The influence of EU agencies and supervisory bodies in shaping the legislative framework on interoperability between EU large-scale IT systems.

Universiteit Leiden

Thesis submitted in partial fulfilment of the requirements for the degree of MSc in Public Administration in the International and European Governance track

in the Faculty of Governance and Global Affairs

Leiden University

March 2021

Student: Sophie Reisinger

Supervisor: Dr. Sarah Giest

2nd Reader: Dr. Alex Ingrams

Table of Contents

Table of Tables

Abstract

EU agencies and comparable institutional advisory bodies have proliferated and gained increasing prominence within the politics of the European Union in recent decades, leading scholars to assert that these bodies influence the decision-making procedures in the EU through their information provision. This thesis aims to uncover whether and how the EU agencies, Europol, Frontex, eu-LISA and the Fundamental Rights Agency (FRA), as well as the European Data Protection Supervisor exerted influence on the policymaking process on establishing a framework for interoperability between the EU's large-scale information systems. Its theoretical foundation is derived from interest group influence research and empirically it synthesises evidence from qualitative document analysis and elite interviews conducted with officials from Europol, eu-LISA, and the European Data Protection Supervisor (EDPS). The results suggest that eu-LISA was highly successful in shaping the technical architecture of the interoperability framework, while Europol and Frontex were able to influence the content of the interoperability policies in the agenda-setting stage through their role as end users of the IT systems to be made interoperable. Concerning those advisory bodies with a rights-based mandate, the FRA appears to have achieved its policy goals of adapting technical details of the interoperability to improve their fundamental rights compliance, while the EDPS was largely unsuccessful in exerting directional influence on the underlying political foundation of the policies.

1. Introduction

In 2017, the European Commission launched two new legislative proposals aiming to create an interoperability framework (IF) between EU databases for third-country nationals (TCN) firstly in the area of borders and visas and secondly in the area of police and judicial cooperation, asylum and migration. These regulations can be viewed as the latest component in the European 'smart border' architecture. After amendments to the proposals in June 2018, both legislative proposals came into force in June 2019 (EPRS, 2019). Interoperability means that EU information systems, which contain vast amounts of biometric data of TCN, should be able to "talk to each other" (EPRS, 2019:2). Such interoperability contains four components: The European Search Portal (ESP), a Biometric Matching Service (BMS), a Multiple Identity Detector (MID) and a Common Identity Repository (CIR). Taken together, these interoperability components streamline law enforcement access to these databases since access rights to *one* of the databases allow law enforcement agents to check whether any records of their person of interest exist in *any* of the databases within the IF. This has led to concern of observers that interoperability will allow law enforcement *de facto* routine access to all the diverse databases contained in the respective interoperability framework (Vavoula, 2020:175). In Bigo and Jeandesboz' (2009) assessment of the Stockholm Programme, which outlines the Commission's ambition to further the EU Information Management Strategy, they argue that the Commission's proposals for the use of technology in EU security policies are largely based on the input and viewpoints of security professionals. They also point out that there is no clear specification on how the principles of proportionality and purposefulness would be respected when the interoperability of IT systems, which was already envisioned in the 2009 Stockholm Programme, is implemented (Bigo and Jeandesboz, 2009:1, 2). To this end, the authors recommended that the European Agency of Fundamental Rights (FRA), the European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB, then still the Article 29 Working Party) should be involved in the development of any new policies on information processing and exchange systems in the field of border security (Bigo and Jeandesboz, 2009:5). These assertions by academics studying the potential interoperability of EU information systems, namely that the idea of interoperability is largely driven by security actors and that any legislative process on interoperability should closely involve EU advisory bodies with a rights-based mandate, prompted the questions guiding this research. As the recent policymaking process on interoperability involved EU agencies both with security-oriented as well as those with rights-based mandates, the question is raised whether the involvement of

these agencies shaped the policy outcome at all and if it did, whether these agencies with different mandates were able to influence the policy to differing degrees. In particular, the EU agencies and supervisory authority of interest for this thesis are the European Union Agency for Law Enforcement Cooperation (Europol), the European Border and Coast Guard Agency (Frontex), the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), the European Union Agency for Fundamental Rights ('Fundamental Rights Agency', FRA) and the European Data Protection Supervisor (EDPS). The former four bodies are EU agencies, while the EDPS is a supervisory and consultative authority. In this thesis, for the sake of brevity, they may all collectively be referred as 'EU advisory bodies' since it is the advisory role of these bodies that is under investigation in this thesis.

The research question guiding this thesis is concerned with investigating *whether and how EU agencies and the supervisory authority involved in the legislative process of the interoperability proposal were able to influence the legislative process and shape the policy outcome through their specialised expertise and their policy recommendations*. In other words, the research question is geared towards illuminating the role these EU agencies and bodies played in the interoperability policymaking process and how their involvement in the process may have led to a different overall policy outcome than if they had not been involved in it. It also seeks to compare the potentially varying success these actors had in shaping the policy process and outcome and find out whether they (attempted to) shape the policymaking process in different ways and through different strategies. This thesis will answer the research question by tracing the participation of those advisory bodies in the interoperability policymaking process, analysing the issue framing employed by these bodies and the extent to which their framings of interoperability are congruent with those of European decision-makers, and by triangulating the perceptions of the influence exerted by those bodies through interviews with actors involved in the policymaking process.

1.1. Societal and Academic Relevance

The legislative proposal towards establishing EU database interoperability has been chosen as a case study for this research over other legislative processes in the field that established or amended individual EU databases, such as the policymaking process for the revised Eurodac regulation. This decision was motivated by the decisive nature that leading academics and data protection authorities in the field of technological border management attached to the interoperability legislation, making it appear as a critical juncture in the development of EU

policies on ‘smart borders’. Indeed, the decision to make the EU’s large-scale IT systems interoperable has been described as “the ‘cherry on top’ of a multi-layered cake of databases [through which] the landscape of information processing through centralised databases will be forever changed” (Vavoula, 2019a) and as marking a “point of no return” by the EDPS (2018:10). Therefore, a significant academic relevance has been identified for studying this legislation due to the far-reaching societal implications that have been ascribed to making the EU’s large-scale IT systems interoperable. The potential societal implications identified by researchers and data protection authorities range from discriminatory, criminalising and stigmatising effects on TCN through streamlined law enforcement access to EU border and migration management databases to being a step towards generalised surveillance and a reconceptualization of the EU’s databases from administrative management instruments to intelligence tools (see for instance Bigo et al., 2020:13, 22; Brouwer, 2020:84-86; Carrera, 2020; Vavoula, 2019a, 2019b:264-265, 2020:175-176).

Thus, the substantive interest in studying the impact of EU agencies and other EU advisory bodies on the policymaking process on EU database interoperability is motivated in large part by the assertion of their importance by one of the leading scholars in the study of borders and border technologies in the field of security, Didier Bigo. Bigo is one of the founders and leading scholars of the ‘Paris School’ of securitisation studies, or the PARIS (Political Anthropological Research for International Sociology) approach as he prefers it to be called (Bigo and McCluskey, 2018). This approach focuses on practices of securitisation, i.e. how certain bureaucratic and technological practices can construct a referent object as a security threat and justify particular ways of governing. Crucially, a main research focus of this approach is on actors involved in border control and how they define the meaning of security as well as how they relate to and aim to develop border technologies, they consider necessary for their objectives (Bigo, 2014:210; Bigo and McCluskey, 2018:121-122). Against this backdrop, Bigo et al. (2020:10) have asserted that the recently established EU agency for large-scale IT systems, eu-LISA, has been “one of the driving forces on the smart border initiative”. They argue that this demonstrates a “political strategy by eu-LISA” (Bigo et al., 2020:18) that seeks to define interoperability as a technological necessity in policy discussions about interoperability (Bigo et al., 2020:16-18). Similarly, Galli (2019:14-15) argues that there has been an increasing ‘agencification’ within the area of freedom, security and justice (AFSJ), whereby the powers and discretion of the involved EU agencies have increased. She posits that this led to EU agencies increasingly steering policies in the AFSJ both through implementation

practices as well as through providing research and scientific advice in the legislative process (Galli, 2019:14). Particularly, Europol and Frontex have increasingly become pro-active in the 'knowledge production' for security responses, in the development of methods and instruments for policing information and intelligence, and in lobbying to enhance their competences in border management, particularly via database interoperability (Galli, 2019:15). These assertions by security scholars motivate studying the actual role and influence of such technical and security-focused EU agencies in the interoperability policy process. However, one should not neglect that another EU agency, the FRA, and one EU supervisory authority, the EDPS, were also involved in the policy elaboration process on database interoperability and voiced critical opinions on the proposal in the process (Bigo et al., 2020:22-23; Galli, 2019:3). The involvement of the FRA and EDPS in the development of further EU systems of information processing and exchange was a central recommendation in Bigo and Jeandesboz' (2009:2, 5) policy brief on the Commission's Stockholm programme, which already called for interoperable databases. For the interoperability proposals, the Commission did consult the FRA and EDPS, which each drafted opinions and statements on these proposals. However, simply the existence of these opinions does not guarantee that their recommendations were taken into account in the final policy. The purpose of this research project is therefore to illuminate whether and how the expert advice of EU advisory bodies influenced the legislative process of the interoperability proposals and their final outcome. Additionally, it is also of substantive interest whether there was a significant difference in the degree of influence EU agencies and advisory bodies with a rights-based mandate (FRA, EDPS) were able to exert on the policy outcome compared to EU agencies with a security and/or technical and operational mandate (Europol, Frontex, eu-LISA).

1.2. Thesis Outline

This thesis will answer the research question regarding the influence EU advisory bodies were able to exert on the interoperability policymaking process by first introducing the theoretical concept of influence and how it can be definitionally delineated from the related concept of power. The 'literature review' chapter then moves on to reviewing the literature on the influence exertion of interest organisations, particularly on the conditions under which policy actors with no formal decision-making powers (from hereon called 'non-decision-making actors') can shape policymaking processes. The final section of the literature review is concerned with outlining how non-decision-making actors may be able to exert policy influence through framing a policy issue according to their preferences and having this framing

adopted by decision-makers. In the subsequent 'methods' chapter, the research design of within-case analysis and the methodology of process-tracing that guide this research are introduced and justified. This chapter also outlines how the empirical data to answer the research question was collected through a qualitative document analysis of policy contributions from the EU advisory bodies under investigation, of reports of panel conferences on interoperability, and of legislative texts and discussions by the Commission and the Parliament. Additionally, it outlines how this document analysis was supplemented with semi-structured elite interviews with officials from the EU agencies and the supervisory authority involved in the policymaking process in order to gain insight into the activities of their organisations in the interoperability policymaking process and their influence perceptions. This section is followed by a 'case description' chapter that introduces the history of large-scale IT systems in the EU and how the idea of interoperability between those systems came into being. It also describes the technical components of interoperability, the involvement of the EU advisory bodies in as well as the stages of this legislative process. Finally, this chapter also outlines the main criticisms levelled at interoperability from a data protection and fundamental rights perspective. Subsequently, the 'empirical results' chapter first presents the access channels and frequency of interaction with decision-making bodies by the EU agencies and supervisory authority investigated. It then identifies the framings used by EU advisory bodies when discussing interoperability and the extent to which those framings were taken up by the European decision-making institutions. In the final section of the results chapter, the perceptions of the influence exerted by EU advisory bodies, both self-perception and how other actors involved in the policymaking process perceived them, as well as documentary evidence of their influence exertion are synthesised and examined. Finally, in the 'analysis' section, these empirical results are connected with the theoretical expectations derived in the theoretical framework established in the literature review.

2. Literature Review

In order to investigate the influence that EU agencies and the supervisory authority exerted on the interoperability policymaking process, it first needs to be established what influence is and what the act of exerting influence as a non-decision-making policy actor entails. Therefore, the first section of this literature review is concerned with reviewing different definitional approaches to the concept of influence as well as reviewing the literature on influence in political decision-making. Crucial to this theoretical undertaking is also to properly delineate the concept of influence from the related concept of power and to establish that even actors without formal powers are capable of exerting influence. This leads over into the next section of the literature review, which focuses specifically on the conditions under which actors without such formal political decision-making powers can exert influence on the political decision-making in legislative process. The majority of literature on the influence of non-decision-making actors is focused on interest groups as the units of analysis. However, it is argued that the insights derived from this literature can be applied more broadly to other non-decision-making actors involved in legislative processes, such as the EU agencies and the advisory authority analysed in this thesis. Within this section, the conditions of access, informational activities and types of influence exerted are identified as being relevant conditions for non-decision-making actors to be able to exert influence. Finally, the framing of a policy issue in a certain way that highlights particular aspects of an issue and excludes others, is identified as a powerful instrument through which non-decision-making actors can influence a policy process and its outcome. In order to identify relevant frames in my analysis, the last section of the literature review outlines potential framings of emerging technologies, such as the interoperability technology, based on insights from the academic fields of Critical Security Studies and Science, Technology and Society studies. All of these theoretical insights are subsequently consolidated in the last section of the literature review to outline the theoretical expectations identified previously.

2.1. Conceptualisation of Influence

Central to the study of influence on political decision-making is the lack of a generally agreed definition of the term influence, which oftentimes leads to the situation that a clear conceptualisation of influence is avoided in empirical studies (Dür, 2008a:1220; Michalowitz, 2007:133; Betsill and Corell, 2001:72). In order to devise a clear definition of influence, one has to delimitate the concept from the related concept of power, which is often used

interchangeably with influence and is similarly difficult to define (Arts and Verschuren, 1999:413; Betsill and Corell, 2001:72; Kim, 2018:31).

2.1.1. Relation between Influence and Power

To distinguish between power and influence, it is important to ask about the attainment, intentionality and awareness of actors having power or influence. Concerning attainment, Kim (2018:33, 35) argues that contrary to power, which is given to actors through their social position and formal rules, influence is attained rather than conferred to actors. Thus, while power generally has a formal character of competences and capabilities that provide actors with the ability to impose binding constraints on others, actors with influence do not necessarily derive this influence from formal capabilities (Kim, 2018:35). Therefore, influence can be exerted even by actors who do not possess any formal decision-making powers, which is crucial to this research. Secondly, the intentionality of using power/influence is an important point of distinction. While power can be transformed into influence, having power does not necessarily mean that this power will be exercised (Arts and Verschuren, 1999:413). In contrast, we can only speak of an actor *having* influence if they are *exercising* influence. In this sense, power can be a passive attribute describing the general ability of an actor to wield influence, while influence is necessarily an active attribute that refers to the realisation of wielding influence (Arts and Verschuren, 1999:413; Kim, 2018:35). Similarly, Cox and Jacobson (1973 in Betsill and Corell, 2001:73) distinguish between the concepts by arguing that power is a *capability*, i.e. something that is possessed but not necessarily exercised, while influence refers to a certain type of relationship between actors. Finally, according to Zimmerling (2005:90 in Kim, 2018:34), an actor being aware of possessing power is conceptually necessary in the sense that choosing to exercise power is an intentional, purposeful exercise. However, influence is not necessarily intentional on the part of the actor that exerts influence. Someone's actions can influence other actors without them meaning to exercise influence at all (Kim, 2018:35).

Taking all these conceptual differences into account, some generalisations of the relationship between power and influence emerge. Firstly, having power (in the form of formal capabilities) is not a necessary condition for exerting influence. Actors can be influential without possessing any traditional forms of power (Betsill and Corell, 2001:73). Secondly, actors that have power can use those capabilities to attain influence and may more easily become influential than actors without power. However, it is not given that actors convert their power into influence, and they may not do so (Arts and Verschuren, 1999:414; Betsill and Corell, 2001:73). Given these conditions, Kim (2018:38-39) posits that power, or rather the exercise of power, can be

viewed as a special case of influence in the sense that power is conceptualised as a sub-category of the more general concept of influence. From this view, the ability of actors with power to exert influence with the threat of sanction is the crucial difference between the general concept of influence and the special case of power. Thus, power is a type of influence that can rely on the threat of sanctions. Alternatively, following Max Weber's definition of power, Michalowitz (2007:134) characterises influence as a weaker form of power. However, her reasoning for this is very similar to Kim's (2018:39) reasoning for classifying power as a special case of influence. Essentially, Michalowitz (2007:134) also makes the distinction that power gives actors the ability to *impose* their own preferences on others even against their will, while actors with influence can only *persuade* other actors to act according to their interests. Therefore, in her view, actors without power only have weaker tools to shape the actions of other actors, leading her to conceptualise influence as a weaker form of power. However, arguably, Kim's and Michalowitz' conceptualisation of influence and powers can be reconciled by conceptualising the *exercise* of power as a stronger special case of influence with the caveat that the passive possession of power is a distinct concept from influence.

2.1.2. Different Definitional Approaches

Once one has distinguished the concept of influence from the concept of power, the definition of influence can be expanded on. To reiterate, there are several differing approaches to defining what influence means in the academic literature on the concept. Firstly, there are differing views on whether influence is exerted on an object, e.g. a policy outcome, or on a subject, i.e. another actor (Arts and Verschuren, 1999:413). According to the former approach, an actor can be said to have asserted influence if their policy positions are reflected in the policy outcome (Dür, 2008b:566; Klüver, 2009:536). In order to operationalise the degree of 'preference attainment' or 'goal attainment' of an interest organisation, their influence on a decision, not on decision-makers, is measured (Arts and Verschuren, 1999:413; Dür, 2008b:566-569). As Klüver (2011:490) puts it: "[the preference attainment approach] therefore measures lobbying success understood as the convergence of policy outcomes with the policy preferences of an actor rather than interest group influence directly". Therefore, the preference attainment approach is, strictly speaking, a measure of goal achievement/lobbying success rather than actual influence and can thus be understood as a proxy measure of influence (Arts and Verschuren, 1999:413; Klüver, 2011:490). In contrast, Michalowitz (2007:133-134) argues in favour of a procedural, subject-oriented view on influence since a final policy outcome that signals a shift from a decision-maker's initial standpoint does not necessarily mean that this

change can be attributed to external actors that were trying to influence the decision. Such changed preferences of decision-makers could instead be due to certain political developments, political strategies, or institutional pressures that decision-makers face (Michalowitz, 2007:134). Therefore, focusing only on end results makes it nearly impossible to ascertain the actual channels of influence as well as who or what was the driving force for modified policy outcomes (Dür, 2008b:568). In other words, an actor achieving their policy goals does not necessarily coincide with them having exerted influence (Arts and Verschuren, 1999:413). Consequently, Michalowitz (2007:134) adopts a definition of influence as "mind change", meaning that influence is exercised when an actor is being persuaded to take certain actions that they did not initially want to take. Another important point to note, is that modification of decision-makers' behaviours, thoughts and actions need not necessarily be due to concrete interventions in decision-making procedures. Instead, the sheer existence and policy positions of certain actors, if decision-makers are aware of these, can influence decision-makers since they may anticipate the preferences of such actors and incorporate them into their decisions (Arts and Verschuren, 1999:412-413).

Secondly, while many studies implicitly or explicitly assume that the exercise of influence is necessarily tied to the modification of either the behaviour of other actors or the outcome of a policy decision (Arts and Verschuren, 1999:412; Michalowitz, 2007:134), some studies have doubted that influence is determined by "changed minds and policy outcomes" (Chalmers, 2011:475). Instead, many of those actors attempting to influence the policymaking process are trying to exert influence on decision-makers who already share similar interests to the influence-taker. In terms of interest groups, Chalmers (2011:474) asserts that there is overwhelming evidence that "interest groups tend to lobby friends rather than foes". In this conception, therefore, influence is conceived of in terms of information asymmetry between interest groups and decision-makers. Well-informed organisations possessing specialised expertise can influence the policymaking process by providing informational resources to those decision-making actors that represent their interests. According to this view, information processing capabilities are the currency of influence (Chalmers, 2011:474).

Thirdly, approaches to studying political influence differ in the significance they assign to perceptions of influence. Perceptions of influence can be captured by the reputation an actor has among peers and other participants in the policymaking process regarding their importance in such a process (Ingold and Leifeld, 2014:2). Ingold and Leifeld (2014:2) argue that a reputation for being influential is "an antecedent condition for factual political influence and

success". Importantly, perceptions of the influence of actors can have a bi-directional effect (Kim, 2018:53, 57). On the one hand, Ingold and Leifeld (2014:2) argue that the reputation of an actor of being influential can considerably increase the likelihood that they can exert actual influence on decision-making processes. In this sense, influence reputation is an explanatory factor for an actor exerting actual influence (Kim, 2018:57). On the other hand, influence perceptions can go into the other direction as well, namely that actors can gain a reputation for being influential by exerting actual influence in policymaking processes. When actors can influence the policymaking process through providing high-quality advice and exemplifying good performance, then this is also likely to be reflected in their reputation (Kim, 2018:53). In this sense, influence reputation is not an explanatory factor but a proxy for actual influence (Kim, 2018:53, 57).

Altogether, for the purpose of this study, policy influence can be defined as the ability of an actor to modify the contents of legislative proposals through their communicative interaction with other actors, most importantly decision-making actors, in the policymaking process. Such communicative interaction need not necessarily change the minds of decision-makers, it can also simply provide a set of policy alternatives from which decision-makers can choose from (Kim, 2018:41). The transmission of information can be expected to be the most central communicative instrument used by actors without decision-making powers to try to influence decision-makers and shape the policymaking process (Corell and Betsill, 2008:23).

2.2. Conditions for exerting influence

A large part of the literature on influence of non-decision-makers in policymaking is concerned with the analysis of interest group influence. In recent years, more and more scholars have also started examining the influence of interest group in the special context of EU policymaking. There is, however, a relative lack of literature on other non-decision-making political entities, especially intra-EU entities such as EU agencies, that may exert influence on EU policymaking processes. However, influence studies focusing on organisations that fulfil similar functions in the EU policymaking process as EU agencies, such as interest groups, can provide important theoretical insights and structure this research on how influence is exerted in EU legislative processes (Kim, 2018:49). Kim (2018:49-50) asserts that in EU policymaking processes, the roles of interest groups and institutionalised EU advisory bodies, such as EU agencies, are similar in the sense that they both provide specialised expertise and advice to EU decision-makers. In the following section, I will therefore primarily use the literature on interest group influence to synthesise insights on the conditions under which political entities without final

decision-making powers can influence policymaking. One notable exception to this lack of attention to intra-EU political entities, is Hönnig and Panke's (2013) study on two EU consultative committees, the European Economic and Social Committee (EESC) as well as the Committee of the Regions (CoR). These also share some important characteristics with EU agencies, arguably even more so than interest groups do, as they both have the mandated institutional role to act as policy advisors and provide policy recommendations based on their specialised expertise when requested to do so by EU institutions or on their own initiative (Kim, 2018:26). Finally, Kim's (2018) dissertation is another exception, as it is the first piece of research gathering systematic empirical evidence on the influence of EU agencies on EU policymaking (Kim, 2018:25). Altogether, the research on interest group influence as well as the research by Hönnig and Panke (2013) and Kim (2018) on the policy influence of intra-EU entities, has produced a range of potential conditions under which non-decision-making actors can exert influence on policymaking processes in the EU. In the following section I will outline these conditions from access to the policymaking process to the type of expertise an interest organisation may provide to decision-makers and the type of influence they try to exert.

2.2.1. Access

Access as a necessary condition for exerting influence

One of the fundamental conditions for influencing the policymaking process is to have access to the policymaking process and/or decision-makers in the first place. In one of the seminal works on interest group politics, Truman (1951) already asserted that without access to decision-making nodes, interest groups *cannot* exert influence. This view is echoed by Bouwen (2002:366) who views access as a "conditio sine qua non" for influence, i.e. an indispensable condition without which no influence can be attained. In their discussion on the definition and measurement of interest group access, Binderkrantz and Pedersen (2016) relativise this view somewhat by contending that, on average, actors with access to the policymaking process are more likely to shape policy outcomes than those without access (Binderkrantz and Pedersen, 2016: 307). However, at the same time, access does not guarantee influence (Betsill and Corell, 2001:69-70; Binderkrantz and Pedersen, 2016:307; Bouwen, 2002:366; Eising, 2007:331-332; Gornitzka and Sverdrup, 2011:49). This was shown empirically by Dür and Bièvre (2007:80-81, 91-92) who found that despite NGOs having access to European trade policymaking processes, they have largely failed to shape political outcomes. Therefore, simply showing that actors have formal rights of access to policymaking processes is not sufficient to infer that they utilise their access rights effectively nor that they exert any kind of influence on these

processes. In other words, access is not deterministic (Gornitzka and Sverdrup, 2011:49; Bouwen, 2002:366). Following these insights, access to decision-making processes can be conceptualised as a necessary but not a sufficient condition of influencing the policymaking process.

Definitional Approaches

There have been many different definitional approaches to the study of interest group access. While some approaches employ a very narrow definition that requires direct (physical) contact for access to take place (Orman, 1988 as cited in Binderkrantz and Pedersen, 2016:309; Eising, 2007:331), others define access more broadly. In this broader conception of access, interest organisations are characterised as having gained access once they have "successfully entered the political arena", which can be achieved simply by receiving attention from relevant gatekeepers, such as politicians, bureaucrats or the media (Binderkrantz and Pedersen, 2016:309-310; Binderkrantz et al., 2015:9). Finally, another definitional approach to interest group access is based on the transmission of information (Beyers, 2004; Bouwen, 2002), whereby access is gained through the "exchange of policy-relevant information with public officials through formal or informal networks" (Beyers, 2004:213). For the purpose of this study, access will be defined as a result of an exchange of information between interest organisations and policymakers, which is controlled by relevant political gatekeepers such as politicians and bureaucrats. This definition combines Beyers' (2004) focus on information transmission with Binderkrantz and Pedersen's (2016:310) emphasis on defining access as being controlled by political gatekeepers. The latter is important to distinguish successful access that gained decision-makers' attention from information transmission strategies that do not reach or are ignored by decision-makers (Binderkrantz and Pedersen, 2016:310-311).

Structural Conditions of Access in EU Policymaking

Structural conditions governing the rules and realities of access to decision-makers and decision-making procedures are important determinants of whether and to what extent non-decision-making actors can exert influence on the policy process (Dür, 2008a:1215). In the context of the EU, the European institutions, i.e. the European Commission ('Commission'), the European Parliament ('Parliament'), and the Council of the European Union ('Council'), have the formal power to set the policy agenda and make legally binding decisions respectively. They are therefore the decision-making institutions that interest groups are interested in influencing and the ones that act as gatekeepers to EU policymaking by deciding which groups to grant access to decision-making procedures (Hönnige and Panke, 2013:453; Michalowitz,

2007:136). In order to theorise how access conditions affect interest groups' ability to influence EU policymaking, one has to take institutional differences between the Commission, the Parliament and the Council into account (Klüver et al., 2015a:453). Of particular relevance to intra-EU non-decision-making bodies, such as consultative bodies or EU agencies, are the institutionalised consultation procedures which can provide windows of opportunity for these bodies to exert influence on the policy process. There are three ways for these bodies to access the policy process. In certain policy areas their consultation is mandatory, in others EU institutions can request their specialised opinions, or they can provide policy opinions on their own initiative (Hönnige and Panke, 2013:454, 456; Kim, 2018:59). In their study on the influence of consultative committees, Hönnige and Panke (2013:457-458) tested whether the type of access used by a consultative body impacted how influential they were in shaping the policy output. One of their hypotheses was that committees might be more influential in a legislative process if their opinion was requested as this implies a higher interest by EU institutions in their expertise. They also outline the alternative expectation that policy opinions provided on a committee's own initiative could be more influential in the policymaking process as this would imply a great intrinsic interest in the legislative proposal (Hönnige and Panke, 2013:454). However, their empirical results led to the rejection of both hypotheses, indicating that the type of consultative access is not decisive for exerting influence. Instead, Kim (2018:60) suggests that the frequency with which these access points are utilised by non-decision-making actors is a crucial determinant for their ability to shape the policymaking process. This corresponds with Chalmers' (2013:47) argument that based on the idea of 'more is better', more frequent information transmission will result in more access and thereby in more opportunities to exert influence. His empirical results supported this argument as they show that supplying information frequently and through different information strategies, from writing emails and participating in open consultations to writing policy papers, was crucial in securing access to decision-makers (Chalmers, 2013:52). Following this discussion of the access condition, it becomes clear that any study on the influence of non-decision-making actors on policy processes first needs to establish that those actors actually had access to the relevant decision-making channels as a necessary condition for influence exertion. Additionally, we can *derive the expectation that a greater frequency of access to the policymaking process by non-decision-making actors increases the influence they are able to exert.*

2.2.2. Types of Expertise and Influence

The conditions under which interest groups participating in a policymaking process can actually shape this process also vary considerably by the type of issue they try to get involved in and the type of interests they pursue in the policymaking process. In essence, it is not just structural conditions, but also the "substantive nature of specific policies [that] affect politics" (Klüver et al., 2015a:451). Whether a policy is concerned with largely technical issues or with issues of 'high politics' shapes the type of influence interest groups are likely to exert (Beyers, 2008:1191). The literature suggests that decision-makers' demand for the specialised information that interest groups can provide may be greater when dealing with very technical policy issues (Dür, 2008a:1217). Thus, when policy issues are highly complex, technical and have the potential to impact many different issue areas, then European institution tend to rely more on external expertise and incorporate information provided by external actors into their policy positions (Klüver et al., 2015a:451). In other words, an important factor of expertise-based influence of interest groups is the extent to which decision-makers may possess insufficient scientific and information processing capacities to deal with very complex and highly technical policy issues. If there is a case of information asymmetry between interest organisations and decision-makers, with the former possessing specialised knowledge that the latter does not have, then interest organisations are more likely to exert influence through their information transmission (Hönnige and Panke, 2013:457; Dür, 2008b:1215). In the context of EU politics, especially the Commission and the Parliament seek out external actors to provide them with policy-relevant information (Beyers, 2008:1198). For the Commission this may be due to its broad policy competences coupled with relatively limited administrative resources (Dür, 2008a:1215), while the Parliament requires external information through which it can assess different stakeholders' viewpoints on the Commission's legislative proposals from supranational, political, and electoral perspectives (Bouwen, 2002:380-381). While most interest group influence studies only tend to distinguish between 'expert/technical information' and 'politically salient information', Chalmers (2013:46) has created a list of six information types that interest organisations may provide to EU institutions. These include legal information, feasibility evaluations, information to make technical information understandable to laymen, public opinion data, as well as information about the economic and/or social impact of a policy proposal (Chalmers, 2013:46). In terms of providing such information to decision-makers, the timing of information transmission and the exclusivity of the information seems to play a central role. The provided expertise must be timely since the chances of influencing the

decision-making process are higher when interest groups can shape the policy preferences of central actors early on in the process (Hönnig and Panke, 2013:456-457; Chalmers, 2013:52). Therefore, interest groups need to have the capacities to anticipate the agenda of EU institutions so that they can make use of the "premium on early, efficient and reliable information" that decision-makers put on expertise received at the right time in the policymaking process (Chalmers, 2011: 477). Furthermore, early information is argued to be even more valuable if it is exclusive and not readily available information that decision-makers might not be able to access through other means (Chalmers, 2011:477).

When participating in a policymaking process and providing their expertise to decision-makers, interest organisations can follow different types of interests depending on the manner in which they aim to influence a policy issue (Beyers, 2008:1191). Michalowitz (2007:136) defines the 'type of influence' as the degree to which interest groups aim to influence the political core of a particular legislative proposal. Interest groups wishing to exert 'technical influence' (or 'instrumental influence') are concerned with changing technical details and adapting policy instruments without modifying the underlying policy aim. Such instrumental influence aims to modify only the finer details of existing policy tools – for instance to make them work more efficiently or effectively – but does not try to challenge the political interests of decision-makers or other stakeholders involved in the policymaking process (Beyers, 2008:1191; Michalowitz, 2007:136). However, interest organisations trying to exert 'directional influence' aim to change the political or ideological core upon which a policy is premised. In other words, directional influence challenges the prevailing policy frames and fundamental beliefs that a policy is based on (Beyers, 2008:1191; Michalowitz, 2007:136). Following the same idea as the concept of a 'premium on early information' introduced above, Michalowitz (2007:136) argues that directional influence is most likely to be exerted successfully by interest organisations when they are able to shape the initial political core of a policy issue from the outset by exercising influence in the agenda-setting process. However, overall, the literature suggests that interest organisations are more likely to exert influence on a policymaking process when they pursue technical rather than directional interests (Dür, 2008a:1217; Michalowitz, 2007:137). This is due to directional influence exertion likely generating conflict with the decision-makers who first decided on the policy direction and core contents, whereas instrumental influence exertion does not challenge the core political interests of decision-makers (Michalowitz, 2007:137). From this we can *derive the expectation that non-decision-making actors pursuing policy goals of technical nature will be more influential in shaping the*

policy process according to their preferences than those pursuing more political policy goals. A caveat to this expectation is that non-decision-making actors may be successful in exerting directional influence when they are able to shape the core of a policy issue from the outset through providing their expertise very early on in the conceptual stages of a policymaking process.

