential indirect discrimination against the categories of persons whose data is held in the systems, and how law enforcement access relates to the purpose limitation principle. Assuming that the necessity and proportionality of law enforcement access is demonstrated, safeguards building upon those already in place can then be further refined as required.

Consideration should be given to uniform, high thresholds for law enforcement access to data gathered for other purposes. While the EES and ETIAS require "evidence or reasonable grounds" for law enforcement access to the systems in cases of terrorism and serious crime, in the case of the VIS and Eurodac there must be reasonable grounds to believe that such access "will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question." The offences for which access may be granted differ between the instruments – references to different provisions of the Terrorism Directive are used and qualifications concerning the sentencing length for relevant offences under national law are not necessarily included. In the specific case of Eurodac, while the legislative proposals refer to law enforcement access to children's data only being permitted in the best interests of the child, the text permits access on the same grounds as apply for adults.

Finally, the procedures for granting access to law enforcement authorities should be closely evaluated. All four systems are based on the same process – the nomination of a central access point for verifying requests for access to data by law enforcement authorities. These central access points can be part of the same organisation as the authority seeking access and, while the legislation requires that they act fully independently, it must be assessed in the future whether, in practice, this meets the requirements of EU law and CJEU jurisprudence for "prior review carried out by a court or by an independent administrative body".[341]

340 See *infra* 4.2.3

341 Digital Rights Ireland, para 62.

7.2.1 Recommendations

- Forthcoming evaluations of the EES, ETIAS, Eurodac and the VIS must be taken as a genuine opportunity to consider all aspects of law enforcement access to personal data gathered primarily for the purposes of migration policy, taking into account the substantive and procedural aspects of that access, including whether the designated central access points meet independence and impartiality requirements, and key related issues such as non-discrimination and the purpose limitation principle.
- Law enforcement access to non-policing databases (Eurodac, VIS, EES and ETIAS) should be provided on a uniform procedural basis that applies equally high standards to all relevant instruments.
- Union law should only provide law enforcement authorities access to non-law enforcement data when a sufficient evidence base relevant to the issue is available, and such access has been fully considered in light of its necessity, proportionality and appropriateness.
- Where the Union operates and manages migration databases there is a responsibility to collect and publish detailed statistical data about law enforcement's access requests to migration databases and facilitate the independent supervision of the legality of law enforcement access to non-policing databases, through both the carrying out of evaluations and the provision of sufficient resources to the responsible data protection authorities.

7.3 Expansion of centralised databases (categories of personal data/new purposes)

There should be no further expansion of EU databases or information systems – whether with regard to their purposes or the categories of personal data which they are used to process – without sufficient justification based on robust evidence, detailed and meaningful consultation and debate, and granular impact assessment that considers all potential policy options. It is a requirement of EU law that the processing of personal data be demonstrably necessary and proportionate and the EU's centralised databases and information systems must meet these requirements if they are to be considered legitimate.

No impact assessments were provided with the proposals to revamp Eurodac to open it to law enforcement access (2013) and to include non-EU nationals irregularly present in EU territory in the database (2016); to introduce the ETIAS (2016); or to expand the Schengen Information System (2016). While there has been a clear attempt to demonstrate necessity and proportionality of introducing a centralised database for the EES, the authors of this report consider that it has not been sufficiently justified. The proposal to introduce a centralised database for the ECRIS-TCN system was also according to the authors of the report not based on a clear assessment of the potential policy options, and the proposal to include biometric data in that centralised database was not subject to any fundamental rights assessment. Likewise, no impact assessment accompanied the Terrorism Directive,[342] which is crucial in this context as the crimes set out in that Directive serve as the basis for law enforcement access to numerous EU databases and information systems. Furthermore, while the 2016 proposals for Eurodac and the 2018 proposals for the VIS seek to significantly expand the scale and scope of the databases, no separate impact assessment was conducted concerning law enforcement authorities' ability to access this expanded pool of data.

It is deeply unfortunate that, at the same time as the EU institutions were completing new data protection rules which have introduced a requirement to undertake data protection impact assessments in cases where processing "is likely to result in a high risk to the rights and freedoms of

342 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.

natural persons,"[343] the Commission proposed a number of new centralised databases and information systems (as well as a framework for making them interoperable) and in a number of cases did not undertake any such assessment, despite them posing precisely such a risk. While this was not at the time a legal requirement, it would certainly have demonstrated good will to comply with the requirements of the new data protection rules being negotiated and implemented. Indeed, as far back as 2010 the Commission committed itself to assess all new initiatives'"expected impact on individual rights and set out why such an impact is necessary and why the proposed solution is proportionate."[344] It has not fully delivered on that commitment. Improving the quality of Commission-led impact assessments could be facilitated by using a template or structure that requires the collection of each personal data to be justified and every instance of data processing to be assessed separately for its compatibility with the principles of data protection laws.

