From Theory To Practice: Exercising The Right Of Access Under The Law Enforcement And PNR Directives

by **Plixavra Vogiatzoglou, Katherine Quezada Tavárez, Stefano Fantin and Pierre Dewitte***

Abstract: The right of access is often considered as the most important prerogative in the data subject's toolkit because it grants individuals the possibility to complement the information made available through privacy notices, but also because it paves the way for the exercise of other rights enshrined in data protection law, such as the rights to erasure or rectification. While the efficiency of the right of access under the General Data Protection Regulation has already been abundantly documented, there is a lack of empirical evidence as to its counterparts in the area of law enforcement and security. This contribution aims to fill that gap and provide insight into the practical exercise of the right of access in the Law Enforcement and Passenger Name Record Directives. Through both traditional desktop research and a legal-empirical study, the present paper delves into the national transpositions of those texts in a selection of Member States, and highlights the issues encountered when practically exercising the right of access against competent authorities and Passenger Information Units. It also draws upon the lessons learned from that exercise and suggests solutions and ways forward in order to overcome the obstacles faced along the way.

Keywords: Law Enforcement Directive; PNR Directive; data subject's rights; data access requests; legal-empirical study

Recommended citation: Plixavra Vogiatzoglou, Katherine Quezada Tavárez, Stefano Fantin et al., From Theory to Practice: Exercising the Right of Access under the Law Enforcement and PNR Directives, 11 (2020) JIPITEC 274 para 1

A. Introduction

1 The "EU data protection reform package", as introduced in 2016, comprises the widely known General Data Protection Regulation (GDPR)[1] as well as the Law Enforcement Directive (LED)[2]. The latter, on which this paper is partly focused, governs the collection and use of data in a security-related environment, as it applies to the processing of personal data by controllers for law enforcement

* Plixavra Vogiatzoglou is a doctoral researcher, Katherine Quezada Tavárez is a legal researcher, Stefano Fantin is a doctoral researcher and Pierre Dewitte is a doctoral researcher at the KU Leuven Centre for IT & IP Law (CiTiP) – imec. All authors have contributed equally to this paper.

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 (GDPR).

2 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89 (LED).

purposes.[3] The second focal point of this paper is the Passenger Name Record (PNR) Directive[4], which was enacted at the same time and regulates the transfers of passenger information to authorities that process the data for the purposes of prevention, detection, investigation and prosecution of serious crime, including terrorism.

2 Given the scarce empirical evidence documenting the exercise of the data subject's rights in the contexts of law enforcement and security, we decided to gather empirical evidence by testing the right of access under the LED and the PNR Directive against national competent authorities and Passenger Information Units (PIUs), respectively. Given the nature of those instruments, we also investigated how the LED and the PNR Directive have been transposed into national laws, paying close attention to the provisions dealing with the exercise of the right of access. The empirical data used for this study originate from Subject Access Requests (SARs) submitted to competent authorities and PIUs in eleven European countries, namely: Belgium, Cyprus, France, Greece, Ireland, Italy, Luxembourg, Malta, the Netherlands, Portugal, and the United Kingdom (UK).

3 This paper proceeds as follows. Section B sets the scene by detailing the rationale and scope of the research. Section C delves into the methodology adopted for the gathering of the empirical evidence. Section D outlines the legal frameworks under scrutiny and highlights the relevant provisions for the analysis performed in the subsequent sections. Section E, divided into two core parts, is devoted to the results of the empirical research. First, it sets out the theoretical framework by examining the scope of the right of access in the LED and the PNR Directive and investigating its relevance in security-related situations. Second, it examines the practical implementation of the right of access under the LED and the PNR Directive across the investigated Member States by summarising the results of our study. Section F then provides an assessment of the overall research findings and identifies common trends and areas for improvement in the national practices regarding the exercise of informational rights in security. Finally, Section G concludes this study and outlines some recommendations that may facilitate the exercise of the data subject's rights in a security context.

B. Rationale and scope

I. Rationale: Legality, accessibility and safeguards

4 When implementing norms into law, states must abide by national and international requirements aiming at safeguarding democratic values such as the rule of law. In addition, when adopting legal instruments that regulate the processing of personal data, fundamental rights, namely to privacy and to data protection, must not be impermissibly interfered with. More specifically, as enshrined in the European Convention on Human Rights (ECHR) and the Charter of Fundamental Rights of the EU (the Charter), interferences with fundamental rights can be justified upon the condition that they meet the requirement of legality, pursue a legitimate aim of general interest, and are necessary and proportionate to achieve the said aim.[5]

5 In accordance with the jurisprudence of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU), legality derives from the rule of law principle and incorporates the protection of citizens against arbitrary interferences with their fundamental rights.[6] For an interference to be considered lawful, two conditions must be satisfied: the existence of a national law – a requirement easily met – and the quality of law.[7] The latter requires the said legislation to be accessible, foreseeable and to provide judicial safeguards, especially in cases where the law

3 Considering that the scope of the LED is restricted to the processing of data carried out by competent authorities (as defined in art 3(7) of the LED) for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

4 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2016] OJ L119/132 (PNR Directive).

5 See Council of Europe, European Convention on Human Rights (last amendment 2010) (ECHR), art 8(2). Charter of Fundamental Rights of the EU [2016] OJ C202/391 (Charter), art 52(1). Moreover, according to the Charter, art 52(3), legality and proportionality under both the Charter and ECHR may be interpreted in a similar fashion, at least in the sense that the fundamental rights safeguards established under the ECHR are the baseline of protection for the Charter rights.

6 *Malone v the UK* App no 8691/79 (ECtHR, 2 August 1984); *Sisojeva and others v Latvia* App no 60654/00 (ECtHR, 15 January 2007).

7 For an in-depth analysis of the requirement of legality under the ECtHR jurisprudence, see Geranne Lautenbach, *The Concept of the Rule of Law and the European Court of Human Rights* (Oxford University Press, 2013).

grants wide discretionary powers to governmental authorities.[8] Accessibility, more specifically, is achieved insofar as citizens are able to know the rules applicable to a given situation.[9] Besides, the requirement of foreseeability is met when the law is clear enough to enable individuals to grasp the consequences of an infringement and the conditions under which the government may take actions.[10]

6 For an interference to be justified, the principle of proportionality *lato sensu* must also be respected. In other words, the interfering measure must be suitable and appropriate to meet the objective of general interest (here, security), strictly necessary and least onerous in relation to that objective. It must also be proportionate *stricto sensu*, i.e. achieve a fair balance.[11] In cases of legislation relating to security authorities and the rights to privacy and to data protection, proportionality and strict necessity are assessed by virtue of minimum safeguards providing individuals with sufficient guarantees to effectively protect their rights against the risk of abuse.[12] Such safeguards include the clear delineation of the conditions and circumstances under which authorities may undertake the interfering measures; for instance in relation to access to and use of personal data, as well as the existence of prior authorisation, supervision, notification and effective remedies for the affected individuals.[13]

7 The existence of judicial safeguards, linked to both legality and proportionality[14], is mainly discussed in cases where a Member State enjoys wide discretionary powers, such as in the field of security, and requires the existence of effective control, preferably by the judiciary, over the interfering measure.[15] According to both the ECtHR and the CJEU, any legislation imposing surveillance measures must also provide for the possibility of an individual to seek effective remedy in order to obtain information and/or access to the data relating to her or him. In the security field, discretionary powers conferred upon public authorities must be balanced through safeguards ensuring that individuals are adequately protected against arbitrary or abusive exercise of said powers.[16]

8 States have the responsibility to comply with and guarantee citizens' rights at a level that is considered acceptable as per national, international and European human rights legal instruments. When implementing a national law that may affect the rights of individuals, states have the obligation to meet the threshold of protection guaranteed by these instruments, which may be considered higher for states than for private entities given the constitutional and primary nature of human rights. Against this backdrop, it may be expected from states, when implementing laws on personal data processing by governmental security authorities, to comply with the legality requirement and set the example for the effective exercise of citizens' rights. The national transposition of the conditions for the exercise of the right of access before security authorities is instrumental in fulfilling these requirements.

1. Scope: The LED and the PNR Directive

9 One of the driving forces behind the EU data protection reform package was to increase the effectiveness of data protection rules by enhancing the control of individuals over their personal data.[17] The resulting instruments therefore include strong data protection safeguards aiming at ensuring the

8 *Malone* (n 6).

9 ibid.

10 ibid, *Leander v Sweden* App no 9248/81 (ECtHR, 26 March 1987); *Roman Zakharov v Russia* App no.47143/06 (ECtHR, 04 December 2015).

11 Jonas Christoffersen, *Fair balance: proportionality, subsidiarity and the primarity in the European Convention on Human Rights,* (Martinus Nijhoff Publishers, 2009).

12 For an extensive overview of the jurisprudence and minimum requirements in question see *Big Brother Watch and others v the UK* Apps nos. 58170/13, 62322/14 and 24960/15 (ECtHR, 13 September 2019); *Zakharov* (n 10); Joined cases C-203/15 and C-698/15 *Tele2 Sverige AB v Postoch telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, [2016] ECLI:EU:C:2016:970; Opinion 1/15 [2017] ECLI:EU:C:2016:656.

13 ibid.

14 The existence of judicial safeguards as part of the legality assessment may be assessed through the lens of proportionality and may overlap with the guarantees provided for by the right to an effective remedy enshrined in ECHR, art 13 and Charter, art 47. See Lautenbach (n 7).

15 *Klass and others v Germany* App no 5029/71 (ECtHR, 6 September 1978).

16 ibid.

17 European Commission, 'COM(2010) 609 final - Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - A Comprehensive Approach on Personal Data Protection in the European Union' (European Commission 2010) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264> accessed 20 June 2020.

highest standards of data protection across the EU. In that spirit, the LED was adopted in 2016 as an evolution of the Council Framework Decision 2008/977/JHA (CFD)[18]. The LED had the effect of broadening the scope of the CFD and the realm of legal safeguards and protections of individual rights when data processing takes place in the context of criminal investigations and proceedings.

10 Concomitantly, the terrorist attacks of the 21st century and the growing pressure towards enhanced cooperation on security and crime-related information led to the establishment of a passenger data exchange system in the EU.[19] A passenger name record (PNR), in particular, consists of a record of a passenger's information, which is necessary to enable reservations for each journey the passenger embarks on by plane.[20] While discussions on an internal EU PNR data exchange system date back to 2007, concerns on its nature and necessity raised by the European Parliament stalled its adoption until 2015, when the terrorist attacks in Europe raised that matter into swift motion.[21] The PNR Directive finally entered into force on 4 May 2016. The controversy, however, follows the PNR Directive which was challenged before German and Austrian administrative courts and the Belgian Constitutional Court. The German and Belgian courts decided to submit references for preliminary rulings before the CJEU, with questions regarding the compatibility of the directive with the fundamental rights to privacy and to data protection, due to its broad scope and the generalised processing of data it imposes.[22]

11 Similar to the GDPR, both the LED and the PNR Directive provide data subjects with "informational power"[23] by incorporating the right of access as part of the data subject's prerogatives. In particular, the right of access can function as a mechanism to address power asymmetries resulting from information imbalances in a security environment.[24] Yet, this informational empowerment is subject to a more limited scope in a security-related context, as explained in more detail under section E.

12 Data subjects' rights would, however, be worthless if they did not work in practice, be it because access to information is limited under domestic law or because of procedural obstacles to their exercise. While the right of access used to be disregarded and rarely exercised by data subjects,[25] it is currently growing

18 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L350/60 No longer in force (CFD).

19 In particular, following 9/11, the first EU-US Passenger Name Records (PNR) Agreement was adopted in order to provide US authorities access to passenger data collected by air carriers. The Agreement, later substituted by a newer version with a different legal basis, essentially provides US authorities with access to the traveling information of every passenger flying from the EU to the US, but not vice-versa. See Maria Tzanou, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance*, Modern Studies in European Law (Oxford: Hart Publishing, 2017), https://doi.org/10.5040/9781509901708.; Cristina Blasi Casagran, 'The Future EU PNR System: Will Passenger Data Be Protected?' (2015) 23 European Journal of Crime, Criminal Law and Criminal Justice 241.

20 PNR Directive, art 3(5) states that "PNR means a record of each passenger's travel requirements which contains information necessary to enable reservations to be processed and controlled by the booking and participating air carriers for each journey booked by or on behalf of any person, whether it is contained in reservation systems, departure control systems used to check passengers on to flights, or equivalent systems providing the same functionalities". PNR data are further explained through a list of 19 data categories in Annex I PNR Directive, including inter alia name, payment information and advance passenger information (API) data collected (e.g. nationality, family name, gender, date of birth).