2.3. Framing

Once interest organisations have gained access to the policymaking process and start their communicative interactions with decision-makers, these communications and the information they provide tend to be framed in a certain way in order to best convince decision-makers of the importance and value of their arguments and information. Even in order to gain access, interest organisations might selectively frame an issue to conceptualise it in a way that suggests the necessity to include their specific expertise in the policymaking process. For example, an interest organisation for security professionals trying to gain access to a policymaking process would try to frame this policy issue in security terms in order to necessitate and legitimise their participation in the legislative process. Corell and Betsill (2008:33) highlight issue framing as an important indicator of influence exerted by non-decision-making policy actors. In their conception, interest organisations exert influence by selectively highlighting particular aspects of a problem and thereby conceptualising, or framing, an issue from a particular perspective. By successfully framing an issue, interest organisations then construct the boundaries within which decision-makers approach a policy. Issue framing can be an important indicator of an interest organisation's goal attainment since one can expect that a successful issue framing by an interest organisation results in a correlation between the issue frames employed by the interest organisation and those utilised by decision-makers when discussing the policy issue at hand and in the frames present in the written legislation (Corell and Betsill, 2008:30).

2.3.1. Definition: Frames and Framing

The concept of 'framing' has first been defined by anthropologist Gregory Bateson in 1955 and has since found application and elaboration in a range of different fields of study, ranging from psychology to social movement and communication studies all the way to linguistics. In the field of public policy, it was Daniel Schön and Martin Rein who adapted the concept and devised a policy analytic approach to framing (see van Hulst and Yanow, 2016:92-97 for a broader account of the development of framing theory in public policy analysis). Rein and Schön's (1996:88) framing theory emphasises that all policy discourse is based on some kind of "assumptional basis" that often remains implicit and shapes the boundaries and direction of

the more visible language and behaviours exhibited in policy processes. The authors argue that in the context of public policy analysis, frames can be viewed as generic diagnostic and prescriptive narratives that guide the analysis of policy issues by identifying how to approach and define an issue and what ought to be done about it (Rein and Schön, 1996:89). Building on Rein and Schön's (1996) conceptualisations, van Hulst and Yanow (2016:93) stress that it is important to differentiate between 'frames' and 'framing'. Frames are static, definitional schemes of interpretation. In contrast, 'framing' denotes a dynamic intersubjective process through which policy actors, from decision-makers and stakeholders to spectators, socially construct and disseminate their interpretations of the meaning of an issue (van Hulst and Yanow, 2016:93, 97).

2.3.2. Framing as a means for exerting influence

Unsurprisingly, selecting and highlighting certain aspects of a policy issue, while ignoring or deemphasising others, as well as pushing a particular narrative on what actions ought to be taken, is a crucial means for policy actors to influence the policymaking process and its outcomes (Eising et al., 2015:516; Klüver et al., 2015b:481). In the EU policymaking sphere of contested competencies and multiple competing stakeholders, framing of an issue in a specific direction has the potential to "empower certain actors over others" (Harcourt, 1998:370 as cited in Eising et al., 2015:517). This is particularly the case for complex policy proposals, in which various policy issues with differing impacts on different societal groups are subsumed in a single legislative initiative. As a result, the various policy actors involved in the process – such as different decision-makers, professional associations, societal interest groups, and specialised agencies – will likely be concerned with different aspects of such a complex proposal. Framing comes into play when these actors then seek to highlight the salience of those aspects of the proposal that they are concerned with in order to delimit the viable policy alternatives to be considered in the decision-making process. Therefore, framing can be conceptualised as a lobbying strategy that policy actors employ to influence the direction of a legislative proposal according to their (strategic) interests (Klüver et al., 2015b:481-482; Bauer and Bogner, 2020:494). Such issue framing can then be employed as an indicator for an interest organisation's goal attainment in a policymaking process. From this we can *derive the expectation that when an interest organisation's issue frames correlate with those employed by decision-makers and those used in the legislative text, then interest organisations can be expected to have had an effect on the issue framing surrounding the policy, which is a part of their goal attainment* (Corell and Betsill, 2008:30).

2.3.3. Identifying frames: Science, Technology and Society & Critical Security Studies

Naturally, frames employed by policy actors will differ according to the type of policy issue under consideration. Therefore, in order to establish a theoretical basis for analysing frames and framing in this case study, this research will draw on literature in science, technology and society studies (alternatively called science and technology studies) (STS) combined with critical security studies (CSS) to study the potential frames to emerge in the policy discourse around the legislation considered in this thesis' case study. This is motivated by the observation that the interoperability proposals concerning the EU's biometric border management databases have been conceptualised in the Commission's communications as a technological tool for facilitating internal security. Before delving into the frames implied by these two study approaches, I will briefly summarise the main ideas behind STS and CSS. STS denote a field of study concerned with analysing the interplay between society, culture and politics on the one hand and science and technology on the other hand. The main underlying assumption upon which STS scholars base their research is that the role of science and technology is crucial to studying modern societies as they infuse all aspects of modern life and must therefore be subject to political debate, rather than being viewed as apolitical (Bijker, 2003:444). CSS take a social constructivist approach to security by conceptualising security issues as constructed through intersubjective social processes and acknowledging that security logic is prevalent in many areas beyond the traditional focus of (realist) security scholars on military issues (Williams, 2005:135). Therefore, whether an issue constitutes a 'security' issue is not a question of apolitical, supposedly objective judgement, but subject to an issue being successfully framed as an existential threat to a referent object that is perceived to have a legitimate claim to survival (Buzan et al., 1998). The common thread of STS and CSS is that both reject the notion that their objects of study – science and technology, and security respectively – are apolitical reflections of some objective reality. In other words, both STS and CSS take the "ontological multiplicity" of their objects of study as the starting point of their research (Evans et al., 2020:5). This suggests that there exists no single version of 'reality' nor a single 'essence' of technology or security, but rather several interpretations of it (Bauer and Bogner, 2020:493).

This is where framing comes into play as a way to push a specific interpretation of reality and frame complex issues selectively. Vermeersch and de Pauw's (2017) 'framing' experiment on the acceptance of new security-oriented technologies provides a starting point of analysing

potential frames utilised when discussing such technologies. They argue that technology acceptance is conditioned by security concerns, privacy concerns and technology optimism, which are expected to either increase or decrease the probability of technology acceptance of those exposed to them (Vermeersch and de Pauw, 2017:56-57). Firstly, in a **security frame**, technology is presented as a tool to fight crime (Vermeersch and de Pauw, 2017:58) and a view of "technology as a security enabler" is advanced (Ceyhan, 2008:120). Ceyhan (2008:106) argues that such a security frame entails portraying civilian high-tech technologies, such as biometrics, video cameras, scanners and databases, which were not originally developed for military or security purposes, as necessary to respond to 'new threats' and 'manage' risks by identifying and monitoring 'risky' people. Oftentimes such a security framing is also legitimised by establishing a 'continuum of threats' that links different policy areas, such as migration and asylum management, with security themes of crime and terrorism (Ceyhan and Tsoukala, 2002). Additionally, the security frame often employs discourses of fear that justify the necessity and urgency of expanding the use of emerging technologies with reference to extreme and dramatic examples of terrorist attacks, organised crime, state failures, natural disasters, and pandemics (Ceyhan, 2008:107; Fisher and Monahan, 2011:549). Secondly, in a **privacy frame**, the perceived risk of the erosion of privacy and undermining of data protection principles through new technologies is brought to the foreground. Associated with this frame is the so-called 'surveillance perspective', which associates the employment of emerging identifying and monitoring technologies with 'Big Brother' and 'Brave New World' mass surveillance (Vermeersch and de Pauw, 2017:52, 57). Privacy frames and security frames are frequently put up against each other as security frames are expected to increase the acceptance of new technologies and preoccupation while privacy frames are expected to decrease it (Vermeersch and de Pauw, 2017:57; Fisher and Monahan, 2011:550). Associated with this privacy frame is a more general (social) **risk frame** of employing emerging technologies. Bauer and Bogner (2020:500-501) identify two narratives common to the risk frame in their empirical study on the framing of synthetic biology as an emerging technology. In the first narrative, the risks associated with the technology are presented as controllable by taking the proper precautions in the form of security standards, good governance, and risk assessments. This narrative emphasises the notion that the benefits of the new technology outweigh the risks. In contrast, the counter-narrative is marked by scepticism that science is able to anticipate and control the unintended consequences and repercussions of the new technologies (Bauer and Bogner, 2020:500-501). In the context of security technologies, such a more general social risk frame is often exemplified by voicing concerns on the impact of such technologies on the

protection of fundamental rights (Ceyhan, 2008:115, 119). Another pertinent frame is associated with **technology optimism**, which describes the notion that new technologies positively contribute to a better life as well as increased efficiency, control, and flexibility (Bauer and Bogner, 2020:499-500, 503-504; Vermeersch and de Pauw, 2017:56). Within this frame, technological innovations are viewed as the optimal solutions to various societal, economic and political challenges, which Bauer and Bogner (2020:500, 504) call a 'solution narrative'. A central theme in the technology optimism frame is the ability of technology to increase the efficiency and effectiveness of the practices aimed at facilitating certain policy goals (Huysmans, 2011:378). In their study on the framing of monitoring technologies in healthcare delivery, Fisher and Monahan (2011:548) discuss how these technologies are often portrayed in terms of the 'returns on investment' they can generate. In particular, the focus is directed on how these new technologies speed up customer interaction processes, reduce redundant working practices and more efficiently manage personnel (Fisher and Monahan, 2011:548). A counter-frame to such technology optimism and efficiency frames deconstructs the 'solution narrative' by arguing that these technologies are just solutions looking for a problem and that "when you have a hammer, everything looks like a nail" (Bauer and Bogner, 2020:500). In other words, this counter-frame rejects the notion that certain technologies are the only possible alternative to tackle certain problems and criticises that other potential solutions are ignored in favour of fixating on technological innovations (Bauer and Bogner, 2020:500). Apart from the types of frames employed in a policymaking process, the literature also suggests that it is important to determine whether these frames are employed in a generic or specific manner (Bauer and Bogner, 2020:503-504; Eising et al., 2015:518). In their empirical study on technology framing, Bauer and Bogner (2020:502) observed that the matter of ethics was frequently addressed merely in a very generic manner that pointed out the general value of ethics without going into much detail on specific ethical concepts or linking it to the case under discussion. The authors argue that this transformed the ethics frame into a 'meta-frame' (Bauer and Bogner, 2020:503), whereby "ethics became a default element to address" (Bauer and Bogner, 2020:502), however, predominantly in a very abstract, standardised, and generic way. Arguably, the generic reference to ethics may also be applied to the matter of data protection or fundamental rights as it makes a difference whether these concerns are addressed through reference to specific rules, regulations, and principles (Eising et al., 2015:519) or simply mentioned as a legal constraint to be overcome or a default element that has to be mentioned as legitimation.

2.4. Theoretical Expectations

Throughout this literature review, three main theoretical expectations were derived about the factors that determine whether non-decision-making actors are able to successfully exert influence on a policymaking process. Firstly, access to the policymaking process was identified as a pre-condition of exerting influence, while the frequency of access is expected to be a crucial determinant of how successful a non-decision-making actor is in shaping a policy process and its outcome. In order to test this expectation in my case study, I will trace the indicators of access of each EU advisory body under investigation, such as the frequency of requested and own initiative reports and opinions published by those bodies as well as the frequency of their participation in formalised working groups, consultations and informal contact with decision-makers. Additionally, the frequency of access will also be traced through participants' accounts of how often and through which access channels their organisation interacted with decision-makers and participated in the policymaking process. The second theoretical expectation identified in the literature review is that non-decision-making actors pursuing technical and instrumental interests that merely aim to modify finer details in a policy are more likely to exert influence in a policymaking process than those pursuing directional interests that aim to change the political core of a policy. For this expectation a caveat was identified relating to the role and timing of a non-decision-making actors' involvement in the policymaking process. They are more likely to be successful in exerting directional influence when they are able to shape the core of a policy issue from the outset through providing their expertise very early on in the policymaking process. In order to operationalise the type of influence EU advisory bodies tried to exert in the policymaking process, I will analyse their stated policy preferences to see whether those preferences are of a technical nature or follow more directional and political goals. In addition, I will also triangulate the self-perceptions and outsider perceptions from other policy participants regarding the type of influence the various actors under investigation aimed to exert in the interoperability policymaking process. Finally, another theoretical expectation concerns the impact successful issue framing by a non-decision-making actor has on the policy process and outcome and their goal attainment. When an EU advisory body's issue framing correlates with those employed by decision-makers and those used in the legislative text, then this body can be expected to have attained their framing goals by shaping the issue framing surrounding the policy. In order to analyse the issue framings utilised by EU advisory bodies and decision-makers respectively, I will identify the frames outlined in the literature review that are used by advisory bodies in their policy opinions and

statements as well as in the rhetoric by representatives of those agencies in relevant conferences or interviews. The same will be done for the rhetoric of EU decision-makers and I will also identify the most prevalent framings in the legislative texts on interoperability. Through the identified framings utilised by advisory bodies and decision-makers respectively, the extent to which they are congruent with each other can then be analysed and provide insight into the degree of goal attainment by the advisory body through their issue framings.

3. Methods

3.1. Research Design: Within-Case Analysis

This research is based on a within-case study design, which seeks to uncover the causal paths that connect a range of variables of interest to one another (Toshkov, 2016:291). In particular, this research seeks to investigate the causal paths that connect the participation of EU agencies and other institutional advisory bodies in a policymaking process to their influence on the policy outcome. Toshkov (2016:285) calls this research design a Single-Case Study Design, however, the term Within-Case Analysis is arguably more appropriate as it stresses the point that the analysis is conducted by examining observations from *within* rather than *across* cases. It thereby distinguishes this research design from another small-N research approach, namely comparative research. The single case that this research will focus on is the policymaking process leading up to the adoption of the legislative package on interoperability, which contained the adoption of the following two regulations on interoperability – one in the field of borders and visa, and the other one in the field of police and judicial cooperation, asylum and migration:

- Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA
- Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816

These regulations will be referred to simply as the 'interoperability regulations' or 'interoperability legislations', and as 'interoperability proposals' when referring to them before they were adopted by the co-legislators, in this thesis. As these regulations are largely very similar in content and structure, whenever legislative texts are analysed in this thesis, only the legislative texts pertaining to Regulation (EU) 2019/818 on police and judicial cooperation, asylum and migration will be analysed for reasons of simplicity. As Toshkov (2016:289, 294) explains, one reason for conducting single-case studies is the substantive relevance of a specific

case due to its broader societal importance, which I outlined in the introduction for my case study. Additional to its societal relevance, single-case studies can also apply established theories in new environments and settings and thereby test theoretical ideas under previously un(der)explored conditions (Toshkov, 2016:290). In the following section, I will first outline my selection of actors to be studied and then explain the theoretical relevance that this case study may additionally have.

3.1.1. Selection of Advisory Bodies

This sub-section will outline why these specific four EU agencies and the supervisory authority, the EDPS, were chosen as the non-decision-making actors whose influence on the interoperability policymaking process will be examined in this thesis. The rationale for selecting them is firstly that they were all involved in the legislative process on interoperability and secondly that they took on a role of providing specialised expertise and advice to participate in this process in accordance with their institutional mandates. The European Commission (2008:2) defines the task of EU agencies as supporting the "decision-making process by pooling the technical or specialist expertise available at European and national level". For instance, the tasks of the Fundamental Rights Agency are described as providing "independent, evidence-based advice to EU and national decision makers, thereby helping to make debates, policies and legislation on fundamental rights better informed and targeted" (European Union, n.d.). Similarly, the EDPS also has an explicit role as an advisor to the Commission and the co-legislator in all decision-making processes that concern the rights to personal data protection and privacy (EDPS, n.d.). Part of Frontex' tasks is to provide their technical expertise as input into the legislative proposals of the Commission and the Council's legislative deliberations, as well as to regularly attend European Parliament Committee hearings (Frontex, n.d.-a, n.d.-b, n.d.-c). eu-LISA also actively interacts with EU institutions and bodies and participates in relevant working groups and committees convened by these institutions to provide its expert input (eu-LISA, n.d.-a). Finally, Europol has an administrative agreement with the Commission that they should exchange information and regularly consult each other on policy issues in which they have a common interest (Commission and Europol, 2003). Other EU agencies and bodies that also participated in the policymaking process on the interoperability regulations, such as the European Asylum Support Office (EASO), Eurojust or the Counter-Terrorism Coordinator (CTC), are not included in the analysis as they were sufficiently peripheral to the legislative process and have also not been identified as potentially relevant policy actors in the academic literature on interoperability (see chapter 1.1. on Societal and Academic Relevance).

Thus, for the purpose of limiting the scope of the analysis, the roles of these bodies have been excluded from analysis.

The described advisory roles of the EU agencies and bodies to be analysed imply that, at least to a certain extent, EU agencies are envisioned to shape policies based on their evidence-based policy advice and recommendations to the EU institutions. In this sense, the potential influence of EU agencies can be defined as being able to shape EU policy output by providing specialised input to formal decision-makers (Kim, 2018:41). Studying the policy influence of intra-EU agencies is an understudied field in the literature on the policy influence of non-decision-making actors. Kim (2018:25-26) highlights in her dissertation that her research is the first one to systematically assess the *de facto* influence of EU agencies on EU policymaking. This is despite early assertions by scholars such as Vos (2000:1130) that "the provision of information and evidence by agencies clearly influences decision-making and could be considered as a kind of 'regulation by information'". Therefore, this thesis may also add an important theoretical contribution to the study of the policymaking influence of EU agencies and advisory bodies that are taking on a greater and greater role in EU policymaking as the 'agencification' in the EU progresses (Galli, 2019:14; Kim, 2018:178-179, 184).

3.1.2. Unit and Level of Analysis and Observation

In this research, the units of analysis are intra-EU advisory bodies. Specifically, the units of analysis are EU agencies, namely Frontex, Europol, eu-LISA, and the FRA as well as an independent supervisory authority called the EDPS, whose advisory mandate gives it a comparable consultative role in the EU policymaking process to EU agencies (EDPS, n.d.). The level of analysis will be on the organisational level, i.e. not on the level of individual staff of those agencies but on the output and activities of the organisations as a whole. The units of observation will vary by the two data collection methods employed in this thesis: document analysis and interviews. As the advisory documents of EU agencies and the EDPS are products of the organisation as a whole and not attributable to specific staff within the organisation, the unit of observation of advisory bodies' policy documents is on the organisational level. In contrast, it is not possible to interview organisations, therefore, interviews are conducted with individual staff of the EU agencies and advisory bodies, i.e. the unit of observation is individuals, who will be asked to provide insights into the activities of their organisation. The goal of the interviews is to provide the researcher with a comprehensive overview of the policymaking process and the interviewees' perceptions about their own and other agencies'/advisory bodies' influence on this process. Therefore, I will select those individuals

in the organisations who were actively involved in the legislative process on interoperability and interacted with decision-makers as well as actors from other EU agencies and advisory bodies in relation to the interoperability legislations. These individuals were identified either through their job position in the policy unit/department of their organisation, participation in intra-organisational project teams on interoperability, or through their participation as a representative of their organisation in the eu-LISA conferences in panels focussed on interoperability – or, ideally, a combination of those characteristics. This ensures that the individuals interviewed both have an intra-organisational perspective on the policy work of their own organisation and have interacted with other policy actors and decision-makers.

3.2. Methodology: Process-Tracing

Process tracing has become the standard method for within-case analysis and aims towards collecting, selecting, and synthesising evidence from within a case to trace a sequence of causal processes in order to explain a case (Toshkov, 2016:297-298). The goal of the process tracing method in influence studies is to demonstrate how a variety of independent variables relating to interest groups' participation in the policymaking process are causally linked to their influence on the policy outcome as the dependent variable (Dür, 2008b:562). According to Betsill and Corell (2001:72, 77, 2008:19, 30), process tracing is a relevant and appropriate method for studying interest organisations' influence on policymaking processes. As a first process-tracing step, researchers need to show that interest organisations engaged in intentional communication and information transmission with decision-makers (Betsill and Corell, 2001:77). Therefore, in this thesis I will outline how frequently and in what ways EU advisory bodies accessed the policymaking process and the type of information and specialised expertise they provided to decision-makers. Subsequently, researchers must examine whether a modification in decision-making actors' behaviour occurred that is consistent with the communication and information exchange that interest organisations engaged in with them (Betsill and Corell, 2001:77, 2008:30-31). This entails assessing the degree to which interest organisations attained their policy goals in the final policy outcome. In this thesis, the effect non-decision-making actors' communications had on the policy decisions taken by the European institutions is analysed firstly in the framing section of the analysis. Since Corell and Betsill (2008:36) suggest that the level of interest organisations' 'goal attainment' can be evaluated by assessing the extent to which their issue framing was taken up by decision-makers, I will first identify which framings the individual EU advisory bodies employed in relation to interoperability. Then, I will assess the extent to which these framings were taken up and

repeated by relevant decision-makers from the European institutions to gauge the effect each EU advisory bodies had on the overall issue framing of the policy. Secondly, the degree to which EU advisory bodies attained their policy preferences in the interoperability policymaking process will be analysed in the analysis chapter on influence perceptions. Here, I will triangulate self-perceptions of the relevant EU bodies of their own influence and preference attainment with outside perceptions on their influence from other actors participating in the legislative process.

3.3. Data Collection

3.3.1. Qualitative Document Analysis

Qualitative document analysis, defined as the "systematic procedure for reviewing and evaluating documents" (Bowen, 2009:27), will be one of my main sources of evidence to trace the influence EU agencies exerted on the policymaking process in my case study. I will conduct a qualitative document analysis of EU advisory bodies' opinions and reports as well as documents providing insight into the European decision-makers' policy preferences and legislative documents pertaining to my case study (see Table 1 for a timeline of the relevant documents). Generally, the timeframe for this study is defined as starting from the first Commission communication signalling renewed interest in EU database interoperability, "Stronger and Smarter Information Systems for Borders and Security", on **6 April 2016**, up to the adoption of the final legislations on the interoperability of EU large-scale IT systems on **20 May 2019**. The only exception to this is the inclusion of an open letter by the Supervision Coordination Groups (SCGs) of the SIS II, VIS and Eurodac, which was published in January 2020, into the analysis because it provides insight into the EDPS' retrospective perception of their influence during the legislative process that falls within the timeframe of this research.

First, I will analyse the formal and informal policy papers published by EU agencies and the EDPS about interoperability of EU databases. While Europol and Frontex only published informal policy papers, titled 'contribution' and 'non-paper' respectively, eu-LISA and FRA published expert reports on the technical feasibility and fundamental rights compliance of interoperability respectively. Additionally, the FRA and EDPS published formal legislative opinions on the interoperability proposals as well as additional statements, reflection papers and/or policy reports. The SCGs, which are staffed partly by EDPS staff, also wrote two open letters to European decision-makers to highlight their concerns with the legislative process on interoperability. These formal and informal policy documents were selected to be analysed for

this research because they contain the policy preferences of the EU advisory bodies that are the focus of this research. The second category of selected documents are those containing the contributions of decision-makers from the European institutions. These include the Commission's communication on the interoperability proposals, the proposals themselves as well as the Parliament's suggested amendments to the proposals and the minutes of the debate between MEPs in the Parliament's LIBE committee. The reports of the eu-LISA conferences bridge the first and the second category of documents since they provided a platform for exchange between EU decision-makers and EU advisory bodies. Speakers from all EU advisory bodies under investigation as well as from the European decision-making institutions gave speeches and/or participated in panel discussions relating to interoperability. By assessing the similarities and differences between the policy preferences and issue framings expressed by the EU advisory bodies' representatives in comparison to those expressed by European decision-makers, I will trace the degree of agreement between EU advisory bodies' policy positions and those of decision-makers (see Kim, 2018:54). This will be done by comparing the type and frequency of issue framings utilised by EU advisory bodies with those used by decision-making actors in order to analyse the extent to which they are congruent.

Publishing Date	**Authors**	**Type of Document**	**Name of Document**
06.04.2016	European Commission	Policy Paper	Stronger and Smarter Information Systems for Borders and Security
02.05.2016	Europol	Informal Policy Paper	Europol contribution on improving the EU information exchange architecture and interoperability in the fight against terrorism and serious and organised crime
27.10.2016 (date of conference)	eu-LISA	Conference Report	Conference Report - eu-LISA Annual Conference JHATech 2016: Aligning the capabilities of technology with policy priorities in the areas of migration and internal security
15.05.2017a	EDPS	Informal Policy Paper	European Data Protection Supervisor statement on the concept of interoperability in the field of migration, asylum and security
07.07.2017	FRA	Report	Fundamental rights and the interoperability of EU information systems: borders and security
19.10.2017	European Commission (consultation answer by the FRA)	Public Consultation	Consultation on the interoperability of EU information systems for borders and security
16.10.2017	Frontex	Informal Policy Paper	Non-paper by Frontex on its access to central EU systems for borders and security

17.10.2017 – 18.10.2017 (date of conference)	eu-LISA	Conference Report	Conference Report - eu-LISA Annual Conference Going Digital for a Safe and Secure Europe
17.11.2017b	EDPS	Policy Paper	Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice
12.12.2017	European Commission	Legislative Proposal	Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration)
28.03.2018	FRA	Report	Under watchful eyes: biometrics, EU IT systems and fundamental rights
09.04.2018	eu-LISA	Report	Shared Biometric Matching Service (sBMS): Feasibility study - final report
11.04.2018	FRA	Policy Opinion	Interoperability and fundamental rights implications – Opinion of the European Union Agency for Fundamental Rights
16.04.2018	EDPS	Policy Opinion	Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems
22.06.2018	SCGs (staffed by DPA and EDPS staff)	Open Letter to Decision-Makers	Joint letter on the new EU legislative framework for interoperability between EU large-scale information systems
23.07.2018	European Parliament	Amendments to Legislative Proposal	Amendments 192-777 to the Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration)
27.03.2019	European Parliament	Debate Minutes	Debate CRE 27/03/2019 – 24: Interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration - Interoperability between EU information systems in the field of borders and visa (debate)
20.05.2019	European Union	EU Legislation	Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816
13.01.2020	SCGs (staffed by DPAs and EDPS)	Open Letter to Decision-Makers	Joint letter on the new EU legislative framework for interoperability between EU large-scale information systems

Table 1: Timeline of relevant documents for this research

Document analysis also allows the researcher to track developments in the policymaking process by comparing various drafts of documents to subsequent versions to identify changes over time (Bowen, 2009:30). Therefore, in this research, when EU advisory bodies make specific recommendations in their policy opinions for the inclusion or exclusion of specific clauses in the proposals, I will trace whether their recommendations were taken up in the final legislations. In this regard, it is important that the amendments suggested by MEPs for a legislative proposal generally contain a short justification for the amendment. In the European Parliament's amendments regarding the interoperability proposal, several amendment justifications are based on recommendations put forward by the EDPS and the FRA. While not a definite measure for causality, the inclusion of EP amendments based on such recommendations in the final legislation, would point towards the causal influence of the relevant EU agency or supervisory authority.

3.3.2. Semi-Structured Interviews

It is common practice for researchers in the qualitative social sciences to combine multiple qualitative research methods in one study in order to cross-check and validate their findings across different data sources and methods (Bowen, 2009:28). Therefore, as a supplement to the document analysis, I also aim to conduct semi-structured elite interviews with officials from those EU advisory bodies that were involved in the policymaking process of my case study.

Selection of Interviewees

For this thesis, I conducted six semi-structured interviews between the 3rd and 19th of February 2021 with staff members or former staff members of the EU agencies and supervisory authority, who were involved in the policymaking process on the interoperability legislations. I contacted officials from these agencies based on their position in the policy or technology unit of their organisation and/or based on their participation in the eu-LISA conferences where they spoke on interoperability as representatives of their organisation. Three of the people I interviewed were ones that I had contacted on this basis, namely Olivier Burgersdijk (Europol official), Krum Garkov (eu-LISA director) and a former eu-LISA official who wishes to remain anonymous. Burgersdijk was responsible for the information management in Europol during the interoperability policymaking process and was the main representative of Europol in the HLEG on interoperability. As the director of eu-LISA, the agency responsible for the IT administration of the systems to be made interoperable, Garkov also represented his agency in the HLEG and to the European institutions. The former eu-LISA official interviewed was also heavily involved in the interoperability policymaking process on the working level. The other

interviewees were identified through the snowball technique, whereby the people I contacted for interviews put me in contact with other people within their organisation who were also involved in the interoperability policymaking process. The interviewees identified through this snowball technique were Krzysztof Klebek (Europol official), Dina Kampouraki (EDPS official) and another EDPS official who wishes to remain anonymous. Klebek's job responsibilities within Europol are focused on business-IT alignment, so he was involved in the interoperability process from a technical and operational perspective and also attended some of the HLEG meetings on interoperability as an alternate. While the anonymous EDPS official was involved in the interoperability policymaking process from a policy-oriented side, Kampouraki's role within the EDPS was to ensure the data protection compliance of the EU's large-scale IT systems from an IT perspective. Altogether, I conducted two interviews per organisation for three out of the five EU agencies and supervisory authority that make up the focus of my research. Unfortunately, none of the officials I contacted at Frontex and the FRA were available to participate in an interview. However, some questions asked to the interviewees also pertained to the contributions and influence of Frontex and the FRA in the interoperability policy process, thus providing at least an outside perspective on those organisations' involvement.

Purpose of Interviews

The purpose of interviews in my research project is two-fold. Firstly, elite interviews are important sources of information about both the process and sequence of political events as well as the motivations of actors involved in the events (Beach and Pedersen, 2013:134). Therefore, I asked interviewees about the various ways in which their organisation participated in the policymaking process; about the access channels they used to participate, the kind of information they provided to decision-makers and how frequently they engaged in the decision-making process. The purpose of this was to gain a deeper insight into how their organisations contributed to the policymaking process in order to analyse the ways in which they may have exerted influence on the interoperability policy. Secondly, interviews can also be geared towards measuring perceptions of actors' influence on the policymaking process among stakeholders, which has been termed the 'attributed influence' approach in the literature (Arts and Verschuren, 1999). Drawing on Ingold and Leifeld (2014:2), Kim (2018:53, 57) argues that such perceptions of influence can serve as a proxy indicator for an actor being influential as their influence will be reflected in their reputation. Therefore, researching whether and why interviewees perceived their own organisation and the other relevant actors involved in the

policy process as influential is relevant to answer the research question of EU advisory bodies' influence in the policymaking process since influence perceptions act as a proxy for actual influence.

'Ego' and 'Alter' Perceptions of Influence

The perceptual dimension of influence is conceptualised in Arts and Verschuren's (1999) 'EAR instrument' for assessing stakeholder influence. It consists of two perceptual dimensions, ego-perception ('E') and alter-perception ('A'), and a third dimension, the researcher's analysis ('R'). Ego-perception refers to a self-assessment of an interest organisation of their own influence, while alter-perception is the perception of other key players in the decision-making process of that interest organisation's influence. The researcher's analysis complements these perceptual dimensions by reconstructing the interest organisation's interventions in the policymaking process and their degree of goal achievement (Arts and Verschuren, 1999:416; Dür, 2008b:570). During the interviews conducted for this thesis, I asked variations of the following three questions geared towards finding out the interviewees' perception on their own influence on the policymaking process on interoperability as well as the influence of the other actors under investigation.

1. How satisfied are you, from an organisational viewpoint, with the policy outcome on interoperability? Do you think your organisation achieved its aims?
2. Do you think the policymaking process, or the final legislation would have been different if your organisation had not been involved in it? If yes, which aspects of the legislation would have been different?
3. Which other EU agencies or advisory bodies – such as Frontex, Europol, eu-LISA, the Fundamental Rights Agency, or the European Data Protection Supervisor – did you perceive as most successful in shaping the policy process?