The expanding collection of and purposes for which data is used has also facilitated novel methods of data processing. Profiling forms an integral part of the ETIAS, is set to be introduced as part of the VIS and is also fundamental to the functioning of the EU-wide PNR system. The limited research and evidence available on the effects of the profiling, in particular the discriminatory effects it may have even when 'only' non-sensitive categories of data are fed into profiling systems, suggests it should be employed with great caution, if at all. The ETIAS Regulation contains an obligation to carry out an evaluation of the "screening rules used for the purpose of risk assessment". There is a need to ensure that the same is required from the evaluations of the VIS and the PNR Directive.

7.3.1 Recommendations

- The Commission should strengthen its capacity to conduct meaningfully granular impact assessments that take into account all relevant fundamental rights issues, and no further centralised databases or large-scale information systems should be developed or extended without such an impact assessment.
- The Commission should continue to allow for sufficient consultation with Union bodies such as the European Data Protection Supervisor, the Fundamental Rights Agency, for public deliberation and seek independent advice in order to ascertain the necessity and proportionality of each and every intended measure.
- It must be ensured that the reviews foreseen in legislation establishing EU databases and information systems that make use of profiling functions include in-depth investigation and evaluation of the procedural and substantive aspects of those functions; the view of the authors of this report is that no further profiling functions should be included in EU-level systems until those reviews have taken place and confirmed the compatibility of the practice with fundamental rights standards.
- Inject a fundamental rights and non-discrimination clause in the governing instrument of each Union centralised database analogous to Article 14 of the ETIAS regulation declaring that: "Processing of personal data within the ETIAS Information System by any user shall not result in discrimination against third-country nationals on the grounds of sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation. It shall fully respect human dignity and integrity and fundamental rights, including the right to respect for one's private life and to the protection of personal data. Particular attention shall be paid to children, the elderly and persons with a disability. The best interests of the child shall be a primary consideration."

343 Article 35 GDPR, Article 27 LED, Article 39 of the Regulation on data protection in Union institutions, bodies, offices and agencies.

344 European Commission, 'EU information management instruments', 20 July 2010, available at : http://europa.eu/rapid/press-release_MEMO-10-349_en.htm.

7.4 Questionable data retention periods

The study has identified certain instances in EU legislation in which the retention periods for personal data are not defined or are considered excessive by the authors of this report.[345] There are several underlying causes which apply in different cases: the law does not define an upper boundary of the retention period defined; extensions of the maximum retention periods may be repeatedly applied (e.g. in the case of Europol and data transferred under the inter-agency agreements); the law fails to differentiate retention periods for different categories of data and individual.

7.4.1 Recommendations

- The Commission should strengthen its capacity to assess data retention periods in a granular and differentiated manner taking into account the necessity of the personal data to achieve the purposes pursued and the fundamental rights of the individuals concerned.
- Union legislation in the AFSJ that provides for the processing of personal data but does not establish a maximum retention period should be amended.
- Sharing of and access to personal data between Member States' competent authorities in the AFSJ should not leave personal data in a legal limbo as to which legal framework applies and which retention periods should prevail to the personal data. Union legislation has to provide for unambiguous rules for ascertaining retention periods in situation when personal data is accessed and used by various EU agencies and national competent authorities.
- The proposed 10-year retention period for children's fingerprints in the recast Eurodac proposal is deemed disproportionate by the authors of this report given that the study serving as justification for the measure made clear that a fingerprint set "does not allow for seamless conclusions from birth to adulthood."

7.5 Information duties

Data protection law governing EU institutions, bodies and Member States sets out a series of information duties for competent authorities, with certain derogations to the presumption in favour of disclosing information (e.g. in the case of ongoing criminal inquiries). The study maintains that there is a strong interrelation between data protection law's information duties and the right to an effective remedy and to a fair trial. The effective implementation of measures on information rights and duties is thus imperative for safeguarding a number of fundamental rights.