21 See Tzanou (n 19); David Lowe, 'The European Union's Passenger Name Record Data Directive 2016/681: Is It Fit for Purpose?' (2016) 16 International Criminal Law Review 856.

22 From Germany: request for a preliminary ruling in joined Cases C-148/20, C-149/20 and C-150/20 *Deutsche Lufthansa* [2020] OJ C279/21 (pending) and Case C-222/20 *Bundesrepublik Deutschland* [2020] OJ C279/30 (pending); from Belgium: Case C-817/19 *Ligue des droits humains* [2020] OJ C36/16 (pending).

23 Jef Ausloos, Michael Veale and René Mahieu, 'Getting Data Subject Rights Right: A Submission to the European Data Protection Board from International Data Rights Academics, to Inform Regulatory Guidance' (2019) 10 JIPITEC 283, 296.

24 René LP Mahieu and Jef Ausloos, 'Recognising and Enabling the Collective Dimension of the GDPR and the Right of Access. A Call to Support the Governance Structure of Checks and Balances for Informational Power Asymmetries' [2020] LawArXiv <https://osf.io/preprints/lawarxiv/b5dwm> accessed 14 July 2020.

25 As widely shown by empirical evidence. See Antonella Galetta, Chiara Fonio and Alessia Ceresa, 'Nothing Is as It Seems. The Exercise of Access Rights in Italy and Belgium: Dispelling Fallacies in the Legal Reasoning from the "Law in Theory" to the "Law in Practice"' (2016) 6 International Data Privacy Law 16, 21; Clive Norris and others (eds), *The Unaccountable State of Surveillance: Exercising Access Rights in Europe* (Springer International Publishing 2017) 106; Jef Ausloos and Pierre Dewitte, 'Shattering One-Way Mirrors. Data Subject Access Rights in Practice' (2018) 8 International

in popularity as a tool to foster transparency of data controllers, perhaps as a consequence of the increasing awareness resulting from recent privacy backlashes. This is certainly the case in the private sector, as illustrated by the extensive empirical evidence gathered and documented in the current literature.[26] Nevertheless, we suspect that the right of access remains a largely unknown and underused prerogative, at least in the area of law enforcement and security – an idea that seems supported by the research findings upon which this paper is based.[27] In other words, while scholars have already thoroughly explored the practical exercise of the right of access under the GDPR, the functioning of its counterparts in both the LED and the PNR Directive is still largely undocumented. This is particularly timely for the PNR Directive, since the European Commission issued its review[28] on 24 July 2020, the conclusions of which were "overall positive".[29] It was found that, although some Member States "have failed to fully mirror all [data protection requirements] in their national laws", overall compliance is achieved. No mention is made of the practical exercise of data subjects' rights, however.[30] Besides, it is not clear to what extent the data protection reform has contributed to the enhancement of the right of access.[31] Thus, it is still necessary to determine how the "architecture of empowerment"[32] brought by the EU reformed data protection legal framework works in practice in security-related data processing.

C. Methodology

13 The findings discussed in the present contribution build on two distinct initiatives. First, traditional desk research exploring the right of access as well as the transposition of both the LED and PNR Directive into national law. Second, a legal-empirical study during which we analysed the transparency measures adopted by competent authorities and PIUs, and exercised our right of access against the relevant controller(s). This section briefly introduces the reader to the methodology deployed in order to gather and analyse the results detailed in the remainder of the paper.

Data Privacy Law 4, 7.

26 For a detailed account of the experiences of an individual's attempts to access CCTV data through SARs, see Keith Spiller, 'Experiences of Accessing CCTV Data: The Urban Topologies of Subject Access Requests' (2016) 53 Urban Studies 2885; for a thorough overview of the practical exercise of the right of access under the now repealed 1995 Directive and an empirical analysis involving organisations in the public and private sectors across different EU countries, see Norris and others (n 25); for a study on the exercise of the right of access under the national implementation of the 1995 Directive in the Netherlands, as well as an assessment of to what extent the right of access involves a mechanism for citizens to obtain meaningful actual transparency in the public and private sector, see René LP Mahieu, Hadi Asghari and Michel van Eeten, 'Collectively Exercising the Right of Access: Individual Effort, Societal Effect' (2018) 7 Internet Policy Review <https://policyreview.info/articles/analysis/collectively-exercising-right-access-individual-effort-societal-effect> accessed 29 April 2020; for an empirical examination of the right of access under the 1995 Directive against online platforms, as well as a detailed account on the difficulties encountered by data subjects when attempting to exercise access rights, see Ausloos and Dewitte (n 25); for a study uncovering the flaws in policies and practices on how the right of access under the GDPR is handled, as well as the dangers in that relation, see Mariano Di Martino and others, 'Personal Information Leakage by Abusing the GDPR "Right of Access"', *Proceedings of the Fifteenth Symposium on Usable Privacy and Security* (2019); other right of access initiatives and experiences by individuals, journalists, and civil society are inventoried in Mahieu and Ausloos (n 24).

27 Some of the referenced literature somewhat relate to security (as they included SARs to obtain CCTV footage, police records and data collected by Europol (see Spiller (n 26); Galetta, Fonio and Ceresa (n 25); and Norris and others (n 25)). However, none of the SARs in those earlier studies was filed under legal instruments specifically covering the processing of data in law enforcement and security (such as the LED and the PNR Directive).

28 Due by 25 May 2020, PNR Directive, art 19(1). Similarly, a review for the LED is due to take place by 6 May 2022, in accordance with LED, art 62(1).

29 European Commission, 'Report from the Commission to the European Parliament and the Council, On the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime', (Communication) COM (2020) 305 final.

30 ibid. According to the report, under footnote 17, '[a] comprehensive assessment of the completeness and conformity of the national transposing measures and their practical implementation has been carried out in the framework of the compliance assessment, conducted by an external contractor, under the supervision of the Commission.' This compliance assessment has nonetheless not been made public nor was made available upon the submission by one of the authors of an application for access to documents, due to protection of court proceedings, of the purpose of investigations and of the decision-making process.

31 As claimed in Norris and others (n 25), chapter 3.

32 Mahieu and Ausloos (n 24) 2.

I. General set-up

14 Both the desk research and the legal-empirical study were conducted by three researchers in Law at the KU Leuven Centre for IP & IT Law assisted by three students of the KU Leuven Advanced Master of Intellectual Property & ICT Law acting in the context of their Master's Theses. The desk research was conducted in January 2020, while the legal-empirical study spanned over a period of four months between February and June 2020. Initially, the intention was to investigate twelve countries, selected on the basis of the languages we speak as well as the countries we had flown to, from or through during the six months preceding the sending of the SARs[33]. Amongst the initially selected countries was Spain, which had not, at the time, transposed neither the LED nor the PNR Directive.[34] The workload on the remaining eleven countries[35] was then evenly shared based on the above-mentioned criteria. At each step of the process, we shared our findings through dedicated online surveys designed to orient the empirical research and provide an appropriate means to obtain meaningful, structured results at the end of the allocated time frame. Those surveys raised both quantitative (e.g. how many days did it take for the PIU to provide a first substantive answer?) as well as qualitative (e.g. how satisfied are you with the process of sending the access request?) issues. Regular meetings between the researchers and the students were held in order to ensure a shared understanding of the questions included in the surveys as well as the consistency of the results.

II. The desk research: The transpositions of the LED and PNR Directive into national law

15 Unlike the GDPR, which materialised the long-awaited shift from a directive to a regulation, the law enforcement reform was achieved through the means of directives. As a result, it was agreed to delve into the national transposition of the LED and PNR Directive for each of the investigated countries with the aim of uncovering the extent to which Member States had – or had not – diverged from the European texts. More specifically, the emphasis was put on the way each Member State had transposed the provisions related to data protection safeguards and the right of access as well as the modalities surrounding its exercise. We compiled our findings into two surveys: one for the LED and one for the PNR Directive. The results were then shared in order to have a common understanding of the transposing acts and relevant provisions in national law.

III. The legal-empirical study: Transparency measures and exercise of the right of access

16 The desk research served as a basis for the legal-empirical study, which itself consisted of two distinct efforts. First, we performed an analysis of the transparency measures put in place by each Member State according to the relevant provisions of both the LED and the PNR Directive as well as the national transposing acts. To that end, we went through the relevant texts in order to find the identity of the controller as well as (potential) instructions as to how to file an access request. We also browsed the websites of the said entities in order to assess their compliance with the transparency obligations stemming from European and national law. The second effort substantiated in the sending of an actual access request under both the LED and the PNR Directive. Here, the goal was to gather practical evidence as to how – and, in some cases, if – competent authorities and PIUs would handle the exercise of the data subject's rights. In order to ensure the comparability of the results, we relied on pre-defined templates when exercising our right of access.[36] Regular meetings also helped smooth out the obstacles faced along the way by systematically agreeing on a common pathway in the individual interactions we had with the competent authorities. At the end of the allocated time frame, we

33 This follows from the obligation for PIUs to depersonalise the Passenger Name Record (PNR) data after a period of six months by masking a series of data points that could serve to identify directly the passenger to whom the PNR data relate. See PNR Directive, art 12(2).

34 Because of that, the European Commission brought action before the CJEU against Spain to declare the failure to fulfil its obligations under Article 63(1) LED and to impose financial penalties for such failure and for as long as the infringement continues to take place. Case C-658/19 *European Commission v Kingdom of Spain,* [2019] OJ C357/27 (pending). At the time of submission of the paper (29 October 2020) Spain had still not transposed the LED. However, Spain published the national law transposing the PNR Directive on 17 September 2020. The latter was not taken into account for this paper, since the empirical study was concluded in June 2020. See Spain: Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del Registro de Nombres de Pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves.

35 Namely Belgium, Cyprus, France, Greece, Ireland, Italy, Luxembourg, Malta, the Netherlands, Portugal and the UK.

36 Attilia Ruzzene, 'Drawing Lessons from Case Studies by Enhancing Comparability' (2012) 42 Philosophy of the Social Sciences 99.

compiled our findings into two surveys dealing with transparency obligations and the sending and following-up of the access requests, respectively.

IV. Limitations

17 Before proceeding with the analysis of the results, it is worth highlighting some of the limitations of this research. First, several questions raised in the online surveys are subjective in nature (e.g. how easy/difficult would you describe the process of finding whom to send the access request to?). While the answers might therefore differ depending on the perception of each participant, this was mitigated by the introduction of more quantifiable indicators (e.g. Likert scales, amount of interactions during the follow-up process), the regular meetings and the experience of the researchers and students in the fields of European privacy and data protection law. Second, the selection of countries investigated is limited. The languages spoken by the participants as well as their travel history did not allow us to cover all EU countries. It should also be noted that the UK, which is currently in the process of leaving the EU, is among the selected countries. Moreover, it was decided to submit the SARs in an official language of each investigated country, so as to facilitate the process. We therefore cannot know whether language has been an impediment to or requirement for the requests, while the findings could potentially be different if they were submitted in English. Third, the legal-empirical study was conducted at a time when the COVID-19 pandemic started to escalate in Europe. While this had a limited impact on the desk research, it has potentially affected the accuracy of the findings related to the handling of the requests by (allegedly or genuinely) overwhelmed competent authorities and PIUs.

V. Objective

18 Beyond gathering and presenting concrete evidence as to the compliance of competent authorities and PIUs with data subjects' rights, the goal of this initiative is also to highlight the added-value of supplementing classic desk research with empirical findings in order to explore the many facets of an issue that might – at first sight – seem rather theoretical. Building on a similar initiative conducted throughout the academic year 2016-2017[37], the involvement of Masters students is also seen as a way to both offer a more interactive research path compared to traditional Master's Thesis topics and expand the coverage of the empirical part of the initiative. While the findings presented below certainly are the core contribution of this paper, we also aim to raise awareness on and promote the benefits of the potential of this type of research.

37 Ausloos and Dewitte (n 25).

D. The Directives and their transposition into national law

I. The Law Enforcement Directive

1. Scope of application

19 According to Articles 1 and 2, the scope of application of the LED extends to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection and prosecution of crimes, the execution of criminal penalties, and the safeguarding of public security. While the rather broad definitions of the term "public security"[38] and "competent authorities"[39] have sparked academic interest[40], what seems to converge in both scholars' and policymakers' views[41] is that law enforcement agencies *stricto sensu* (i.e. national police bodies and their local ramifications) fall under the scope of the LED. Moreover, as "public authorities competent for the prevention [..] of criminal offences" and "other bodies or entities entrusted by Member State law to exercise public authority and public powers" for the same law enforcement purposes also fall under the LED[42], its scope is much broader than criminal justice authorities.