The first question aims to elicit a response about the interviewees' perception of the level of goal attainment achieved by their organisation, i.e. the level to which their organisation's policy preferences were reflected in the final legislations on interoperability (see Corell and Betsill, 2008:36). The second question is expected to uncover the perceived influence of the interviewees' own organisation through counter-factual assessment of what would have been different in the legislative process and outcome if their organisation had not participated in the process. In other words, it measures the interviewees' organisational 'ego' perception (see Arts and Verschuren, 1999:416) through the counterfactual analysis recommended by Corell and Betsill (2008:28) to measure interest groups' policy influence. The third question is geared

towards measuring each interviewee's 'alter' perceptions (see Arts and Verschuren, 1999:416) of the influence other EU agencies and the EDPS exerted on the policymaking process. Overall, these questions allow me to get an overview of the perceived influence individual EU advisory bodies had on the process. By triangulating these influence perceptions provided by various interviewees from different organisational perspectives, they can be used as a proxy for actual influence exertion by the policy actors investigated.

3.4. Advantages & Shortcomings of Research Design

There are several advantages to the process-tracing method. The depth of knowledge of a specific case that can be acquired through small-N research designs allows researchers to be knowledgeable of and control for a wide range of alternative causal explanations that may explain a particular outcome (Dür, 2008b:563). This can ensure high internal validity of inferences made from process tracing as such in-depth knowledge of the details and context of an individual case (Trampusch and Palier, 2016:14). However, while process tracing is likely to generate high internal validity, this comes at the expense of external validity in the sense that generalisations beyond the analysed case are unlikely to hold (Toshkov, 2016:304; Waldner, 2012:67-68 in Trampusch and Palier, 2016:5). In other words, the insights uncovered in this case study about whether and why particular EU advisory bodies were able to exert influence in the most recent interoperability policymaking process cannot be generalised to hold in another EU legislative process nor in any other context. However, as generalisations do not have to be the goal of all research, and are not the goal of this research, the limited external validity of my findings should not be considered a major limitation (Toshkov, 2016:305).

Additionally, by supplementing documentary analysis with semi-structured elite interviews with actors that participated in the policy process analysed, researchers can derive in-depth insights that allow them to achieve a detailed assessment of interest organisations' influence in a particular case – with the caveat that claims made by interviewees may not always be reliable (Dür, 2008b:563). Combining evidence from various types of sources (e.g. documents and interviews), different sources of the same type (e.g. interviewing different types of actors), and different types of evidence (e.g. evidence on access patterns vs evidence on accounts of activities) in one study is called methodological triangulation. The purpose of triangulation is to strengthen the credibility and reliability of research findings by cross-checking support for a hypothesis through different independent methodologies and to compensate for individual measures' shortcomings and blind spots (Arts and Verschuren, 1999:416, 422; Beach and Pedersen, 2013:128; Betsill and Corell, 2001:78, 80; Bowen, 2009:28; Dür, 2008b:569).

Therefore, by employing two qualitative data collection methods, namely document analysis and elite interviewing, the reliability of findings can be strengthened through corroboration of evidence. Additionally, deeper insight into the case through elite interviewees' insights can also increase the internal validity of the findings. However, Dür (2008b:563) contends that there are still considerable difficulties in accounting for an entire causal chain from interest group activities to final policy outcomes through available sources. This opens the possibility that "the absence of proof may be taken as proof of absence" (Dür, 2008b: 563) when lobbying is unobservable, e.g. because it took place behind closed doors, potentially leading the researcher to underestimate the influence exerted. Interviewing participants of the policy process can mitigate this shortcoming somewhat, but the potential of unavailable or inaccessible crucial evidence remains a major limitation of process tracing studies that is difficult to completely eliminate.

4. Case Description

4.1. Background: EU Large-Scale IT Systems

The story of large-scale IT systems for border management purposes in the EU started in 1990 when the Schengen Information System (SIS) was extended from just five European countries to all members of the Schengen area and went operational in 1995. The SIS was set up to collect, inter alia, data on persons wanted for arrest, to be refused entry to the EU as well as on missing persons or witnesses to facilitate security-oriented border control (Balzacq, 2008:84). Through a Council regulation in 2000, the next large-scale IT system for the management of the Union's asylum policy was set up to facilitate the implementation of the Dublin II regulation. Eurodac (The European Dactylographic System) became operational in 2003 and is used by all EU members not just those in the Schengen area. This biometric database was originally clearly confined to dealing with asylum and migration matters, such as to tackle 'asylum shopping', without the intent to use the database for internal security purposes. As such it contained data on persons applying for asylum as well as those apprehended in irregular border crossings or irregular residence in an EU member state (MS). Additionally, this database was originally intended only for migration management purposes and law enforcement or security authorities did not have access to it (Balzacq, 2008:87-88; Balzacq and Léonard, 2013: 134-135). The last of the 'first generation' of EU large-scale IT systems for border control is the Visa Information System (VIS), whose establishment was agreed upon in 2002 and which became operational in 2015 to support the Union's common visa policy (Balzacq and Léonard, 2013:136-137). The VIS was intended as a 'multipurpose tool' for border control as well as security purposes from its inception, which is evidenced by granting access to the database not only to border control and immigration authorities but also to security agencies (Balzacq, 2008:89; Brouwer, 2006:137; Vavoula, 2020:143). Balzacq and Léonard (2013:137) attribute the fact that, contrary to SIS and Eurodac, the VIS served a security function from the outset to the securitising role 9/11 played in Western security policies. Additionally, since their inception, both Eurodac and the SIS regulation have been amended and their scope increased to cover security purposes additionally to their original border control functions. Following the Council conclusions "after the events of 11 September 2001 […], the idea of using the SIS data for other purposes than those initially foreseen and specially for police information purposes" (Council, 2002 as cited in Balzacq, 2008:85) was agreed upon and nowadays serves a dual purpose as a migration control and criminal law tool (Bigo et al., 2020:2; Vavoula, 2020:142). Similarly, the amended Eurodac regulation adopted in 2013 also granted national law

enforcement authorities and Europol access to the database (Vavoula, 2020:144), widening its scope and purpose from enforcing the Dublin regulation to the prevention, detection and investigation of terrorism and crime (Bigo et al., 2020:2).

The 'second generation' of large-scale IT systems for border control are those biometric databases that were initiated in the aftermath of and justified with reference to the 2015 Paris terrorist attacks and the 2015 refugee crisis (Vavoula, 2020:145; Bigo et al., 2020:3). At the time of the interoperability policymaking process, these 'second generation' IT systems did not exist yet as the legislative process to establish them was still ongoing (EDPS, 2018:30). The Entry/Exit System (EES) was adopted in 2017 and will record the entry and exit data of TCN visiting the EU for short stays. It aims to make border checks more efficient through automation, help identify irregular immigrants and overstayers as well as uncover identity fraud. The European Travel Information Authorisation System (ETIAS), adopted in 2017 and modelled after its US equivalent ESTA, fulfils the purpose of vetting visa-exempt travellers through online forms before entering the EU. Finally, the Criminal Records Information System for third country nationals (ECRIS-TCN) was adopted in 2019 to exchange criminal records of convicted TCN, notably including dual nationals with EU citizenship, through a centralised system. It aims to complement the existing decentralised ECRIS database for the exchange of criminal records of EU nationals (Vavoula, 2020:145-146; Bigo et al., 2020:3-4). Two of these new databases, EES and ETIAS, are conceived as multipurpose tools and will be made accessible, inter alia, to national law enforcement authorities and Europol, thereby blurring the boundaries between immigration control and security purposes. To date, the SIS II database is the only large-scale IT system whose primary purpose is fighting terrorism and serious crime. However, over time this has been made an additional purpose for every other old and new border management database (FRA, 2018a:65; Vavoula, 2020:146-147).

4.2. Interoperability Framework

Two interoperability regulations establishing a framework for interoperability between EU information systems came into force on 11 June 2019 after being signed by the Parliament and the Council in May. One of the interoperability regulations is situated in the area of borders and visa and enables data exchange between VIS, SIS, the EES and ETIAS. The other interoperability regulation is situated in the fields of police and judicial cooperation, asylum and migration and applies to the SIS, Eurodac, ECRIS-TCN as well as Europol's database (EPRS, 2019:5). However, as asserted by the EDPS (2018:9) in their opinion on the interoperability proposals, they are 'sister proposals' which are highly similar in content as

well as the numbering of the legislative articles and thus should be read together. As such, many insights this research unveils about the policymaking process establishing the interoperability regulation on police and judicial cooperation, asylum and migration are likely to apply to a large extent to the regulation on borders and visas as well. It is also important to point out that this research focuses on the policy process of designing the EU's interoperability framework for its large-scale IT systems, rather than on assessing interoperability from a legal or technical perspective. However, naturally the technical and legal aspects of such a policy proposal are relevant in the policymaking process of designing, amending, and adopting the interoperability regulations. Therefore, such technical and legal aspects and perspectives will be referred to where relevant.

4.2.1. Interoperability and its components

The purpose of making EU border management databases interoperable is to facilitate the sharing of information across technically differentiated large-scale IT systems by enabling the exchange and use of data from multiple databases (Galli, 2019:2). In a factsheet on the interoperability of EU information systems, the Commission defined interoperability as "the ability of information systems to talk to each other. It is about a targeted and intelligent way of using existing data to best effect, without creating new databases or changing the access rights to existing information systems" (European Commission, 2019:1). As outlined in the Commission proposal (2017:5), interoperability is envisioned to be facilitated by four "necessary technical components to achieve interoperability", namely the European search portal (ESP), the shared biometric matching service (shared BMS), the common identity repository (CIR) and the multiple-identity detector (MID). The ESP is a single-search interface that is designed to facilitate the simultaneous querying of multiple databases using alphanumerical (i.e. biographical) and biometric data. It then provides the users of EU information systems with the information from all those systems to which they legally have access through a single search rather than having to search each system separately (Commission, 2017a:6; FRA, 2017:13; EDPS, 2018:8). The Commission proposal emphasises that the ESP does not store any additional data and simply functions as a 'message broker' (Commission, 2017a:6). The shared BMS is the technical tool that enables to ESP to simultaneously query the different databases with biometric data as it will store a mathematical template of all the biometric samples contained in the underlying IT systems. In this regard, the Commission proposal stresses that the shared BMS will not contain the actual biometric data, i.e. the visual representations of fingerprints or facial images, but only the mathematical

representations thereof (Commission, 2017a:6-7). The CIR is a common repository of data that links together all the information on an individual contained in all underlying systems, except the SIS, through biometrics and makes it available to the user in a single 'view'. There are two crucial aspects to note about the CIR. Firstly, the CIR is the only facilitating element of the interoperability framework that actually stores identity data and does not just provide links to the data contained in the underlying systems. This data is stored logically separated according to the particular information system from which it originates. Secondly, the CIR facilitates the streamlining of law enforcement access to non-law enforcement databases through a two-step process. The process starts with a law enforcement officer, who does not need to fulfil any prior authorisation conditions or have access rights to the underlying systems, querying the ESP to check whether data on a specific person is stored in one of the underlying systems – *without* gaining access to the contents of this data. The reply the user receives is called a 'flagged hit' because it flags in which underlying system the data is recorded without providing access to it. Then in a second step, the officer needs to request access to the flagged data following the established rules and procedures for access to the underlying database (Commission, 2017a:7-9; EDPS, 2018:8; FRA, 2017:14; Vavoula, 2020:174-175). The final facilitating component of the interoperability framework is the MID, whose function is to store so-called 'identity confirmation files' that link data from the different databases to detect whether there are multiple identities linked to the same biometric data. Its purpose is to tackle identity fraud and facilitate correct identifications (Commission, 2017a:7-8).

4.2.2. EU agencies, the EDPS and interoperability

On the operational level, interoperability is delivered by the EU Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), which was established in 2011 with the mandate of fulfilling the operational management tasks for large-scale IT systems in the area of freedom, security and justice (Regulation (EU) No 1077/2011; Galli, 2019:15). In 2018, eu-LISA's legal act was revised to include an Article on interoperability, requiring the agency to "develop the necessary actions to enable […] interoperability" as stipulated in the relevant legal acts on interoperability (Regulation (EU) 2018/1726, Article 13). Additionally, the agency's mandate was expanded to allow it to be more proactive in giving advice on relevant technical changes in the IT systems it operates (Regulation (EU) 2018/1726, Recital 19). Therefore, enabled through its expanded mandate, eu-LISA is responsible for supporting the development and leading the technical

implementation of the interoperability of the large-scale IT systems that it is responsible for operating (eu-LISA, n.d.-b).

Through interoperability, other EU agencies, such as Europol and Frontex, are also conferred new roles and powers as their access to data stored in the EU's large-scale IT systems increases and they are given the task to analyse and act on the information the data generates (Galli, 2019:8, 14). The key features of Frontex' mandate are to ensure the effective functioning of the EU's external border control, implement integrated border management (IBM), carry out risk analyses, and provide operational and technical assistance to Member States (Regulation (EU) 2019/1896, Recital 3). In this role, Frontex has access to and can use the various EU databases under specific restricted access conditions (Frontex, 2017:5-8). Through the interoperability regulations, this access has been expanded significantly for the purpose of accessing statistical data from these databases to carry out risk analyses and vulnerability assessments (Carrera, 2020; Regulation (EU) 2019/818, Article 62 (4); Regulation (EU) 2019/817, Article 66 (4)). Europol's mandate is to support cooperation between EU law enforcement authorities, without having any enforcement powers of its own, and to act as an information hub for criminal intelligence and analysis (Europol, 2018). Similar to Frontex, Europol also has access to the EU's large-scale information systems under specific access conditions and within the limits of Europol's mandate (Vavoula, 2020). Through interoperability, these access modalities have been streamlined and expanded for the purpose of accessing statistical data from these databases to carry out strategic, thematic and operational analyses (Vavoula, 2020:174; Regulation (EU) 2019/818, Article 62 (5); Regulation (EU) 2019/817, Article 66 (5)). Through the access to these databases for operational use, Europol and Frontex can be described as 'end users' of these information systems and thereby as having an operational stake in the design of the interoperability framework.

To ensure that data protection principles are adhered to, the EDPS monitors the activities of EU institutions and bodies that engage in the processing of personal data through interoperability, while the national supervisory authorities are responsible for monitoring that the MS process personal data in a lawful manner (Recital 58, Regulation (EU) 2019/818). Within this supervisory role, the EDPS has the mandated task to supervise the EU's large-scale IT systems since they are operated by an EU agency, namely eu-LISA. As MS also use and have specific responsibilities regarding these systems, the EDPS coordinates this supervisory role with the MS' national data protection authorities (DPAs) through the SCGs, in which EDPS and DPA staff are members and for which the EDPS provides the secretariat (EDPS,

2015:3). Additional to its supervisory role, the EDPS also has a consultative and advisory role to support the European institutions in legislative processes on all matters relating to personal data processing. The EDPS' legal advice and recommendations build on the legal bases of several EU data protection legislations, such as the GDPR and the Regulation (EU) 2018/1725 on the processing of personal data by the Union institutions, bodies, offices and agencies (EDPS, n.d.). While the FRA also has a rights-based mandate, it does not have a specific supervisory role like the EDPS. Instead, the role of the FRA is to largely informational in the sense that its main task is to collect relevant data and publish research and legal opinions on the fundamental rights situation in the EU within the scope given by the Charter for Fundamental Rights of the European Union. Its role regarding interoperability is limited to providing (legal) advice on the fundamental rights compliance of the interoperability legislations through its expertise as well as monitoring the operational implementation of interoperability to evaluate its impact on fundamental rights (Commission, n.d.; Regulation (EU) 2019/818, Article 62 (7); Regulation (EU) 2019/817, Article 66 (7)).

4.3. Stages of the Legislative Process on the Interoperability Framework

While the idea of establishing interoperability between EU large-scale IT systems was officially put forward in a Commission Communication as early as 2005 (Commission, 2005), the legislative process under investigation in this thesis only regained momentum with the Commission Communication "Stronger and Smarter Information Systems for Borders and Security" published in April 2016. This Communication already detailed the objectives of interoperability, a rough outline of the technical components envisioned to achieve it and informed of the Commission's intentions to set up a high-level expert group (HLEG) on information systems and interoperability comprising experts from EU agencies, member states and institutional stakeholders – among them the five advisory bodies selected for analysis in this thesis (Commission, 2016:14-15). Over the course of five meetings, starting in June 2016 and ending in April 2017, the HLEG discussed and produced an interim- and final report on the existing and new IT systems and interoperability (Commission, 2018). Around the same time as EU agencies and advisory bodies published their first statements and reports related to the interoperability policies, the Commission launched a public consultation titled "Consultation on the interoperability of EU information systems for borders and security", which was open for submissions from 17 July until 19 October 2017. The FRA was the only one of the EU agencies that participated in and filled out this consultation (Commission,

2017b). After receiving these inputs, the Commission published its two legislative proposals on interoperability on 12 December 2017 accompanied by an impact assessment report (EPRS, 2019:4). In reaction to these proposals, in April 2018, the FRA, the EDPS, and the Article 29 Data Protection Working Party (now the EDPB) published official opinions on these proposed regulations in light of their fundamental rights and data protection implications respectively. Additionally, eu-LISA conducted a feasibility study of the shared BMS following a request in the HLEG's final report for eu-LISA to "analyse the technical and operational aspects of the possible implementation of a shared biometric matching service" (HLEG, 2017:31; eu-LISA, 2018b:5). As these opinions were being drafted and published, the European co-legislators, the European Parliament and the Council, began to examine the Commission's proposals in the beginning of 2018. Within the European Parliament, the interoperability proposals were assigned to the LIBE committee with MEPs Nuno Melo (EPP) and Jeroen Lenaers (EPP) becoming the rapporteurs for the interoperability proposals on police and judicial cooperation, asylum and migration and on borders and visa respectively (EPRS, 2019:9). The LIBE committee engaged in various meetings with representatives of the EDPS, eu-LISA, Europol, the FRA, and Frontex, before the rapporteurs published their draft proposals. Close to 2000 amendments to the proposals were tabled by MEPs in the LIBE committee before the committee adopted its two final reports on interoperability on 15 October 2018 by a majority of votes (EPRS, 2019:9). Meanwhile, in the Council, the working party on information exchange and data protection (DAPIX) examined the interoperability proposals, focussing largely on the technical implications and challenges of the proposed interoperability architecture. DAPIX also invited representatives of Europol, eu-LISA and Frontex to some of its meetings to provide insights into specific operational questions (EPRS, 2019:10). Ultimately, the Council Presidency and the Parliament reached a provisional agreement in their negotiations on the interoperability proposals in February 2019. Both co-legislators signed the final legislations into EU law on 20 May 2019 and they came into force on 11 June 2019 (EPRS, 2019:10-11).

4.4. Main Criticisms of Interoperability

While the Fundamental Rights Agency (FRA) stresses that interoperability is not inherently mutually exclusive with protecting fundamental rights, the agency's first report on the topic stresses that a number of fundamental rights, particularly those connected to the right to private life and the protection of personal data, are likely to be implicated by interoperability (FRA, 2017:3). This section will briefly outline the fundamental rights and particularly data protection

challenges that the FRA has identified as being created or amplified through the interoperability of large-scale border management databases.

4.4.1. Data Protection issues

One central principle of data protection is data minimisation in the sense that all personal data collected and processed must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" (Article 5, Regulation (EU) 2016/679 (GDPR)). Interoperability impacts the way data is processed and may allow the user to view a larger set of information on a queried individual than would be the case without a connection between databases (FRA, 2017:21). Another central concern is given by the principle of purpose limitation, which states that personal data may only be collected and processed for specified purposes and cannot be used beyond these explicitly defined purposes (Article 5(1)(b), Regulation (EU) 2016/679 (GDPR)). By connecting the previously compartmentalised structures of the underlying information systems, interoperability undermines a principal safeguard against the use of data for illegitimate purposes. The two-step process for streamlining law enforcement access to the information system may undermine the principle of purpose limitation as simply the knowledge that information on a person is stored in a particular database already gives the law enforcement officer information that they otherwise would not have had, representing a function creep (FRA, 2017:21-23). Another element of privacy protection is ensuring the security of data stored in large-scale information systems, which may be endangered by interoperability as it provides increased points of access to the data stored in these systems. Such increased access points may also increase the likelihood of data being unlawfully shared with third countries, which can put the individuals whose data is concerned and their families at risk of persecution. Additionally, since larger amounts of data can be accessed through one access point, interoperability may make such connected databases a more attractive target for hacking attacks (FRA, 2017:25-28). It is also a central concern that the data stored in interoperable databases is accurate and of high quality as interoperability can exacerbate the fundamental rights risk associated with low quality data that informs the decision-making of border guards and law enforcement actors. This is because interoperability allows the use of results that without it may not have been consulted in the first place. However, through comparing data between different systems, data quality can also be improved as inconsistencies are more easily spotted and errors corrected (FRA, 2017:29).

4.4.2. Fundamental rights issues

One of the central concerns of the FRA in relation to fundamental rights challenges associated with interoperability are the rights of the child, as children are a particularly vulnerable segment of persons and their best interests must be at the heart of all actions taken in relation to them. The increased accessibility of children's data in the context of interoperability is a problem insofar as it creates a situation where law enforcement authorities can access the personal data of children that was collected for non-law enforcement purposes. In the case of data collected in Eurodac, children typically do not have a choice in their parents' decision to migrate and seek asylum but are still subject to the possible disproportionate consequences of having one's data retained in large-scale information systems, especially when immigration related offenses are criminalised. Additionally, the reliability of biometric data collected from children is likely to be lower, leading to lower accuracy of children's data. However, the FRA also notes that interoperability can have positive effects on the child protection, particularly when the greater availability of information is utilised to search for missing children more effectively (FRA, 2017:35-37). The FRA also stresses that making EU IT systems interoperable with databases that derive (some of) their data from non-EU MS, such as the Interpol Stolen and Lost Travel Documents Database, can have negative consequences on fundamental rights. For example, repressive regimes may feed information into those databases aimed at preventing political opponents from seeking international protection. Therefore, strict checks and balances must be established for interpreting such data so that street-level end users of interoperable systems do not place disproportionate confidence into such information (FRA, 2017: 40). Furthermore, the increasing availability and accessibility of comprehensive data on irregular migrants can discourage them from exercising their fundamental rights such as the right to education, healthcare, and effective remedy out of fear of apprehension by law enforcement (FRA, 2017:41-42). Finally, the interconnection of large amounts of data also brings with it the possibility of using it for risk assessment and profiling purposes. Such profiling is illegal when it is discriminatory, i.e. when profiling is based on sensitive personal characteristics, such as race, ethnicity, sexual orientation, religious beliefs or health status. Since the biometric data contained in interoperable databases can reveal such characteristics and interoperability increases the amount of sensitive data about a person that is simultaneously accessible, the risk of discriminatory profiling is enhanced (FRA, 2017:43-44).

5. Empirical Results & Discussion

In the following section, I will outline and synthesise the empirical findings from the qualitative document analysis and semi-structured interviews conducted. While the discussion of these empirical findings already connects the relevant evidence to the theoretical expectations identified in the literature review, the results of my case study presented in this chapter will be analysed from a theoretical viewpoint in the subsequent analysis chapter.

5.1. Access to and Participation in the Policymaking Process

As a first step to tracing the influence exertion of non-decision-making policy actors, the researcher has to determine that the necessary condition of access to the policymaking process was present and trace the access channels used by these policy actors. According to the expectation identified in the theoretical framework, more frequent access to the policymaking process in the form of communication with and information transmission to decision-makers is expected to increase the success of a policy actor in shaping the process and policy outcome.

By tracing the activities of the four EU agencies and the one supervisory authority under investigation throughout the interoperability policymaking process, it emerges that some of those bodies accessed the policymaking process more frequently than others. In terms of access to the legislative process, all of these EU bodies were given an official institutional access point to the legislative process through the establishment of the HLEG by the Commission (EPRS, 2019:4), in which they were all invited to participate. However, out of the EU bodies analysed in this thesis, the FRA and the EDPS were the only ones that delivered official expert opinions to the European decision-making institutions. The consultation of the EDPS' opinion was mandatory according to Article 28(2) of Regulation (EC) No 45/2001 [processing of personal information by Community institutions], while the FRA's opinion on interoperability was requested by the Parliament in its preparation for the LIBE committee's draft report on interoperability (FRA, 2018b:5; EPRS, 2019:9). Generally, there was a widespread perception that the FRA and the EDPS accessed and participated in the policymaking process very frequently. One Europol official stated that his perception was that both the FRA and EDPS were "very much visible and also involved from the very beginning" in the discussions on interoperability and that "they always have the right to say something like 'This is too much, this is not proportionate. This might violate some fundamental rights of individual persons.'" (Interview with Klebek, Europol). His perception was that the EDPS and FRA were given the room to voice their concerns, which the Commission then either had to take into account or

explain its reasons not to take them into account (Interview with Klebek, Europol). This view was echoed by a former eu-LISA official who stated that the EDPS was "involved in the process throughout, and they had the opportunity to intervene at all times" and even emphasised that, out of all the agencies involved and even compared to the EDPS, "the most active in that process was probably FRA" (Interview with former eu-LISA official). The view that the FRA was one of the most active participants in the interoperability policymaking process is also supported by the fact that out of all EU agencies, the FRA was the only one to participate in the public consultation on the interoperability proposals set up by the Commission to provide its views and expert opinions on the proposals (Commission, 2017b). Additionally, the FRA also published two lengthy policy papers, one focused on the fundamental rights implications of interoperability specifically and another one on the implications of biometrics and EU large-scale IT systems more generally, in addition to their legislative opinion on interoperability (FRA, 2017, 2018a, 2018b). Taken together, this represents a more frequent official information transmission in the form of various formal information strategies, from providing official opinions and relevant policy papers to participating in public consultations, on the part of the FRA than any other of the involved EU advisory bodies. Such frequent information transmission was perceived as being connected to the FRA's broader fundamental rights mandate, compared to the narrower data protection mandate of the EDPS. This broader mandate, according to one interviewee, provided the FRA with "probably more opportunities within their mandate to input […]; allowed them to intervene on more topics […] [and] gave them a probably more significant voice in many of the conversations because they could input more frequently." (Interview with former eu-LISA official). Thus, the frequency of input to the policymaking process is connected to giving the FRA a 'more significant voice' – in other words, a potentially more influential voice – in the policymaking process. This perception supports the expectation identified in the theoretical framework that a higher frequency of information transmission results in more access and thereby allows a policy actor to exert a higher degree of influence (see Chalmers, 2013:47).

The frequency of access to the policymaking process and to decision-makers seemed to have been equally or even more frequent on the part of eu-LISA. However, its information transmission activities appear to have been much more informal than those of the FRA or the EDPS. According to eu-LISA's director, the agency was present and provided its technical and operational expertise in the relevant committees and working groups of all three European institutions in order to advise them which aspects of the interoperability proposals still needed

to be changed or finetuned (Interview with Garkov, eu-LISA). He described the frequency of contacts with the European decision-making institutions as "very intense" and as "using all the access channels [eu-LISA] had" to establish such contacts (Interview with Garkov, eu-LISA). On the one hand, eu-LISA used formal access channels by establishing a number of working groups on interoperability with the Commission, participating in working groups in the Council and in committees in the Parliament. On the other hand, eu-LISA also frequently used informal access channels such as phone calls, emails, etc. particularly for work done at the expert level (Interview with Garkov, eu-LISA). As both eu-LISA affiliates interviewed for this thesis professed to be satisfied with the policy outcome on interoperability and eu-LISA's contribution to it (Interview with Garkov, eu-LISA; Interview with former eu-LISA official), the agency appears to have attained their goals in the policymaking process. Therefore, this frequent transmission of the agency's technical and operational expertise to the European institutions through a large variety of both formal and informal access channels seems to have allowed eu-LISA to attain its policy goals and preferences.

In contrast to the three bodies described above, Europol and Frontex appear to have accessed the policymaking process less frequently. According to a Europol official interviewed, Europol accessed the policymaking process primarily in the conceptual stage through the HLEG to "think along and to share our expertise and to also explain what we would need from the interoperability concept." (Interview with Burgersdijk, Europol). However, in the legislative stage that commenced once the Commission's interoperability proposals were published and presented to the co-legislators, Europol did not access the policymaking process directly. Rather, the Commission was tasked with managing anything related to Europol and representing Europol's interests in this legislative stage (Interview with Burgerssijk, Europol). This perception was corroborated by the director of eu-LISA, who described Frontex and Europol as "not directly involved in the policymaking process" in the sense that while they were involved in the HLEG, they did not try to access the legislative process when the deliberations between the co-legislators were taking place (Interview with Garkov, eu-LISA). However, despite this lack of, or at least only infrequent and indirect, access to the policymaking process on interoperability in the later stages of the process, Frontex was described as a 'winner' of the process by one Europol official (Interview with Burgersdijk, Europol) as well as academic observers (Galli, 2019; Carrera, 2020). Additionally, both Europol officials interviewed were satisfied with Europol's contribution to and the content of the policy outcome on interoperability (Interview with Burgersdijk, Europol; Interview with

Klebek, Europol). Therefore, a lower frequency of access to the legislative process on interoperability by Europol and Frontex did not appear to lead to them being less successful in shaping the policymaking process, as will be expanded upon in the following chapters.

Overall, by tracing the activities of the EU agencies and one supervisory authority involved in the interoperability policymaking process, a mixed picture emerges on the correlation of the frequency of access and the amount of influence these individual bodies could exert on the policymaking process. On the one hand, frequent information transmission through various access channels appears to have led to a high level of goal attainment in the case of eu-LISA and is also perceived to have increased the degree to which the FRA could shape the interoperability legislations. However, on the other hand, Europol and Frontex accessed the policymaking process much less frequently, particularly after the early, conceptual stages of the process, and still managed to attain their policy preferences in the legislative process on interoperability through their more limited early interventions.

5.2. Framing Interoperability: Security, Technology and Risk Framings

Within this analytical section, I will first outline which types of framings of the new interoperability technology were employed by the four EU agencies and one supervisory authority under investigation, namely Europol, Frontex, eu-LISA, FRA and the EDPS. Crucial to analysing the influence these framings had on the legislative actors in the European institutions – or more accurately their level of goal attainment as influence can only be approximated from confluence in framings employed by advisory body representatives and decision-makers – is the extent to which the framings of the bodies under investigation correlate with the framings employed by decision-makers. When an interest organisation's issue framing correlates with those employed by decision-makers and those used in the legislative text, then interest organisations can be expected to have had an effect on the issue framing surrounding the policy. Such a framing effect can be conceptualised as a part of their goal attainment (Corell and Betsill, 2008:30). Therefore, the last sub-section in this chapter analyses the extent to which the various framings identified in this sub-chapter were adopted by decision-makers in their own discussions of interoperability.

5.2.1. Security Framing

Within the eu-LISA conferences and Parliament debates focussing on interoperability, the security frame was frequently employed both by representatives from the European

Commission, national ministers, and MEPs as well as by representatives from EU agencies such as Europol, Frontex and eu-LISA. This security frame was employed in equal measure as a general reference to interoperability being necessary to ensure and improve internal security, and as a more specific frame. For the latter, the speaker would reference specific terrorist attacks or go into detail on how exactly interoperable databases might improve specific areas of internal security.