Data collection instruments in the AFSJ should conform with information duties using multiple channels, languages and age-appropriate materials to inform individuals about the collection of their personal data, the purposes and retention periods, data subjects' rights, etc. A 'standardised' set of information rights and duties has, over time, been established with regard to EU databases and information systems and is also laid down in the EU data protection legal framework. However, there are certain instruments in which information duties and rights are lacking or insufficient – for example in the Frontex Regulation (there are no specific references regarding the need to inform data subjects of the processing of their data), or Europol's access to VIS and SIS II (no requirement to inform data subjects that their data has been transferred to Europol).

7.5.1 Recommendations

1. The obligation to conform with information duties needs clear recognition in all Union instruments providing for the processing of personal data, and standard rights and duties should be complemented by more specific provisions, where appropriate.
2. In order to effectively monitor EU bodies and Member States' competent authorities' compliance with information duties more closely, it must be ensured that EU and national data protection authorities are provided with sufficient resources to carry out their tasks effectively.

345 This issue was also raised in relation to national data retention legislation.

ANNEX I

The Steering Committee

Barbara De Micheli (project manager) is Senior Project Manager at the FGB. Since 2014, she has been Project Manager monitoring research services on Fundamental Rights implementation in Italy for FRA NET of the EU Fundamental Right Agency Framework Contract. Since 1998, she has been Project Manager in several EU funded projects at local, national and international level (EU programmes: EASI, Progress, Horizon, Leonardo da Vinci, Adapt, Now, V, VI and VII Framework Programme, EQUAL). She has more than 15 years of experience as project manager for national and EU projects, including research projects dealing with social issues, gender equality, discrimination, and access to employment, social and labour policies. Since December 2016, she has been working as Project manager in the EUfunded project "Fundamental Rights Review of EU Data Collection instruments and Programmes – study for DG JUST (CALL FOR TENDERS JUST/2015/RPPI/PR/RIGH/0218", on the issue of data protection in EU legislation and related borders' control instruments. Since 2012, she is the Coordinator of the Master in "Gender Equality and Diversity Management"(www. mastergedm.it). She has been in the coordination team of GenisLab, GenPort and TARGET projects funded by DG Research. She is a PhD student at Fondazione "Marco Biagi" (Modena University).

Franziska Boehm (scientific coordinator and group leader) is Professor Franziska Boehm is law professor at the Karlsruhe Institute of Technology and the Leibniz Institute for Information Infrastructure where she leads a research group on questions of data protection, IT and IP law. She is involved in several EU and German national projects in the fields of data protection and IT-law and provides advisory services to different eu institutions as well as the German parliament.

Fernando Galindo is Chair of Philosophy of Law of the University of Zaragoza, teaching "Philosophy of Law", "Ethics and the Law", "Computers and Law", "Ethics and Legislation for engineering" and "Electronic Government". He is responsible of the research Group on Data Protection and Electronic Signature. He is also adviser of the public key certification services SISCER y FESTE and several telecommunications and software firms. Among other things, he was the organizer of the 1995 Workshop on "Cryptography, privacy and informative selfdetermination", School of Engineering and Faculty of Law, University of Zaragoza.

Silvia Sansonetti is a sociologist with a PhD in statistics and over 10 years of experience in coordinating EU networks of experts. Actually, in the role of senior expert, she is in charge of coordinating and reviewing all the research reports FGB is delivering in the Framework of the FRANET for Italy. In addition to being part of the scientific board of Fondazione G. Brodolini, Silvia is an internal staff of FGB and thus acted as a full-time link with the management team for this research project.

Marta Capesciotti holds a Phd in Law and Economics at the "Sapienza" University of Rome and in Constitutional Law at the University of Granada, with a research on social rights of migrants living in Italy and Spain. She cooperates sin 2015 with FGB and is the fieldwork researcher and legal expert supporting FGB staff in the FRANET research activity on fundamental rights, protection of crime victims, migration policies and rights of persons with disabilities mainly.

The Experts Group

Bilyana Petkova is Assistant Professor of International and European Law at the Faculty of Law of the Maastricht University (UM). She is affiliated as a Visiting Scholar at the Yale Information Society Project since 2014. Before joining UM, Bilyana was a Max Weber postdoctoral fellow at the European University Institute in Florence, Italy and at New York University where she was a part of the Jean Monnet Center and later, the NYU Information Law Institute. Her research interests are in comparative constitutional law, judicial legitimacy, federalism and human rights, with a recent focus on data-driven cities, US-EU privacy law and freedom of speech in a digital age. Her paper "The Safeguards of Privacy Federalism" won a Young Scholars Award at the Eight Privacy Law Scholars Conference in the University of Berkeley, California. Among others, her book chapters have appeared with Oxford and Cambridge University Press, and articles – in the Lewis & Clark Law Review, the Northwestern Journal of Technology and Intellectual Property, the Common Market Law Review, the International Journal of Constitutional Law (I-CON) and the Maastricht Journal of European and Comparative Law.