38 European Data Protection Supervisor (EDPS), 'A further step towards comprehensive EU data protection - EDPS recommendations on the Directive for data protection in the police and justice sector' (Opinion No. 6/2015).

39 LED, art 3(7).

40 For a scholarly account of the broad limits of the term 'competent authorities', see Plixavra Vogiatzoglou and Stefano Fantin, 'National and Public Security Within and Beyond the Police Directive', in Anton Vedder, Jessica Schroers, Charlotte Ducuing and Peggy Valcke (eds), *Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security* (Intersentia, Cambridge, Antwerp, Chicago, 2019).

41 Diana Alonso Blas, 'The proposed Directive on data protection in the area of police and justice: A closer look – The omission of Europol and Eurojust from the draft Directive', (ERA Conference: Data Protection in the Area of European Criminal Justice Today – Speakers' Contributions, Trier, November 2012).

42 LED, art 3(7).

20 Territorially speaking, the LED is the first attempt by the EU to regulate both cross-border and internal data processing by law enforcement agencies at the same time and within the same legislation. The territorial scope is therefore extended at the domestic level (including intra- or inter- agencies of the same country) and at the cooperation level between law enforcement agencies based in different Member States of the Union. Such an approach is one of the most important differences between the LED and its predecessor, the CFD, which only applied to the processing of personal data in the context of cross-border police and judicial cooperation.[43] Overall, Article 1(3) of the LED allows Member States to apply higher data protection standards than the ones enshrined in the LED itself. This, in addition to the fact that the legal instrument used by the European legislator requires a national transposition, triggered high expectations among observers about how this potentially fragmented landscape would work in practice at its full operational capacity.[44]

2. Main provisions

21 The LED draws its foundations in the legacy of both the EU and the Council of Europe (CoE) legal instruments dealing with data protection. In particular, the CoE's Convention 108 is amongst the first international legal instruments to lay down, back in 1981, a series of principles which have served as a basis for many developments in the field. Along these lines, the so-called data protection principles play a crucial role in establishing the main safeguards for the processing of personal data in the LED. Those include lawfulness, fairness, purpose limitation, data minimisation and the security of processing.[45] The LED also specifically deals with the retention of data by competent authorities, emphasising that storage and retention periods should be reviewed periodically.[46]

22 The LED establishes specific data categories, which correspond to clear guidelines on the governance of data processing. Accurate distinctions should accordingly be made between different classifications of data subjects (suspects, convicted, victims, other persons)[47] and the diverse nature of the data (personal data linked to facts v. those based on personal assessments)[48]. Moreover, the processing of special categories of data, i.e. data revealing racial or ethnic origin, political opinions, sexual life and orientation, religious or philosophical beliefs, trade union membership and biometrics, is only allowed when strictly necessary and authorised by EU or domestic law, unless the processing is conducted to protect someone's vital interest or if the data was manifestly made public.[49]

23 Chapter IV[50] introduces a series of obligations for controllers. Those provisions mirror, to a large extent, the basic requirements that are also enshrined in the GDPR, and include the duty to implement data protection by design and by default, record-keeping policies, data protection impact assessment exercises, the security of processing, data breach notifications and the appointment of a data protection officer (DPO).[51] Additionally, the sector-specific obligation is imposed to maintain a record of logs when the processing operation is automated, which should be designed to comply with prompt accessibility in case of internal or supervisory audits.[52]

24 Chapter VI describes the governance of supervisory authorities. Interestingly, the LED leaves room for national implementing acts to appoint a different supervisory body than the data protection authority

43 Another significant difference is the legal context under which the LED is adopted (Treaty on European Union (Consolidated version 2016), OJ C202/1 (TEU), art 16), in contrast with the CFD, which was instead adopted in the context of the so-called 'third pillar' (also known as *Justice and Home Affairs-JHA*, then renamed *Police and Judicial Co-operation in Criminal Matters - PJCCM*).

44 Thomas Marquenie, 'The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework', (2017) Computer Law & Security Review: The International Journal of Technology Law and Practice, 33(3), 324–340.

45 LED, art 4.

46 ibid, art 5.

47 ibid, art 6.

48 ibid, art 7.

49 ibid, art 10.

50 In Chapter III, the LED enshrines a series of information rights (more on this will be elaborated in section E.I.2.). Accordingly, law enforcement agencies (LEAs) are required to provide data subjects with information about data processing in a clear, concise, intelligible and easily accessible form. Such information should be made public proactively (LED, art 12), or under the direct request of a data subject, who is entitled to exercise his right of access (LED, art 14), rectification, erasure or restriction (article 16). While a deeper analysis on LED, arts 12 to 17 will be conducted in a separate section, it is useful to mention here that a number of limitations to the exercise of such rights may apply.

51 LED, arts 20, 27, 29, 30-31, 32.

52 ibid, arts 24-25.

established under the GDPR, while it remains possible to designate the same national supervisory authority (NSA).[53] As analysed below, this resulted in a fragmented landscape since some Member States decided to appoint a different supervisory body than the one competent under the GDPR. Nonetheless, according to Chapter VIII, NSAs are tasked with receiving the first instance of data subjects' complaints.[54] Data subjects are also entitled to seek effective remedy before national judicial bodies against decisions of supervisory authorities or alleged violations of the LED.[55]

3. Results from desktop research on national implementing acts

25 All the countries we investigated had transposed the LED between March 2018 – the earliest being Belgium[56] – and August 2019 – the latest being Greece[57]. They all used a wording similar to the LED when circumscribing its scope of application, namely the prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties and the protection of public security. Cyprus, however, states that national security activities carried out by police bodies do not fall under the scope of the transposing act. This suggests that the original mandate of the Cypriot police authorities is not limited to law enforcement duties, but also includes national security and intelligence competences (which are excluded by the national LED transposition)[58]. Finally, only six out of the eleven Member States (the UK, Belgium, Portugal, Malta, Cyprus and Italy)[59] name the competent authorities that are included in the scope of such acts, either by explicit mention, such as in the UK[60] where the said list is included as an annex in the law, or by clear cross-reference in the text to the statutory laws establishing or regulating the competent authority, as in the case of Italy[61].

II. The PNR Directive

1. Scope of application

26 The legal basis for the PNR Directive is found in the Area of Freedom, Security and Justice of the Treaty on the Functioning of the EU,[62] and in particular in its provisions on judicial cooperation in criminal matters[63] and police cooperation for the collection,

53 ibid, art 41(3).

54 ibid, art 52.

55 ibid, art 53. For the sake of completeness, the LED includes Chapter V (transfers to third countries or international organizations), Chapter VII (cooperation), Chapter IX (implementing acts) and Chapter X (final provisions).

56 Belgium: Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

57 Greece: Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προ- στασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις.

58 Cyprus: Ο περί της Προστασίας των Φυσικών Προσώπων Έναντι της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα από Αρμόδιες Αρχές για τους Σκοπούς της Πρόληψης, Διερεύνησης, Ανίχνευσης η Δίωξης Ποινικών Αδικημάτων ή της Εκτέλεσης Ποινικών Κυρώσεων και για την Ελεύθερη Κυκλοφορία των Δεδομένων Αυτών Νόμος του 2019, art 2.

59 See scope of application and competent authorities within the following national acts: UK: Data Protection Act 2018; Belgium: see (n 56); Portugal: Lei n.º 59/2019, de 8 de agosto, que aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016; Malta: Data Protection Act (CAP. 586), Data Protection (Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties) Regulations, 2018; Cyprus: see (n 58); Italy: Attuazione della direttiva UE 2016/680 del Parlamento Europeo e del Consiglio, del 27.4.2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

60 UK: (n 59) Schedule 7.

61 Italy: (n 59) art 2(cc).

62 Treaty on the Functioning of the European Union (Consolidated version 2016), OJ C202/1 (TFEU).

63 ibid, art 82(1): "Judicial cooperation in criminal matters

storage and exchange of relevant information[64]. According to its Article 1, the PNR Directive establishes the obligation for air carriers to transfer PNR data to a designated national authority, and regulates the processing by and the exchange of PNR data amongst Member States. While this obligation is imposed only in relation to extra-EU flights, the PNR Directive leaves the possibility for Member States to extend such a system to intra-EU flights.[65] The processing of PNR data pursuant to the PNR Directive is limited to the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime.

2. Main provisions

27 Air carriers must provide PNR data of every passenger traveling from or landing in the territory of a Member State to the national PIUs.[66] PIUs process PNR data against predetermined assessment criteria to "identify persons who require further examination by competent authorities" as well as analyse PNR data in order to update or provide for new assessment criteria.[67] They are also responsible for transferring PNR data and the processing results to Europol and to the nationally appointed authorities entitled to request or receive them.[68] Such authorities must be competent for the prevention, detection, investigation or prosecution of terrorist offences or serious crime and may vary from law enforcement to customs to broader security authorities.[69]

28 The PNR Directive sets a number of safeguards surrounding the processing of personal data.[70] PIUs must appoint a DPO in order to monitor the processing activities and act as a single point of contact for data subjects.[71] The predetermined criteria on the basis of which PIUs further process some passengers' data must not be based on characteristics that consist of discriminatory grounds, such as ethnic origin, health or religion.[72] Automated positive matches and transfers to competent authorities must be reviewed by a human.[73] PNR data must be depersonalised through masking after a period of six months, be retained for a total period of five years and then be permanently deleted.[74] Disclosure of PNR data after the period of six months is only allowed under specific conditions.[75] Competent authorities are bound to process the transferred PNR data only for the specific purposes of preventing, detecting, investigating or prosecuting terrorist offences or serious crime.[76]

29 Member States should introduce a prohibition on automated decision-making with adverse legal or similarly significant effects on a person.[77] In addition, such decisions may not be based on sensitive characteristics that consist of discriminatory grounds.[78] The PNR Directive points to the CFD – now repealed and replaced by the LED – when it comes to data subject's rights, data security, processing records and notification of data breaches.[79] In addition, it prohibits the processing of special categories of data.[80] Fur-

in the Union shall be based on the principle of mutual recognition of judgments and judicial decisions and shall include the approximation of the laws and regulations of the Member States in the areas referred to in paragraph 2 and in Article 83. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall adopt measures to: (a) lay down rules and procedures for ensuring recognition throughout the Union of all forms of judgments and judicial decisions; [..]".

64 ibid, art 87(2): "For the purposes of paragraph 1 [police cooperation], the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, may establish measures concerning: (a) the collection, storage, processing, analysis and exchange of relevant information; (b) support for the training of staff, and cooperation on the exchange of staff, on equipment and on research into crime-detection; (c) common investigative techniques in relation to the detection of serious forms of organised crime."

65 PNR Directive, art 2.

66 ibid, arts 4 and 8.

67 ibid, art 6.

68 ibid, art 4.

69 ibid, art 7.

70 ibid, art 6.

71 ibid, art 5.

72 ibid, art 6(4).

73 ibid, art 6(5).

74 ibid, art 12(2).

75 ibid, art 12(3).

76 ibid, art 7(4).

77 ibid, art 7(6).

78 ibid.

79 ibid, art 13.

80 ibid, art 13(4) which states that Member States shall prohibit the processing of PNR data revealing a person's race or

thermore, it includes procedural provisions regarding the exchange of information between Member States,[81] the conditions for access to PNR data by Europol[82] and the transfer of data to third countries.[83] Finally, an NSA must be appointed in each Member State for advising on and monitoring the application of the PNR Directive.[84]

3. Results from desktop research on national implementing acts

30 Out of the investigated countries, only Ireland did not extend the PNR scheme to intra-EU flights.[85] It is noticeable that two Member States, namely Belgium[86] and France[87], expanded the purposes of the PNR scheme to also include border control and the fight against illegal immigration.[88]

31 Most transposing laws adopted the same definitions for PNR data and data categories. Insofar as competent authorities entitled to receive or request PNR data are concerned, most Member States specifically enumerate them in the law, apart from the UK[89]. Nevertheless all of them have notified the list of competent authorities to the European Commission.[90] Interestingly, besides law enforcement authorities, most Member States also include national security/intelligence services (Belgium, Cyprus, Greece, Luxembourg, Malta, the Netherlands and Portugal) as well as customs authorities (Belgium, Cyprus, Greece, Luxembourg, Malta and Portugal) in the list of competent authorities.[91] Cyprus, Greece and Malta have also explicitly included financial and anti-money laundering units in the list, while Ireland and Malta also refer to immigration authorities.[92] Even more strikingly, the list of authorities competent to receive PNR data from PIUs also include the Dutch Military, the Irish Department of Employment and Social Protection, and the Hellenic Coast Guard and Fire Department.[93]

32 Almost half the Member States investigated (Cyprus, France, Greece, Ireland and Portugal)[94] require approval only by a judicial authority before a competent authority can access the data held by the domestic PIU upon expiry of the period of six months. The Dutch law does not explicitly prohibit the competent authorities from taking automated decisions producing adverse legal or similarly significant effects to persons, nor on the basis of

ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation. In the event that PNR data revealing such information is received by the PIU, they shall be deleted immediately.