A prominent theme in the issue framing surrounding interoperability is the framing of "technology as a security enabler" (Ceyhan, 2008:120) that was identified in the theoretical framework. This was particularly evident in the framing employed by Frontex officials with Frontex' Executive Director, Fabrice Leggeri, emphasising that "interoperability […] will also help fill insecurity gaps" (Leggeri, 2018:10) and a senior Frontex official stating that "technology plays a critical role in assuring security" (Malinowski, 2016:8). This narrative also played a large role in eu-LISA's framing of interoperability as the agency's Executive Director, Krum Garkov, emphasises that "an essential element of an adequate response to these challenges [of new threats such as cybercrime, terrorism and cross-border organised crime] can be summed up with the key words of skills and technologies – equipping law enforcement, border guards and migration officers with the right skills and sufficient technology prepares us for the challenges of tomorrow." (Garkov, 2018:6). Europol's strategy for influencing the policymaking process also seemed to entail framing the need for interoperability in security terms:

> "We [Europol] were not influencing the process, leading away, […] but we were just trying to convince through really tangible arguments. And there were some very tragic and very, you know, based on real stories and examples, it was basically black and white that we're doing something wrong. So, we have to change that, that's why Europol has to also play a role, you know, in the whole process." – Interview with Klebek, Europol

In essence, this quote highlights that Europol sought to shape the policymaking process on interoperability by providing their operational security expertise and experience. By framing the interoperability policy as primarily a security issue, this presentation is legitimating a greater role for Europol in the process of establishing interoperability and in the EU's information system architecture more generally. To rephrase this in theoretical terms, the framing of interoperability in security terms legitimates empowering Europol over other

competing stakeholders in the interoperability sphere (see Harcourt, 1998:370 as cited in Eising et al., 2015:517). Furthermore, the above quote also explicitly frames the topic of interoperability through tragic case examples. At the heart of this security framing was the narrative that past terrorist attacks in Europe could have been prevented through the interoperability of different European information systems, as exemplified in the following statement from a Europol official:

> "I think that the drivers behind [starting the policymaking process on interoperability] was the series of terrorist attacks that we've seen in 2014, 2015. Those were really the elements where we identified that we did have a lot of information on the perpetrators in different databases, but that they managed to get through all the safety measures we had because they were using false names and not identifying themselves by biometrics. So, our information position was there, but it was fragmented and was not using strong and reliable types of data to protect ourselves." – Interview with Burgersdijk, Europol

In this quote, the Europol official is framing the interoperability of European databases as a necessary step to "protect ourselves" by pointing out how the information gaps that interoperability seeks to close inhibited law enforcement actors from stopping the series of terrorist attacks taking place in Europe in the mid-2010s. Therefore, he frames the terrorist attacks in 2015 as "not only the triggering events [for the interoperability legislations], [but] also [as] containing the details of what we had to look at […], underlining the importance that we would have to interconnect and know who is who" (Interview with Burgersdijk, Europol). In both of my interviews with Europol officials, the interviewees referred to terrorism and specific instances of terrorist attacks frequently to highlight the need for interoperability. While such a justification for interoperability is borne out of their professional experience and expertise in cross-border law enforcement, these frequent references to dramatic examples of terrorism and attacks still represent a discourse of fear that is used to justify the necessity of expanding the use of emerging technologies as outlined in the theoretical framework. According to Fisher and Monahan (2011:549), employing such discourses of fear serves to provide a strong rationale for building and using new technologies that are praised for their "dual-use" of improving efficiency and security. Such a security framing based on discourses of fear was also referenced by a former eu-LISA official as a major reason for why the silo-

based compartmentalisation of the EU's large-scale IT systems was abandoned in favour of establishing interoperability between those databases:

> So, the idea that, you know, for example, what's done by the police in the territory and what's done at the border are different things and there's no relationship with the different systems [changed]. […] It's all part of Home Affairs and what they do there has impacts on what's done elsewhere, and I think that thinking came around a lot because of maybe the terrorism elements, you know, terrorist attacks, where it was noted that... For example, the Berlin market attack: You know, this guy had, I think, if I recall correctly, what we call an alert in SIS. This guy had also crossed a lot of borders, internal and external, [so he was in] the visa system. And there were some instances where even the asylum system had come into play. […] So, I think it advanced thinking a little bit towards that there are dependencies and interdependencies between these systems... or between these fields and that should be reflected in the systems to an extent where it is sensible as well. – Interview with former eu-LISA official

In essence, what the former eu-LISA official is emphasising here is that specific instances of terrorist attacks led to a reframing of the silo-based architecture of European databases from being regarded as necessary to guard the data protection principle of purpose limitation to being viewed as a hinderance to ensuring internal security and preventing terrorist attacks. This demonstrates that a security framing was a dominant factor in portraying interoperability as a necessary technology in the EU's Home Affairs architecture to ensure security.

5.2.2. Technology Optimism Framing

Easily the most prominent frame used in the discussions and policy documents regarding the interoperability legislations is one of technology optimism. Within the eu-LISA conferences, this technology optimism frame permeated the discussions regarding both technology in general as well as interoperability specifically. New technologies for the EU information architecture, such as interoperability, were frequently described in terms of the increased efficiency and effectiveness of information systems they are envisioned to generate, the speeding-up of working processes as well as in terms of making these processes easier, more systematic and more user-centric. These issue framings are clearly part of the technology optimism narrative identified in the theoretical framework, which frames technology as

positively contributing to efficiency, effectiveness and control (see Bauer and Bogner, 2020:499-500, 503-504; Vermeersch and de Pauw, 2017:56). Interoperability was also frequently described as enabling relevant actors to be better able to deliver on a variety of policy goals – it is presented as leading to better systems utilisation, better use of IT, better information, better decision-making and better solutions in general. This focus on portraying the interoperability of EU databases as making a variety of processes 'better' contributes to a very positive and optimistic framing of this technology and technology in general. Among the EU agencies, representatives from eu-LISA, Frontex and – to a somewhat lesser extent – Europol employed such technology optimism framings regarding interoperability most frequently. Frontex' Executive Director, Fabrice Leggeri, demonstrated optimism about "[becoming] smarter through technology" and "[harnessing] the power of transformation that innovative new technologies can offer" (Leggeri, 2018:9, 10) to address several challenges in the field of external border management. As Executive Director of eu-LISA, Krum Garkov generally provides the opening speech to the eu-LISA conferences and routinely employs a technology optimism narrative in this opening. This is best illustrated by the report on Garkov's opening speech in the 2017 eu-LISA conference, in which he is paraphrased as having stated the following:

> "While for previous revolutions the engines were water, steam, electricity and electronics, when it comes to the digital revolution, the engine is data, which is the main fuel that creates value. Mr Garkov stated that how we use this data will be the measure of our success. We have to work even smarter, customise tools and services and use them best to serve the demands of society." – Garkov, 2017:6 (indirect quote from eu-LISA 2017 conference report)

The essence of the technology optimism narrative is evident in this statement as it portrays technology as revolutionising, creating value and, crucially, as capable of being utilised to positively contribute to society. As demonstrated in his statement, the technology optimism narrative surrounding interoperability is often characterised by a business-centric presentation of the benefits of interoperability with a focus on value creation or the 'added value' that EU information systems and interoperability can generate (eu-LISA, 2018a:19). This emphasis on business benefits mirrors the technology optimism narrative identified by Fisher and Monahan (2011:548), which focusses primarily on the 'returns on investment' that new technologies are expected to bring. In a similar vein, a Europol representative interviewed for this thesis also

emphasised that the interoperability policymaking process, in his opinion, "was business-oriented" in the sense that it responded to business needs and operational (information) gaps (Interview with Klebek, Europol). The technology optimism narrative was also employed by eu-LISA in a more specific manner, for example when a discussion moderator from eu-LISA listed the expected benefits of an EU single search interface as including "workflow improvements, facilitation of interrogation of new data systems and the introduction of standardized analytics" (Carolan, 2016:21). Cost-saving efficiencies and increasing effectiveness were also cited as the major benefits to be reaped from making the EU's large-scale IT systems interoperable by a former eu-LISA official:

> "But a second [benefit] was probably most prominent with the biometric matching service, so the shared BMS. What was probably the case across the systems is consolidation of infrastructure to save costs and bring efficiencies. That was something eu-LISA, as kind of its own organisation and the technical administrator of the systems, I think, quickly realised that just having one shared biometric matching system rather than - at the time it was three, but it would soon be five or six with the new systems – could save a lot of money, could be more effective, could mean that as we ran our systems there was a biometric expert per system, in each system team." – Interview with former eu-LISA official

Thus, the technology optimism framing by eu-LISA was built on very specific expectations of how interoperability components could make their operational work more efficient and cost-effective.

Senior representatives from both eu-LISA and Frontex emphasised particularly the notion that interoperability between databases would optimise decision-making. Thereby, interoperability was portrayed as providing not only operational benefits, in the form of allowing border guards to make decisions quicker and more easily, but also wider societal benefits since it was presented as helping border guards make the 'right' decisions. In the words of Frontex' senior strategic advisor, "with interoperability, we are getting different layers of information about a person and gradually the capacity to make the right decisions is increasing." (Ares-Baumgartner, 2018:24). Among Europol representatives such technology optimism narratives were somewhat less pronounced although representatives did present the view that "interoperability is increasingly one of the key drivers of progress and success in the JHA

field." (Burgersdijk, 2016:14). In the two interviews with Europol representatives conducted for this thesis, technology optimism frames were limited to emphasising the simplifying operational benefits of "easier access and more streamlined access to various databases" (Interview with Burgersdijk, Europol) and that "it will be relatively easy to run a simple cross-check whether there is anything in the large systems on this person" due to interoperability (Interview with Klebek, Europol). Overall, this demonstrates that the three technical and operational EU agencies involved in the policymaking process, especially eu-LISA and in a more general framing also Frontex, framed interoperability through a lens of technology optimism by ascribing the virtues of enabling greater efficiency, effectiveness, better decision-making, etc. to the new technology.

5.2.3. (Social) Risk Frame: Fundamental Rights and Privacy

Apart from a security and technological issue framing, a privacy framing was also often employed by policy actors in the eu-LISA conferences and Parliament debates on interoperability as well as in the policy documents on interoperability. In particular, this frame was employed by the large majority of actors involved, from decision-makers to representatives from all involved EU agencies, through frequent references to the importance of data protection as well as specific data protection principles, such as the requirements of purpose limitation, necessity and proportionality as well as well-defined data access rights. However, despite the relative frequency with which data protection was referred to, this frame was often employed in a relatively generic manner. This took the form of, for instance, a speaker finishing an elaboration of a concept related to interoperability with a qualifier such as "in line with the legal constraints" or "in line with data protection and security regulations" (Rozenburg, 2017:27; Ruginis Andrei, 2017:33) without elaborating on these data protection concepts further. The same applies, even more pronouncedly, to fundamental rights other than data protection and privacy that may be implicated by interoperability. While various speakers referenced the importance of any interoperability legislation being in full compliance with fundamental rights in a generic manner, specific fundamental rights challenges (apart from personal data protection) associated with interoperability were almost exclusively addressed by representatives of the FRA and to a lesser extent by Commission officials. As addressed in the theoretical framework, such generic references to the data protection and fundamental rights frames can be viewed as so-called 'meta-frames' (Bauer and Bogner, 2020:503). This means that while data protection and fundamental rights more generally are considered default

elements that need to be addressed, this is often done in a standardised and abstract manner and without linking these 'virtue' frames concretely to the topic of discussion.

However, when data protection and fundamental rights were addressed in a more specific manner, it makes sense to distinguish between the two narratives common to the social risk frame identified in the theoretical framework (Bauer and Bogner, 2020:500-501). The first narrative, which presents risks to privacy and other rights as controllable through the anticipation and safeguarding against potential risks, was by far more dominant in the discussions surrounding interoperability. Within this narrative, risks to privacy are consistently discussed by presenting strategies and precautions taken to mitigate any potential risks for privacy that may arise through interoperability. Thereby, the signal is sent that these risks are not ignored or downplayed, but instead responsibly prepared for. In the case of eu-LISA, this narrative was employed through representatives highlighting that the agency was ensuring that visibility, transparency and respect for privacy are built into the interoperability architecture by following 'privacy by design' principles (eu-LISA, 2017: 33) and taking precautions "to anticipate and minimise risks" (Syrigos, 2018:23). The concept of 'privacy by design' – which the EDPS (2018:19) recommended to be followed when making systems interoperable – fits well in the first social risk narrative as it implies that the risks a technology poses to privacy are manageable and can be mitigated through the right system design. Indeed, eu-LISA's executive director stated that a study the FRA conducted on the effects of interoperability "demonstrated what eu-LISA also advocated for a long time, namely that, today, technologies are not threats for fundamental rights and for privacy" (Interview with Garkov, eu-LISA), exemplifying the view that any risks of technologies to fundamental rights can be eliminated.

Unsurprisingly, as it is contained in their mandate to ensure that EU regulations are fundamental rights/data protection compliant, the social risk frame was most frequently employed by the FRA and the EDPS. In the foreword to a FRA publication on fundamental rights and interoperability, the first narrative of the social risk frame was exemplified:

> "Interoperability does not intrinsically violate fundamental rights. However, adequate safeguards and mechanisms to protect the rights set out in the EU Charter of Fundamental Rights are essential." – FRA, 2017:3

This statement frames interoperability as a technology that, while it holds certain risks and threats for fundamental rights, only holds risks which are controllable and can be managed through safeguards built into the technology. Accordingly, in the 2017 eu-LISA conference, a

FRA representative challenged the view that fundamental rights hinder data exchange in favour of arguing that interoperability can be effectively managed to be in full respect of fundamental rights. She also argued for the need for ex-ante and ex-post fundamental rights impact assessments, framing the risks of interoperability as controllable through risk assessments and the right system design (Goodey, 2017:48-50). It is notable that both the FRA representative at the eu-LISA conference as well as the director of the FRA, Michael O'Flaherty, in his speech to the HLEG, highlighted not only the risks interoperability may pose to fundamental rights, but also the benefits for the protection of fundamental rights it can bring. O'Flaherty noted that "interoperability can provide new opportunities to offer more robust and timely protection to those entering the EU" and then outlined the ways in which interoperability can positively impact the detection of missing or trafficked children, improve security by fighting terrorism and crime, as well as help protect asylum seekers who have difficulties proving their identity (O'Flaherty, 2017). Thus, both the director of the FRA and the representative attending the eu-LISA conference presented the narrative that the benefits the interoperability technology can bring to the protection of fundamental rights may outweigh the risks to those rights – as long as the risks are adequately safeguarded against through precautions built into the system. Overall, the FRA's use of the risk frame is predominantly focused on outlining the necessary safeguards to be built into the interoperability system to guard against specific risks for fundamental rights.

Similarly, the EDPS representative at the 2018 eu-LISA conference emphasised that "data protection is about responsible data use" and that the organisation and data protection authorities in general "are not interested in keeping anyone from doing their work; they just want to make sure that it is done in an accountable and responsible way in practice" (Langfeldt, 2018:38, 39). According to an IT expert from the EDPS, 'privacy by design' was also considered a key aspect that the EDPS wanted to see included in the final legislation, stating that "all these key elements of privacy and data protection have to be designed into the system." (Interview with Kampouraki, EDPS). Thus, the EDPS also employed the first social risk narrative to frame the risks of interoperability to data protection as manageable as long as it is designed and implemented in a responsible and accountable way. However, it is notable that the EDPS was the only policy actor who also repeatedly employed the second social risk narrative identified in the theoretical framework. This second risk narrative is a counter-narrative to the first one and frames the new technology in a rhetoric of scepticism around the assumption that the full impact and repercussions of interoperability can be fully anticipated

and controlled (see Bauer and Bogner, 2020:500-501). Within the EDPS' opinion there are many instances of this sceptical social risk narrative, starting with the EDPS' warning that interoperability would "mark a 'point of no return'" (EDPS, 2018:10) in the sense that not only the technical and operational functioning of the EU's large-scale IT systems would be irreversibly changed, but also the interpretation of legal principles in this area would change. Additionally, the EDPS was the only one out of the EU agencies and advisory bodies involved in the interoperability policymaking process to outright question whether "the data exchange [through interoperability] is necessary, politically desirable or legally possible" (EDPS, 2018:6) and demanded that "it should be demonstrated that no other means which would be less invasive are available to achieve the envisaged purpose(s)." (EDPS, 2018:8). The EDPS, thus, questions the necessity of using new technologies, instead of considering other, less risky solutions for the challenges the technology is supposed to solve. This counters the framing – typical for the first social risk narrative – that the benefits of such a technology outweigh its risks. It also represents a counter-frame to the 'solution narrative' advanced by the technology optimism framing by challenging the notion that interoperability is the only possible solution to achieve the purposes that are used to justify the adoption of the interoperability technology (see Bauer and Bogner, 2020:500). Such a counter-framing is also apparent in the concerns voiced by the EDPS that interoperability is treated more as a technical, rather than a political choice, and that the mere technical feasibility of a technology is used to justify its use (EDPS, 2018:6, 8, 10). In their opinion, the EDPS emphasises that "making exchange of data technically feasible becomes, in many cases, a powerful drive for exchange these data. One can safely assume that technical means will be used, once they are made available; in other words, the risk is that in such case the means justify the end." (EDPS, 2018:6). The EDPS expands on this point in another section of their 2018 opinion by stressing that "[t]echnology should always come in support of policies and user needs, not the other way around. What is technically feasible might not necessarily be legally justifiable or ethically desirable." (EDPS, 2018:8). Those quotes embody a social risk framing of interoperability, whereby the mere existence of a technology is framed as a powerful driver of further changes (and risks) that are not easily controllable once set in motion. This is further illustrated by the warning given by an EDPS representative at a conference on interoperability that by building systems to be interoperable, there is an increased risk for further function creep and that "one should not become too greedy" (Langfeldt, 2018:39). In an interview conducted for this thesis, an EDPS official also framed the interoperability technology as a steppingstone for further development in the use and exchange of data from EU's IT systems, by calling interoperability "a step towards more

surveillance" with the consequence that eventually any TCN is in at least one of the databases of the EU (Interview with EDPS official). Such a 'surveillance perspective' is a typical feature of the privacy framing, which frames emerging technologies, particularly those in the security realm, as steps towards mass surveillance (see Vermeersch and de Pauw, 2017:52). In their opinion on interoperability, the EDPS (2018:9) also framed interoperability through a lens of securitisation by arguing that the growing tendency in EU policymaking to associate migration management with internal security and terrorism both in practice and discursively may contribute to blurring the boundaries between those (formerly) separate fields. Thereby, the EDPS frames interoperability as establishing a 'continuum of threats' between migration management and internal security, which "may even contribute to creating assimilation between terrorists and foreigners" (EDPS, 2018:9). This view was echoed in an interview with an EDPS official conducted for this thesis, who argued that by interconnecting EU databases one is mixing different purposes together, which is "a bit like considering each asylum seeker or each migrant as a potential criminal." (Interview with EDPS official). Thereby, interoperability is framed as a risk to TCNs by arguing that this technology may indiscriminately criminalise foreigners. Another characteristic of the second narrative of the social risk frame is the emphasis put on possible unintended consequences, and uncertainties associated with the impact of the technology on fundamental rights. In a 2018 press release, the EDPS (2018b:1) employed such a framing by stating that "the Proposals add another layer of complexity to existing and future EU databases with unclear implications for data protection and other fundamental rights and freedoms, as well as for the governance and supervision of the databases." By emphasising that the societal, legal and operational implications of interoperability are still unclear at this point in the legislative process, the EDPS frames interoperability as a risky and unpredictable new technology. Overall, the EDPS' framing of interoperability, at the very least, implies it to be a societal, legal and ethical risk with unclear implications that may not be possible to be mitigated by building safeguards into the system.

5.2.4. Goal Attainment

Crucial to utilising such issue framing as an indicator of the EU agency's goal attainment, and as an approximation of their influence, in the interoperability policymaking process is whether their narrative correlates with the narrative employed by decision-makers and in legislative texts. Broadly, this seems to be the case in the interoperability policy for the security and the technological optimism framing as well as the first, more optimistic, social risk framing narrative.

Security Framing

During the 2016 eu-LISA conference, the Commissioner for the Security Union, Sir Julian King, justified the need for interoperability according to the same narrative that was employed by Europol officials by stating that "the horrific terrorist attacks of the past year […] highlighted that available, accurate and complete data is crucial for law enforcement authorities." (King, 2016:2). Additionally, he also used the terrorist attack on a police station in Paris in 2016 as an illustrating example for blind spots that would be solved through interconnecting databases (eu-LISA, 2016:3). Similarly, the rapporteur for the interoperability proposal in the field of police and judicial cooperation, asylum and migration in the LIBE committee of the Parliament, Nuno Melo (EPP), illustrated the need for interoperability with examples of past terrorist attacks in Germany and France, where the perpetrators were registered under multiple different identities in various European databases (Melo, 2019). It is notable that this justification was challenged later in the debate by MEPs from left-wing factions, who pointed out that in the German example, the perpetrator had already been known to German police as a potential danger to security before he carried out his attack. These MEPs argued that his multiple identities in different systems were not the real problem since the relevant authorities knew he was a threat, even without interoperability, and still failed to act (European Parliament, 2019). Similarly prominent was the "technology as a security enabler" framing being employed by European decision-makers, which echoes the framings employed particularly by Frontex and eu-LISA officials. From the side of the Commission, it was made clear by the Commissioner for the Security Union that Europe needs to "become quicker and smarter" to build an effective security union, while the Commissioner for Migration, Home Affairs and Citizenship stated that "going digital in security is […] a must to effectively target security threats" (Avramopoulos, 2017:11). From the side of the Parliament, particularly MEPs from conservative groupings, such as from the EPP or the ECR group, also justified the need for the legislation in security terms and framed interoperability as a security enabler (European Parliament, 2019). The rapporteur for the interoperability proposal, Nuno Melo (EPP), emphasised the speed, efficiency and systematic manner in which interoperability can provide access to information that he portrayed as crucial to control the EU's borders and fight against crime and terrorism (European Parliament, 2019). By emphasising the speed and efficiency of interoperable technology as well as its necessity for ensuring security from crime and terrorism, the rapporteur combines the "technology as a security enabler" narrative from the security frame with a technology optimism frame.

Technology Optimism Framing

Such a technology optimism framing of interoperability, was generally taken up enthusiastically by Commissioners and Commission officials. Officials from DG HOME employed this frame by describing the elimination of silos through interoperability as overcoming various operational issues "by making checks faster, easier and more systematic" (Rozenburg, 2017:28) and as "making systems work better, individually and together to provide for a seamless experience for all user groups" (Rinkens, 2016:11). This rhetoric of interoperability making operations work better and more efficiently was also taken up in the Parliament, particularly by the conservative rapporteurs for the two interoperability proposals as well as a representative of the liberal ALDE group. While being more cautiously optimistic towards the new technology, social-democrat MEPs from the S&D group also highlighted the increased effectiveness and efficiency gains interoperability brings (European Parliament, 2019). Additionally, just as in the rhetoric of eu-LISA and Frontex officials, the envisioned improvement for the decision-making capability of border guards through interoperability featured prominently in the framing of interoperability by Commission representatives. For instance, the Commissioner for the Security Union remarked that "all parties need accurate information from information systems to make the right decisions at the right time" when discussing interoperability (Avramopoulos, 2017:11). Commission officials were more specific about the decision-making benefits expected from interoperability components such as the ESP. They described the ways in which the ESP could facilitate easier decision-making for border guards and stated that the ESP would "work its 'magic' and give the answer straight away" (Rozenburg, 2018:42). By describing the interoperability technology in such superlative terms of working its 'magic' and ascribing it the unequivocal ability to make the right decisions, this technology is portrayed as the uncontestably optimal solution to a range of policy challenges. Such a fixation on a technology as the ultimate, fix-all solution can obscure the actual causes of the societal and other challenges it aims to tackle and leads to other, less invasive, solutions to be omitted from consideration (Bauer and Bogner, 2020:500).

A combination of the "technology as a security enabler" narrative, the fear discourse of terrorist attacks, and the technological optimism and efficiency frame is also apparent in the explanatory memorandum of the interoperability proposal, which outlines its context:

> "In the past three years, the EU has experienced an increase in irregular border crossings into the EU, and an evolving and ongoing threat to internal security as demonstrated by a series of terrorist attacks. EU citizens expect

> external border controls on persons, and checks within the Schengen area, to be effective, to enable effective management of migration and to contribute to internal security. These challenges have brought into sharper focus the urgent need to join up and strengthen in a comprehensive manner the EU's information tools for border management, migration and security." – European Commission, 2017a:1

In this segment, the need for action is justified by reference to dramatic examples in the form of multiple terrorist attacks, exemplifying a discourse of fear. Subsequently, the expansion of EU information technology is presented as the effective solution to such insecurities, representing a 'solution narrative' that is typical for the technology optimism frame, and as necessary to ensure security (Bauer and Bogner, 2020:500, 504). Altogether this analysis of the technological optimism and security framing present in the discourse surrounding the interoperability proposal demonstrates that the use of these narratives by the three EU agencies Europol, Frontex and eu-LISA correlates with the narratives employed by political decision-makers from the Commission and particularly conservative and liberal decision-makers in the Parliament. Additionally, both the security and technology optimism framings feature heavily in the legislative texts on interoperability as the are frequently used to justify the necessity of establishing interoperability between EU databases. Following Corell and Betsill's (2008:30) definition of interest organisations' goal attainment through issue framing, this indicates that these EU agencies attained their goal through the policy issue of interoperability being widely conceptualised as a security issue and an innovative technological solution to various operational, societal and security challenges.

Social Risk Framing

Overall, the legislative actors from the European institutions predominantly employed general meta-frames in referring to the importance of fundamental rights and data protection and the first narrative of the social risk framing, which frames risk factors as manageable through careful system design. The exception to this are primarily left-wing MEPs from the GUE/NGL and Greens/EFA groups in the LIBE committee of the Parliament, who often employed the second narrative of the social risk framing, namely that the risks of the interoperability technology outweigh any benefits it may bring. The first narrative of interoperability being a manageable social risk was clearly taken up by the then Estonian Interior Minister and member of the JHA configuration in the Council of the EU. He encompassed this social risk narrative in a metaphor:

> "When developing a digital strategy, it must be considered that technology is only a tool, and every tool can have hiccups. Like skyscrapers have stairs, similar measures need to be in place for IT" – Anvelt, 2017:9

Here, he explicitly references the risks of interoperability – the 'hiccups' – but argues that by putting in place precautionary measures, possible failures of the technology can be mitigated. Taking a more direct approach, the Commissioners closely involved in the legislative process emphasised repeatedly that the legislation is compliant with fundamental rights and data protection principles. In a speech to the LIBE committee, Commissioner King stated that "in doing all of this [work on the interoperability regulations], we have been very careful to maintain purpose limitations and safeguard those fundamental rights. Data processing will be limited to what is strictly necessary and proportionate. No new kinds of information will be collected for the purpose of interoperability." (King, 2019). The Security Commissioner also framed any potential risks to such rights as having been sufficiently mitigated through safeguards by stating that throughout the legislative process on interoperability it was made sure "that fundamental rights will be fully respected, that interoperability is no big brother or super database and that nothing changes in terms of the access of each official or authority to the underlying data in our information systems." (Avramopoulos, 2019). The Commission officials involved in the legislative process also employed an optimistic risk framing by stressing that technologies can always take account of and be designed to be compatible with fundamental rights considerations, providing illustrating examples on how specific fundamental rights concerns can be mitigated operationally and by design (eu-LISA, 2016:11, 2018:50). In the European Parliament, almost all member of the LIBE committee that spoke in the debate on adopting the interoperability proposals mentioned the importance of data protection and fundamental rights. While the rapporteurs and MEPs from conservative and liberal Europarty groupings tended to frame the interoperability regulations as successfully safeguarding fundamental rights and guaranteeing the protection of personal data, social-democrat MEPs showed themselves more cautiously optimistic (European Parliament, 2019). They framed their discussions of the risks of interoperability in terms of all the work they put into ensuring that fundamental rights were sufficiently protected in the regulation. In the words of MEP Miriam Dalli on behalf of the S&D group:

> "That's why as S&D we were pushing to include very strong wording on non-discrimination and fundamental rights provisions, together with specific references that will protect our citizens' privacy and their personal data. […]

> We need to ensure that in our quest to address security issues, we do not sideline rights that our citizens have worked hard for, including the right to protect fully the data. A balance can and should always be reached." – MEP Miriam Dalli (S&D), 2019

By emphasising that a balance between security and privacy considerations can be reached in the context of interoperability, she employed the first social risk narrative, which presents the risks of interoperability as manageable as long as sufficient safeguards are included in the legislations governing the technology. This approach to the risks presented by interoperability also appeared in the legislative work done particularly by the S&D group in the LIBE committee. Compared to other political groupings in the LIBE committee, MEPs from the S&D party cited the EDPS' 2018 opinion disproportionately often as their justification to amend the legislative proposal on interoperability in a certain way. Their proposals for amendment justified with reference to the EDPS opinion ranged from arguing against streamlined law enforcement access to the databases in favour of continuing the cascade approach, to the automatic deletion of stored identity data and to granting supervisory authorities access to logs stored by the interoperability components for data protection and monitoring purposes (European Parliament, 2018). These proposals for amendment show that the S&D MEPs' legislative actions were shaped by the risk framings included in the EDPS' 2018 opinion, but that they still perceived those risks as manageable and controllable by amending certain sections of the proposals to build in data protection safeguards. Therefore, the EDPS was evidently successful in having its framing using the first social risk narrative taken up by social-democrat decision-makers in the EP.

Interestingly, the second social risk narrative – employed almost exclusively by the EDPS among the EU advisory bodies involved in the policymaking process – was adopted predominantly by MEPs from the GUE/NGL and Greens/EFA European political groups, which represent green, socialist and (far) left-wing political orientations. Representatives of both of these groupings even explicitly referenced the risk framing of the EDPS in their debate speeches in the LIBE committee.

> "Der Europäische Datenschutzbeauftragte hat uns gewarnt: Solch ein Schritt markiert einen Punkt, an dem es kein Zurück mehr gibt. – MEP Romero Franz (Greens/EFA), 2019

> Und dazu sagt der EDSB, wie auch mein Vorredner [Anm.: Romero Franz], das ist ein point of no return. Wird einmal die Zweckbestimmung aufgehoben, ist sie im Eimer, dann ist sie weg, um es mal so auszudrücken – und damit auch die Daten der Bürger eine leichte Beute für den Staat, der umfassend überwachen kann.“ – Cornelia Ernst (GUE/NGL), 2019

In the above quotes both MEPs explicitly refer to the statement of the EDPS that interoperability marks a ‘point of no return’ to underline their arguments. Thereby, they are using the expert status of the EDPS as a data protection authority to emphasise their warnings about the impacts of interoperability – in Ernst’s case, she uses it to emphasise her warning that interoperability would facilitate a European surveillance state. This is one of the most direct ways, European decision-makers have adopted one of the framings of the EU advisory bodies in their own rhetoric on interoperability. In this case, these left-wing MEPs have adopted the second narrative of the risk framing employed by the EDPS by repeating the framing of interoperability as a ‘point of no return’. In her role as the shadow rapporteur for the interoperability proposal, Cornelia Ernst even used a quote from the EDPS’ opinion on interoperability to justify her proposal for rejection of the Commission’s interoperability proposal (European Parliament, 2018:3). In the justification of this proposal for rejection, she cited the EDPS:

> "Interoperability is not primarily a technical choice, it is first and foremost a political choice to be made, with significant legal and societal implications in the years to come. Against the backdrop of the clear trend to mix distinct EU law and policy objectives, as well as granting law enforcement routine access to non-law enforcement databases, the decision of the EU legislator to make large-scale IT systems interoperable would not only permanently and profoundly affect their structure and their way of operating, but would also change the way legal principles have been interpreted in this area so far and would as such mark a ‘point of no return’." – EDPS, 2018:30 cited by Cornelia Ernst in European Parliament, 2018:3

This is a substantial proposal because it does not simply seek to amend the Commission’s proposal but calls into question its entire foundation and seeks to reject it altogether. As such it can be viewed as an attempt to reframe the narrative from focusing on how to minimise data protection and fundamental rights issues contained in the proposal to a narrative that seeks to

overturn the proposal entirely instead of improving the finer details. In other words, by filing a proposal for rejection instead of a proposal for amendment, MEP Ernst reframed the discussion on interoperability from the first social risk narrative, which portrays interoperability as manageable through building appropriate safeguards into the legislation, to the second social risk narrative, which portrays new technologies as dangerous. While the MEP's proposal for rejection was not successful, it does show that the more sceptical risk framing used by the EDPS in their opinion on interoperability influenced and was used as justification for the political actions of some decision-makers.

Additionally, several left-wing MEPs, even a social-democrat MEP who was ultimately in favour of the interoperability legislations, echoed concerns brought up by the EDPS that migrants and other foreigners may be framed as security risks through interoperability. One MEP from the GUE/NGL group argued that the proposals facilitate a general presumption of guilt by blurring the boundaries between migration, crime and terrorism and treating everyone recorded in the EU's border management databases as potential criminals. While not wording his concerns quite so strongly, a MEP from the S&D group highlighted the reservations against interoperability voiced by the FRA and the EDPS and warned that it should never be assumed that TCNs are an inherent security risk for the EU (European Parliament, 2019). This implies that the risk framing of the FRA and EDPS in this regard was taken up, at least to some extent, across all left-wing groups in the European Parliament, even those who eventually voted in favour of adopting the interoperability proposals. Both of the above quotes frame interoperability as posing a (potential) risk of criminalising TCNs with the former linking this to concerns brought forward by the FRA and EDPS. This implies that the EDPS' framing of interoperability as potentially establishing a migration-security continuum informed the decisions of a range of left-wing decision-makers in the Parliament. Such an influence of the EDPS' framing is also reflected in a proposal for amendment filed by S&D MEPs to reword a section in the regulation in order to linguistically separate migration from internal security matters. Again, this proposal was justified by reference to the EDPS recommendation not to conflate migration management and internal security measures (European Parliament, 2018:112). However, this amendment was ultimately unsuccessful.