Chris Jones (group leader) is a researcher and journalist working with the civil liberties organisation Statewatch and as a freelance. His work focuses on migration, policing, surveillance, privacy and data protection, in particular in relation to EU justice and home affairs law and policy. As an author and co-author, he has been published by numerous organisations, online and print outlets, as well as academic publisher Routledge. He holds a degree in history and a master's degree in human rights, both from the University of the West of England.

Diego Naranjo (group leader) is a qualified lawyer and co-founder of the Andalusian human rights organisation (Grupo 17 de Marzo). During the last six years, Diego has been specialising on human rights law. He owns a Master's degree in human rights from the European Inter-University Centre for Human Rights and Democratisation in Venice. Diego joined the association "European Digital Rights" (EDRi) in October 2014 where he currently works as Senior Policy Advisor. In the past, Diego gained experience in the International Criminal Tribunal for former Yugoslavia, the EU Fundamental Rights Agency (FRA) and the Free Software Foundation Europe. Previously to all that he worked as a lawyer in Spain. He is part of the expert group on digital rights of the Spanish Ministry of Energy, Tourism and Digital Agenda. Diego is co-author of the Council of Europe's Study DGI(2014)31 "Human Rights Violations Online", prepared by EDRi for the Council of Europe on 4 December 2014.

Dorota Glowacka (group leader) is a lawyer at the Helsinki Foundation for Human Rights and coordinator of the "Observatory of Media Freedom in Poland", a legal programme run by the Helsinki Foundation for Human Rights. Dorota is an expert on data protection, privacy, media and Internet laws. She is experienced in strategic litigation (both before national courts and the ECtHR), advocacy and running educational activities in these areas. Between 2010 and 2011 she also worked for Panoptykon Foundation in Poland, a non-governmental watchdog organisation focused on protecting human rights in the context of fast-changing technologies and growing surveillance. She was a coordinator of the working group on data protection and privacy rights in the project "HELP in the 28" run by the Council of Europe. She is also a national legal expert in the research network run by the EU Agency for Fundamental Rights (FRANET). Currently she a coordinator of the research project "Protecting journalistic sources in the age of digital surveillance" focused on identifying legal standards and examining practical experience of journalists with regard to surveillance in Poland, Bulgaria and Romania, funded by the OSCE. Dorota is also a PhD candidate at the Law Faculty of the University of Lodz, Poland, alumni of the Summer Doctoral Programme at the Oxford Internet Institute, University of Oxford and of the summer school "Online Free Expression and Communication Policy Advocacy: A Toolkit for Media Development" at the Central European University in Budapest. Her PhD thesis is about managing online media archives in the context of the right to be forgotten on the Internet.

Estelle Masse (group leader) is Senior Policy Analyst and Global Data Protection Lead at Access Now. Her work focuses on data protection, privacy, surveillance and telecoms policies. In particular, Estelle leads the work of the organisation on data protection in the EU and around the world. She is a member of the Multistakeholder Expert Group of the European Commission to support the application of the General Data Protection Regulation (GDPR).

Fanny Hidvegi (group leader) is Access Now's European Policy Manager based in Brussels. She develops Access Now's European policy strategy and manages the EU office. Fanny got appointed to the European Commission's expert group on artificial intelligence and she is on the board of the Hungarian Civil Liberties Union (HCLU). Previously, Fanny was International Privacy Fellow at the Electronic Privacy Information Center in Washington, D.C. For three years Fanny led the Freedom of Information and Data Protection Program of the HCLU where she engaged in strategic litigation. She gained experience on how to operate as an advocate in a restrictive environment.