81 ibid, art 9.

82 ibid, art 10.

83 ibid, art 11.

84 ibid, art 15.

85 Ireland: European Union (Passenger Name Record Data) Regulations 2018, arts 3-4.

86 Belgium: Loi du 25 décembre 2016 relative au traitement des données des passagers, Chapitre 11.

87 France: Décret n° 2018-714 du 3 août 2018 relatif au « système API-PNR France » et modifiant le code de la sécurité intérieure (partie réglementaire), art R-232.15.

88 A matter that has been raised by the Belgian Constitutional Court before the CJEU in the pending case *Ligue des droits humains* (n 22).

89 UK: The Passenger Name Record Data and Miscellaneous Amendments Regulations 2018, art 2.

90 Notices from Member States, Passenger Name Records (PNR) — Competent authorities — List of competent authorities referred to in Article 7 of Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (This list reflects the authorities entitled, in each Member State, to request or receive PNR data or the result of processing those data from their national Passenger Information Unit (PIU) or for the purpose of Article 9(3) of Directive (EU) 2016/681 directly from the PIU of any other Member State only when necessary in cases of emergency) (2018) OJ C194/ 1.

91 ibid.

92 ibid.

93 ibid.

94 Cyprus: Ο περί της Χρήσης των Δεδομένων που περιέχονται στις καταστάσεις Ονομάτων Επιβατών (ΠΝΡ) για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και σοβαρών εγκλημάτων Νόμος του 2018, art 16; France: (n 87), art 9; Greece: Υποχρεώσεις αερομεταφορέων σχετικά με τα αρχεία επιβατών - προσαρμογή της νομοθεσίας στην Οδηγία (ΕΕ) 2016/681 και άλλες διατάξεις, art 14; Ireland: (n 85), art 11; Portugal: Lei n.º 21/2019 de 25 de fevereiro - Regula a transferência, pelas transportadoras aéreas, dos dados dos registos de identificação dos passageiros, bem como o tratamento desses dados, transpondo a Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, e procede à terceira alteração à Lei n.º 53/2008, de 29 de agosto, que aprova a Lei de Segurança Interna, art 8.

discrimination grounds, although the overarching prohibition on special categories of data has been included.[95] Nonetheless, the Dutch law refers to the LED implementing law, and subsequently to the conditions for automated decision-making therein.[96] Finally, most Member States name a specific supervisory authority, which is the same one responsible for monitoring the application of the GDPR and the LED provisions (apart from Belgium, France and the Netherlands)[97].

III. Relation between the LED and the PNR Directive

33 Through our desktop research on the national transposition of the PNR Directive, it was uncovered that most Member States repeated the reference to specific data protection rights and obligations by merely adapting the reference to the LED provisions instead of the CFD ones. The applicability of the LED in place of the CFD, however, may be of particular importance for data protection in the context of the PNR Directive. More specifically, as mentioned above, the CFD had a significantly limited scope of application, excluding internal, non-cross-border processing of personal data. Given the limited scope of the CFD and the concerns raised by the European Parliament about adopting such an EU PNR scheme, the reference to core data protection rights and obligations sought to reassure the wary. Nevertheless, the LED that took its place emphatically raised the level of protection of personal data in comparison to the previous framework, by virtue of, inter alia, its applicability to competent authorities at large, as explained above.

34 Pursuant to the definition of competent authorities under the LED[98], it may be deduced that PIUs fall under this definition and are therefore subject to the LED.[99] Consequently, the LED may be considered as *lex generalis* in the sense that, unless explicitly stated otherwise, it should be applicable in its entirety to PIUs. In that way, it is not clear what meaning the reference to specific provisions in the CFD holds now that the latter is no longer applicable, or whether such reference implies a limited applicability of data protection safeguards under the currently-in-force LED. The equivalent reference to specific provisions within the LED should be considered as superfluous rather than restricting its scope of application as *lex specialis*, given that such interpretation would diminish the level of protection. Of course, as both legal instruments consist of directives that must be transposed into national law, leeway is given to Member States. That discretionary power, however, should not be used to the detriment of data protection safeguards.

E. The right of access

I. From theory...

1. The many facets of the right of access

35 The right of access was explicitly incorporated within the provision on the fundamental right to data protection in the Charter[100], which entered into force in 2009. Both the CJEU and the ECtHR have acknowledged that the right of access plays an important role in the protection of other data protection rights. For instance, in its Rijkeboer ruling,[101] the CJEU stated that the right of access is a prerequisite for the exercise of other data subject's rights, a position that the Court confirmed in its subsequent case law (such as YS[102] and Nowak[103]). Moreover, in Nowak, the Court further stated

95 The Netherlands: Wet van 5 juni 2019, houdende regels ter implementatie van richtlijn (EU) 2016/681 van het Europees Parlement en de Raad van 27 april 2016 over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit (PbEU 2016, L 119) (Wet gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven).

96 ibid, art 17.

97 Belgium: (n 56), art 184; France: (n 87); the Netherlands: (n 95).

98 LED, art 3(7).

99 Discussions on the potential applicability of the LED already to private entities such as air carriers which are obliged to process personal (PNR) data for further law enforcement purposes have also taken place, see for example Nadezhda Purtova, 'Between the GDPR and the Police Directive: Navigating through the Maze of Information Sharing in Public–Private Partnerships' (2018) 8 International Data Privacy Law 52; Vogiatzoglou and Fantin (n 40).

100 Charter, art 8(2).

101 Case C-553/07 *College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer* [2009] ECR I-3889, paras 51-52.

102 Joined Cases C-141/12 and C-372/12 *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S* [2014] EU:C:2014:2081, para 57.

103 Case C434/16 *Peter Nowak v Data Protection Commissioner* [2017] ECLI:EU:C:2017:994, para 57.

that the right of access under data protection law meets the goal of guaranteeing the protection of "[the individual's] right to privacy with regard to the processing of data relating to him or her".[104] A similar reasoning may be found in the case law of the ECtHR, although in cases related to the right of access to information more broadly rather than the right of access under the data protection regime per se, but nevertheless yielding similar effects as those intended by the CJEU. Examples of that ECtHR case law include Leander[105] and Rotaru[106], which form part of the analysis in sub-section 3 below (on the relevance of the right of access in the context of security).[107] The ECtHR has also indicated that, when access requests are denied or disregarded by actors either in the public or private sector, such behaviour could amount to a disproportionate interference with the right to privacy under Article 8 ECHR, if that decision fails to strike a fair balance between competing interests.[108]

36 Considering the way in which the right of access is framed in the GDPR[109] and the interpretations of the two European courts, it can be argued that the right of access plays at least two essential roles. On the one hand, it provides data subjects with access to their personal data. On the other, it enables the data subject to have his or her data rectified, erased, or to object to the processing, thus becoming not only an end in itself, but also an instrument in support of the exercise of other information rights. In this manner, the right of access is an essential component of the informational empowerment of data subjects and, as the European Data Protection Supervisor (EDPS) put it, can be considered as a "precondition to allow [individuals] more control over their data".[110] In the same vein, the right of access enables data subjects to verify the accuracy of their personal data and the lawfulness of the data processing carried out by controllers. Moreover, it is the first mechanism that data protection law grants data subjects against data protection violations[111], which could make it instrumental in improving transparency of data processing practices.

37 In addition, the right of access can be considered an empowerment mechanism that lends itself for both private and societal interests. On the one hand, it helps citizens to pursue individual interests; namely, to learn more about particular data processing activities involving their personal data through SARs. On the other hand, the right of access serves broader societal interests of addressing existing information asymmetries between controllers and data subjects.[112] For example, the exercise of the right of access could eventually result in an improvement of data processing practices by unveiling illegitimate processing activities or gaps in the practical implementation of the law. To that end, the exercise of data access rights could be particularly effective when realised in a joint effort by several data subjects.[113] The above may be included in the reasoning underpinning the European Commission's consideration of "data protection as a pillar of citizens' empowerment"[114].

38 Furthermore, considering the importance of citizen access to information held by state authorities,[115] access rights can have the potential to serve as a tool for citizens to foster transparency in the processing

104 ibid, para 56.

105 *Leander* (n 10), para 48.

106 *Rotaru v Romania* App no 28341/95 (ECtHR, 4 May 2000, para 46).

107 Other ECtHR case law providing evidence of the importance of access rights to balance conflicting interests are *Gaskin v the UK* App no 10454/83 (ECtHR, 7 July 1989, paras 43 and 49), *Haralambie v Romania* App no 21737/03 (ECtHR, 27 October 2009, paras 86 and 96), and *I v Finland* App no 20511/03 (ECtHR, 17 July 2008, para 47).

108 As stated by the ECtHR in the following rulings: *Leander* (n 10), *Gaskin* (n 107), *Z v Finland* App no 22009/93 (ECtHR, 25 February 1997), *M.G. v the UK* App no 39393/98 (ECtHR, 24 December 2002), *I v Finland* (n 107), and *Haralambie* (n 107).

109 GDPR, art 15.

110 EDPS, 'Opinion 7/2015: Meeting the Challenges of Big Data. A Call for Transparency, User Control, Data Protection by Design and Accountability' (2015) 5 <https://edps. europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf> accessed 20 June 2020.

111 Antonella Galetta and Paul De Hert, 'A European Perspective on Data Protection and the Right of Access' in Norris and others (n 25).

112 Mahieu, Asghari and van Eeten (n 26).

113 ibid.

114 As highlighted in its recent report on the two years of application of the GDPR. European Commission, 'COM(2020) 264 Final Communication from the Commission to the European Parliament and the Council - Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition - Two Years of Application of the General Data Protection Regulation' (European Commission 2020) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264> accessed 4 July 2020.

115 See Paivi Tiilikka, 'Access to Information as a Human Right in the Case Law of the European Court of Human Rights' (2013) 5 Journal of Media Law 79, 81–83.

practices by the government. In other words, the right of access may serve as a means to scrutinise the activities carried out by public authorities[116], as the ECtHR and CJEU case law seems to suggest.[117] The right of access can therefore provide citizens with the awareness of data processing operations carried out by public authorities. This is the case when the exercise of a SAR provides citizens with information necessary to act upon potential unlawful practices or data suggesting potential abuses of power (such as collection or processing of data without a legal basis, for example). Furthermore, the right of access can empower individuals to have a direct impact on policies and legislative initiatives.[118]

39 It should be noted, however, that despite the wide acceptance in scholarly literature regarding the reasoning surrounding the citizen empowerment stemming from data protection law[119], this idea is not supported in all academic works. For example, Koops argued that the correlation between data protection law with the notion of "control" is fallacious.[120] Put briefly, Koops' argument is that the data protection framework cannot provide control over one's own data, particularly because of the complexities characterising modern data processing activities coupled with the intricacies that distinguish the data protection architecture. On a similar note, Lazaro and Le Métayer disputed the potential of the right of access to work as an empowerment mechanism.[121] Lazaro and Le Métayer considered that the correlation between data protection law and the notion of "control" results from a flawed view of the theories concerning privacy and data protection.[122]

40 It is also worth noting that, even if the right of access can be considered as a tool for informational empowerment, the data protection regime does not establish a right of access to any particular document or file containing personal data concerning the individual. This was confirmed by the CJEU in its YS ruling,[123] where the Court provided clarifications as to the scope of the right of access under the now repealed Data Protection Directive[124] but nonetheless relevant for the current understanding of the right of access. In YS, the CJEU held that data subjects are not entitled to have access to a legal analysis made in an administrative document (in the case at hand, the "minute", i.e. a document containing the reasoning of the case officer of a data subject's entitlement to a lawful residence permit). This relates to the fact that such legal analysis is not "personal data" within the meaning of data protection law, as the Court concluded. That clarification gains particular importance in the context of the citizen-state relationship at stake when it comes to the right of access under the LED and the PNR Directive.