Overall, particularly far left-wing MEPs applied a very sceptical risk and a very strong privacy framing to interoperability, framing the technology as building up a surveillance state at EU level (Lopes, 2019; Ernst, 2019). This exemplifies a strong 'surveillance perspective' typical for the privacy framing of technology. While such a surveillance framing was not explicitly

employed by the EDPS in their official publications and communications on interoperability, it may have still been prevalent in informal discussions of the topic as one of the EDPS officials interviewed for this thesis also framed interoperability as a "step towards more surveillance" (Interview with EDPS official). Interestingly, in an interview conducted for this thesis, the Executive Director of eu-LISA implied that this more sceptical narrative of the social risk frame may have been more prevalent among European decision-makers in the first rounds of discussions on the interoperability of EU large-scale IT systems in 2005:

> "And I shall say that interoperability is in the agenda of eu-LISA's existence but in the past the legislators had a different view on interoperability. They looked at it as something that is dangerous and shouldn't be allowed, but the developments in the last years, I think, had political influence on their understanding about the benefits of interoperability and the capabilities of modern technologies. […] [It] is an evolution in thinking. If you now go to the European Parliament and speak with different political groups, none of the groups, even the most extreme left or right, will deny the benefits of interoperability. Of course, you have a lot of different views with regards to implications of interoperability on data protection and privacy, but that's a legitimate concern when we speak about the use of technologies broadly. There is a consensus, I would say, between the policymakers that interoperability is something necessary and beneficial for internal security and border management today and in the future." – Interview with Garkov, eu-LISA

In this statement, Garkov suggests that, while a sceptical risk framing of interoperability as something dangerous was prevalent in the early discussions on interoperability among European legislators, this framing had all but disappeared in the recent legislative process on interoperability. His perception of widespread support and understanding of the benefits of interoperability does need to be viewed critically, as the above analysis demonstrated that particularly the (far) left-wing groupings in the Parliament have largely not joined into a consensus that interoperability is necessary or beneficial. However, overall, it seems that while a sceptical risk narrative of interoperability may have dominated in the discussions on interoperability in the mid-2000s, this appears to have shifted largely – with the exception of a range of left-wing MEPs – towards the more optimistic risk narrative that frames the risks of interoperability as controllable through the right system design. This, along with the security

and technology optimism framings also being dominant among many of the involved EU agencies and decision-makers alike, has likely contributed to the successful adoption of the interoperability regulations in the most recent round of interoperability discussions.

5.3. Perceptions and Evidence of EU Agencies' and Supervisory Body's Influence

In very general terms, the perceptions among the EU agency and supervisory authority staff with whom I conducted interviews about the interoperability policymaking process for this thesis, were that all actors had the opportunity to participate in the policymaking process and provide their input. In the following section, I will trace the participation, policy preferences and influence perceptions of the five EU advisory bodies involved in the legislative process on interoperability on which this research is focused.

5.3.1. eu-LISA

In terms of goal attainment, eu-LISA appears to have been a very successful actor in the process establishing the interoperability framework. Both the Executive Director of the agency as well as the former eu-LISA staff member interviewed stated that they were very satisfied with the outcome of the legislative process on interoperability (Interview with Garkov, eu-LISA; Interview with former eu-LISA official). The agency's director summarised his perception on the goal attainment of eu-LISA on the interoperability legislations:

> "[S]ince the start of eu-LISA, I personally and the agency as a whole was a strong advocate of the need for interoperability. At that time, of course, interoperability was considered, well, on a much smaller scale, something like exchange of data between a few systems rather than this comprehensive architecture that we have in place. So, in that sense, I'm very satisfied that the EU and EU policymakers recognised the need to change the approach towards utilising capabilities of modern technology, the digital technologies, for the purposes of internal security, border management and migration management." – Interview with Garkov, eu-LISA

This demonstrates that eu-LISA was a strong proponent of interoperability since its inception and attained, or even exceeded, its goals in relation to interoperability when the issue was taken up by EU decision-makers and translated into legislations that the agency's director professed to be very satisfied with. This suggests that the agency attained its goals in the interoperability

policymaking process, which can be viewed as a proxy for the successful exertion of influence. His statement also suggests that over time a much less ambitious vision of interoperability was transformed into a much more comprehensive framework in line with eu-LISA's vision of utilising modern technologies to their full capabilities. Naturally, this also served to enhance eu-LISA's role in the architecture of the EU as well as its importance and responsibility. This is also demonstrated by how a former eu-LISA official described the atmosphere in the agency when the 2016 Commission communication, which started the legislative process on interoperability, became known. He stated that within the agency "it was quickly realised that this was a big opportunity for eu-LISA to play a big role in the very, very significant EU development" and that "it was quite clear that eu-LISA had to be a significant part of the discussion" (Interview with former eu-LISA official). So, although both the agency's director and the former eu-LISA staff member I interviewed emphasised that eu-LISA was not an "*active* player […] in the policymaking process" (Interview with Garkov, eu-LISA) and only implemented policy priorities decided by the decision-makers in the European institutions, the agency still had an organisational stake in the interoperability legislation. Firstly, being entrusted with designing and implementing interoperability increases eu-LISA's importance in the landscape of EU agencies. Secondly, since interoperability consolidates the databases' infrastructure – in the sense that, for example, it makes it possible to have only one shared BMS for multiple databases rather than having to operate a BMS for each database separately – it can "save costs and bring efficiencies" and allow the agency to "put money into specific aspects that would benefit *all* the systems." (Interview with former eu-LISA official). Furthermore, it also emerged from the interview with a former eu-LISA official that the mere existence of eu-LISA as the EU's new IT agency was likely an enabling, if not driving, factor of the interoperability policy making its way through the legislative process successfully in the mid- to late 2010s, whereas the idea of it was dropped again when it was first discussed in the mid-2000s. In comparing the situation in the first round of interoperability discussions with the most recent legislative process on interoperability, the perception emerged that "the business needs were always there. It was more the confidence in the technology and the landscape there, but maybe also on the business side there was increasing realisation with the terrorist attacks, etc." (Interview with former eu-LISA official). This increased confidence in the technology, according to the interviewee, stemmed, on the one hand, from the general advancement in the IT sphere in the intermittent years, which made it possible to procure off-the-shelf instead of bespoke tools for interoperability in a competitive way – something that may not have been the case back in the mid-2000s. On the other hand, the establishment and the IT capabilities of eu-

LISA also contributed to the confidence that the EU could manage such a complex new technology:

> "eu-LISA was relatively new, so I won't say there was necessarily a long track history that this is going to work because we have eu-LISA. But at least there was a dedicated structure there, there were dedicated, responsible people whose sole job was running IT systems and developing IT systems. And there was already, I think, at that stage […] four, five years of operations of eu-LISA that gave evidence and confidence that they could do this." – Interview with former eu-LISA official

Thus, eu-LISA's capabilities and unique IT expertise in handling the EU's large-scale IT systems likely contributed greatly to interoperability being considered a viable option among European decision-makers. Additionally, with their relatively exclusive expertise on EU IT administration, eu-LISA was well-positioned to shape the technical details of interoperability.

However, despite eu-LISA's organisational interests in driving forward interoperability, the agency was perceived by its own (former) staff as well as the interviewees from the other bodies as a purely technical and operational actor. eu-LISA's role in the policymaking process was perceived on the staff level as a "responsible kind of collaborator of the co-legislators, to be upfront about what was possible, what wasn't possible and to advise on the best, from our point of view, technical approaches to implementation." (Interview with former eu-LISA official). In other words, the advice eu-LISA provided to policymakers was described as being based entirely on eu-LISA's technical and operational expertise about the technical feasibility of particular policy ideas as well as on the agency's ability to explain these technical concepts to the laymen among the decision-makers (Interview with Garkov, eu-LISA; Interview with former eu-LISA official). This self-perception as a purely technical actor is also reflected in a leaflet on interoperability published by the agency, in which it describes its role in the legislative process as "[ensuring] that the technical and procedural solutions applied optimally cover business requirements while remaining technically feasible." (eu-LISA, 2019a). The agency's director also emphasised that, despite agreeing with the EDPS' statement that interoperability is "not primarily a technical choice, but […] a political choice to be made" (EDPS, 2018:10), eu-LISA's role in the process was not political:

> "[A]s far as we're concerned, for us interoperability is not so much a political challenge because we're on the implementation side. We come after

> policymakers, as soon as they decide something, to make sure that it will be implemented, and it will work. So, for us interoperability is a huge technical, for sure, but also an operational challenge." – Interview with Garkov, eu-LISA

This self-perception as a purely technical actor seemed to also be shared by representatives of the other agencies, which described eu-LISA's role to be primarily in the context of technical implementation (Interview with Klebek, Europol; Interview with Kampouraki, EDPS) as the "main technical implementing entity" (Interview with Burgersdijk, Europol). Accordingly, the only policy papers on interoperability published by eu-LISA are technical feasibility studies which outline a plan for the technical migration to the new interoperability architecture within eu-LISA and architectural options for implementing the shared BMS (eu-LISA, 2018b, 2019b). In view of the technical focus of eu-LISA' information transmission, eu-LISA can be characterised as an actor wishing to exert technical influence in the sense that it aims to change technical details of policy instruments, while the directional policy aims are decided by other actors such as the Commission or the co-legislators. As both interviewees involved in the policymaking process as eu-LISA representatives professed to be very satisfied both with their own and their agency's role in the policymaking process as well as with the eventual policy outcome, the agency appears to have been successful in having their technical and operational expertise reflected in the final interoperability legislations.

However, it is often seemingly technical or operational decisions that actually have far-reaching directional implications. For example, the inclusion of the 'second generation' of EU large-scale IT systems in the interoperability package, despite the complication that those databases did not exist yet and the establishment of their legal bases was still ongoing during the legislative process on interoperability, was perceived as a technical and business necessity in eu-LISA. A former eu-LISA official described this perceived technical necessity in the following terms:

> "And you look at these systems, ECRIS-TCN and EES again, and you say 'Well, we're going to be building new biometric matching systems for them. Is this sensible?'. And then if we're going to do interoperability, does it make sense to wait for five years or 10 years to build those biometric matching systems, to then have to integrate more five years down the line to make it into a shared BMS? Or we do it now and build a shared BMS and make it

> usable for those systems? So, there was the element of reducing costs and reducing expenditure on the new systems by doing it right now. And then also in the business requirements, you know, we develop these systems and if we know they are interoperable already, we can take that into account in the system design and in the system development, and make sure that gaps are not there from the beginning." – Interview with former eu-LISA official

The inclusion of the not yet finalised 'second generation' databases is, however, not a simple technical matter, but also has implications for data protection. According to the EDPS' opinion (2018:30), establishing interoperability between systems that had no 'stable' legal founding acts during the assessment of the interoperability proposals made "assessing the precise implications for privacy and data protection of a very complex system with so many "moving parts" […] all but impossible". Therefore, despite the insistence from eu-LISA's director as well as the former staff member that eu-LISA is a purely technical and operational actor, and not a policy actor, this does not exclude the possibility that their technical advice may have far-reaching directional influence on the policy. Overall, eu-LISA seems to have been successful in exerting the technical and operational influence it set out to exert and managed to secure itself a stronger role in the European Home Affairs landscape. While this influence appears to have been mostly technical in nature, this does not necessarily exclude their technical advice from having a directional influence on more far-reaching, highly political aspects of the legislative proposals.

5.3.2. Europol and Frontex

I will discuss the perceptions of Europol and Frontex' influence on the interoperability policy in the same section because they have one important feature in common – both are end users of the interoperability technology as well as participants in the legislative process designing the interoperability framework. This dual function is based on, on the one hand, their role as the operational actors consulted by the Commission on their business requirements in relation to the EU's large-scale IT systems and, on the other hand, their role as policy actors contributing to the HLEG in designing the legislative basis for the interoperability proposals. Frontex' and Europol's role as users of the EU's information systems becomes clear in their few publicly available written contributions to the policymaking process (Europol, 2016a, 2016b; Frontex, 2017). Both agencies' papers profess the explicit aim to be used as input into the policymaking process, showcasing the agencies' roles as policy actors. However, within the policy papers, they highlight the need for European decision-makers to take their business

needs as users of the IT systems into account. For instance, in Europol's 2016 contribution to the Standing Committee on Operational Cooperation on Internal Security of the Council, the law enforcement agency emphasises its business need for rethinking the purpose limitation of databases in the context of a disconnect between the different databases:

> "[T]here is much fragmentation of relevant data, as it is held in many disconnected databases. A deeper analysis is needed on the purpose limitations of systems such as VIS and EURODAC to make them more usable to law enforcement authorities and Europol. Such analysis should focus on the needs of the user community." – Europol, 2016a:3

Similarly, the 'non-paper' published by Frontex in 2017 had the express purpose of contributing to the policy discussions in the Council's DAPIX working party and the Commission's work on interoperability. In this 'non-paper', Frontex outlined its business needs as an end user of the EU's IT systems and advocated for the decision-makers to address those needs in the legislative package on interoperability:

> "Therefore, Frontex proposes that the Commission addresses this discrepancy [of Frontex' access to EU databases being more restricted compared to the access by other competent national authorities] in the interoperability package ('Omnibus') by: (1) taking into account the need **to align the access rights of the members of the Agency's teams with those of the national authorities performing equivalent tasks**, and (2) supporting Frontex in undertaking risk analysis, vulnerability assessments and providing the situational picture **by improving the Agency's access to statistical data from these EU systems**." – Frontex, 2017:1 (bold highlights in original)

Here, Frontex is using its role as an end user of the IT systems included in the interoperability package to shape the policymaking process by convincing decision-makers in the European institutions that their operational and business requirements should be included in the interoperability legislations. This is further emphasised in the next excerpt from this 'non-paper', in which Frontex presents the expansion of its access rights to EU information systems as necessary to carry out its operational mandate:

> "[E]nsuring the fullest access to EU systems **facilitates the Agency's *shared responsibility* in implementing IBM** [Integrated Border Management] **at the external borders**. Stipulating this explicitly in the IT systems' founding Regulations by including it in the upcoming interoperability package **does not entail and expansion of the Agency's tasks**. On the contrary, this ability to access these systems (for personal and depersonalised data) is envisaged by the Regulation, and is the very essence of a fully functioning obligation to ensure the security of the Union's external borders *collectively*." – Frontex, 2017:2 (bold and cursive highlights in the original)

These quotes demonstrate that both Europol and Frontex utilised their role as end users of the EU's large-scale IT systems as a way to shape the policymaking process on interoperability according to their organisational interests and business needs.

Throughout the interviews conducted for this thesis as well as the rhetoric by Commission officials and Commissioners on interoperability being needed to facilitate the work of the users of the EU's large-scale IT systems, it became clear that such user needs were a key aspect shaping the interoperability policies. The 2016 Commission communication on interoperability, which started the legislative process analysed in this thesis, was perceived to be a communication "driven by business needs and business requirements" inspired by the "outreach [the Commission] did with Member states and experts and people involved in different fields, you know, borders, police, etc." (Interview with former eu-LISA official). This shows that the opinions and preferences of end users were likely incorporated into the shaping of the interoperability policies very early on in the process. Indeed, according to the Commissioner for the Security Union, Sir Julian King, the outline for the interoperability proposals was shaped by consulting end users:

> "We started by asking those on the front line how we could help, what they needed. And they replied that there were some issues surrounding the handling, the use of information. In particular, there was a challenge surrounding picking up, identifying people who were using multiple identities. We've heard that that led to some horrible terrorist attacks." – King, 2019

It is notable here, that the challenges identified by the frontline users in Commissioner King's statement, namely the issue of multiple identities and their link with terrorism, mirror exactly

how the two Europol officials interviewed for this thesis justified the need for interoperability. These perceptions – that the business needs of the end users of EU databases were key in shaping the content of the interoperability proposals – suggest that utilising their roles as such end users may have provided Frontex and Europol with a stronger position to influence the interoperability policies, particularly early on in the policymaking process. As outlined in the theoretical framework, there is expected to be a "premium on early, efficient and reliable information" by interest organisations, especially if that information is exclusive and not easily obtainable by decision-makers through other sources (Chalmers, 2011:477). Thus, since end users were consulted very early on in the policymaking process on interoperability – likely even before the 2016 Commission communication was published – Frontex and Europol may have been able to act as agenda-setters and shaped the core of the interoperability policies already at the outset of the policymaking process. As outlined in the theoretical framework, such an agenda-setting role by providing relevant information and expertise early on in the conceptual stage of a policymaking process makes it more likely that non-decision-making actors are able to exert directional influence on a policy. This is because they then do not have to *change* the political core of a policy but are instead involved in *generating* the political direction of a policy (Michalowitz, 2007:136). Thus, Europol and Frontex made use of such a premium on early information about their operational and business needs, which are a type of exclusive and not easily accessible information, through their role as end users of the EU's databases to shape the political core of the interoperability policy from the very beginning. Therefore, they can be characterised as having exerted directional influence on the interoperability policies through the agenda-setting power conferred to them as end users of the EU's large-scale IT systems.

The 'alter' perception of one of the Europol officials interviewed for this thesis on the success of Frontex in shaping the interoperability policymaking process supports this argument:

> "I think also when looking at the focus of the work; the focus of the work was predominantly at, to a large extent, at border management. So, I think that Frontex is the agency that was most affected, I would say. I'm not sure whether it was entirely what they wanted themselves, although I do think they were actively lobbying for that stronger role. So, I think Frontex has been one of the key winners, but hopefully it is the European citizen that is the eventual winner of all of this effort." – Interview with Burgersdijk, Europol

This description of Frontex as "one of the key winners" suggests that Frontex attained their goals in the policymaking process. Furthermore, this quote demonstrates that the Europol official perceived Frontex' goal attainment to be connected to Frontex being the "most affected" agency, by virtue of their operational role in the field of border management, as well as Frontex actively lobbying for a stronger role. Therefore, Frontex' role as an end user of EU large-scale IT systems for border management may have been instrumental in Frontex successfully exerting influence on the policymaking process and shaping the interoperability legislation according to its organisational interests. Europol appears to have similarly exerted directional influence on the policymaking process through its operational role in the EU information system architecture. The Europol officials interviewed for this thesis described their agency's way of shaping the interoperability legislations as presenting the gaps in the little details of the proposal and trying to convince decision-makers through "really tangible arguments […] some very tragic and very, you know, based on real stories and examples" (Interview with Klebek, Europol). In other words, Europol was trying to influence the policymaking process through their operational expertise on the business needs, or 'gaps', they identified in their experience as users of the IT systems subject to the interoperability proposals. The following quote suggests that Europol may have sought to motivate the EU's decision-makers to take Europol's requests for the design of the interoperability architecture into account by relating these business needs to tragic real stories and examples, such as terrorist attacks:

> "And also, if the systems are talking to each other, but really identifying possible irregularities – that is only in our advantage. So, I think that there has been always a very strong business need to have this architecture, but it has never reached the, let's say, it didn't motivate properly the political levels to do something before this wave of terrorist attacks. I think that even though the motivation is perhaps not very good, the end effect, I think, it is very good." – Interview with Klebek, Europol

From the perspective of another participant in the policymaking process, Europol, as well as Frontex, "had very specific elements that they were interested in […] [that] would be specific in particular areas" (Interview with former eu-LISA official). These specific elements appear to have been mostly connected to the business needs Europol identified in relation to interoperability, such as their main concern that "user friendliness and quick access to the information held in different relevant databases is of paramount importance for any law enforcement activity" (Europol, 2016a:5). The type of specialised expertise that Europol

brought into the policymaking process appears to have been to a large extent operational information about the way Europol uses and accesses data and how these processes can be improved. In other words, the specialised expertise that Europol supplied to decision-makers in the legislative process on interoperability was information on the "Europol reality in which we operate" and to "explain what [Europol] would need from the interoperability concept" (Interview with Burgersdijk, Europol). As this type of operational expertise is closely tied to the business requirements of Europol as an end-user of the EU's large-scale IT systems, it can be considered exclusive information that would be difficult to access by decision-makers in another manner. When asked about the satisfaction with the policy outcome on interoperability from an organisational viewpoint, it was indeed the achievement of easier and more streamlined access to EU databases as well as an enhanced operational role for Europol that was highlighted as a success:

> "[W]e are very happy that Europol has been given a much more prominent role in the whole EU security ecosystem. We are drawing closer to border management; we are drawing closer to migration and questions to be answered in making sure that dangerous persons are prevented from travelling to the EU. We're happy with easier access and more streamlined access to various databases." – Interview with Burgersdijk, Europol

By focusing their policy efforts on a smaller number of priorities connected to their business needs as users of the information systems, Europol achieved their goal for easier access as well as becoming a more prominent actor in the security and increasingly also the border and migration management sphere of the EU. Overall, Europol seems to have attained their goals in the interoperability policymaking process as both officials interviewed for this thesis described the policy outcome as a great success for Europol and the EU's internal security (Interview with Klebek, Europol; Interview with Burgersdijk, Europol). One Europol official describes this in terms of a fundamental mind change, connected to the wave of terrorism attacks in the mid-2010s, among EU decision-makers:

> "I think, looking back at the reality of 2015, the Commission has truly done an amazing job [with the interoperability legislations]. An amazing job in partnership with the Council and the Parliament, obviously, but they've made a major step forward in realizing things that before these terrorist attacks we

> never thought would have been possible." – Interview with Burgersdijk, Europol

> "I think there was a deep political choice that had to be made. I think that perhaps for you it's difficult to compare with the reality that we had in 2014, 2015, but what we have now as a reality is fundamentally different. There's completely a different look on how we deal with information about what the relationship is between border management, migration, criminal investigation, movements of travellers. That is fundamentally different. […] What has been achieved here is a change of mindset, a number of fundamental principles that have altered, which make it possible to make the technical changes." – Interview with Burgersdijk, Europol

While the Europol official attributes this fundamental change in mindset to the external triggering events of terrorist attacks and a fundamentally changed reality, arguably, what has changed is not the reality itself but how these events have been framed. Bigo et al. (2020:9) argue that the 9/11 terrorist attacks and the attacks in Madrid and London in 2004 and 2005 created a window of opportunity to reframe EU border management databases in security terms. Arguably, the 2015 terrorist attacks created another window of opportunity to take this blurring of boundaries between security and migration management technology a step further by interconnecting border management databases, such as Eurodac and VIS, with law enforcement databases, such as SIS and the Europol database. From the previous section on framing, it has become evident that Europol is one of the actors frequently framing technology as a security enabler and interoperability as a necessary step to ensure security within the EU. Thus, this fundamental change in mindset among European decision-makers that, according to the Europol official, made the interoperability legislative package possible this time around, can be, at least partially, attributed to the influence Europol exerted through framing the technology as a necessity to prevent further terrorist attacks from happening. Naturally, this mechanism also works in the other direction. A shift in mindset among decision-makers would make it easier for Europol to influence the interoperability policy outcome according to their own preferences and to have their business needs met by the interoperability legislations since decision-makers' preferences shifted closer to the security preferences of Europol due to this fundamental change in mindset. This would be in line with the conception of influence exertion taking place between decision-makers and actors trying to exert influence that already share similar interests in the sense that "interest groups tend to lobby friends rather than foes"

(Chalmers, 2011:474). Thereby, Europol (and Frontex) can use this fundamental change in mindset among European decision-makers to attain their policy preferences more easily through their transmission of operational information since their security and efficiency framings are now more easily accepted by decision-makers. Altogether, thus, Europol and Frontex can be characterised as having attained their policy preferences and emerging as the 'winning' agencies out of the interoperability process. Arguably, this goal attainment has been achieved through their dual role as active policy actors in shaping the basis for the interoperability proposals in the HLEG as well as their role as the end users of the IT systems in question. In their latter role, they were likely consulted on their business requirements for interoperability in the early, conceptual stage of the discussions on interoperability, allowing them to act as agenda-setters and exerting directional influence by helping to generate the political core of the interoperability legislations.

5.3.3. FRA and EDPS

In contrast to eu-LISA, Frontex and Europol, the FRA and the EDPS are not involved in operating or using the EU's large-scale IT system that interoperability seeks to connect to one another. Instead, these two bodies took on more of a legal advisory role, rather than the role of end users of the information systems that characterised Europol's and Frontex' involvement in the policymaking process or the role of a system operator that characterised eu-LISA's involvement. The perceptions of the FRA and EDPS are discussed together in this section because they both have a similar rights-based mandate and role in the policymaking process and most interviewees discussed their perceptions of the FRA and EDPS together or in relation to one another.

'Alter' Perceptions of EDPS and FRA influence

Overall, the interviews I conducted with representatives of the agencies involved in the process painted a relatively mixed picture of the influence the FRA and EDPS exerted on the interoperability policies, respectively. On the one hand, the director of eu-LISA described both the FRA and the EDPS as influential actors in the policymaking process and stated that they shaped discussions to a large extent:

> "EDPS definitely is and was influential in shaping the proposals because the EDPS provided quite strong opinions about interoperability, which to a great extent influenced and to some extent shaped discussions, at least in the

> European Parliament, on the interoperability proposals. Same with the Fundamental Rights Agency. – Interview with Garkov, eu-LISA

His perception that the EDPS and its 2018 opinion on interoperability shaped policy discussions especially in the Parliament is congruent with the instances identified in the framing section, in which the EDPS' recommendations were paraphrased extensively by left-wing MEPs in the parliamentary debate and used as justifications for proposals for amendment or rejection of the interoperability proposals. He attributed similar influence to the FRA and its study on the fundamental rights implications of interoperability. The view that the EDPS' expertise was particularly in demand by the Parliament out of the three European decision-making institutions was also echoed by an EDPS official, who stated that the EDPS' opinion was a "very important source" for the Parliament and that it invited the EDPS for hearings to further explain its opinion on interoperability and to ask further questions (Interview with EDPS official). In light of the views of other participants in the policymaking process interviewed for this thesis, which will be shown to conflict to varying degrees with Garkov's portrayal of the EDPS and FRA as very influential actors in the legislative process on interoperability, it has to be noted that Garkov holds the most public and high-level role out of all the interviewees. As the director of eu-LISA, his job position necessitates being the outward representation of eu-LISA's official views, which may lead to strategic, or 'desirable' answers, given to the interviewer. The most 'desirable' answer to the question of how influential the FRA and EDPS were in the policymaking process, is, arguably, to say that they were very influential since protecting human rights and privacy is generally viewed as a virtue. In this sense, Garkov's answer is congruent with the 'expected' answer and therefore a very probable answer, which in process-tracing terms actually makes it less reliable than unexpected, improbable answers (Beach and Pedersen, 2013:129-132).

In order to find out whether and to what extent this interviewee's perception of the FRA's and the EDPS' influence was strategic, I will triangulate it with perceptions of interviewees from other agencies involved in the policymaking process as well as an 'ego' perception from EDPS staff on their organisation's influence in the policymaking process. Overall, it emerged through the interviews that while the EDPS' and FRA's concerns were listened to and there was willingness to address them from the side of decision-makers, this was limited to the extent that their concerns did not interfere to a significant extent with the business challenges and needs that interoperability was envisioned to solve. The first evidence pointing in this direction was the perception of one Europol official that the policy outcome of interoperability "was

quite balanced, but it was business-oriented" when asked about the influence the FRA and EDPS had on the interoperability policy outcome (Interview with Klebek, Europol). His portrayal of the end result of the interoperability policies as balanced between fundamental rights and business needs, while remaining "business-oriented", implies that the FRA and EDPS did succeed in bringing certain safeguards into the policies, while the overall direction of the policies remained focussed on the business needs of end users – such as those of Europol and Frontex. While this perception was still quite vague and qualified by the interviewee's statement that he did not follow the EDPS' and FRA's involvement very closely, another interviewee articulated a similar perspective in more detail. According to a former eu-LISA official, who attended all HLEG meetings and was otherwise also closely involved in the external work of eu-LISA on interoperability with other agencies and decision-makers, the FRA succeeded in having its opinions considered more than the EDPS. In his point of view, this was due to the FRA being more constructive in their interventions:

> "I'd say FRA gave a more balanced and encompassing oversight of all the things that needed to be considered and probably managed through those interventions to have their points of view considered more than the EDPS. The EDPS tended to more say… their point of view was very much and kept being the kind of one line they kept following 'It might be the 'point of no return'. And, you know, 'If we do this, we might not be able to come back.' That was very much their point of view. And I think by some parties that wasn't [considered to be] very constructive. It was like, 'Give us a bit more. Give us... So, but if we want to move on in general, how can we put some things to make sure that risk is mitigated. We want to develop our things; we want to evolve; we want to do something!' You know, we wanted to address some of the business challenges that they are there to help us, tell us what the concerns are." – Interview with former eu-LISA official

Here it becomes apparent that the FRA was perceived as more constructive because their advice tended to explicitly address how to mitigate specific fundamental rights risks contained in the interoperability technology. In other words, their advice was viewed as constructively helping to make sure that business challenges could be addressed in the way envisioned by decision-makers while still taking into account and safeguarding against specific fundamental right concerns. In this sense, the FRA can be characterised as having exerted so-called technical or instrumental influence by seeking to change technical details and adapting policy instruments

to make them more fundamental rights compliant (see Beyers, 2008:1191; Michalowitz, 2007:136). This focus on adapting smaller details rather than modifying the underlying political direction of the proposals is again highlighted in the following statement:

> "Like FRA might be saying, like you know, 'Well, we need to think of the rights of asylum seekers. We need to think of the rights of children. This particular aspect here could infringe on the rights of children. Can we adapt it?' You know, they look at specific elements and say 'These particular areas are elements for concern.' And they bring it forward and everybody, I think most people, would understand and say 'Okay, what can we change? What can we do? How can we develop or change the infrastructure? How can we put safeguards in there to mitigate against that?' So, I think it was really constructive." – Interview with former eu-LISA official

Overall, the FRA highlighting particular areas of concern and suggesting specific safeguards to be built into the legislations seems to have been received by other policy participants and decision-makers as a welcome and constructive input to the policymaking process. However, in the FRA's reply to the Commission's public consultation on the interoperability proposals, the agency stated outright that it did not view the CIR as necessary to achieve the objectives of interoperability, arguing that "most likely the European Search Portal could achieve the same results in terms of efficiency, while keeping the compartmentalised database architecture." (Nygård in Commission, 2017b). This suggests that the FRA did have directional preferences regarding the interoperability policies, namely eliminating an entire interoperability component. However, even in the above example, the FRA also outlined possible ways to make the CIR more fundamental rights compliant if it was to be implemented, despite preferring it to be replaced entirely with the ESP, by including specific data protection safeguards in its architecture and excluding certain data from being accessed via the CIR (Nygård in Commission, 2017b). Therefore, even when the FRA had transmitted specific directional preferences to the Commission, it also outlined alternative, more technical solutions to its most-preferred policy recommendation.