Joanna Kulesza is an assistant professor of international law at the Faculty of Law and Administration, University of Lodz. She currently serves as an expert for the Council of Europe on human rights online (Ukraine 2015, Moldova 2016) and for the Sino-European Cybersecurity Dialogue. Kulesza is the author of over 50 peer-reviewed papers and five monographs on international and Internet law, including "Cybersecurity and Human Rights in the Age of Cyberveillance" (together with R. Balleste, Rowman and Littlefield 2015) and "Due Diligence in International Law" (BRILL 2016). Her research focus is on the intersection of human rights and cybersecurity. She has been a visiting lecturer with the Oxford Internet Institute, Norwegian Research Center for Computers and Law, Westfälische Wilhelms Universität Münster and Justus-Liebig-Universität Gießen. She was a post-doctoral researcher at the University of Cambridge and Ludwig Maximilians University Munich, her research was funded by the Robert Bosch Stiftung, Polish Ministry of Foreign Affairs and the Foundation for Polish Science. She worked for the European Parliament and the Polish Ministry of Foreign Affairs. She currently is the Membership Committee Chair of the Global Internet Governance Academic Network (GigaNet). She is a member of Internet Society, Diplo Internet Governance Community and the ICANN Non-Commercial Stakeholder Group (NCSG). Polish reviewer for the World Intermediary Liability Map (WILMap) project done by the Center for Internet and Society at Sanford University, Faculty of Law. She serves as a reviewer for i.e. the Utrecht Journal of International and European Law, SCRIPTed – A Journal of Law, Technology & Society, Internet Policy Review and on the academic board of the Communication and Media Research Center.

Kristina Irion is a Senior Researcher at the Institute for Information Law (IViR) at the University of Amsterdam. She is Associate Professor (on research leave) at the School of Public Policy at Central European University in Budapest. Her research covers law, regulation and public policy in the information-driven society, in particular privacy and data protection. Kristina is a recognized academic and expert in her field, she has published widely and is frequently invited to give talks at international conferences and seminars. Kristina was key personnel of four collaborative European research projects on privacy, independent media regulatory bodies, and building functioning media institutions. As a Marie Curie Fellow, she accomplished her individual research project on Governing Digital Information. She provided expertise to the European Commission, the European Parliament, ENISA, the Council of Europe, and the OECD, among others.

Stefano Montaldo holds a PhD in EU law at the University of Milan Bicocca. He is Assistant Professor of EU law at the University of Turin and affiliated research fellow at VUB. Author of a monograph (2015 - I limiti della cooperazione in materia penale nell'Unione europea) and various articles concerning judicial cooperation in criminal matters in the EU, EU institutional law and fundamental rights protection in the EU, published in national and European reviews. Principal investigator within the framework of a project funded by the University of Turin (2017-2019), and of two JCOO research projects co-funded by the European Union, Justice Programme 2014-2020.

Tony Bunyan is an investigative journalist and writer. He specialises in justice and home affairs, civil liberties, the state and freedom of information in the EU. He has been the Director of Statewatch since 1990 and edits Statewatch News online. Tony is the author of "The history and practice of the Political Police in Britain" (1977) which became a seminal text. "Secrecy and openness in the EU" (1999) and "The Shape of Things to Come" (2009) and edited "The War on Freedom and Democracy" (2005). He has edited six more publications for Statewatch. In 2001 (for access to EU documents) and in 2004 (for work on the war on terrorism and civil liberties) the "European Voice" newspaper selected him as one of the "EV50" - one of the fifty most influential people in the European Union. On behalf of Statewatch he has submitted thirteen successful complaints to the

European Ombudsman against the Council of the European Union and the European Commission on public access to EU documents. In November 2011 he was given a Liberty Human Rights Award. He is a Visiting Research Fellow at London Metropolitan University and the University of Bristol.

Valeria Ferraris is Assistant Professor of sociology of Law at the Law Department of the University of Turin. In 2008 she earned her doctorate in Criminology at the Catholic university in Milan. In 2010 she was visiting professor at the University of Hong Kong teaching Law and Society and Social Theory and Criminology at the Master of Social Science in Criminology. Her main research topic are related to immigration control and corruption prevention. She has published a monograph on immigration and crime and several articles and book chapters in English and Italian on her research interests. She is part of the board of the Italian journal Studi sulla questione criminale.

Walter van Holst is a legal practitioner with an analytical approach and a strong focus on the organisational context of legal issues and their solutions. His education in Business Administration and his extensive experience in both large corporations and the public sector, enable him to translate the legal context into practical, fit-for-purpose solutions with an eye on their consequences in the IT landscape of organisations. He is employed by Mitopics, a Dutch consultancy firm specialised in the intersection of ICT, legal and organisational questions.