2. The right of access under the LED and the PNR Directive

41 The LED in its Article 12(1) requires controllers to implement reasonable measures to provide the necessary information to the data subject in a concise, intelligible and easily accessible form and using clear and plain language. Such information, to be provided by appropriate means, including electronic ones, shall be designed to facilitate the exercise of any data subject's right enshrined in the LED. Article 13(1)

116 As it enables the verification of legitimacy of data practices. Mahieu, Asghari and van Eeten (n 26) 3; European Union Agency for Fundamental Rights, 'Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II: Field Perspectives and Legal Update' (2017) 124 <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf> accessed 6 September 2019.

117 As follows from the case law included in the analysis at the beginning of this section, namely *Rijkeboer* (n 101), *YS* (n 102), *Nowak* (n 103), *Leander* (n 10), and *Rotaru* (n 106).

118 As illustrated by the success stories relating to the privacy activist Max Schrems, who has pursued privacy campaigns that started by SARs. Xavier L'Hoiry and Clive Norris, 'Introduction – The Right of Access to Personal Data in a Changing European Legislative Framework' in Clive Norris and others (n 25).

119 See A.O. Steven Lorber, 'Data Protection and Subject Access Requests' (2004) 33 Industrial Law Journal 179, 180; Norris and others (n 25) 1–8; Ausloos and Dewitte (n 25) 7; Ausloos, Veale and Mahieu (n 23) 286; Mahieu, Asghari and van Eeten (n 26) 16; Mahieu and Ausloos (n 24).

120 Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (2014) 4 International Data Privacy Law 250.

121 Christophe Lazaro and Daniel Le Métayer, 'Control over Personal Data: True Remedy or Fairy Tale?' (2015) 12 SCRIPTed <https://script-ed.org/article/control-over-personal-data-true-remedy-or-fairy-tale/> accessed 27 July 2020.

122 For a similar line of reasoning, see Mark Leiser and Bart Custers, 'The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680' (2019) 5 European Data Protection Law Review 367.

123 *YS* (n 102).

124 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

further lists the minimum information to be made available to all data subjects, namely: (a) the identity and contacts of the controller, (b) the contact details of the DPO, (c) the purposes of the processing, (d) the existence of the right to lodge a complaint with the supervisory authority and (e) the existence of rights of access, to rectification, to erasure and to restriction.

42 The requirements prescribed in Articles 12 and 13(1) LED can be considered as ex ante obligations, i.e. obligations that need to be satisfied ahead of the data processing activities by making that information available through, for instance, the website of the competent authority[125]. Those information obligations are complemented with the ex post right of access envisaged in Article 13(2) LED for specific cases and in Article 14 LED. According to the latter, data subjects are entitled to obtain more information about the data processing activities undertaken by the controller than the general information made available to the public on an ex-ante basis. In that way, the right of access entails the possibility for data subjects to require more transparency from the controller on the actual data processing activities concerning him or her. Insofar as the information obligations under the PNR Directive are concerned, the text only refers to the applicability of the CFD (now LED) provisions for the exercise of the right of access.[126] Therefore, it might be inferred that the LED and the PNR Directive differ in their information obligation measures, while the conditions for and limitations to the exercise of the right of access are identical for both instruments. This is an example of how interpreting the reference within the PNR Directive to specific CFD provisions as *lex specialis* (see above section D.III.) may result in lowering the level of protection of personal data.

43 By virtue of Article 14 LED, the LED and the PNR Directive grant data subjects the right to access their personal data.

This means that citizens are entitled to receive from security-related bodies (including competent authorities and PIUs subject to the directives):

- Confirmation as to whether or not personal data concerning them are being processed;
- Where that is the case, access to several categories of information, including:
  - Information at least as to the purposes of the processing operation, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed; and
  - Communication in an intelligible form of the data undergoing processing and of any available information as to their source.

44 However, the LED – and the PNR Directive, indirectly – also limit the right of access. According to Article 15 LED, Member State law can implement measures that enable controllers to fully or partially restrict SARs in case such requests interfere with the achievement of security interests in any way (for instance, by potentially obstructing official or legal inquiries, investigations or procedures).[127] These limitations may mitigate or reduce the positive effect of the information empowerment tool granted to individuals in a security or law enforcement context.[128] Hence, the right of access is not absolute, and, since the grounds for denial of access are worded in very broad terms, the limitations that Member States can implement may potentially provide controllers with broad discretionary powers in security.[129]

45 Having said that, it is worth noting that the limitations applicable to the right of access should not be interpreted as the possibility for competent authorities to adopt a blanket approach of refusing to provide any of the data falling under any of the grounds for refusal. This follows from Article 15(3) LED, which provides that, when the right of access is restricted or refused, Member States' laws must stipulate the obligation for controllers to document the factual or legal reasons leading to such a decision. When requested, such information must also be made available to the NSA, which provides an additional layer of control over the justification. The importance of the justification obligation can be illustrated by a recent case concerning the restriction of an SAR by national competent authorities in the UK, where an Administrative Court recently handed

125 LED, rec 42.

126 According to the PNR Directive, art 13(1), the corresponding articles on data subjects' rights of the CFD, which has now been repealed and replaced by the LED, are applicable.

127 It is worth noting that the limitations to the right of access are not exclusive to the processing of data in the security field. The GDPR also contemplates equivalent limitations to the data subject rights enshrined therein, as per its art 23.

128 As De Hert and Papakonstantinou argue in 'The New Police and Criminal Justice Data Protection Directive: A First Analysis' (2016) 7 New Journal of European Criminal Law 12–13.

129 Diana Dimitrova and Paul De Hert, 'The Right of Access Under the Police Directive: Small Steps Forward' in Manel Medina and others (eds), *Privacy technologies and policy* (Springer 2018) 122.

down a decision in the Dalton case[130]. One of the main questions was precisely whether the justification supporting the initial refusal – then partial restriction – of the right of access was adequate.[131]

46 In addition, Article 17 LED introduces the so-called "indirect access", which should, in principle, offer an additional path to data subjects for the exercise of their rights. Accordingly, the exercise of a data subject's rights enshrined in the LED can also be performed by the supervisory authority on behalf of the data subject, in cases when the controller denies a data subject the exercise of his or her information rights.[132] In such a case, the NSA acting as a proxy shall inform the data subject at the very least that the appropriate verifications before the law enforcement agency have been undertaken. As we will be able to explain below, such a path was instead chosen and interpreted as a default procedure for the filing of SARs by the authorities of one of the Member States, *de facto* turning the rationale of Article 17 LED from providing an additional choice to data subjects to restricting the actual access to their personal data.

47 Overall, the scope and reach of the right of access in the legal instruments under analysis seem to match the balancing effort between the competing interests at stake.[133] Yet, the possible effects of the right of access in a security context very much depends on the national transpositions of the LED and the PNR Directive.[134] In other words, each Member State may take into account their specific national characteristics and adapt the provisions to their national legal culture. As a result, it is necessary to examine the national implementations of the EU law and the operationalisation of the law in each country to fully understand the potential effects of the right of access in a security context.

3. Relevance of the right of access in the context of security

48 While data protection law grants individuals control over their data and therefore acts as a means to scrutinise government agencies, it can also be used to scrutinise security-related personal data processing. This is particularly the case when considering that data subjects' rights in the LED and the PNR Directive aim at empowering individuals by providing them control over their data held by state authorities. In that sense, the right of access allows citizens to learn more about how the data collection and processing practices take place at the state level.

49 In its Rijkeboer ruling, the CJEU highlighted the importance of the right of access as a mechanism to remedy data protection violations.[135] When it comes to the role that access plays in a security context, the ECtHR has considered that the refusal to grant access to the information stored by public authorities (including security bodies, such as the secret police[136] or the intelligence service[137]) deprives individuals of the opportunity to refute it. That, in turn, entails an interference with the right to privacy, the Court concluded.[138] Moreover, the ECtHR has indicated that authorities have a "positive obligation" to offer citizens an effective procedure to obtain access to "all relevant and appropriate information" they hold, even if the personal information concerned is stored in the archives of the former secret services.[139] Following this line of reasoning, the right of access under the LED and the PNR Directive could operate as a mechanism to empower citizens by addressing information asymmetry issues in the citizen-state relationship. In particular, it arguably provides citizens with the possibility to scrutinise and question data processing practices in a security environment. This appears to be the case at least from a conceptual perspective.

130 *Dalton, R (On the Application Of) v The Crown Prosecution Service (CPS)* [2020] EWHC 2013 (Admin).

131 However, the Court's findings are more about procedural aspects, rather than the merits of the case. As the Court itself expressly said, it is for the NSA to determine whether the restriction was justified based on a necessity and proportionality assessment (ibid, para 70).

132 See also LED, rec 48.

133 As discussed by De Hert and Boehm's analysis of relevant ECtHR case law in relation to security-related processing of data. See Paul De Hert and Franziska Boehm, 'The Rights of Notification after Surveillance Is over. Ready for Recognition?' in Jacques Bus and others (eds), *Digital Enlightenment Yearbook 2012* (IOS Press 2012).

134 Considering that a directive is only binding for Member States as to the results to be achieved, but each Member State is free to decide how to transpose the legal text. This differs from what happens with a regulation, which has binding legal force throughout every Member State (TFEU, art 288).

135 *Rijkeboer* (n 101), para 52.

136 *Leander* (n 10).

137 *Rotaru* (n 106).

138 ibid.

139 *Haralambie* (n 107), paras 85-88.

II. ...to practice

50 The first two sub-sections below focus on the national implementation of Articles 12 and 13(1) LED, which deal with the general modalities through which information must be presented to data subjects. Not only one-to-one communication between controllers and data subjects, but also – and most importantly – the communication between the controller and the general public. Articles 12 and 13(1) therefore detail the practical and procedural steps controllers must undertake to enable data subjects to exercise their prerogatives. The rationale behind these two provisions is captured by Article 12(2) itself, which obliges controllers to "facilitate the exercise of the rights of the data subject". According to the above-mentioned provisions, the modalities surrounding the exercise of the right of access and the information on the processing operations shall be easily accessible. The research undertaken for this study therefore started with an investigation of the national laws implementing both directives as well as of the information made available on the websites of competent authorities and PIUs, through the use of online surveys (Survey 1 and Survey 2, respectively). By combining a legal and an empirical study, we aimed at determining how that information was presented to data subjects. The results are hereby presented separately for the LED and the PNR Directive.

51 The three remaining sub-sections are of purely empirical nature. In particular, they detail the manner in which SARs were submitted in accordance with the information found, the interactions that took place with the controllers, and the final responses we received regarding the processing of our personal data by the respective competent authorities and PIUs. Given the commonalities in approach, the results for submission, follow-up and final responses of the SARs under both the LED and PNR Directive are presented under a common subtitle. All national competent authorities' and PIUs' websites, where information on privacy and data protection policies were sought, as well as the contact details of the addressees to whom SARs were submitted, are included in a comprehensive manner per each country under Annex I.

1. National transposition

a) LED

52 The first step was to look directly into domestic laws to check what pieces of information mentioned in Articles 12 and 13(1) LED were already included in the national transposing acts. With respect to the identity of the controller, only four Member States include the specific competent authority within their respective legislation (Ireland, the UK, Italy, Cyprus)[140]. For all other Member States, the research was focused on the relevant national police authority's website or the relevant Ministry's website.

53 Starting with Article 12 LED, in spite of idiomatic differences across Member States due to language diversity, a handful of countries includes transposing Articles he wording of which differs from the original LED formulation. The Dutch law[141], for instance, does not explicitly mention the duty of the controller to prove the request is manifestly unfounded or excessive before refusing to act on it. Nonetheless, a higher level of granularity in the transposition of Article 12 LED appears when the Dutch law explains the procedure that the competent authority must follow when answering a request for access: data subjects shall be informed in a timely manner by the authority of (i) the reception of the request, (ii) the deadline for referral and (iii) the possibility to lodge a complaint.[142] The Belgian law, furthermore, limits the right of access in two ways. First, it obliges data subjects to exercise their rights indirectly through the "Organe de Contrôle" and, second, the said "Organe de Contrôle" can only let data subjects know that the necessary verification as to the legality of the processing operations have been done.[143]

54 With regard to the implementation of Article 12(3) and (4) LED, which respectively concern timing, fees and denials of requests, we found that national implementations diverge from one another, too. For instance, whilst the Portuguese law[144] requires authorities to respond within thirty days (renewable for another thirty), other countries have adopted the original wording of the LED, i.e. "without undue

140 Ireland: Data Protection Act 2018, sec 69; UK: (n 59) Schedule 7; Italy: (n 59), art 2; Cyprus: (n 58), art 2.

141 The Netherlands: Wet van 21 juli 2007, houdende regels inzake de verwerking van politiegegevens (Wet politiegegevens), arts 24a and 26(1); Wet van 7 november 2002 tot wijziging van de regels betreffende de verwerking van justitiële gegevens en het stellen van regels met betrekking tot de verwerking van persoonsgegevens in persoonsdossiers (Wet justitiële gegevens), arts 17b, 20(1) and 25.