In contrast to the FRA, the EDPS was perceived, according to the above quote, to be relatively unconstructive in their advice, especially when they were making more general comments about the risks of interoperability as a whole rather than on specific details of the interoperability technology that could be adapted. In essence, when the EDPS did not limit

itself to giving specific advice on how to address the business challenges at hand through interoperability in a data protection compliant way, but instead questioned the desirability of interoperability in general, it was perceived as unconstructive. The interviewee further elaborated on this perception of the EDPS as unconstructive:

> "EDPS was a little bit more stuck on one thing. […] I just feel that the interventions into discussion sometimes, where they could be more constructive, were received better. That's not to say they didn't have constructive input on some occasions, but sometimes maybe their input was a little bit more of 'We should do nothing.' And when you're in a big collaborative effort to kind of achieve something, that's less, less looked upon." – Interview with former eu-LISA official

This statement demonstrates the perception that when the EDPS was more 'constructive' – or, in theoretical terms, when they exerted instrumental influence with targeted recommendations or specific concerns – this was received better by decision-makers than when they were being 'unconstructive' by trying to exert so-called directional influence. As discussed in the theoretical framework, directional influence aims to change the political and ideological core of a particular policy (see Beyers, 2008:1191; Michalowitz, 2007:136). By framing interoperability as the 'point of no return' and seemingly arguing for keeping the status quo instead of pursuing interoperability, the EDPS was perceived as trying to exert directional influence. The interviewee suggests that this directional influence was not received particularly well by most decision-makers. He described this further by recalling a meeting convened by the Parliament, which he, as a representative of eu-LISA, the Commission and the EDPS attended. He recalled that when the Parliament asked to hear the EDPS' data protection concerns and the EDPS started talking about interoperability leading to a 'point of no return', the parliamentary decision-makers "came back and said 'What do we want then? Do we do nothing?'. It was kind of the question 'So, what *can* we do?'." (Interview with former eu-LISA official). This portrays the co-legislator as being very interested in hearing the concerns and recommendations of the EDPS but perceiving them as not fitting in with the larger directional goal of meeting business needs that they had already decided on. This is congruent with the expectation identified in the theoretical framework that interest organisations may be more influential in shaping a policy process when they exert instrumental rather than directional influence. Since directional influence can be viewed as challenging the original policy aim and generating conflict with those decision-makers that first decided on a particular policy direction

and its core contents, actors who attempt to exert such directional influence are expected to be less successful (see Michalowitz, 2007:137). A similar view was also emphasised by another Europol official interviewed for this thesis, who opined that when the new round of discussions on interoperability began in 2016 "the public point of view had already moved beyond the political reality in Brussels, of how very protective and data protection compliant we had to be with everything and separating everything just for the sake of human rights and everything." (Interview with Burgersdijk, Europol). In his perception, the European decision-makers then had to catch up with this changing point of view of the public. Then, once they had caught up with these fundamental mind changes on how to deal with information in border management and security matters, the new direction was accepted and set by the European decision-makers (Interview with Burgersdijk, Europol). A consequence of this was, in the interviewee's perception, that the supervisors, such as the EDPS, had to essentially take a step back and work within this already decided new reality:

> "The public opinion had moved on. This was a matter of having to catch up. So, for the Commission, they didn't have to compete with journalists or public protests or anything when they went in this direction. So, the focus then was to explain to the supervisors exactly what would be done. And it is, often the debate that results is: 'We are not infringing on anything because this is exactly how it works in detail'. And then, automatically, it becomes a technical discussion. EDPS is right, from *their* perspective, saying that there's not much attention to the political and societal consequences over this. That is right from *their* perspective because *their* societal reality was different. And they had to adjust to this new reality. Whereas the rest of the outside world had moved on already after a couple of attacks, shifting the mindset like 'we're not going to accept this, we're going to make better use of data. This is a no brainer' – if you like. So, this is for them, where they had to change their mind, whereas the rest essentially didn't really see that as a problem." – Interview with Burgersdijk, Europol

The perception articulated in this quote is, again, that the EDPS was only able to exert instrumental influence on the technical details, while they 'had to change their mind' when it came to the greater political and societal concerns they had identified in relation to interoperability. Such a perception of the EDPS' influence once again strengthens the argument

that the supervisor was not successful in exerting the directional influence that it attempted to project and was essentially left with joining into technical discussions on smaller details.

'Ego' Perceptions of EDPS Influence

This perception of a limited directional influence was also echoed by an EDPS official interviewed for this thesis. In their so-called 'ego' perception, this official was under the impression that the EDPS' call for a wider political and societal debate on the purposes, future scope, risks and advantages of the interoperability of EU information systems was not realised by the Commission or the co-legislators. While she highlighted that it was positive that the Commission involved the EDPS, the FRA and the Parliament relatively early on in the policymaking process, in her opinion, the debate on interoperability was limited to highly academic discussions and discussions between the co-legislators, rather than debates involving the wider public (Interview with EDPS official). This demonstrates that the advice of the EDPS to further debate and think about the risks and future implications of interoperability, and thereby potentially reconsider the current direction of the interoperability policies, went largely unheeded by the relevant decision-making institutions. Another key problem the EDPS official highlighted in regard to how the interoperability policy process was handled was her perception that the political decision-makers in the EU put "the cart before the horse" (Interview with EDPS official). This idiom generally suggests that things were done in the wrong order (Merriam-Webster Dictionary, n.d.). Specifically, she was concerned that interoperability was decided between systems whose legal basis was not stable and, in some cases, did not exist yet during the policymaking process on interoperability. Therefore, she had the "feeling that it was done a bit too quickly" and that "maybe it would have worked to first have all the databases to see how they work and then think about interoperability." (Interview with EDPS official). This perception of a rushed legislative process was also echoed by the SCGs for the individual EU databases to be made interoperable – staffed by EDPS and DPA officials – which wrote a joint letter to the presidents of the Commission, Parliament and Council in 2018. In it, they lament that interoperability "would have required a cautious approach and a thorough prior assessment on the impact of those changes on fundamental rights [and that] it is therefore unfortunate that the discussions on this complex process were rushed." (Cauchi et al., 2018:2). In other words, the sense of urgency in which interoperability was often framed by European decision-makers and other policy actors, was a major point of critique from the perspective of the EDPS official as well as the SCGs. This is in essence a directional critique of interoperability as it does not simply seek to change small technical details in the interoperability components. Instead, it

seeks to change the much more far-reaching questions of whether to pursue interoperability at all at this point in time and of whether the 'second generation' of EU databases should have even been included in the interoperability legislations.

Unsurprisingly, therefore, the EDPS official shared that she was not satisfied with the policy outcome on interoperability. This is noteworthy in the sense that, in contrast to the EDPS official, both interviewees from eu-LISA and Europol professed to be almost entirely satisfied with the end result of the interoperability policymaking process. This dissatisfaction within the EDPS was also reflected in another joint letter of the SCGs to the Commission in January 2020, after the interoperability legislations had already been adopted. This letter used even stronger wording on their dissatisfaction with the policy outcome on interoperability and their perception that the concerns of data protection authorities had been ignored by decision-makers:

> "We regret that neither the European Commission, nor the co-legislators, took into account the issues raised by data protection authorities in the process of defining and adopting this new framework establishing interconnection through interoperability. […] The new architecture and functionalities of EU information systems being established by these successive proposals, negotiated with tremendous speed and with a continuous flow of complex and intertwined legislative proposals, poses enormous risks to the rights for privacy and data protection." – Cauchi et al., 2020:1-2

Essentially, this statement shows that the SCGs, and in extension the EDPS since the SCGs are staffed, inter alia, with EDPS staff, did not think that their policy input was sufficiently taken into account by decision-makers. This implies that they did not think they were successful in exerting as much influence on the policy outcome on interoperability as they wanted to. However, despite being dissatisfied with major directional aspects on which the EDPS did not manage to make its voice heard, the EDPS official interviewed did emphasise that the EDPS was able to exert some influence:

> "I think that we had an influence in narrowing better the scope and to… I wouldn't say finetune because then you'd get the impression that it was very good and just needed finetuning – but we had an influence at each stage to

> recall the importance to clearly frame the project. […] Maybe it's not enough but it's already better than before." – Interview with EDPS official

Here she emphasises that the EDPS was primarily successful on narrowing the scope and finetuning the technical details, while stressing that in her opinion the proposals needed more than just finetuning for them to be considered as 'good' by the EDPS. This once more suggests that although the EDPS wanted to exert more directional influence, it had to contend itself with exerting technical influence on the proposals, which she did not consider as good enough but as at least leading to a better outcome than if the EDPS had not been involved at all. In this counterfactual view of influence, the EDPS can be characterised as having exerted influence since its involvement was perceived to have changed the overall outcome of the policymaking process. However, the EDPS cannot be characterised as having fully attained its goals in the policymaking process as their larger concerns appear to have not been taken into account by the decision-makers. In contrast, at least according to the former eu-LISA official's perception, the FRA focused primarily on specific details to be made fundamental rights compliant instead of trying to modify the overall direction of the proposals, which allowed it to attain more of its goals in the policymaking process.

Goal attainment of EDPS and FRA

The extent of the FRA's and the EDPS' goal attainment in terms of their influence on particular articles and paragraphs of the interoperability regulations can be measured by comparing how many of their legislative recommendations outlined in their legislative opinion papers were incorporated into the final legislation. Since the two sister proposals are described as highly similar in content and numbering of the legislative articles (EDPS, 2018:9), only one of the regulations was compared with the opinions, namely Regulation (EU) 2019/818 on establishing a framework for interoperability in the field of police and judicial cooperation, asylum and migration.

Recommendation Incorporated into Final Regulation*?	FRA opinion (2018)	EDPS opinion (2018)
Yes	21	20
No	18	20
Partially	5	5

Table 2: Number of recommendations from the FRA's and the EDPS' legislative opinions on interoperability that were incorporated into the final interoperability regulation

**Only the final interoperability regulation on police and judicial cooperation, asylum and migration (Regulation (EU) 2019/818) was compared to the recommendations of the FRA and the EDPS. However, its 'sister regulation' in the field of borders and visa is sufficiently similar that most of the same conclusions should hold.*

***See appendix for the full tables detailing the specific recommendations in the FRA and EDPS opinion and the corresponding section of the final interoperability regulation in which these recommendations were or were not or were partially incorporated into the final legislative text.*

As shown in table 2, the amount of the FRA's and EDPS' recommendations incorporated in the final interoperability regulation suggests that they were successful in attaining their instrumental goals on modifying specific parts of the interoperability proposal in about half of their recommendations. It can also be seen that the FRA and the EDPS had about the same amount of success in having their recommendations incorporated into the final regulation by the European co-legislators. Overall, therefore, both the FRA and the EDPS were able to exert a non-negligible amount of instrumental influence on the final regulation by achieving a change in the legislative text from the proposal to the final regulation in about half of the cases in which they voiced concerns in their legislative opinions. Since the FRA was perceived as having been predominantly focused on exerting such instrumental influence, its participation in the policymaking process can be characterised largely as a success since it managed to have many of its voiced preferences reflected in the final policy outcome. In contrast, the EDPS also attempted to exert directional influence on the overall framing and handling of interoperability, which, according to the perception of almost all the actors interviewed for this thesis as well as textual evidence, it was not successful in. Therefore, the EDPS can only be characterised as having marginally achieved its goals through its participation in the policymaking process since it at least had a relatively significant success in having its more technical preferences reflected in the policy outcome.

6. Analysis

The following analysis chapter will seek to connect the empirical results outlined in the previous chapter to the theoretical expectations derived in the literature review. First, the expectation that the frequency of access to the policymaking process by EU advisory bodies is a determinant of their influence on the process will be evaluated against the accumulated empirical evidence. Secondly, it will be evaluated whether EU advisory bodies pursuing technical and instrumental rather than directional interests in the legislative process on interoperability were more successful in exerting their influence. Finally, the theoretical expectation that EU advisory bodies attain their policy goals by having their selective issue framing taken up by decision-makers in their own policy framing is analysed based on the evidence gathered on the policy actors' framing activities.

6.1. Frequency of Access

According to the literature on interest group influence on legislative process, a first step of analysis is to demonstrate that the non-decision-making actors of interest had access to the policymaking process in the first place since access is a necessary, but not sufficient, condition for exerting influence (see Truman, 1951; Bouwen, 2002:366; Betsill and Corell, 2001:69-70; Binderkrantz and Pedersen, 2016:307). The empirical results showed that all four EU agencies and the EDPS indeed had access to the legislative process on interoperability, first and foremost through their participation in the HLEG, but also through various other access channels that differ between the five bodies. However, it is not only access in general, but also the frequency of access to the policymaking process that was identified as an important condition for exerting influence in the literature review (see Kim, 2018:60; Chalmers, 2013:47). In other words, *a greater frequency of access to the policymaking process by non-decision-making actors is expected to increase the influence they are able to exert.* The empirical results in this case study paint a mixed picture on whether the frequency of access determined how much influence an EU advisory body was able to exert on the policymaking process. On the one hand, the influence perceptions of the FRA's contributions to the policymaking process suggested that its broader mandate and corresponding greater input in the policymaking process, along with the multitude of access channels used by the FRA to participate in the legislative process, gave the agency a more influential voice in the legislative process than the EDPS. This supports the theoretical argument that 'more is better' in the sense that a greater frequency of information transmission and, thus, a greater frequency of access to the policymaking process provides actors with more opportunities to turn their contributions into influence (see Chalmers,

2013:47). Similarly, eu-LISA was also identified as an actor making use of all of its access channels to decision-makers frequently throughout the policymaking process. The empirical results suggested that this frequent transmission of eu-LISA's technical and operational expertise to the European institutions through a variety of formal and informal access channels allowed the agency to successfully exert a significant amount of technical influence on the policy process and outcome. Both the case of the FRA and eu-LISA support the theoretical expectation that more frequent access to the policymaking process and to decision-makers by EU advisory bodies increases the influence that those bodies can exert on the policymaking process. However, the cases of Europol and Frontex, which according to the empirical evidence have shaped the content of the interoperability policy significantly despite comparatively infrequent access to the policymaking process, appear to disconfirm the theoretical expectation as it does not seem to hold across all actors analysed. Despite having primarily accessed the policymaking process on interoperability in its early conceptual stages in their role as end users of the EU's IT systems and as participants in the HLEG, their preferences seem to have shaped the interoperability policy outcome significantly. Consequently, in the cases of Europol and Frontex it seems not to be the frequency of access, but their organisational role and the timing of access that played a role in determining their influence on the interoperability policymaking process. Therefore, overall, the expected positive correlation between the frequency of access and the amount of influence exerted on a policymaking process cannot be confirmed by the empirical evidence gathered in this case.

6.2. Technical vs. Directional Influence

Whether interest organisations can exert influence on a policymaking process is also expected to depend on the type of interests they pursue in policymaking process and, in turn, the type of influence they try to exert. While technical, or instrumental, influence is concerned with adapting smaller technical details of a policy, directional influence seeks to modify the underlying policy aim (Beyers, 2008:1191; Michalowitz, 2007:136). According to the theoretical expectations identified in the literature review, *EU advisory bodies pursuing instrumental policy goals are expected to be more successful in influencing the policy process than advisory bodies that pursue directional interests*. Following the empirical results of this case study, eu-LISA has emerged as particularly successful in exerting the technical influence on the interoperability legislative process that it set out to exert. Representatives of eu-LISA repeatedly emphasised, and this was echoed by outside perspectives as well, that the agency did not seek to determine or change the political core of the proposals and instead focused on

making the policy aims of the European decision-makers workable through technical means. While it was demonstrated in the result section that such technical influence can also have some directional implications on the policymaking process, eu-LISA's projected and widely accepted technical role and technical interests in the interoperability process allowed it to exert a significant amount of instrumental influence on the finer details of the interoperability regulations. From the perceptions of the interviewed policy participants and the textual evidence it appears that it was precisely eu-LISA's projected apolitical and technical status that allowed it to shape the IT architecture of interoperability to a great extent and even at times impact directional decisions regarding the policies through portraying them as technical necessities. This affirms the expectations that following technical/instrumental interests, or at least appearing to only follow technical interests, in a policymaking process made EU advisory bodies more likely to exert their influence in the process.

The expectation that pursuing more technical/instrumental rather than directional interests makes it more likely for an advisory body to exert influence in the policymaking process appears to also hold for the FRA, especially in comparison to the EDPS. This is reflected in the perception that the FRA was a more constructive participant in the policymaking process on interoperability by focusing on modifying finer details of the proposals instead of questioning its very basis and that this made the FRA more successful in influencing the policy outcome than the EDPS. In other words, focusing primarily on exerting instrumental influence by making specific policy tools more fundamental rights compliant allowed the FRA to have a more influential voice in the policymaking process and attain its policy preferences. On the other hand, the evidence in the empirical results section suggests that the EDPS wanted to exert more directional influence but had to contend itself with exerting technical influence on the proposals since its attempts at pursuing its directional interests were not received well by decision-makers. In this sense, the EDPS cannot be characterised as having fully attained its goals in the policymaking process as their larger directional concerns appear to have not been taken into account by the decision-making actors. The case of the FRA and EDPS, and especially comparing the different types of influence they tried to exert and how they were differently received by decision-makers, affirms the theoretical expectation that advisory bodies pursuing technical over directional interests are more likely to influence a policymaking process according to their preferences.

While non-decision-making actors are generally expected to be more influential in a policymaking process when they exert technical rather than directional influence, the

theoretical framework also introduced a caveat to this expectation. When non-decision-making actors get involved in a legislative process from its outset, they can act as agenda setters and exert directional influence by helping to generate, rather than modify, the political core of a developing policy (see Michalowitz, 2007:136). The empirical evidence gathered on Frontex' and Europol's roles in the legislative process on interoperability suggests that this caveat applies to them as their roles as end users of the EU's large-scale IT systems is hypothesised to have put them in a privileged agenda-setting role particularly in the early conceptual stage of the interoperability policies. Since end users were consulted very early on in the process of establishing a legislative framework on interoperability, Frontex and Europol were able to provide operational expertise in the form of exclusive information gathered from their operational experience with the EU's databases at the very start of discussions around interoperability. Therefore, Frontex and Europol may have been able to use their roles as end users of the EU information systems for border management and law enforcement purposes to act as agenda-setters and shape the core of the interoperability policies from the outset of the policymaking process. In this way, it appears that those two EU agencies were successful in exerting directional influence on the interoperability proposals through helping to set the agenda in their role as end users. This directional influence is, arguably, reflected in the focus of the interoperability legislations being primarily on the operational and business needs voiced by Europol and Frontex, such as improving user friendliness and efficiency of procedures as well as streamlining law enforcement access to the EU's databases. Overall, this confirms the theoretical expectation that while the pursuit of technical/instrumental rather than directional interests makes it more likely for an advisory body to successfully influence a policymaking process, directional influence can still be exerted through the right timing and positioning of an actor in relation to the policy issue at hand.

6.3. Framing Success

The final expectation identified in the literature review is that the selective framing of a policy issue by a non-decision-making actor can influence the direction of a legislative process according to their perspective and preferences (Klüver et al., 2015b:481-482). The mechanism through which framing by non-decision-making actors can lead to actual influence on a policy outcome is the degree to which their framings are accepted and adopted by decision-makers in the policymaking process (Corell and Betsill, 2008:30). Therefore, the empirical results outlined for this case study traced the degree to which the EU advisory bodies' issue framings regarding interoperability correlated with those of decision-makers and those employed in

legislative texts to measure the advisory bodies' goal attainment in the legislative process. In other words, through empirical evidence the theoretical expectation that *when advisory bodies' issue framings correlate with those employed by decision-makers and those used in the legislative text, then those bodies are expected to have affected the issue framing surrounding the policy and thereby attained their policy goals,* was examined. As revealed in the framing section, Europol was, among other actors, very active in framing interoperability in security terms by portraying interoperability as the technological solution to close the information gaps that it identified as responsible for a number of terrorist attacks that took place in Europe in the mid-2010s. Europol can be characterised as having been successful in affecting the issue framing surrounding the interoperability policy as its general security framing as well as its specific examples of information gaps leading to undetected attackers have been taken up by a significant amount of the decision-makers involved in the policymaking process. Additionally, the perception shared by Europol interviewees that Europol participated in the policymaking process specifically to raise awareness of such 'information gaps' among decision-makers and advocate specific products of interoperability, such as streamlined law enforcement access to the EU's databases, as the solution to those gaps suggests that this security framing was a lobbying strategy that Europol employed to affect the interoperability policy according to their organisational preferences (see Klüver et al., 2015b:481-482). As interoperability was framed in security terms and justified by security reasons in its legislative texts, their successful security framing has helped Europol in shaping the policy outcome and attaining their policy goals. Similarly, the technology optimism framing, primarily employed by eu-LISA and Frontex among the EU advisory bodies investigated for this thesis, was taken up as a major justification for establishing interoperability among the European decision-makers both in their rhetoric as well as in legislative texts. Thus, the framing of interoperability as a technical tool generating efficiency benefits employed by those bodies had successfully shaped the issue framing surrounding the interoperability policy among decision-makers. As with Europol's security framing, this suggests that eu-LISA and Frontex attained their goals in framing the overall policy process according to their policy preferences and perspectives.

In terms of the social risk framing, the first risk narrative, which frames the risks of interoperability to fundamental rights as existent but manageable through the right design, was employed by virtually all EU advisory bodies as well as the decision-makers in the European institutions. Thus, the body employing this framing most frequently and in the most detailed manner, the FRA, can be characterised as attaining their policy goal of framing interoperability

as a real risk that must be anticipated and controlled through built-in safeguards. Virtually all European decision-makers and the legislative texts affirmed the need for such built-in safeguards in line with the first risk narrative. However, the EDPS' framing of interoperability through the second risk narrative, which framed interoperability as a more uncontrollable risk, can only be characterised as partially successful. While it was taken up by a variety of left-wing MEPs with decision-making power over the policy, who even directly referenced the EDPS' framing to support their arguments against interoperability, it was not accepted by a sufficiently large number of decision-makers in the Parliament nor by Commission or Council decision-makers and thus failed to impact the final policy outcome. Therefore, the EDPS was only successful to a very limited extent in affecting the issue framing surrounding interoperability and attaining their policy goals through their framing strategy.

Altogether, this analysis of the framings present in the discourse surrounding the interoperability proposal demonstrates that the use of these narratives by the four EU agencies Europol, Frontex, eu-LISA and the FRA correlates with the narratives employed by political decision-makers and the legislative proposals. Following Corell and Betsill's (2008:30) definition of interest organisations' goal attainment through issue framing, this indicates that these EU agencies attained their policy goals through the policy issue of interoperability being widely conceptualised as an innovative technological solution to security concerns, whose risks can be controlled by relevant built-in safeguards. Overall, the theoretical expectation that EU advisory bodies can affect the policymaking process and outcome and attain their policy goals through their selective framing of the policy issue was traced and confirmed through the empirical evidence gathered.

7. Conclusion

This research focused on the policymaking process leading up to the adoption of the two EU regulations that established a framework for the interoperability of the EU's large-scale IT systems that collect biometric and biographic personal data of third-country nationals for border management and, increasingly, law enforcement, purposes. An interesting feature of this legislative process was the extent to which four EU agencies, namely eu-LISA, Frontex, Europol and the Fundamental Rights Agency (FRA), as well as the independent supervisory authority of the EU, the European Data Protection Supervisor (EDPS), were involved in it. Previous academic discussions around the topic of EU database interoperability attributed a high organisational stake in interoperability to three of those EU agencies, namely eu-LISA, Europol and Frontex, and argued that they actively lobbied and strategized to achieve their political preferences in the establishment of interoperability (Bigo et al., 2020:16-18; Carrera, 2020; Galli, 2019:15). Regarding the FRA and the EDPS, scholars have recommended the greater involvement of these two EU bodies in designing an interoperability framework so that their specialised expertise would ensure that fundamental rights and data protection concerns would be sufficiently considered and mitigated in any resulting legislations (Bigo and Jeandesboz, 2009:5). This prompted the research question of this thesis asking whether and how these EU advisory bodies were able to influence the legislative process on interoperability and shape the policy outcome through their specialised expertise and policy recommendations.

Findings

Firstly, this thesis demonstrated, based on evidence from the empirical results gathered, that all EU advisory bodies analysed in this thesis had access to the policymaking process on interoperability and made use of this access in varying degrees of frequency. While particularly eu-LISA and the FRA accessed the policymaking process and communicated with decision-makers very frequently through various access channels, Europol and Frontex gained access much less frequently especially after the conceptual stages of the interoperability policymaking process were finished. The theoretical expectation that the frequency of access is positively correlated with influence could not be confirmed because, while eu-LISA's and the FRA's frequent access was associated with increased influence, Frontex and Europol could be characterised as influential despite infrequent access to the policymaking process.

Subsequently, it was demonstrated that eu-LISA was very successful in influencing the technical details and trajectory of interoperability, while Frontex and Europol were able to

influence the content of the interoperability policies in their early conceptual stages through their mandated roles as end users of the EU's large-scale IT systems. These findings corroborate the assertions in the existing literature on interoperability that Frontex and eu-LISA were the 'winners' of interoperability (Carrera, 2020), that interoperability was shaped to a great extent by the IT specialists in eu-LISA (Bigo et al., 2020:23), and that Europol and Frontex have been increasingly pro-active in lobbying to increase their operational competences via interoperable databases (Galli, 2019:14-15). This research also showed that the participation of the FRA and the EDPS in the policymaking process did allow them to shape the interoperability policies to better safeguard fundamental rights and privacy than if they had not been involved in the process. By focusing on providing expert advice on how to mitigate specific fundamental rights concerns identified in the interoperability proposals, the FRA was perceived as a constructive policy participant and was thereby able to exert significant instrumental influence on the policymaking process and achieve its policy preferences. However, it has to be noted that such instrumental influence is limited to modifying smaller technical details of a policy within the directional and political boundaries established by other actors. While the EDPS was also found to have exerted a non-negligible amount of instrumental influence, it failed to have its more fundamental directional preferences and recommendations taken into account by decision-makers. Therefore, the EDPS was identified as the body among the EU advisory bodies analysed in this thesis that was the least successful in attaining its policy preferences in the legislative process on interoperability.

It was furthermore demonstrated in the framing section of this thesis that EU advisory bodies' issue framings of interoperability were congruent with and had successfully shaped the issue framing surrounding the interoperability policy among decision-makers in the European institutions. Particularly the technology optimism framing coupled with a security framing was a very dominant framing among eu-LISA, Frontex, Europol as well as decision-makers in the Commission and among conservative and liberal MEPs alike. While the first social risk narrative was also employed by all EU advisory bodies – most predominantly by the FRA followed by the EDPS – as well as virtually all European decision-making institutions, the more technology-sceptical second social risk narrative was exclusively employed by the EDPS among the EU advisory bodies and only resonated with (far) left-wing MEPs among the decision-makers. This demonstrated that those advisory bodies who successfully shaped the issue framing of interoperability widely among decision-makers were ultimately better able to attain their preferences in the policymaking process, while the EDPS' less successful issue

framing along the second social risk narrative resulted in it not achieving its more far-reaching directional policy interests.

Academic Contribution

One of the key academic contributions of this research to the academic field is that it provided an empirical account of the previously understudied research field on the influence of EU agencies and other EU advisory bodies in EU decision-making procedures, particularly in the field of Home Affairs. In her dissertation, Kim (2018:184) suggested that a future research agenda should include empirical research on the influence of EU agencies on EU migration policies by arguing that the most recent 'agencification' process has occurred in this policy area of EU politics. Therefore, this thesis contributes to the field by taking up this suggested research agenda and thereby contributing both additional empirical evidence and theoretical insights to existing academic scholarship on the 'agencification' of EU politics and the influence of JHA agencies and other EU advisory bodies involved in EU migration policy. A second contribution of this research is that it deepened the theoretical understanding of studying the influence of non-decision-making actors other than traditional interest groups by applying theoretical expectations from the study of interest group influence to institutional non-decision-making actors that are formally included in the EU's architecture. Furthermore, this thesis has collected and analysed original empirical evidence on the 'ego' and 'alter' perceptions of the influence exerted by EU agencies and the supervisory authority involved in the interoperability process. This has provided evidence for the intentions, perceptions and awareness of EU agency and EDPS staff that in previous scholarship have predominantly only been indirectly deduced from official documents or public speeches. Therefore, this original data collection has contributed to a deeper understanding of the perceptions and motivations of EU advisory body officials participating in policymaking processes. Additionally, the results section provided a novel empirical account on the dominant framings surrounding the interoperability concept as well as on the extent that EU advisory bodies' framings were congruent with those of decision-makers. Since the framings identified are continuously connected to and based on the theoretical insights from Science, Technology and Society studies and Critical Security Studies, these findings on framings employed in relation to interoperability can be incorporated into the wider trends identified by these fields of study. In other words, the identified framings provide empirical insights on the securitisation of migration management and the technologization of security in the EU as well as on the manner in which new technologies are perceived and framed in modern societies.

Limitations of Research

One of the major limitations of this study, as with the majority of process tracing studies, is that there is little potential for generalisations of my findings beyond the case analysed here. In other words, the insights uncovered in this case study about whether and why particular EU advisory bodies were able to exert influence in the most recent interoperability policymaking process cannot be generalised to hold in other legislative processes. Additionally, as it is very difficult to fully ascertain influence, this research relied on proxies for actual influence such as actors' goal attainment and influence perceptions to measure, or at least approximate, the actual influence exerted by the studied actors. In other words, it is difficult to ensure that a change in policy outcome was actually influenced by a particular advisory body and not another actor or external event even if the outcome was changed according to studied actor's policy preferences. Additionally, influence perceptions can be consciously or unconsciously biased, although this limitation was mitigated through the triangulation of influence perceptions across multiple interviewees.

Future Outlook

This research focused exclusively on the influence EU advisory bodies exerted during the policymaking process on interoperability. However, multiple of my interview partners from those advisory bodies remarked that their organisations would still be fully involved and potentially able to shape the trajectory of interoperability during its implementation phase. Therefore, a fruitful avenue for future research would be to study the influence of EU agencies and supervisory authorities on the development of interoperability during the implementation or even the subsequent operational stage when interoperable databases will be accessed and used by street-level officials like border guards and police officers. On a more theoretical note, there is a surprising dearth of research into the influence EU agencies and comparable intra-EU advisory bodies exert on EU politics and policymaking process. Despite scholars on the 'agencification' in the EU having long asserted that EU agencies wield a certain policy influence through their information transmission (see Vos, 2000:1130), there has been very little empirical research done to underpin such assertions. Therefore, it would be in the interest of the research communities on 'agencification' and those on interest group influence in the EU to collaborate on a common research agenda into illuminating the prevalence and mechanisms through which EU agencies and comparable bodies can exert and have exerted influence on EU policymaking processes.

8. References

Anvelt, A. (2017, October 17-18). *Going Digital for a Safe and Secure Europe*. Conference Report eu-LISA Annual Conference, Tallinn, Estonia.

Ares Baumgartner, R. (2018, October 17). *EU Borders - Getting Smarter Through Technology.* Conference Report eu-LISA and Frontex joint conference, Tallinn, Estonia.

Arts, B., & Verschuren, P. (1999). Assessing Political Influence in Complex Decision-making: An Instrument Based on Triangulation. *International Political Science Review, 20*(4), 411–424.

Avramopoulos, D. (2017, October 17-18). *Going Digital for a Safe and Secure Europe*. Conference Report eu-LISA Annual Conference, Tallinn, Estonia.

Balzacq, T. (2008). The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies. *Journal of Common Market Studies, 46*(1), 75-100.

Balzacq, T., & Léonard, S. (2013). Information-sharing and the EU Counter-terrorism Policy: A 'Securitization Tool' Approach. In C. Kaunert (Ed.), *European security, terrorism and intelligence : tackling new security challenges in Europe* (pp. 127-142). Basingstoke: Palgrave Macmillan.

Bauer, A., & Bogner, A. (2020). Let's (not) talk about synthetic biology: Framing an emerging technology in public and stakeholder dialogues. *Public Understanding of Science, 29*(5), 492-507.

Beach, D., & Pedersen, R. B. (2013). Process-Tracing Methods. In R. B. Pedersen, & D. Beach (Eds.), *Process-Tracing Methods: Foundations and Guidelines.* (pp. 120-143). Michigan: University of Michigan Press.

Betsill, M. M., & Corell, E. (2001). NGO Influence in International Environmental Negotiations: A Framework for Analysis. *Global Environmental Politics, 1*(4), 65-85.

Beyers, J. (2004). Voice and Access: Political Practices of European Interest Associations. *European Union Politics, 5*(2), 211–240.

Beyers, J. (2008). Policy Issues, Organisational Format and the Political Strategies of Interest Organisations. *West European Politics, 31*(6), 1188-1211.

Bigo, D. (2014). The (in)securitization practices of EU border control: Military/Navy – border guards/police – database analysts. *Security Dialogue, 45*(3), 209–225.

Bigo, D., & Jeandesboz, J. (2009). Border Security, Technology and the Stockholm Programme. *INEX Policy Brief - Centre for European Policy Studies, No. 3*, pp. 1-6.

Bigo, D., & McCluskey, E. (2018). What Is a PARIS Approach to (In)securitization? Political Anthropological Research for International Sociology. In A. Gheciu, & W. C. Wohlforth (Eds.), *The Oxford Handbook of International Security* (pp. 116-130). New York: Oxford University Press.

Bigo, D., Ewert, L., & Kuşkonmaz, E. M. (2020). The Interoperability Controversy or How to Fail Successfully: Lessons from Europe (Working Paper). *International Journal of Migration and Border Studies, 6*(1-2), 1-41. Retrieved from https://spire.sciencespo.fr/notice/2441/6j8ik22jv18u98pncq99ufhvo9

Bijker, W. E. (2003). The Need for Public Intellectuals: A Space for STS. *Science, Technology, & Human Values, 28*(4), 443-450.

Binderkrantz, A. S., & Pedersen, H. H. (2016). What is access? A discussion of the definition and measurement of interest group access. *European Political Science, 16*, 306–321.