142 As we will explain further, in our application for SARs, the Dutch authorities followed this Article by informing the data subject in writing and via post about such three elements.

143 Belgium: (n 56), art 42(1)-(2).

144 Portugal: (n 59), art 13.

delay". Some slight differences persist with respect to other features. The UK law[145], for instance, stipulates that any delay can be justified until the controller has reasonably ascertained the identity of the applicant. With respect to potential fees to be charged to the data subjects, some countries like Portugal expect the controller to make a "reasoned decision" for refusal[146], whereas the UK delegates the specification of the fee to further regulation by the Secretary of State[147].

55 In general, all national laws scrutinised except for Belgium[148], Portugal[149] and Malta[150], mirror the (almost exact same) formulation of the LED when prescribing that the information must be provided and presented in a concise, easily accessible form, using clear and plain language. Moreover, whilst some countries like Italy[151], Belgium[152] and the Netherlands[153] explicitly state within their national laws that the provision of information shall respect domestic limitations arising from police statutes and criminal procedures, only two Member States' laws explicitly mention how to find the preliminary information to exercise any data subject's rights. In particular, only Greece[154] and Italy[155] expect that the contact details of the controller shall be found online on the controller's website. A similar reference to the controller's website is also present in the Irish Data Protection Act[156], even though the scope of the provision is slightly different, as it requires the whole list (not just the controller's details as per the cases of Greece and Italy) of information ex Article 13(1) LED to be published.

56 With regard to the transposition of Article 13 LED, our research suggests that national formulations differ from the LED for almost half of the investigated Member States. In Portugal, for instance, the controller shall make the information "publicly available and permanently accessible" (as opposed to limiting the provision of that information to data subjects actively engaged in the exercise of their information rights).[157] Furthermore, whereas Article 13(2) LED (additional information to be provided to the data subjects) applies to specific cases, the Belgian Law[158] does not make such a distinction, thereby suggesting that the controller shall in any case provide the information listed in both Articles 13(1) and 13(2) LED.

57 With regard to the modalities of the exercise of the right of access under Article 14 LED, our research revealed a few countries with a different wording and additional requirements in their national laws. In the Dutch law[159] there are extra provisions on the timeframe for a response from the controller: no more than six weeks for a definite answer on the processing of personal data, which can be postponed for no more than four weeks. Additionally, France[160] lays down a very specific discipline for the exercise of the right of access and the procedures to be put in place by the controller when identifying the data subject: he or she must prove his or her identity by any means (including using digital identity) that is deemed sufficient by the controller for the authentication. If the controller has reasonable doubts as to the identity of the person, he may request additional information, including, if necessary, a copy of an identity document bearing the individual's signature. Within such procedures, the response period is suspended if additional information were requested for the identification of the data subject.

58 Finally, whilst all scrutinised Member States seem to have implemented Article 15 LED laying down a framework of exceptions to the right of access for security or investigative reasons, some countries embed noteworthy differences. For example, both

145 UK: (n 59), sec 45.

146 Portugal: (n 59), art 13(5).

147 UK: (n 59), sec 53.

148 Belgium: (n 56), art 36.

149 Portugal: (n 59), art 13.

150 Malta: (n 59), art 12.

151 Italy: (n 59), art 9.

152 Belgium: (n 56), art 37.

153 The Netherlands: (n 141) 2007, arts 24a and 26(1).

154 Greece: (n 57), art 57.

155 Italy: (n 59), art 10.

156 Ireland: (n 140), sec 90.

157 Portugal: (n 59), art 14.

158 Belgium: (n 56), art 37.

159 The Netherlands: (n 141) 2007, art 25.

160 France: Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art 105 and Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art 135.

the Dutch[161] and the Portuguese[162] transpositions of Article 15 LED do not seem to fully implement its paragraph 4, thereby not requiring controllers to document (and make available to the supervisory authorities) the factual reasons for a denial. Nonetheless, the Dutch law adds the explicit requirement that the rejection shall be in writing stating the reasons for the rejection. Interestingly, in Cyprus[163], the denial from the controller must be validated after consultation with the NSA (in casu the Commissioner). Upon request from the controller, the Commissioner may draft and publish a catalogue with processing categories that may be subject partly or wholly to restriction. Similarly, the Irish law[164] includes the possibility for a legislative act to expressly lay down a list of data categories to be restricted from the exercise of the right to access on the same grounds as the ones included in Article 15 LED.

b) PNR Directive

59 As mentioned, the very first step before submitting SARs regarding our PNR data was to identify the relevant controllers. Pursuant to the PNR Directive, all Member States appointed in their national laws a single authority to act as the PIU, which functions as the primary controller receiving PNR data from air carriers. It was then deemed important to investigate whether any detailed information on the modalities of exercising the right of access was foreseen by the domestic laws transposing the provisions on the DPO and on the protection of personal data.[165]

60 All scrutinised Member States refer to the national PIU as the designated competent authority to collect and process PNR data from the air carriers. Either through repeating the directive's wording, or by providing further information on, for example, the qualifications and the procedure for appointing a responsible person or entity, all domestic laws refer to the PIUs' DPO. Moreover, all Member States except from France[166] and the UK[167] ensure that the DPO serves as a single point of contact for data subjects to exercise their prerogatives. Luxembourg and Italy are the only countries that further elaborate on the modalities surrounding the right of access. In particular, the Luxembourgish law[168] imposes a specific transparency obligation upon the PIU to disseminate information on the data controller and the processing operations. The Italian law[169], on the other hand, provides that application should be submitted to the central directorate of criminal police, which communicates to the data subject all acts adopted therein.

61 The most intricate legislative framework proved to be the one applicable to the processing of personal data by the Belgian PIU. In particular, the Belgian law transposing the PNR Directive[170] specifies that the provisions included in the general privacy law apply on the processing of personal data by the PIU. While examining the latter, it was discovered that passengers' rights as data subjects are regulated under Title 3, Subtitle 5 of the general privacy law, which stipulates that data subjects only have the right to ask for the rectification or deletion of their data, or the verification, by the "Comité permanent R" that their data are processed in accordance with the guarantees stemming from the general privacy law.[171] These prerogatives, adds the Belgian law, can only be exercised indirectly through the said "Comité permanent R".[172] In any case, the PIU must legally refrain from mentioning that it is even in possession of personal data.[173]

2. Implementation of information obligations

a) Competent authorities

62 After having analysed the national transposition act for each of the investigated countries, we focused on the existence of adequate ex ante transparency

161 The Netherlands: (n 141) 2007, art 27 and (n 141) 2002, art 21.

162 Portugal: (n 59), art 16.

163 Cyprus: (n 58), art 17.

164 Ireland: (n 140), sec 94.

165 PNR Directive, arts 5 and 13, respectively.

166 France: (n 87), art 1.

167 UK: (n 89), art 4.

168 Luxembourg: Loi du 1er août 2018 relative au traitement des données des dossiers passagers, art 30.

169 Italy: Attuazione della direttiva UE 2016/681 del Parlamento Europeo e del Consiglio, del 27.4.2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi e disciplina dell'obbligo per i vettori di comunicare i dati relativi alle persone trasportate in attuazione della direttiva 2004/82/CE del Consiglio del 29.4.2004., n. 53, art 23.

170 Belgium: (n 86), art 15(3).

171 Belgium: (n 56), art 173.

172 ibid, art 174.

173 ibid, art 49(3).

measures on the websites of the relevant competent authorities. We looked for both general information detailing the processing operations happening within a law enforcement context, as well as for the practical details necessary for data subjects to exercise their right of access.

63 Since, as discussed above, very few countries clearly indicate the relevant controller in their national transposing laws, we looked for the website of the centralised entity governing the LEAs (either national police authority or the competent ministry) or of the NSA. Our research team then ranked the ease with which it was possible to find meaningful information detailing the modalities and procedure for submitting access requests. On a scale between 1 (very difficult) to 10 (very easy), the average answer was 5.9. Individually, Member States scored very differently, with some websites providing very easily accessible information (like Cyprus or Luxembourg National Polices) and others a more complex presentation (for instance, Belgium's or the Netherland's authorities).

64 After having identified the appropriate websites, our team looked into each of those to understand if and where privacy-related information about the way LED is implemented were present. Out of eleven websites investigated, only Greece did not include any information of such kind.[174] For all the other authorities, information related to privacy policies was included under a dedicated section on their websites. Some countries gather in a single page different links for each privacy policy of the different police databases (e.g. Italy, referring to Schengen, national criminal database, VIS, etc.) or to the relevant legal frameworks (e.g. Greece). Except for Portugal, all competent authorities included the information requested by Article 13(1) LED (controller's and DPO's contact details, purposes for processing, right to exercise access or to lodge a complaint, contacts of the regulators) within the said dedicated webpages. Furthermore, some websites provided additional information such as general retention policy (Italian Police), basic data protection principles (Irish Police) or security of processing (Luxembourg Police). With the exception of the Portuguese Police, all competent authorities' websites also included instructions on how to file a SAR. Out of such a pool, four competent authorities (Ireland, Italy, the Netherlands, the UK)[175] even provided a template SAR to be filled in by data subjects.

174 A data protection policy notice, not easily accessible, was added to the Greek National Police website at a later stage after our access requests were already sent. However, the contact details remained the same.

175 France provides an interactive template on the data protection authority's website (CNIL.fr).

b) Passenger Information Units

65 Having identified the data controller, i.e. each country's PIU, and established that the PIU's DPO serves as a contact point in most Member States, the next step was to look for the DPO's contact details. While locating the PIU online proved an easy task for most Member States, that was not the case for Portugal, Cyprus and Greece. After a careful analysis of the existing ministry and national police websites, national laws and diverse online sources, it was found that the Portuguese PIU belongs to the Single Point of Contact for International Police Cooperation, which in turn works under the authority of the Secretary-General of the Portuguese Internal Intelligence Service.[176] Accordingly, only the general contact details of the overarching authority, i.e. the Portuguese Internal Intelligence Service, were found. More strikingly, the Cypriot and Greek PIUs did not seem to be functional or have any official presence online.[177] Any further research on Cyprus, Greece and Portugal was therefore ceased. The rest of this section refers only to the Member States PIUs for which official information online was found.

66 Out of the eight investigated PIUs, about half were directly linked to law enforcement, and therefore the official website of national police or ministry of justice or defence (Italy, Ireland, Luxembourg, the Netherlands, Malta), and half were linked to another type of governmental website (Belgium, France, the Netherlands, the UK). Interestingly, the British PIU is linked to visas and immigration

176 According to Portugal: (n 59), art 3, the PIU is created within the Single Point of Contact for International Police Cooperation which works under the authority of the Portuguese Internal Intelligence (Portugal: Decreto-Lei 49/2017, art 1), on the website of which no information on the PIU was found <https://www.sis.pt/> accessed 20 October 2020.

177 Several news posts referred to the appointment of a director for the Cypriot PIU without however pointing to any official website of the Cypriot PIU. In order to confirm the existence or non-existence of the Cypriot and Greek PIUs, the national supervisory authorities (NSAs) were first contacted. The Cypriot NSA responded with a three-month delay that any SAR regarding PNR data may be submitted before the Cypriot Police DPO, in the European Union & International Police Cooperation Directorate (EU&IPCD). Regarding the Greek PIU, no specific information was provided by the Greek NSA. One of the authors contacted and submitted a SAR to an airline via which they had travelled to Greece, asking specifically whether their PNR data had been transmitted to the Greek PIU. In their response, the airline confirmed the non-readiness of the Greek PIU to receive data from airlines at the time.

matters, while information on the use of PNR data by the Dutch PIU is divided between the Ministry of Defence and a governmental website on customs and aviation. All but France included a privacy statement, whether generalised (Ireland, Malta, the UK) or more elaborate and PNR-specific (Belgium, Italy, Luxembourg, the Netherlands).

67 Apart from France, these countries also provided information on how to contact the data controller or DPO on the respective websites. To find the relevant information regarding the French PIU and the process to be followed, a general contact form was submitted, the response to which provided the contact details of the PIU Director, to whom the SAR had to be submitted. For the PIUs linked to law enforcement, the SAR had to be submitted to the police/ministry of justice or the police/ministry of justice DPO (Italy, Ireland, Luxembourg and Malta). Concerning the submission of a SAR regarding PNR data within the Netherlands, the option is given to contact customs, the PIU or the respective airline, while it is also made clear that for any rectification or erasure of data all three entities have to be contacted. In order for the SAR to be submitted, most provided an email address though two Member States requested the submission of a physical letter (France and Italy), while a few Member States provided their own template (Italy, Ireland and the UK). All Member States apart from Belgium and the Netherlands further explicitly required identification documents for the submission of the SARs.

68 Taking into account the steps involved in order for the information necessary for the submission of the SARs to be found, the average level of difficulty for all Member States investigated was assessed at 4.6/10 (with 0 being the most difficult and 10 the easiest). Scores varied a lot, with Italy, Luxembourg and Malta being graded the highest.

3. Initial requests

69 After having analysed the national transpositions of both directives in the selected Member States and assessed their compliance with the various transparency obligations, it was time to move on with the actual SARs. In order to ensure the accuracy and comparability of the findings resulting from six individual submissions, we proceeded as follows. First, we shared the results from Survey 1 (dealing with the national transposition of the LED and PNR Directive) and Survey 2 (compiling the findings relating to the transparency obligations) with all participants. More specifically, we highlighted the information related to the contact details that could be used in order to reach the different competent authorities and PIUs as well as the potential procedural requirements. Rather than starting from scratch, all participants could therefore leverage each other's work. Second, all participants filed their initial SARs using templates drafted by and shared among everyone, depending on the countries assigned. Those were redacted in (one of) the official language(s) of the selected countries, so as to smoothen the communication. Third, and as to the sharing of the workload, we proceeded as follows: for the LED, on the one hand, each participant sent an access request to all the investigated countries; for the PNR Directive, on the other, each participant sent an access request to all the countries they had flown from, through or to in the previous six months.

70 This section briefly outlines the form and procedural requirements surrounding the sending of initial access requests, i.e. the very first contact established with both law enforcement authorities and PIUs. When it comes to SARs submitted under the LED, it is worth noting that most competent authorities accepted submissions made in an electronic format, whether through a dedicated contact form or via email. For three countries, namely France, Italy[178] and the Netherlands, however, we had to send our request via regular post. Interestingly, the French Ministry of Home Affairs came back to us explaining that our requests were inadmissible since it was necessary to submit them via regular post – which we specifically did according to the instructions we found when going through the privacy notice of the French competent authority. For the Netherlands, it was possible to choose from the ten Regional Units of the police since there was no clear indication as to which one to contact to exercise a data subject's rights under the LED. As to procedural requirements, the Irish police asked for a proof of residence in the country as well for as a list of all the addresses where we lived while residing in Ireland. Similary the Luxembourgish authorities asked for an address certificate in order to provide their answer via post.

71 Roughly the same can be said when it comes to access requests formulated under the PNR Directive. While we submitted most of our SARs via email, France and Italy still required us to send them via regular post. Surprisingly, a and unlike the modalities applicable to the submission of the SAR under the LED, the Dutch PIU accepted the use of the electronic format. In terms of procedural obstacles, France asked us to provide a proof of residence, Belgium redirected our request to the Belgian Privacy Commission and the UK asked for a certified photo ID together

178 While it was possible to send the request via email in Italy, the only possibility to do so was via Posta Elettronica Certificata (PEC), which in turn required a residential address in Italy. We therefore decided to send the request via regular post, as this was the only option for non-residents to exercise their right of access.

with a signed declaration by a barrister. It is also worth emphasising once again that no official online presence of the Cypriot nor Portuguese PIUs was detected, while the Greek PIU did not appear to be operational at the time we sent our SARs.

4. Following up on the SARs: reminders

72 The follow-up of our requests required us to engage in active correspondence with the addressees. We sent reminders to authorities that had not reacted to our initial applications after two weeks, except for the SARs submitted by post for which a longer reaction time was expected.

73 For the SARs submitted under the LED, reminders were sent to the Cypriot, Greek and Maltese competent authorities. In Cyprus, one reminder from only one of us was enough to trigger a final response to all our SARs within three days. In Greece, however, we all had to send a reminder to prompt the Greek competent authority to gradually answer our SARs. When it comes to Malta, only one member of our team sent a reminder two weeks after the initial request, which triggered the remaining pending responses.[179] As to the SAR submitted under the PNR, we did not send any reminders to the addressees. This is because we either received responses within a time span of two weeks, or because the said requests at issue were submitted by post.

74 The key takeaways from the submission process relate to the exercise of the right of access under the PNR Directive, notably our experiences in Belgium and Italy. When it comes to Belgium, one member of our team was contacted by phone by the addressee of our requests two week after the initial submission, with the aim of obtaining more information before proceeding with our requests. Interestingly, the staff member showed a certain lack of linguistic flexibility,[180] despite the fact that PNR SARs can be expected from citizens not necessarily speaking any of the official languages of the country at issue. More striking though is the fact that, by the end of that phone interaction, the Belgian official, recipient of our SARs, asked for the phone number of another member of our team.[181] When in comes to our experiences in Italy, we received access to the PNR data of a person who was totally unrelated to our legal-empirical endeavour.

5. Final responses to the SARs

75 Overall, our SARs have been fully processed in most countries, in the sense that we had received a definitive answer - whether positive or negative - by the end of the allocated time frame. The responses we obtained range from a mere refusal to share anything to the disclosure of the personal data being processed. Yet, our successful attempts mostly resulted in the confirmation as to whether or not personal data concerning us were being processed, as analysed below.

76 Regarding our experiences under the LED, the most common response we obtained consisted of the indication that no data about us was being processed. Only SARs submitted to competent authorities in Greece, the Netherlands and the UK resulted in the provision of any information other than (or in addition to) that. The Greek competent authority provided a list of all the categories of data they held as well as the legal basis for the processing (though not the personal data as such). In the Netherlands, the additional information provided contained a detailed account of the databases that were consulted when processing the SARs, as well as a word of explanation on those databases. Lastly, in its response letter to our SARs, the UK competent authority specified that the information provided to us did not involve data held on local police systems, thus implying the possibility of obtaining a different response if the SARs were submitted to local police forces.

77 In two countries (namely France and Portugal), our SARs were dismissed. The French competent authority refused to comply on the grounds that our requests were "manifestly abusive"[182] given their overly broad scope; thus, to proceed with the requests, we had to indicate the exact files we were requesting access to (as indicated in the response letters). The refusals by the Portuguese competent authority, were based on the lack of compliance with all the formal requirements (according to the refusal letters). Surprisingly though, the alleged procedural shortcomings of our SARs relate to

179 Considering that half of our SARs had already received final responses by that time, as specified in the following section.

180 This lack of flexibility relates to the fact that the staff member reluctantly switched to English during the phone interaction.

181 More than strikingly, we find it a worrying practice whereby, while processing a SAR, another data subject's name is mentioned and personal records about that person are attempted to be extracted in that way. This can be considered a reckless manner of processing SARs. As a result, we reacted informing the authority of the reception of such a mishandled response.' after 'SARs.

182 Own translation from the literal words used in the response letters.

formal requirements that are not specified (or referred to) in the national implementation act of the LED in Portugal.[183]

78 It took competent authorities a median of three to 61 days to fully process our SARs under the LED.[184] The fastest final responses were provided by the Belgian, British and Maltese competent authorities (with a median of three, eleven and fifteen days, respectively), while the Irish, French and Italian competent authorities took the longest to respond (thirty-two, fifty-four and sixty-one days, respectively). It should be noted that Luxembourg was the last country to respond to our SARs (in September 2020, i.e. over six months after the initial requests).

79 At this point, it is worth highlighting some practical insights gathered during the research, mostly related to our experiences when exercising our right of access under the LED. In Malta, we had somewhat diverging experiences as regards to the time it took the competent authority to provide final responses to our SARs. The Maltese competent authority provided final response to half of our SARs within three days after submission. The remaining responses were provided in the subsequent days, following a reminder that one member of our team sent two weeks after submission (as specified in the previous section). Given that the addressees of our requests explicitly expressed facing organisational challenges resulting from the COVID-19 crisis, we assume that the differing experiences in Malta might be due to the possible impacts of the pandemic on the follow-up process.

80 Notwithstanding the above, the Maltese addressee responded to our SARs in time, in a friendly manner, and without trying to make data subjects regret attempting to exercise their access rights. The same can be said for the UK where requesting access to our personal data proved a fruitful and straightforward exercise, in particular because of the availability of an online form and the swiftness with which our applications were processed. Thus, the practical evidence gathered at this stage of the research seems to suggest that Malta - among the investigated countries - and the UK are probably two of the European countries where requesting access to personal data under the LED tends to be a straightforward exercise. Ireland and Luxembourg, on the contrary, proved to be more burdensome. In Ireland, we had to satisfy more formal requirements than the ones listed in the national implementing act of the LED and in the template provided on the website of the competent authority. In particular, we were asked to provide a proof of our address (as specified in the template), but also a proof of previous addresses where we "resided while staying in Ireland".[185] In Luxembourg, our exercise was similarly burdensome, time-consuming, and required more interactions with the addressee.

81 As to our SARs under the PNR Directive, the responses we obtained were more varied than those under the LED. Whereas in some countries we only received the information that no data about us was being processed, in France, Italy and the Netherlands, our SARs resulted in the actual disclosure of data undergoing processing. In France, instead of merely confirming that personal data were being processed, the PIU provided the specific flight information held in the PNR system. We obtained a similar response to part of the SARs submitted in Italy.

82 The response to our PNR requests in the UK deserves particular attention. The UK addressee reacted within two days of our initial requests indicating that, to process the SARs, it was necessary to provide a certified photo ID via signed declaration by a barrister. It was impracticable for us to proceed according to the addressee's instructions, especially in times of the COVID-19 crisis. As a result, we did not follow-up on that request. Given our failure to comply with all the formal requirements, it is reasonable to assume that our SARs would eventually have been refused because of a formal defect.[186]

83 It took PIUs a median of two to 87 days to fully process our SARs. The Irish, British and Maltese PIUs were the fastest to process our requests (within two, two and seven days, respectively), while the Dutch, French and Belgian addressees took the longest time to respond (56, 59 and 87 days, respectively).

183 This seems to indicate that in Portugal it can be difficult for a lay person to understand what are all the formal requirements to exercise their subject access rights, unless individuals can obtain the necessary understanding of the law by seeking legal advice.

184 The median was chosen over the average to avoid outliers relating to the current COVID-19 crisis, which coincided with the empirical study.

185 A requirement that seems to suggest that only individuals who reside or have resided in Ireland are entitled to request access to their personal data, which is nowhere to be found in the national implementing law.

186 Although that was never explicitly said by the UK addressee of our requests.

F. Assessment of law and practice

I. Implementing fallacies

84 Our research on information obligations revealed slight differences in the wording and the formulation of the right of access and its limitation in national transposing laws. Whilst the general line is that such implementations remain rather high level, a few countries opted to include practical provisions on how and where to find useful information for the exercise of access requests. With regard to the modalities for the exercise of the right of access, the study points to very different scenarios. Nevertheless, the majority of the competent authorities scrutinised seem to include the basic information for the exercise of SARs within their websites, in compliance with the spirit of "facilitation of data subject rights" substantiated in Article 12(2) LED. A noteworthy finding regarding both the LED and the PNR Directive in Belgium is that it only seems possible to submit indirect SARs. In other words, the request could only be filed through the NSA, rather than directly to the competent authority or PIU, through the legally appointed single point of contact, i.e. the DPO.

85 The transposition of the information obligations under the PNR Directive was not without issue either. Collecting all relevant information before submitting the SARs before the national PIUs scored an average high level of difficulty due to their absence or inaccessibility. Moreover, the reality of the situation was often at odds with the legal fiction. That was the case with the seemingly non-functional Greek PIU. PIUs are intended to function independently and contact the competent authorities when relevant in accordance with their analyses, they may be "seconded" by competent authorities[187] but remain nonetheless distinct. However, in most Member States, PIUs are institutionally linked to LEAs, as they are founded within the same Ministries[188] or within the Police itself.[189]

86 Finally, requirements such as proof of residency, only came up when looking for the means to submit our SARs, without being stipulated in the national laws. Such requirements came across as arbitrary and impeded our SARs, especially given the commonly present language barriers between the residence of the requesting party and the location of the addressee of the request.

II. Inadequate responses

87 For the most part, our practical exercise of the right of access under both the LED and the PNR Directive resulted in the mere confirmation as to whether or not personal data about us were processed, which appears to be the customary response to SARs in the context of security. The responses obtained in our study rarely disclosed anything else. Moreover, none of the responses we received involved any details that could hint at security-related processing practices in the targeted countries. While somewhat short, such customary responses can nevertheless be considered legally compliant. Interestingly though, while national transposing laws essentially coincide with the LED on the information to be made available to data subjects[190], none of the responses we received disclosed all the pieces of information listed in the LED. This was the case even for the responses which provided the actual personal data. The pieces of information that were left out were details such as the recipients to whom the personal data have been disclosed, the envisaged storage period, and the indication of a right to rectification or erasure.