Bouwen, P. (2002). Corporate lobbying in the European Union: the logic of access. *Journal of European Public Policy, 9*(3), 365-390.

Bowen, G. A. (2009). Document Analysis as a Qualitative. *Qualitative Research Journal, 9*(2), 27-40.

Burgersdijk, O. (2016, October 27). *JHATech 2016: Aligning the capabilities of technology with policy priorities in the areas of migration and internal security*. Conference Report eu-LISA Annual Conference, Tallinn, Estonia.

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: a new framework for analysis.* Boulder, Colorado: Lynne Rienner Publications.

Carolan, C. (2016, October 27). *JHATech 2016: Aligning the capabilities of technology with policy priorities in the areas of migration and internal security*. Conference Report eu-LISA Annual Conference, Tallinn, Estonia.

Carrera, S. (2020, January 29). *Towards interoperable justice: Interoperability and its asymmetry in access rights by EU digital citizens*. Retrieved February 10, 2021, from Migration Policy Centre (MPC): https://migrationpolicycentre.eu/towards-interoperable-justice/

Cauchi, D., Jilderyd, E., & Scheidegger, C. G. (2018, June 22). *Joint letter on the new EU legislative framework for interoperability between EU large-scale information systems.* Brussels: SIS II, VIS and Eurodac Supervision Coordination Groups.

Cauchi, D., Maragou, E., & Scheidegger, C. G. (2020, January 13). *Joint letter on the new EU legislative framework for interoperability between EU large-scale information systems.* Brussels: SIS II, VIS and Eurodac Supervision Coordination Groups.

Ceyhan, A. (2008). Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics. *Surveillance & Society, 5*(2), 102-123.

Chalmers, A. W. (2011). Interests, Influence and Information: Comparing the Influence of Interest Groups in the European Union. *Journal of European Integration, 33*(4), 471-486.

Chalmers, A. W. (2013). Trading information for access: informational lobbying strategies and interest group access to the European Union. *Journal of European Public Policy, 20*(1), 39-58.

Corell, E., & Betsill, M. M. (2008). Analytical Framework: Assessing the Influence of NGO Diplomats. In E. Corell, & M. M. Betsill (Eds.), *NGO Diplomacy: The Influence of Nongovernmental Organizations in International Environmental Negotiations* (pp. 19-42). Cambridge, MA: The MIT Press.

Dalli, M. (2019, March 27). *Interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration - Interoperability between EU information systems in the field of borders and visa (debate) (CRE 27/03/2019 - 24)* . Retrieved from European Parliament Debates: https://www.europarl.europa.eu/doceo/document/CRE-8-2019-03-27-ITM-024_EN.html

Dür, A. (2008a). Interest Groups in the European Union: How Powerful Are They? *West European Politics, 31*(6), 1212-1230.

Dür, A. (2008b). Measuring Interest Group Influence in the EU: A Note on Methodology. *European Union Politics, 9*(4), 559–576.

Dür, A., & de Bièvre, D. (2007). Inclusion without Influence? NGOs in European Trade Policy. *Journal of Public Policy, 27*(1), 79–101.

Eising, R. (2007). Institutional Context, Organizational Resources and Strategic Choices. *European Union Politics, 8*(3), 329–362.

Eising, R., Rasch, D., & Rozbicka, P. (2015). Institutions, policies, and arguments: context and strategy in EU policy framing. *Journal of European Public Policy, 22*(4), 516-533.

Ernst, C. (2019, March 27). *Interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration - Interoperability between EU information systems in the field of borders and visa (debate) (CRE 27/03/2019 - 24)* . Retrieved from European Parliament Debates: https://www.europarl.europa.eu/doceo/document/CRE-8-2019-03-27-ITM-024_EN.html

European Border and Coast Guard Agency (Frontex). (2017, October 16). *Non-paper by Frontex on its access to central EU systems for borders and security*. Brussels: Council of the European Union.

European Border and Coast Guard Agency (Frontex). (n.d.-a). *EU Partners: Council*. Retrieved February 27, 2021, from Frontex: https://frontex.europa.eu/we-build/eu-partners/council/

European Border and Coast Guard Agency (Frontex). (n.d.-b). *EU Partners: European Commission*. Retrieved February 27, 2021, from Frontex: https://frontex.europa.eu/we-build/eu-partners/european-commission/

European Border and Coast Guard Agency (Frontex). (n.d.-c). *EU Partners: European Parliament*. Retrieved February 27, 2021, from Frontex: https://frontex.europa.eu/we-build/eu-partners/european-parliament/

European Commission. (2005, November 24). *Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and*

Home Affairs (*COM(2005) 597 final)*. Brussels: Commission of the European Communities.

European Commission. (2008, March 11). *Communication from the Commission to the European Parliament and the Council: European agencies - The way forward (COM(2008) 135 final)*. Brussels: European Commission.

European Commission. (2016, April 6). *Communication from the Commission to the European Parliament and the Council: Stronger and Smarter Information Systems for Borders and Security (COM(2016) 205 final)*. Brussels: European Commission

European Commission. (2017a, December 12). *Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) (COM(2017) 794 final)*. Brussels: European Commission.

European Commission. (2017b, October 19). *Consultation on the interoperability of EU information systems for borders and security.* Retrieved from European Commission - Migration and Home Affairs Public Consultations: https://ec.europa.eu/home-affairs/content/consultation-interoperability-eu-information-systems-borders-and-security_en

European Commission. (2018, May 31 (last updated)). *High-Level Expert Group on Information Systems and Interoperability (E03435)* . Retrieved from Register of Commission Expert Groups and Similar Entities: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3435

European Commission. (2019, February 5). *Security Union - Closing the Security Gap*. [Factsheet].

European Commission and Europol. (2003). *Administrative Agreement on Co-operation between the European Commission and the European Police Office.* Retrieved from Europol: https://www.europol.europa.eu/agreements/european-commission

European Commission. (n.d.). *Role of the Fundamental Rights Agency.* Retrieved from European Commission: https://ec.europa.eu/info/aid-development-cooperation-

fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/application-charter/role-fundamental-rights-agency_en#areas-of-work-and-scope

European Data Protection Supervisor (EDPS). (2015, December 15). *The EDPS as Supervisor of Large-Scale IT Systems and Member of Supervision Coordination Groups. Policy Paper*. Brussels: European Data Protection Supervisor.

European Data Protection Supervisor (EDPS). (2018, April 16). *Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems*. Brussels: European Data Protection Supervisor.

European Data Protection Supervisor (EDPS). (n.d.). *Our role as an advisor*. Retrieved February 27, 2021, from EDPS Website: https://edps.europa.eu/data-protection/our-role-advisor_en

European Parliament. (2018, July 23). *Amendments 192- 467 to the Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration).* Strasbourg: European Parliament.

European Parliament. (2019, March 27). *Interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration - Interoperability between EU information systems in the field of borders and visa (debate) (CRE 27/03/2019 - 24)* . Retrieved from European Parliament Debates: https://www.europarl.europa.eu/doceo/document/CRE-8-2019-03-27-ITM-024_EN.html

European Parliamentary Research Service (EPRS). (2019, June). *Interoperability between EU border and security information systems. Briefing: EU Legislation in Progress (PE 628.267)*. Strasbourg: European Parliament.

European Police Office (Europol). (2016a, May 12). *Europol contribution on improving the EU information exchange architecture and interoperability in the fight against terrorism and serious and organised crime*. Brussels: Council of the European Union.

European Police Office (Europol). (2016b, September 19). *Europol's updated contribution on its short-term activities in the implementation of the Roadmap on information exchange and interoperability*. Brussels: Council of the European Union.

European Police Office (Europol). (2018). *Europol Data Protection Officer - Freedom and Security: Fighting serious crime and terrorism - defending European values.* Retrieved February 27, 2021, from Europol: https://www.europol.europa.eu/DPF/1.1.EUROPOLS_MANDATE.html

European Union. (n.d.). *European Union Agency for Fundamental Rights (FRA)*. Retrieved February 27, 2020, from European Union Website: https://europa.eu/european-union/about-eu/agencies/fra_en

European Union Agency for Fundamental Rights (FRA). (2017, July 7). *Fundamental rights and the interoperability of EU information systems: borders and security*. Luxembourg: Publications Office of the European Union.

European Union Agency for Fundamental Rights (FRA). (2018a). *Under watchful eyes: biometrics, EU IT systems and fundamental rights.* Luxembourg: Publications Office of the European Union.

European Union Agency for Fundamental Rights (FRA). (2018b, April 11). *Interoperability and fundamental rights implications. Opinion of the European Union Agency for Fundamental Rights*. Luxembourg: Publications Office of the European Union.

European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). (2016, October 27). *JHATech 2016: Aligning the capabilities of technology with policy priorities in the areas of migration and internal security.* Conference Report eu-LISA Annual Conference, Tallinn, Estonia.

European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). (2017, October 17-18). *Going Digital for a Safe and Secure Europe*. Conference Report eu-LISA Annual Conference, Tallinn, Estonia.

European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). (2018a, October 17). *EU Borders - Getting Smarter Through Technology*. Conference Report eu-LISA and Frontex joint conference, Tallinn, Estonia.

European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). (2018b). *Shared Biometric Matching Service (sBMS): Feasibility Study - final report.* Tallinn: eu-LISA.

European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). (2019a). *Interoperability - EU IT systems working together for a safer Europe*. [Leaflet].

European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). (2019b). *Elaboration of a Future Architecture for Interoperable IT Systems at eu-LISA - Summary of the Feasibility Study*. Tallinn: eu-LISA.

European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). (n.d.-a). *EU Institutions*. Retrieved February 27, 2021, from eu-LISA: https://www.eulisa.europa.eu/PartnersStakeholders/Pages/EUInstitutions.aspx

European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). (n.d.-b). *Interoperability*. Retrieved February 27, 2021, from eu-LISA: https://www.eulisa.europa.eu/Activities/Interoperability

Evans, S. W., Leese, M., & Rychnovská, D. (2020). Science, technology, security: Towards critical collaboration. *Social Studies of Science, 00*(0), 1-25.

Fisher, J. A., & Monahan, T. (2011). The "biosecuritization" of healthcare delivery: Examples of post-9/11 technological imperatives. *Social Science & Medicine, 72*, 545-552.

Franz, R. (2019, March 27). *Interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration - Interoperability between EU information systems in the field of borders and visa (debate) (CRE 27/03/2019 - 24)* . Retrieved from European Parliament Debates: https://www.europarl.europa.eu/doceo/document/CRE-8-2019-03-27-ITM-024_EN.html

Galli, F. (2019). Interoperable Law Enforcement: Cooperation Challenges in the EU Area of Freedom, Security and Justice. *EUI Working Papers. Robert Schuman Centre for Advanced Studies*, pp. 1-20.

Garkov, K. (2017, October 17-18). *Going Digital for a Safe and Secure Europe*. Conference Report eu-LISA Annual Conference, Tallinn, Estonia.

Garkov, K. (2018, October 17). *EU Borders - Getting Smarter Through Technology.* Conference Report eu-LISA and Frontex joint conference, Tallinn, Estonia.

Goodey, J. (2017, October 17-18). *Going Digital for a Safe and Secure Europe*. Conference Report eu-LISA Annual Conference, Tallinn, Estonia.

Gornitzka, Å., & Sverdrup, U. (2011). Access of Experts: Information and EU Decisionmaking . *West European Politics, 34*(1), 48-70.

High-level expert group on information systems and interoperability (HLEG). (2017, May 11). *High-level expert group on information systems and interoperability - Final Report*. Brussels: European Commission.

Hönnige, C., & Panke, D. (2013). The Committee of the Regions and the European Economic and Social Committee: How Influential are Consultative Committees in the European Union? *Journal of Common Market Studies, 51*(3), 452-471.

Huysmans, J. (2011). What's in an act? On security speech acts and little security nothings. *Security Dialogue, 42*(4-5), 371–383.

Ingold, K., & Leifeld, P. (2014). Structural and Institutional Determinants of Influence Reputation: A Comparison of Collaborative and Adversarial Policy Networks in Decision Making and Implementation. *Journal of Public Administration Research And Theory*, 1–18.

Kim, J. (2018). The Influence of EU Agencies: Real but guided influence in the policy-making process. Maastricht: Datawyse / Universitaire Pers Maastricht. doi:https://doi.org/10.26481/dis.20181211jk

King, J. (2016, October 27). *JHATech 2016: Aligning the capabilities of technology with policy priorities in the areas of migration and internal security*. Conference Report eu-LISA Annual Conference, Tallinn, Estonia.

King, J. (2019, March 27). *Interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration - Interoperability between EU information systems in the field of borders and visa (debate) (CRE 27/03/2019 - 24)* . Retrieved from European Parliament Debates: https://www.europarl.europa.eu/doceo/document/CRE-8-2019-03-27-ITM-024_EN.html

Klüver, H. (2009). Measuring Interest Group Influence Using Quantitative Text Analysis. *European Union Politics, 10*(4), 535–549.

Klüver, H., Braun, C., & Beyers, J. (2015a). Legislative lobbying in context: towards a conceptual framework of interest group lobbying in the European Union. *Journal of European Public Policy, 22*(4), 447-461.

Klüver, H., Mahoney, C., & Opper, M. (2015b). Framing in context: how interest groups employ framing to lobby the European Commission. *Journal of European Public Policy, 22*(4), 481-498.

Langfeldt, O. (2018, October 17). *EU Borders - Getting Smarter Through Technology*. Conference Report eu-LISA and Frontex joint conference, Tallinn, Estonia.

Leggeri, F. (2018, October 17). *EU Borders - Getting Smarter Through Technology*. Conference Report eu-LISA and Frontex joint conference, Tallinn, Estonia.

Lopes, J. P. (2019, March 27). *Interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration - Interoperability between EU information systems in the field of borders and visa (debate) (CRE 27/03/2019 - 24)* . Retrieved from European Parliament Debates: https://www.europarl.europa.eu/doceo/document/CRE-8-2019-03-27-ITM-024_EN.html

Malinowski, P. (2016, October 27). *JHATech 2016: Aligning the capabilities of technology with policy priorities in the areas of migration and internal security*. Conference Report eu-LISA Annual Conference, Tallinn, Estonia.

Melo, N. (2019, March 27). *Interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration - Interoperability between EU information systems in the field of borders and visa (debate) (CRE 27/03/2019 - 24)* .

Retrieved from European Parliament Debates: https://www.europarl.europa.eu/doceo/document/CRE-8-2019-03-27-ITM-024_EN.html

Merriam-Webster Dictionary. (n.d.). *Definition of 'put the cart before the horse'*. Retrieved Feburary 20, 2021, from Merriam-Webster: https://www.merriam-webster.com/dictionary/put%20the%20cart%20before%20the%20horse

Michalowitz, I. (2007). What determines influence? Assessing conditions for decision-making influence of interest groups in the EU. *Journal of European Public Policy, 14*(1), 132-151.

O'Flaherty, M. (2017, April 25). *Fundamental rights and the interoperability of EU information systems.* Retrieved from European Union Agency of Fundamental Rights (FRA): https://fra.europa.eu/en/speech/2017/fundamental-rights-and-interoperability-eu-information-systems

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

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

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) (Text with EEA relevance).

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 (Text with EEA relevance.).

Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale

IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011Regulation (EU) 2019/817.

Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA.

Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816.

Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624.

Rein, M., & Schön, D. (1996). Frame-Critical Policy Analysis and Frame-Reflective Policy Practice. *Knowledge and Policy: The International Journal of Knowledge Transfer and Utilization, 9*(1), 85-104.

Rinkens, R. (2016, October 27). *JHATech 2016: Aligning the capabilities of technology with policy priorities in the areas of migration and internal security*. Conference Report eu-LISA Annual Conference, Tallinn, Estonia.

Rozenburg, R. (2017, October 17-18). *Going Digital for a Safe and Secure Europe*. Conference Report eu-LISA Annual Conference, Tallinn, Estonia.

Rozenburg, R. (2018, October 17). *EU Borders - Getting Smarter Through Technology*. Conference Report eu-LISA and Frontex joint conference, Tallinn, Estonia.

Ruginis Andrei, A. M. (2017, October 17-18). *Going Digital for a Safe and Secure Europe*. Conference Report eu-LISA Annual Conference, Tallinn, Estonia.

Syrgios, T. (2018, October 17). *EU Borders - Getting Smarter Through Technology.* Conference Report eu-LISA and Frontex joint conference, Tallinn, Estonia.

Toshkov, D. (2016). Single-Case Study Designs. In D. Toshkov (Ed.), *Research Design in Political Science* (pp. 285-309). London: Palgrave.

Trampusch, C., & Palier, B. (2016). Between X and Y: how process tracing contributes to opening the black box of causality. *New Political Economy*, 1-18.

Truman, D. B. (1951). *The Government Process. Political Interests and Public Opinion.* New York, NY: Alfred A. Knopf.

van Hulst, M., & Yanow, D. (2016). From Policy "Frames" to "Framing": Theorizing a More Dynamic, Political Approach. *American Review of Public Administration, 46*(1), 92-112.

Vavoula, N. (2019a). *Interoperability of European Centralised Databases: Another Nail in the Coffin of Third-Country Nationals Privacy?* Retrieved November 18, 2020, from EU Migration Law Blog: https://eumigrationlawblog.eu/interoperability-of-european-centralised-databases-another-nail-in-the-coffin-of-third-country-nationals-privacy/

Vavoula, N. (2019b). Databases for Non-EU Nationals and the Right to Private Life: Towards a System of Generalised Surveillance of Movement? In F. Bignami (Ed.), *EU Law in Populist Times: Crises and Prospects.* (pp. 227–266). Cambridge: Cambridge University Press.

Vavoula, N. (2020). Consultation of EU Immigration Databases for Law Enforcement Purposes: a Privacy and Data Protection Assessment. *European Journal of Migration, 22*, 139-177.

Vos, E. (2000). Reforming the European Commission: What Role to Play for EU Agencies? *Common Market Law Review, 37*, 1113-1134.

Williams, P. (2005). Critical Security Studies. In A. J. Bellamy (Ed.), *International Society and its Critics* (pp. 135-150). New York: Oxford University Press.

9. Appendix

9.1. Interview Guide

The following interview questions are just a general guide of the questions asked in the interviews I conducted since I also tailored the questions to the specific person I was interviewing and asked follow-up questions that I came up with during the interviews.

1. To start off, could you briefly describe your job position and how you and your organisation were involved in the legislative process on the interoperability proposal?

2. What were the key priorities that your organisation wanted to see included in the final interoperability legislation?

3. Do you think that the interoperability proposal was a conflictual issue?

   Follow-up Question: In what way? What were the sides of the conflict?

4. In your opinion, did your organisation try to shape overarching questions and the political direction of the interoperability proposal or did it rather try to influence technical details and practical considerations?

Access to the Policymaking Process:

The next question is about how your organisation gained access to the policymaking process on interoperability. In the EU policymaking process, possible access channels can be, for example, through the European Parliament, the Commission, the Council or the national level. Access can be achieved through direct interaction with decision-makers or through working group and committee members.

5. Which access channels did your organisation use most frequently during the policymaking process?

Informational Activities:

The following questions are about your organisation's activities in the policymaking process and the information it provided to legislative decision-makers. These activities can include participating in formal hearings and working groups as well as having informal contact with policymakers through phone calls, informal personal meetings or emails.

6. Can you outline the type of formal and informal activities your organisation engaged in to participate in the policymaking process and to interact with relevant decision-makers?

7. How frequently did your organisation interact with policymakers involved in the interoperability proposal on average?

8. Did your organisation provide specialised expertise on the interoperability proposals to political decision-makers that they would not have had access to otherwise?

   Follow-up Question: What kind of expertise did your organisation provide to policymakers?

Influence Perceptions:

9. How satisfied are you, from an organisational viewpoint, with the policy outcome on interoperability? Do you think your organisation achieved its aims?

10. Do you think the policymaking process, or the final legislation would have been different if your organisation had not been involved in it? If yes, which aspects of the legislation would have been different?

    OR: Do you think your organisation was influential during the policymaking process?

11. Did you perceive any of the other EU agencies and advisory bodies that also participated in the policy process on interoperability – such as Frontex, Europol, eu-LISA, the Fundamental Rights Agency, or the EDPS – as particularly successful in shaping the policy outcome according to their organisational interests?

9.2. Interview Transcripts

To guarantee the privacy of the respondents, the interview transcripts were only made available to the thesis supervisor and second reader. Therefore, the transcripts are not included in the version of the thesis published in the public online repository. Those interviewees who indicated in the informed consent form that they were happy for their real names to be used in publications and other outputs of the thesis research are identified by name in the thesis and the following table, while the other interviewees are only identified by a job descriptor.

Respondents:

Interviewee	Interview Date	Organisation	Job Description
Olivier Burgersdijk	3 February 2021	Europol	Head of Strategy – European Cyber Crime Centre; Information Manager
Krzysztof Klebek	5 February 2021	Europol	Head of Europol's Business Product Management Team
Krum Garkov	9 February 2021	eu-LISA	Executive Director of eu-LISA
Dina Kampouraki	10 February 2021	EDPS	Staff member in Technology and Privacy Unit of the EDPS
Anonymous (EDPS official)	11 February 2021	EDPS	EDPS staff member
Anonymous (former eu-LISA official)	19 February 2021	Formerly: eu-LISA	Former eu-LISA staff member

9.3. EDPS and FRA recommendations adopted in final regulation

Source: EDPS, 2018		Source: Regulation (EU) 2019/818		
Paragraph in EDPS Opinion	**Recommendation**	**Implemented in final legislation?**	**Counterpart in final legislation**	**Explanation/Additional Notes**
42	The EDPS considers that the purposes of combating irregular migration and contributing to a high level of security in the context of Article 20 are too broad and do not fulfil the requirements of being 'strictly restricted' and 'precisely defined' in the Proposals, as required by the Court. He therefore recommends to further define them in the Proposals.	No	Article 20 (p.62-64)	While Article 20 has been made more precise in general, the purposes for identification have not been further specified and are just as broad as in the proposals.
44	The EDPS considers that access to the CIR to establish the identity of a third country national for purposes of ensuring a high level of security should only be allowed where access for the same purposes to similar national databases (e.g. register of nationals/residents) exist and under equivalent conditions. He recommends to make this clear in the Proposals.	No	Article 20 (p.62-64)	There is no mention in Article 20 of giving access to the CIR only where access for the same purpose to a similar national database exists.
48	Therefore, the EDPS recommends to amend Article 20 to provide that access to the CIR will be allowed: – in principle, in the presence of the person and, – where he or she is unable to cooperate and does not have document establishing his/her identity or, – refuses to cooperate or, – where there are justified or well-founded grounds to believe that documents presented are false or that the person is not telling the truth about his/her identity.	Yes	Article 20 (1) (a)-(e) (p.62-63) Article 20 (2) (p.63)	In Article 20 (1) the circumstances in which CIR may be queried with biometric data are more precisely defined and the contents of these specific circumstances laid out in sub-paragraphs (a) to (e) follow the EDPS' recommendations. The condition that access to the CIR will only be allowed in the presence of the person concerned is included in Article 20 (2).
53	The EDPS therefore recommends to ensure in the Proposals that the data stored in the ECRIS-TCN could only be accessed and used solely for the purposes of the ECRIS-TCN as defined in its founding legal act.	Yes	Article 18 (3)	Article 18 (3) posits, inter alia, that "the authorities accessing the CIR shall do so in accordance with their access rights under the legal instruments governing the EU information systems".
67	He therefore recommends to add in Article 22(1) the conditions related to the existence of reasonable grounds, the	Partial:	Article 22 (1) (p.65)	Article 22 (1) specifies that querying the CIR is permissible only "in a **specific case**, where there are **reasonable grounds** to

	carrying out of a prior search in national databases and the launching of a query of the automated fingerprint identification system of the other Member States under Decision 2008/615/JHA.	Yes – existence of reasonable grounds No – prior search in national database or Prüm system		believe that consultation of EU information systems will **contribute to the prevention, detection or investigation of terrorist offences or other serious criminal offences**". However, there is no provision requiring officers who query the CIR to consult national databases or make use of the Prüm system prior to searching the CIR.
68	In other words, the law enforcement authority getting a hit should always refer to the verifying authority that shall check whether the conditions of accessing the CIR were complied with. In case the ex post independent verification determines that the consultation of the CIR was not justified, the authority shall erase all data originating from the CIR. We recommend to amend Article 22 of the Proposals accordingly.	No	Article 22 (p.65-66) (Article 24 (4) (p.69))	No additional provision added to Article 22 for a verifying authority to check whether conditions of access were fulfilled. However, Article 24 (4) provides that the logs of access to the CIR are regularly verified by the competence supervisory authority to verify whether the conditions set out in Article 22 (1) and (2) are fulfilled (this was already provided for in the proposal though).
72	The EDPS recommends to include in the Proposals a reference to the obligation for eu- LISA and the Member States to follow the principles of data protection by design and by default.	Yes	Recital 61 (p.25)	In Recital 61 specifies that "eu-LISA should apply the principles of privacy by design and by default during the development of the interoperability components."
73	As a preliminary remark, the EDPS observes that some Articles of the Proposals refer to certain provisions of the applicable data protection legislation (i.e. the Regulation 2016/679, the Directive 2016/680 and the Regulation 45/2001), e.g. Articles 46 and 47 of the Proposals. The EDPS understands that these provisions aims at further specifying the relevant articles of the aforementioned legal acts. However to make it clear that these references are without prejudice to the application of other relevant provisions of these legal acts, the EDPS recommends to provide for a provision in the Proposals on the applicability of Regulation 2016/679, Directive 2016/680 and Regulation 45/2001.	Yes	Recital 55 (p.23)	Recital 55 provides that "Regulation (EU) 2016/679, Regulation (EU) 2018/1725 [succeeding Regulation (EC) 45/2001] or, where relevant, Directive (EU) 2016/680 apply to any transfer of personal data to third countries or international organisations carried out under this Regulation."
74	The EDPS welcomes the fact that the Proposals provide a central management on the creation of user profiles with allocation of the legal access rights. However, he stresses that	Yes	Article 8 (3) (p.50)	Paragraph 3 was added to Article 8 and specifies that "the [user] profiles referred to in paragraph 1 shall be reviewed regularly by

	these profiles should be regularly reviewed and if necessary updated. The EDPS recommends to add this obligation in the text of the Proposals.			eu-LISA in cooperation with Member States, at least once per year, and if necessary updated."
75	In Article 7(4) of the Proposals it is defined which EU bodies can access the ESP. The EDPS recommends to add after EU bodies the text "as referred to in paragraph 1".	Yes	Article 7 (4) (p.47)	The addition "as referred to in paragraph 1" was added to the final legislation.
76	The EDPS recommends to add in Article 8 of the Proposals also a reference to the purpose of the query.	No	Article 8 (1) (p.49)	Article 8 (1) makes no reference to the purpose of the query being linked to the user profile.
79	The EDPS recommends to clarify in the Proposals that the reference to dactylographic data in the SIS should only include fingerprints and not palm prints. […] Therefore, the EDPS recommends to change Article 13(1) (c) and 13(1)(d) of the Proposals to ensure that neither the DNA data nor the palm prints will be stored in the shared BMS.	Yes	Article 13 (1) (a)	In Article 13 (1) (a), data on palm prints is explicitly excluded from the specified data referred to in Article 20 (3) (w) and (y) of Regulation (EU) 2018/1862 [SIS regulation]. The reference to Article 20 (3) (w) and (x) of Regulation (EU) 2018/1862 was amended to Article 20 (3) (w) and (y) of said regulation, so that the sub-paragraph (x) on DNA profiles is not referenced anymore in the final proposals.
80	With regard to Article 16(1)(d) of the Proposals the EDPS recommends to provide a definition on the length of the query, since the term is not self-explanatory.	Partial	Article 16 (1)	The reference to the "length of the query" was removed from the paragraph altogether.
83	Therefore, the EDPS is concerned that the Proposals do not sufficiently prevent the possibility of duplication of personal data. He therefore recommends to be more specific in the relevant Articles [Article 17, 18 and 23 (2) and make the necessary changes.	No	Article 18 (p.61) Article 23 (2) (p.67)	The necessary changes were not applied in Article 18 or Article 23 (2
85	Article 23(2) and Article 35 of the Proposals define the retention period of the data stored in the CIR and MID, respectively. […] Therefore, the EDPS recommends to specify in the relevant Articles that automatic deletion of data will apply.	Yes	Article 23 (1) (p.66) Article 35 (p.87)	In the final legislation, an addition was added to both Article 23 (1) and Article 35 specifying that the relevant stored data shall be deleted in an automated manner.
88	Therefore, the EDPS considers that the process of creating links for the purpose of multiple-identity detection would constitute automated decision-making. Consequently, transparency towards the individuals affected and the necessary safeguards for such processing, should be provided for in the Proposals.	Yes	Recital 45 (p.20) Articles 30-33	Recital 45 was added to the final legislation stating that "the creation of such links requires **transparency** towards the individuals affected. In order to facilitate the implementation of the **necessary safeguards** in accordance with applicable Union data protection rules, individuals who are subject to a red link or a white link following manual verification of different identities should be informed in writing". In Articles 30 to 33 on yellow,

				red, green and white links, all references to “verification” are amended to “manual verification” as a safeguard.
90	The EDPS assumes that instead of “different data” it is meant “similar data” and recommend to change Article 30 accordingly. For the sake of clarity, he moreover recommends, to provide in Article 28(4) and Article 30 of the Proposals a uniform definition of a “yellow link”.	No	Article 28 (4) (p.75) Article 30 (p.77-78)	Article 30 was not changed as recommended by the EDPS and still refers to “different identity data” and no uniform definition of yellow link was provided in the two Articles.
91	The EDPS recommends to add in Article 29 of the Proposals that the responsible Sirene Bureau is immediately informed when a yellow link has to be manually verified by it.	No	Article 29 (p.76-77)	No such duty to inform the relevant SIRENE Bureau immediately was added to the Article.
92	The EDPS therefore recommends to introduce a fixed timeframe with specific deadlines and establish a clear procedure to guarantee a timely verification, since such links could potentially have adverse consequences for the person(s) concerned.	No	Article 29	No fixed timeframe and specific deadlines for verifying and updating links are stipulated in Article 29 of the final legislation.
94	Under Article 27(1)(e) of the Proposals the MID is launched when an alert on a person is created or updated in the SIS. However, Article 26(1)(e) and Article 29(1)(e) of the Proposals provide that the Sirene Bureau would only get access to the MID when it updates an alert but not when it creates an alert. The EDPS sees this as an editorial error and recommends to change Article 26 and 29 of the Proposals accordingly.	Yes	Article 26 (1) (a) Article 29 (1) (a) (p.75)	Both Articles were amended to specify “creating or updating an alert” to correct the error pointed out by the EDPS.
95	Since the Proposals do not elaborate when an identity refers lawfully or unlawfully to a person, the EDPS recommends to further clarify the meaning of these terms in the relevant provisions or at least in a recital.	No	/	Could find no clarification on when an identity refers lawfully or unlawfully to a person.
96	Therefore, he recommends to adopt in the Proposals a relevant mechanism under which the Member States themselves can rectify an incorrectly set link.	Yes	Article 31 (3) (p.79) Article 32 (7) (p.83) Article 33 (5) (p.85)	In the Articles on red, green and white links, paragraphs have been added which outline mechanisms by which member states can rectify or erase the links from the MID if they have evidence to suggest that the link has been incorrectly recorded in the MID.