88 Moreover, it is striking that the only "access" to information that we obtained from the Belgian competent authorities and PIU was the indication that the necessary verifications had been made as to the lawfulness of the processing. In other words, our SARs in Belgium did not even result in the customary response we identified in our study (i.e. the confirmation as to whether or not personal data are being processed), but rather the mere indication that the processing of the data (if any) was done lawfully, as the NSA could confirm.

89 The results of this empirical study also show that, in some European countries, it can be difficult for a lay person to decipher all the formal requirements that are necessary for the exercise of the right of access under the LED and the PNR Directive without the advice of legal experts. In some countries, the addressees of our SARs alluded to our lack of compliance with all the formal requirements to make SARs. Yet, in most (if not all) the cases, the alleged deficiencies were not specified (or even referred to) in the national transposing acts. Moreover, the formal requirements at issue were nowhere to be found in the information obligation measures implemented by Member States.

187 PNR Directive, art 4(3).

188 Belgium, Cyprus, Italy, Ireland, the Netherlands, the UK.

189 Greece, Malta, Luxembourg, Portugal.

190 LED, art 14.

G. Ways forward and recommendations

90 Looking back at the findings outlined in this contribution, one can highlight some ways forward and potential recommendations for competent authorities and PIUs, as well as policy makers, to better comply with both their ex-ante and ex-post transparency obligations.

91 First, participants have frequently highlighted the lack, or incompleteness, of proper transparency measures when trying to exercise their right of access. They were often confronted with scarce, hard-to-find or even conflicting information as to the ins and outs of the processing operations taking place in a law enforcement or PNR context. The same goes for the instructions regarding the exercise of data subject's rights. As emphasised in similar empirical initiatives,[191] adequate and comprehensive information is an essential prerequisite for individuals to understand if and how their personal data are processed and, in such case, whether and how to exercise their right to enquire about certain aspects of those processing operations. As such, it is crucial that competent authorities and PIUs implement comprehensive, intelligible and easily accessible transparency measures, since those will pave the way for data subjects to exercise their prerogatives. To that end, it is important to cultivate a data protection culture and understanding amongst security authorities and officers, whereby a data subject's rights do not consist of a and promote data subject's rights that are not a niche reserved to data protection lawyers, but benefit all individuals subject to EU law. Data subjects should, in that sense, not feel bad about exercising their prerogatives; nor should competent authorities and PIUs make them feel so in their answers.

92 Single points of information could, in that sense, prove invaluable by not only providing all the necessary information in one place but also avoiding inconsistencies between the various competent authorities and PIUs, should multiple actors be competent in a single country. This could take the form of a website centralising all the information about the processing of personal data in a security and law enforcement context, together with a dashboard gathering the relevant contact details for individuals to exercise their prerogatives. Similarly, the use of automated submission forms, or the provision of a standardised template, would drastically streamline the process for data subjects who are less familiar with the applicable regulatory framework. Finally, barriers such as the requirement for the SAR to be sent via regular or certified post, as well as the need to provide a certificate of residency or an address in the country, should be lifted – even if that would entail modifying the corresponding transposing legislation.

93 Second, participants experienced significant disparities in the handling of their requests depending on the Member State investigated. Those differences ranged from procedural requirements – as hinted above – to the scope of the right of access itself – as we have seen in Belgium, for instance. While this is inherent to the nature of the regulatory instruments dealing with the matters at stake, it also makes it extremely complex for data subjects to exercise their prerogatives against competent authorities and PIUs in different countries. This is all the more problematic given that the collection and processing of individuals' personal data for law enforcement or PNR purposes is not limited to their country of residence or nationality. As such, data subjects might have an interest in requesting access to their data in multiple jurisdictions.

94 In light of the above, guidance from NSAs, which, according to our research, most commonly act as the oversight bodies for the GDPR but also the LED and the PNR Directive, could orient and complement the transparency measures adopted by competent authorities and PIUs with guidance and best practices as to how to handle requests emanating from data subjects. In the field of law enforcement, such national efforts could also be encouraged and coordinated by the European Data Protection Board on its own initiative, upon request of one of its members or of the European Commission, as foreseen in Article 51(1)(b) LED. This would be especially welcome with respect to the modalities surrounding the handling of a data subject's rights such as the form in which the request should be formulated, the medium to be used for communicating the said data, the appropriate security and identity verification procedure and the extent of the delay to be observed by competent authorities and PIUs.

95 The EU institutions and policy bodies at large are equally entrusted with promoting and facilitating the harmonisation of data protection safeguards in general, and the exercise of data subjects' rights in particular. The European Commission is engaged to disseminate best practices "through its regular meetings with the Member States and the projects financed under the ISF-P Union actions".[192] It is therefore recommended to accentuate the focus on the exercise of data subjects' rights within these best practices, which seem primarily directed to inter-institutional relations. This will become even more important as the expansion of the

191 See Galetta, Fonio and Ceresa (n 25), Norris (n 25), Ausloos and Dewitte (n 25).

192 Commission (n 29).

scope of application of the PNR Directive to other transportation sectors, such as maritime and rail, is currently being considered.[193] National practices regarding air traveling under the PNR Directive will in that case likely consist of the prototypes upon which other domains will be built.

96 Insofar as the relation between the two directives is concerned, the European Commission, in its report "Ways forward on aligning the former third pillar acquis with data protection rules" published in June 2020[194], has provided an assessment of which legislative acts should be modified in order to be better aligned with the LED[195]. In its assessment, the European Commission concluded that the need to align the PNR Directive with the LED will be further assessed, also taking into account the pending cases before the CJEU. A month later, however, the review report on the PNR Directive did not identify the need to amend in any way the directive.[196] Further clarification regarding the relation between the LED and the PNR Directive, in particular regarding the applicability of data protection safeguards, is considered imperative, due to the restricted manner in which the PNR Directive points to specific data protection rights and obligations (in the CFD)[197].

97 Finally, given the discrepancy between the findings of the PNR Directive review report made publicly available until now, and the findings within this paper, we consider that there is room for improvement also in relation to European supervision. In particular, stronger oversight of the implementation of the directives, forcing Member States to fully comply in both law and practice, so as to remedy the identified gaps and fallacies, is strongly recommended.

H. Conclusions

98 This paper sought to outline the legal framework regarding data protection and the data subject's right of access in the contexts of law enforcement and security as well as its implementation under the LED and the PNR Directive. In theory, the right of access is an essential tool that should empower individuals, whilst at the same time preserving the aims of security and security authorities. The process should comprise a careful and well-thought out balancing of interests and informational power asymmetries. Our intent through the empirical study we conducted in eleven Member States was to evaluate the materialisation of the right of access, and point out potential problems and obstacles that may come up during this process in practice. While a valiant effort has been made on behalf of the investigated Member States to properly implement the LED and the PNR Directive, there is still room for improvement in order to facilitate and provide a more transparent and comprehensive procedure to be followed by data subjects who wish to exercise their right to access.

Note: For detailed information about the competent authorities and PIUs websites and Privacy Notices therein see the following page

193 Commission (n 29).

194 European Commission, 'Ways forward on aligning the former third pillar acquis with data protection rules' (Communication) COM (2020) 262 final.

195 LED, arts 60 and 62(6).

196 Commission (n 29).

197 PNR Directive, art 13.

I. Annex: Notice and Addressee per Country

Country	Notice / Addressee	Competent Authorities	Passenger Information Units
Belgium	Notice	Website of the Belgian police) (www.police.be/en/privacy)	Website of the Crisis Centrum (https://crisiscentrum.be/nl/inhoud/belpiu-collection-and-processing-passenger-data)
	Addressee	Organe de contrôle de l'information policière – COC (info@organedecontrole.be)	BelPIU (belpiu.dir@ibz.fgov.b); redirected to Comité permanent de contrôle des services de renseignements – Comité R (info@comiteri.be)
Cyprus	Notice	Website of the Cyprus Police (https://www.police.gov.cy/police/police.nsf/page09_en/page09_en?opendocument)	/
	Addressee	Cyprus Police (police@police.gov.cy)	/
France	Notice	Website of National Police (https://www.police-nationale.interieur.gouv.fr/Presentation-generale/Deontologie-et-controle) linking to the website of the CNIL (https://www.cnil.fr/fr/directive-police-justice-de-quoi-parle-t)	Website of the Passenger Information Unit (https://pnr.gouv.fr/eng/About-PIU)
	Addressee	Direction Générale de la Police Nationale, Ministère de l'Intérieur, 96 place Beauvau, 75800 Paris CEDEX 08	Directeur de l'UIP, Système API/PNR France, BP 16108, 95701 ROISSY-CDG
Greece	Notice	Website of the Greek Police (http://www.astynomia.gr/index.php?lang=EN) and dedicated webpage only available in Greek (http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=93512&Itemid=114&lang=)	/

Ireland	Notice	Website of the Irish Police (https://www.garda.ie/en/information-centre/data-protection/)	Website of the Irish Immigration Service Delivery (https://www.irishimmigration.ie/irish-passenger-information-unit/)
	Addressee	Irish Police's Data Protection Unit (DataProtection@garda.ie)	Irish Passenger Information Unit (IPIUdataprotection@ipiu.gov.ie)
Italy	Notice	Website of the Italian Police (https://www.poliziadistato.it/articolo/4075de1317ccbefa885830601)	Website of the Italian Police (https://www.poliziadistato.it/articolo/4075dd2a3ecbd99f764225475)
	Addressee	Ministero dell'Interno, Dipartimento della Pubblica Sicurezza, Direzione Centrale della Polizia Criminale, Via Torre di Mezzavia 9, 00173 Roma; holders of a certified email box could also submit an access request electronically using dipps.dcpcufficiocontenzioso@pecps.interno.it	Ministero dell'Interno, Dipartimento della Pubblica Sicurezza, Direzione Centrale della Polizia Criminale, Via Torre di Mezzavia, 9, 00173 Roma; holders of a certified email box could also submit an access request electronically using privacy.pnr@pecps.interno.it
Luxembourg	Notice	Website of the Luxembourgish Police (https://police.public.lu/fr/support/aspects-legaux/2018-rgpd.html)	Website of the Luxembourgish Police (https://police.public.lu/fr/legislation/uip-pnr.html)
	Addressee	Luxembourgish Police's Data Protection Officer (dpo@police.etat.lu)	Direction Générale – Direction des relations internationales – Cellule juridique (dri.cj@police.etat.lu)
Malta	Notice	Website of the Maltese Police (https://pulizija.gov.mt/en/police-force/Pages/Data-Protection-Policy.aspx)	Website of the Maltese Police (https://pulizija.gov.mt/en/police-force/Pages/Data-Protection-Policy.aspx)
	Addressee	Commissioner of Police (dpu.police@gov.mtn)	Commissioner of Police (dpu.police@gov.mtn)

Nether-lands	Notice	Website of the Dutch Police (https://www.politie.nl/algemeen/privacy.html?sid=228463d3-72e3-4434-8947-933a8e3d3756)	Website of the Dutch Government (https://www.government.nl/topics/aviation/air-passenger-travel-information) and a dedicated webpage not available in English (https://www.rijksoverheid.nl/onderwerpen/luchtvaart), and website of Ministry of Defence (https://www.defensie.nl/organisatie/marechaussee)
	Addressee	Landelijke Eenheid, T.a.v., Privacydesk, Postbus 100, 3970 AC DRIEBERGEN and Amsterdam Eenheid, T.a.v., Privacydesk, Postbus 2287, 1000 CG AMSTERDAM	Passagiersinformatie-eenheid (FG-Pi-NL@minjenv.nl)
Portugal	Notice	Website of the Portuguese Police (https://www.psp.pt/Pages/Politica_de_Privacidade/PoliticaPrivacidade.aspx)	/
	Addressee	Inspeção da Polícia de Segurança Pública (inspger@psp.pt)	/
United Kingdom	Notice	ACRO – Police Criminal Records Office https://www.acro.police.uk/SA-Further-guidance	Website of Home Office (https://www.gov.uk/government/publications/requests-for-personal-data)
	Addressee	Form online to be filled on the ACRO website https://www.acro.police.uk/Subject-Access-Online	Online form (https://www.gov.uk/government/publications/requests-for-personal-data) or email contact: SARUOnlineID@homeoffice.gov.uk