101	The EDPS therefore recommends to redraft Article 56(2) and (3) of the Proposals and to recognise that the data listed under Article 56(2)(a) to (d) and (3)(a) to (c) may lead to identification of individuals and therefore must be protected. This includes once again, performing a thorough information security risk assessment, and implementing adequate security measures, prior to providing this additional central repository. The EDPS also recommends that privacy by design should also be applied when designing the CRRS.	Partial	Article 62 (1) to (3) (p.141-142)	In Article 62 (1) to (3) provisions were added stating that "it shall not be possible to identify individuals from the data." However, despite the warning of the EDPS in paragraph 100 of their opinion that the "combination of nationality, gender and date [year of birth] of a person could lead to individual identification", this was not removed in the final legislation.
107	Therefore, we recommend designating eu-LISA and the competent authorities of the Member States as joint controllers, each with their clearly defined tasks and responsibilities.	No	Article 40 (p.93-94)	In Article 40, eu-LISA is not identified as a data controller.
109	The EDPS recommends that every reference to information security or security plans in the Proposal should be replaced by, 'the implementation of a comprehensive Information Security Risk Management Process (ISRM)'.	No	Recital 61 (p.25) Article 42 (p.95)	The phrase 'Information Security Risk Management Process (ISRM)' is not included in the final legislation. Recital 61 and Article 42 still refer to 'security plan' instead of calling them ISRM.
110-111	When paragraph (1) and (3) of Article 53 of the Proposals are read in conjunction, it follows that eu-LISA will develop a mechanism to carry out such quality checks only after the new systems are operational. The EDPS strongly recommends that automated data quality checks are established as soon as possible and preferably already tested before the entry into operations.	No	Article 55 (1) & (3) (p.116-117)	Article 55 (1) and (3), corresponding to Article 53 (1) and (3) in the Proposals, was not changed according to the EDPS' recommendation in the final legislation.
113	While the Member States' authorities cannot be responsible for the central system, they can be responsible for the security at the end-points in regard to the access to the systems (security of their national communication lines, access controls, authorizations, data processing, etc.). The EDPS recommends to amend Article 42(1) of the Proposals to reflect this distinction.	No	Article 42 (1) (p.95)	Article 42 (1) was not amended according to the EDPS' recommendation in the final legislation.
114	The EDPS recalls that an adequate security plan as defined in Article 42(3) of the Proposals should be the result of a thorough information security risk assessment, which is why	No	Article 42 (3) (p.	There is no reference to an information security risk assessment in Article42 (3) in the final legislation.

	a relevant reference should be made in Article 42(3) of the Proposals.			
115	As reflected in Article 42(3)(i) of the Proposals, the security measures have to be monitored by eu-LISA which also has to take the necessary organisational measures. The EDPS suggests to enhance this provision in order to allow the establishment of a security governance system that will assess the applied security measures taking into account also new technological developments.	Partial	Article 42 (3) (m)	In the final legislation, the provision to "assess those security measures in the light of new technological developments" was added into Article 42 (3) (m) following the EDPS' recommendation. However, no explicit reference was made to establishing a security governance system.
116	The EDPS recommends to include in Article 46 of the Proposals a reference to Article 13 of Directive 2016/680 and in Article 47 of the Proposals a reference to Article 14 and 16 of the Directive 2016/680.	Yes	Article 47 (1) (p.102) Article 48 (1) (p.103)	/
117	The EDPS welcomes the fact that data subjects are informed of the presence of multiple unlawful identities (cf. Article 32(4) of the Proposals). However, he takes note that the proposed limitations of the data subjects' right to information are not in line with Article 13(3) of Directive (EU) 680/2016. Therefore, he recommends to align Article 32(4) of the Proposals with Article 13(3) of Directive (EU) 680/2016.	No	Article 32 (4) (p.82)	Article 32 (4) of the final legislation was not aligned with Article 13(3) of Directive (EU) 680/2016 against the EDPS' recommendation.
119	The EDPS therefore recommends to add in Article 46 of the Proposals that the data subjects should also be informed about the relevant retention periods, the automated decision-making and the fact that personal data is not transferred or made available to third countries, international organisations or private parties with the exception of transfers to Interpol.	Yes	Article 47 (1)	In Article 47 (1) it is stated that "persons whose data are collected [shall be provided] with the information required under Articles 13 and 14 of Regulation (EU) 2016/679, Articles 12 and 13 of Directive (EU) 2016/680 and Articles 15 and 16 of Regulation (EU) 2018/1725". The referenced Articles include provisions to inform data subjects about the information recommended by the EDPS.
121	The EDPS recommends to add in Article 13(2) and Article 18(2) of the Proposals a reference to the Member State responsible and with regard to Article 26(2) of the Proposals a reference to Article 34(d). This way, it would be ensured that the data subject can effectively exercise his or her rights.	No	Article 13 (2) (p.55) Article 18 (2) (p.61) Article 26 (2) (p.71)	/
122	With regard to Article 47(3) of the Proposals, the EDPS observes that this paragraph only refers to the right to	Yes	Article 48 (p.103)	The right to restriction of processing personal data is included in Article 48 of the final legislation.

	correction and erasure, but not to the right to restriction. The EDPS recommends to add the right to restriction in Article 47(3) of the Proposals.			
123	The EDPS recommends to add in Article 47 of the Proposals a relevant paragraph which should entail an obligation for the Member State to forward the access request to the Member State responsible.	No	Article 48 (3) (p.104)	Just as in the proposals, Article 48 (3) in the final legislation only foresees that a request of correction and erasure, but not for access, should be forwarded by the Member State receiving such a request to the responsible Member State.
124	The EDPS recommends to add in Article 47 of the Proposals an obligation for the Member States to inform the data subject that his or her request was forwarded, while indicating the contact details of the competent authority in the relevant Member State.	Yes	Article 48 (3) (p.104)	A provision was added to Article 48 (3) stating that: "The person concerned shall be informed by the Member State which contacted the authority of the Member State responsible for the manual verification of different identities about the further procedure." This implies that data subjects have to be informed about their request being forwarded and likely also receive contact details of the relevant authority in the responsible MS, although this is not made explicit in the final legislation. The wording in the final legislation about informing the data subject about "the further procedure" is left vaguer than the wording recommended by the EDPS.
125	With regard to Article 47(4) of the Proposals the EDPS recommends to include an obligation for the Member State to immediately inform the data subject after his or her data were corrected or deleted.	Yes	Article 48 (4) (p.104)	The provision that "the person concerned shall be informed by the Member State which contacted the ETIAS Central Unit about the further procedure" after requesting the rectification or erasure of personal data was added to the final legislation. However, the wording in the final legislation about informing the data subject about "the further procedure" is left vaguer than the wording recommended by the EDPS.
126	The EDPS recommends that an adequate awareness rising campaign should be launched by the Member States and at EU level before the interoperability components are implemented and they become fully operational.	Unclear (not discernible from legislation)	/	/
128	However, the EDPS recommends to emphasize in Article 68(3) of the Proposals that eu-LISA should only have access to personal data under strict safeguards and for legitimate and specific purposes. In this respect, the Proposals should clearly define relevant situations when the eu-LISA may legally access personal data, as for example when a Member State	Partial	Article 74	The relevant paragraph 3 of Article 68 in the proposals was deleted from the corresponding Article 74 in the final legislation.

	asks eu-LISA to intervene for deconfliction of data (especially with biometrics) or for support etc. The EDPS therefore asks to explore these circumstances and - if required - amend the Proposals accordingly.			
129	The EDPS furthermore stresses that any access by eu-LISA should be logged and strongly recommends to insert in the Proposals a relevant provision.	Redundant	/	See above.
131-132	However, following the Commission's plan and the feasibility study concerning the CIR, a hybrid solution would apply for a certain period of time. Hence, the data that are stored in the CIR would remain in the underlying systems to ensure the proper functioning of the new system. This means that for an undefined period of time there would be a duplication of data. The EDPS acknowledges the necessity of such a period, however, this hybrid solution should be reflected in the transitional Article of the Proposals and it should be stressed that this hybrid solution should only be in place for a limited time period.	No	/	The hybrid solution concerning the data stored in the CIR and the underlying systems was not reflected in the transitional Articles of the final legislation.
133	The EDPS welcomes that the interoperability components will store logs for the purposes of data protection and monitoring. However, he recommends that the Proposals should also include provisions that will **clarify who shall have access to the logs, and how this access is granted**, since the relevant Article 42 of the Proposals does not provide any additional information concerning the management and access to these logs.	Yes	Article 40 (4) (p.94)	Paragraph 4 was added to Article 40 in the final legislation stating: "For the purposes of data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, **the data controllers shall have access to the logs referred to in Articles 10, 16, 24 and 36 for self-monitoring** as referred to in Article 44".
136	The EDPS recommends to store the logs of the ESP and the shared BMS also at national level, as are the logs of the CIR (Article 24(5)) and the MID (Article 36(2)).	Yes	Article 10 (2) (p.52) Article 16 (2) (p.58)	In the articles on the keeping of logs of the ESP and the shared BMS, a paragraph was added to store the logs also on the national level: "Each Member State shall keep logs of queries that its authorities and the staff of those authorities duly authorised to use the ESP/shared BMS make."
138	The EDPS strongly advises to introduce a provision which states that each Member State shall ensure that the supervisory authority or authorities designated pursuant to	Yes	Article 51 (1) (p.109)	Paragraph 1 was added to Article 51 in the final proposals stating: "Each Member State shall ensure that the supervisory authorities independently monitor the lawfulness of the

	Article 51 of Regulation (EU) 2016/679 and Article 41 of Directive (EU) 2016/680 shall monitor the lawfulness of the processing of personal data under the Proposed Regulations.			processing of personal data under this Regulation by the Member State concerned, including their transmission to and from the interoperability components".
139	The EDPS recommends to add in Article 44 (3) of the Proposals the national supervisory authority.	Yes	Article 43 (3) (p.98)	Competent supervisory authorities were added to the list of bodies to be notified in the case of a security incident in paragraph 3 of Article 43.
140	In order to enable the EDPS to effectively supervise eu-LISA as part of his competencies, he considers that he should be put in the list of recipients of the reports that eu-LISA has to publish in accordance with Article 68(2) and (4) of the Proposals.	No	Article 74 (2) and (3) (p.160)	The EDPS was not added to the list of recipients of the reports eu-LISA has to publish in accordance with Article 74 (2) and (3) of the final legislation.
141	While Article 49 (2) of the Proposals foresees that the national supervisory authorities should have sufficient resources to fulfil their tasks entrusted to them under this Regulation, the EDPS recommends to include a similar provision in Article 50 in order to ensure adequate resources for him.	No	Recital 58 (p.24) Article 52	An addition was made to Recital 58 stating that "for the European Data Protection Supervisor to fulfil the tasks entrusted to it under this Regulation, sufficient resources, including both human and financial resources, are required." However, in the relevant Article 52, no provision was included to ensure that the EDPS should have sufficient resources to fulfil the tasks entrusted to them in the regulation.

FRA, 2018b			Regulation (EU) 2019/818	
Opinion Number	**Recommendation**	**Implemented in final legislation?**	**Counterpart in final legislation**	**Explanation/Additional Notes**
1. Non-discrimination and general fundamental rights safeguard clause				
1	rename Article 5 to "Fundamental rights", thus reflecting the fact that interoperability may impact on a variety of rights enshrined in the EU Charter of Fundamental Rights.	Yes	Article 5 (p.46)	Article 5 was renamed from "Non-discrimination" to "Non-discrimination and fundamental rights".
	add a first paragraph according to which "This Regulation respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union and shall be applied in accordance with those rights and principles."	No	/ (but see Recital 79 on p.35)	While the recommended sentence is found in the final regulation in Recital 79 (and was already included in the Commission's 2017 proposal in Recital 68), it was not added as a first paragraph in Article 5.
	add a horizontal data protection safeguard clause to pay particular attention to ensuring that processing of personal data for the purposes of the proposed regulations do not result, either directly or indirectly, in undue interferences with the right to respect for private and family life, and the right to protection of personal data.	No	Recital 40 (p.17)	In Recital 40, instead of adding data protection safeguard clauses as recommended, interferences with the fundamental rights protected by Article 7 (right to respect for private and family life) and 8 (right to protection of personal data) are justified with reference to the objective of the EU information systems, effective border protection, asylum and visa management and internal security. However, it is up to interpretation whether that interference is 'undue'.
	add "social origin" as well as "colour" to the grounds for non-discrimination listed in Article 5.	Yes	Article 5 (p.46)	"Processing of personal data for the purposes of this Regulation shall not result in discrimination against persons on any grounds such as gender, 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."
	include "persons in need of international protection" among the groups of persons to whom particular attention should be paid in the implementation.	Yes	Article 5 (p.46)	"Particular attention shall be paid to children, the elderly, persons with a disability and **persons in need of international protection**."
2. Objectives of interoperability				
2	The EU legislator should include a new Recital in the proposals referring to the use of interoperability for child protection purposes. In view of strengthening the protection of	No	/	There are only four instances of the word "child" in the final legislation, none of which refer to using interoperability in a targeted way for child protection purposes. The phrases

	unaccompanied children, upon the identification of a missing child, such a Recital should recommend that EU Member States should promptly contact the child's guardian as well as relevant national child protection authorities. They should undertake a needs assessment with a view to finding a sustainable solution for the child in accordance with his or her best interests as required by Union and/or national law.			"unaccompanied children", "child protection", "child protection authorities" or "needs assessment" were not included in the final legislation.
3	The EU legislator should change the wording of proposed Article 2 (2) to reflect the different levels of sensitivity of data stored in the single IT systems. One possibility could be to rephrase Article 2 (2) (e) as follows: "Strengthening and simplifying data security and data protection conditions that govern the respective EU information systems, without prejudice to the special protection and safeguards afforded to certain categories of data".	Yes	Article 2 (2) (e) (p.39)	The wording of Article 2 (2) (e) is very similar to the one recommended by the FRA: "strengthening, simplifying and making more uniform the data security and data protection conditions that govern the respective EU information systems, without affecting the special protection and safeguards afforded to certain categories of data".
3. European Search Portal				
4	The current wording of Article 9 of the proposals is ambiguous and could lead to different interpretations. In Article 9 (1) the wording "in accordance with the user profile and access rights" is connected to the search launched by the officer instead of being related to the response he or she receives. The last sentence of Article 9 (6) seems to suggest that "where necessary" the officer could have access to additional information beyond what the officer is authorised to see. To ensure compliance with the principle of purpose limitation, the EU legislator should adjust the wording of Article 9 (1) to make clearer that a search launched by an officer only queries the systems he or she is authorised to access. In addition, the last sentence of Article 9 (6) should be deleted.	Yes	Article 9 (1) & (6) (p.50-51)	Article 9 (1) was rephrased to exclude any mention of access rights and makes it clear that the phrase "in accordance with the user profile" refers to the query being launched not the response. However, since the rephrasing excludes a mention of access rights altogether, it also does not clarify that "a search launched by an officer only queries the systems he or she is authorised to access" as recommended by the FRA (2018:19). The last sentence of Article 9 (6) was removed in the final legislation as recommended by the FRA and additionally makes it clear that replies to user queries "shall contain only the data to which the user has access under Union and national law" (*Regulation* (EU) 2019/818, p.51).
5	The EU legislator should design interoperability in a way that – while respecting the legal framework regulating Interpol – the data owner would not receive any information that their databases have been queried through the European Search Portal (ESP), at least for those individuals who are registered in Eurodac as asylum applicants.	Yes	Article 9 (5) (p.51	Article 9 (5) was rephrased to clarify that "no information shall be revealed to the owner of the Interpol alert" (*Regulation* (EU) 2019/818, p.51) when Interpol databases are queried through the ESP. This strengthened the clause previously included in the Commission's proposal, which only stated that the "data used by the user of the ESP to launch a query is not shared with the owners

				of Interpol data" (COM(2017) 794 final, p.41). However, even if the data put into the ESP is not shared, simply sharing that a query has been launched by a particular EU MS could put people at risk, which is eliminated by the clause that no information whatsoever can be shared with the owner of an Interpol alert.
4. Biometric Matching Service				
6	The EU legislator should, therefore, amend Article 13 (1) by deleting from Paragraph (1) (d) the reference to Article 20 (3) (x) of the SIS proposal on police and judicial cooperation, since this refers to DNA. Moreover, with regard to Article 13 (1) (c)-(e) the EU legislator should clarify that the references to dactylographic data in SIS should only include fingerprints and not palm prints.	Yes	Article 13 (1) (a) (p.55)	In the final legislation, the reference to Article 20 (3) (x) [DNA profiles] of the SIS proposal on police and judicial cooperation (Regulation (EU) 2018/1862) was removed and replaced with a reference to Article 20 (3) (y) [dactyloscopic data] of the SIS regulation, with data on palm prints being explicitly excluded from the obtained data to be stored in the shared BMS.
7	The EU legislator should add a sentence to Article 13 (2) clarifying that an officer launching a query using the shared Biometric Matching Service will see only the references to those information systems that he or she is authorised to access.	Partial	Article 13 (1) and (2) (p.55)	No sentence like this is added to Article 13 (2). However, in Article 13 (1) a sentence is added clarifying that "the biometric templates shall be stored in the shared BMS in logically separated form according to the EU information system from which the data originate" (Regulation (EU) 2019/818, p.55). This implies that, since the biometric templates are logically separate from one another, the references to the information systems a user receives are likely to be separated in the same way.
8	The EU legislator should include the word "automatically" in Articles 15 and 23 of the proposals dealing with the deletion of stored data.	Yes	Article 15 (p.57) Article 23 (p.66)	This recommendation was implemented in Article 15 (p.58) through the inclusion of the phrase "the data shall be erased from the shared BMS in an automated manner" and in Article 23 (p.67) through the inclusion of the phrase "the data referred to in Article 18(1), (2) and (4) shall be deleted from the CIR in an automated manner in accordance with the data retention provisions".
5. Common Identity Repository				
9	The EU legislator could mention expressly the value of the Common Identity Repository to improve data accuracy in one of the relevant Recitals, taking inspiration from the wording included in Article 2 (2) (c) of the proposals (= "The objectives of ensuring interoperability shall be achieved by […] improving and harmonising data quality requirements of the	No	/	While Recital 10 in the final regulation (and already in the Commission's proposal) states that interoperability between EU information systems can "improve and harmonise the data quality requirements of the respective EU information systems", no recital was included that states this in reference to the CIR. However, in recitals 21-23, the value of the CIR in respect to increasing the accuracy of identification is elaborated (these

	respective EU information systems" (COM(2017) 794 final, p.37)).			recitals were already included in the proposal though, so the FRA's recommendation wanted something more explicit than mentioned in those).
10	The EU legislator should amend the reference to Article 15 (2) (a) of the ETIAS Regulation in Article 18 (1) (c) of the proposals. Such reference should read "[the data referred to in Article 15 (2) (a) to (e) of the ETIAS Regulation, except the first name(s) of the parents of the applicant]".	Yes	Article 18 (1) (c) (p.61)	No reference to ETIAS regulation Article 15 anymore in the final legislation. Instead, the data to be stored in the CIR is defined as the data referred to in the ECRIS-TCN regulation (Regulation (EU) 2019/816) Article 5 (1) (b) and (2) and a listing data referred to in Article 5 (1) (a). The list of this data given in the interoperability regulation does not include parents' first names as recommended by the FRA (despite parents' first names being included in ECRIS-TCN Article 5 (1) (a) (ii)).
11	The EU legislator should clarify in Article 18 – for example by adding a new paragraph after paragraph two – that an officer accessing the Common Identity Repository should only be able to see those components of the identity file stored in the repository which originate from IT systems he or she is authorised to access, indicating the legal provisions relating to the specific situations where the regulation provides otherwise.	Yes	Article 18 (3) (p.61)	A Paragraph 3 was added to Article 18 stating: "The authorities accessing the CIR shall do so in accordance with their access rights under the legal instruments governing the EU information systems, and under national law and in accordance with their access rights under this Regulation for the purposes referred to in Articles 20, 21 and 22."
12	The EU legislator should amend Article 20 – as well as the corresponding Recital 29 – to meet the requirements of foreseeability. To that end, the precise purposes of identity checks allowing to query the Common Identity Repository must be clearly set at EU level.	Partial	Recital 30 (p.12) Article 20 (5) (p.64)	Article 30 (the article corresponding to Article 29 in the proposal) was NOT amended for the final legislation. In Article 20 (5), it still says that member states must adopt national legislative measures that specify the precise purposes for identification using the CIR with the only caveat being that these specified purposes must fall within the realm of the purposes laid down in Article 2 (1) (b) and (c) (p.38) (i.e. preventing illegal immigration and contributing to internal security).
	To comply with necessity and proportionality requirements, the EU legislator should set clear conditions for accessing the Common Identity Repository under Article 20, such as limiting the use of the provision to "the absence of a credible document proving the identity of the person".	Yes	Article 20 (1) (a)-(e) (p.62-63)	In Article 20 (1) (a)-(e) of the final legislation, all the circumstances in which police authorities are allowed to query the CIR are defined on the EU level. Thus, Article 20 (1) does set out clear conditions on when the CIR can be accessed, but these conditions are broader than the example given by the FRA, i.e. a search can also be carried out when there are doubts about the authenticity of documents or the identity of the person and NOT ONLY in the absence of a credible travel document.

	Article 24 (2) should also log the location of access and logs should be designed in a way to establish if the same person is checked multiple times.	Partial	Article 24 (2) (a), (3) (a), (4) (d)	Paragraphs 2, 3 and 4 in Article 24 were amended to state that logs must include the Member State or Union agency querying the CIR. This amounts to logging the location of access as recommended by the FRA. However, there was no provision included in Article 24 to check whether the same person is checked multiple times.
	To reduce the negative consequences of false matches, Article 20 should be amended by enabling only biometric searches and searches with travel document data.	No	Article 20 (3)	Just as in the proposal, the final legislation still allows the CIR to be checked with identity data provided by the person to be checked IF the biometric data and travel document data of that person cannot be used.
13	The EU legislator should reinforce the obligation to correct mistakes by including somewhere in the proposal a provision inspired by Article 35 (3) of the EES Regulation obliging a Member State other than the data controller who has evidence about an erroneous red link to rectify it. Such a provision would support the horizontal efforts to ensure data quality, which are visible throughout the proposals.	Yes	Article 32 (7) (p.83)	Article 32 (7) sets out the conditions on how member state authorities and Union agencies go about rectifying and erasing red links when they have evidence that the red link has been incorrectly recorded in the MID.
14	Provide in Article 22 for a verification of queries to the Common Identity Repository by an authority acting in an independent capacity, such as the national central access point or, preferably, the national supervisory authority. Recital 33 of the proposals should be amended accordingly.	No	Article 22 (p.65-66) Recital 36 (p.15)	Concerns streamlining of law enforcement access: An independent authority for the verification of queries was not provided for in Article 22 of the final legislation. Recital 36 (corresponding to Recital 33 in the proposal) was also not amended accordingly.
	Maintain in the legal instruments governing the individual EU systems as far as possible the cascade system and require, as a minimum, a prior check in national databases before querying the Common Identity Repository. Recital 34 of the proposals should be amended accordingly.	No	/	No mention of requiring prior checks before launching a query in the CIR mentioned in the final legislation. Recital 34 of the proposals was removed from the final legislation altogether.
	Identify a solution for conducting a Prüm check before requesting full access to the information stored in the individual IT systems which does not unreasonably delay the consultation. Recital 34 of the proposal should be amended accordingly.	No	/	No mention of Prüm checks in the final legislation. In the proposals, Prüm checks were argued to become redundant once the CIR was implemented (COM(2017) 794 final, p.9). Recital 34 of the proposals was removed from the final legislation altogether.

	Amend Article 24 (4) (a) replacing the current wording "the national file reference" with "the reference to the national investigation or case".	Partial	Article 24 (4)	The sub-paragraph (a) in Article 24 (4) containing the wording "the national file reference" in the proposal was removed altogether in the final legislation.
6. Multiple Identity Detector (MID)				
15	To reduce possible disproportionate negative effects on women and other categories of persons with multiple lawful identities, the EU legislator should add an explicit reference at the end of the first sentence of Article 28 (5) underlining that such implementing acts should be designed in a manner that protects persons with multiple lawful identities against discrimination	No	Article 28 (5) (p.75) (Recital 39 (p.17))	No such explicit reference was added to Article 28 (5). However, it is mentioned in Recital 39 that "the MID should include safeguards against potential discrimination and unfavourable decisions for persons with multiple lawful identities" (Regulation (EU) 2019/818, p.17).
16	To reduce the negative impact of inaccurate identity information stored in ETIAS, the system should flag to the user when a yellow link is the result of inconsistencies with the identity data contained in ETIAS. The Handbook envisaged in Article 67 should provide guidance to Member States on how to deal with such situations without creating a disproportionate burden on those persons, who, without any intention to deceive the authorities, have entered inaccurate or ambiguous data in ETIAS.	Unclear	Article 73 (p.158)	Article 73 on the practical handbook does not exactly dictate the contents of this handbook, so it is unclear whether guidance on ETIAS data will be included in it.
17	The EU legislator should delete Article 18 (1) (e) thus excluding ECRIS-TCN data from the Common Identity Repository.	No	Article 18 (1) (p.61)	Concerns purpose limitation: The inclusion of ECRIS-TCN data was not deleted from Article 18 (1) in the final legislation.
18	The EU legislator should include a horizontal provision, for example in Article 29, reflecting the statement in Recital 42 and thus requiring, whenever possible, the authority responsible for the manual verification to consider plausible arguments presented by the third-country national when deciding on the colour of the links.	No	Article 29 (3) (p.77) (Recital 43 (p.18))	In the paragraph on assessing multiple identities, there is no provision for including the person concerned by this assessment into the process.
	The EU legislator should introduce a duty for Member States to designate a central verification authority at national level. Such an authority should include staff with fundamental rights expertise. This authority would have the task to provide	No	(Article 72 (p.157))	No provisions for setting up such national central verification authorities. The only provisions that go in that direction are in Article 72 (called "Training"), in which it is stated that MS authorities and Union agencies should provide their staff that

	guidance to the authorities in charge of the verification, monitor their work and develop best practices through cooperation in a network of other central verification authorities in other Member States. It could also support eu-LISA with the improvement of data quality.			processes data using interoperability components with training programmes concerning data security, data quality, data protection rules, etc. It posits that particular attention should be paid to the process of multiple-identity detection and verification while maintaining appropriate fundamental rights safeguards.
19	The EU legislator should strengthen the duty to inform by deleting public order from the list of grounds of restrictions in Articles 32 (4) and by ensuring that, in the case of red links, third-country nationals are still notified, as soon as such a notification is no longer capable of jeopardising on-going investigatory proceedings.	No	Article 32 (4) (p.82) Article 33 (4) (p.85)	Public order was not deleted from the restrictions in the final regulation and no provision was made to notify TCN once the notification no longer poses a threat to on-going investigations.
7. Reporting and Statistics				
20	The EU legislator should consider strengthening the provision in Article 39 (3) by requiring that the personal data be truly anonymised, i.e. made non-identified and non-identifiable, so as to avoid also the risk of indirect identification of individuals whose data are stored in the Central Repository for Reporting and Statistics (CRRS). Additionally, Article 56 (2) (b) and Article 56 (3) (a) referring to "nationality, sex and year of birth of the persons" should be complemented with a safeguard noting that this should "not lead to identification of the person concerned".	Yes	Article 39 (3) (p.92) Article 62 (1), (2), (3) (p.141-142)	Article 39 (3) is strengthened in the final legislation by adding the following provision: "The data contained in CRRS shall not allow for the identification of individuals." Additionally, in Article 39 (4), concerning the composition of the CRRS, it is added that "the CRRS shall be composed of: (a) the tools necessary for anonymising data". The provision "It shall not be possible to identify individuals from the data." was added to paragraph 1, 2 and 3 of Article 62 (= the article corresponding to Article 56 of the proposals).
	To mitigate the risk of discrimination when producing reports on the basis of the Central Repository for Reporting and Statistics, the EU legislator should redesign Article 56 by requiring Member States to assign the responsibility to produce statistics and reports to a designated central point.	No	Article 62 (p.141-143)	Article 62 was not redesigned to assign the responsibility to produce statistics and reports to a designated central point.
	The possibility to receive customisable statistics on the use of the repository by eu-LISA could be extended to relevant EU agencies when needed to evaluate the impact on fundamental rights of the interoperability regulations.	Yes	Article 62 (7)	Article 62 (7) was added for the Commission to make relevant information available to the FRA in order to evaluate the impact of the Interoperability regulation on fundamental rights.
8. Right to Information				
21	The EU legislator should consider the following measures to strengthen the right to information included in Article 46 of the proposals:		Article 47 (p.102)	

	Expressly require that the information provided should also cover the **different purposes** of the data processing, who the recipients of the data are and the **retention time**, as well as the right to **lodge a complaint** with the supervisory authority.	Yes	Article 47 (1) (p.102)	The information to be provided to data subjects as recommended by the FRA is included in the final regulation by pointing (among others) to the relevant articles in the GDPR (namely Article 13 and 14 of the GDPR regulation).
	Add explicit information on the fact that personal data may be accessed by law enforcement authorities, drawing upon Article 50 of the EES Regulation and Article 30 of the Eurodac proposal.	No	Article 47 (p.102)	No explicit information is added in Article 47 that personal data can be accessed by law enforcement authorities.
	Taking into account the target audience (i.e. third-country nationals), add an explicit provision on providing information in a language that the person understands or is reasonably expected to understand, drawing on Article 30 of the Eurodac proposal and Article 50 of the EES Regulation.	Yes	Article 47 (2) (p.102)	Added a second paragraph to Article 47 which states that "all information shall be made available, using clear and plain language, in a linguistic version the person concerned understands or is reasonably expected to understand".
	Add an explicit reference to providing the information to children in an age-appropriate manner, drawing upon Article 30 (2) of the Eurodac proposal, as well as Recital 58 and Article 12 of the GDPR and Recital 39 of the Police Directive.	Yes	Article 47 (2) (p.102)	Added a second paragraph to Article 47 which states that information should be provided "in a manner which is appropriate to the age of the data subjects who are minors".
22	The EU legislator should include in Article 46 (2) (d) also a reference to Articles 13 and 14 in addition to Article 10 of the Eurodac Regulation to cover also the collection of personal data of third-country nationals or stateless persons in an irregular situation.	Unclear	Article 47 (3) (p.102)	Reference to Eurodac deleted altogether from Article 47.
	The EU legislator should extend the duty to inform also to all individuals who are processed under SIS.	No	Article 47 (3) (p.102)	According to paragraph 3 of Article 47, the rules on the right to information shall only apply to personal data recorded in ECRIS-TCN (not SIS).
9. Right of access, correction and deletion				
23	The EU legislator should extend the scope of Article 47 on the right of access, correction and erasure of personal data to cover also the Common Identity Repository.	No	Article 48 (p.103)	The title of Article 48 makes explicit that the right of access, rectification and erasure of personal data only extends to the data stored in the MID, not the CIR.
24	The EU legislator should add a new provision to Chapter VII of the proposed Interoperability Regulations establishing an EU-wide request handling mechanism for all requests for access, correction and deletion of personal data. The EU-wide request handling mechanism should be tasked with providing information, logging the request and actions taken by the	Partial	Article 49 (p.107-108)	Article 49 in the final legislation provides for a web portal to be established to facilitate the exercise of the rights of access to, rectification, erasure or restriction of processing of personal data. However, the Article does not provide for the web portal to log, forward and monitor requests related to those rights – it simply

	responsible authorities, forwarding the request to the responsible authority in the Member States, monitoring that the responsible authority responds, and offering a space where the concerned person could download the national authority's reply. eu-LISA could administer such a single European entry point and be tasked to prepare regular reports on the number of requests submitted, the response time and decision taken by the national authorities.			provides contact details for the competent authorities and template emails for establishing contact.
	In addition, to increase the effectiveness of access, correction and erasure procedures, the EU legislator should:			
	replace the time limit of 45 days in Article 47 (2) of the proposals with the wording "as soon as possible, and at the latest in 45 days".	Yes	Article 48 (2) (p.103)	In the final legislation, the time limit was replaced with the wording "without undue delay and in any event within 45 days of receipt of the request" which is sufficiently equivalent to the FRA's recommended phrasing.
	cover in Article 47 (3) also requests for access to personal data.	No	Article 48 (3) (p.104)	Paragraph 3 of Article 48 in the final legislation still only refers to a request for rectification or erasure of personal data, not access to personal data.
	include in Article 47 (3) a duty to inform in writing any person who has approached a Member State other than the one responsible to review the request, indicating to whom the request has been forwarded.	Yes	Article 48 (3) (p.104)	This duty to inform was provided for by adding the following last sentence to paragraph 3 of Article 48: "The person concerned shall be informed by the Member State which contacted the authority of the Member State responsible for the manual verification of different identities about the further procedure".
	add a provision in Article 47 (4) that a written confirmation on the correction or deletion should be sent to the data subject.	Yes	Article 48 (4) (p.104)	Such confirmation was provided for by adding the following last sentence to paragraph 4 of Article 48: "The person concerned shall be informed by the Member State which contacted the ETIAS Central Unit about the further procedure".
	replace the reference to "the supervisory authority or authorities designated pursuant to Article 49 of Regulation (EU) 2016/679" in Article 49 (1) with "the supervisory authority" so as to cover also supervisory authorities designated to monitor the application of the Police Directive and to be consistent with Article 4 (4) of the proposals.	Yes	Article 51 (1) (p.109)	The reference was replaced with a reference to "the supervisory authorities".