



HAL
open science

Mapping the Use of Facial Recognition in Public Spaces in Europe

Theodore Christakis, Karine Bannelier-Christakis, Claude Castelluccia, Daniel
Le Métayer

► **To cite this version:**

Theodore Christakis, Karine Bannelier-Christakis, Claude Castelluccia, Daniel Le Métayer. Mapping the Use of Facial Recognition in Public Spaces in Europe. Université Grenoble Alpes (UGA). 2022. hal-03956166

HAL Id: hal-03956166

<https://inria.hal.science/hal-03956166v1>

Submitted on 25 Jan 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

MAPPING THE USE OF FACIAL RECOGNITION IN PUBLIC SPACES IN EUROPE

MAY 2022



PART 3

FACIAL RECOGNITION FOR AUTHORISATION PURPOSES

Authors:

Theodore CHRISTAKIS (project leader)
Karine BANNELIER
Claude CASTELLUCCIA
Daniel LE METAYER

With contributions from:

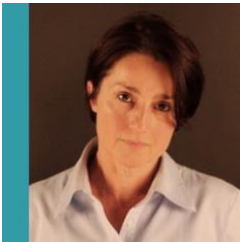
Alexandre LODIE
Stephanie CELIS JUAREZ
Coralie PISON-HINDAWI
Anaïs TROTRY



AUTHORS BIO



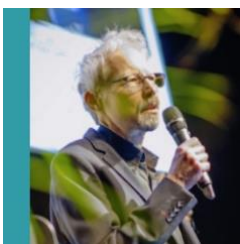
Theodore CHRISTAKIS is Professor of Law at University Grenoble Alpes, director of research for Europe with the Cross-Border Data Forum, Senior Fellow with the Future of Privacy Forum and a former Distinguished Visiting Fellow at the New York University Cybersecurity Centre. He is director of the Chair on the Legal and Regulatory Implications of Artificial Intelligence with the Multidisciplinary Institute on AI (AI-Regulation.com). He has been a member of the French National Digital Council, and he is currently serving as a member of the French National Committee on Digital Ethics and of the International Data Transfers Experts Council of the UK Government.



Karine BANNELIER is Associate Professor of International Law at University Grenoble Alpes. She is deputy director of the Chair of the Legal and Regulatory Implications of Artificial Intelligence at the Multidisciplinary Institute on AI, director of the Grenoble Alpes Cybersecurity Institute and Senior Fellow on Cybercrime at the Cross Border Data Forum. She has served as an expert on cybersecurity issues for French governmental agencies and for international organisations.



Claude CASTELLUCCIA is research director at Inria (France) and a founding member of the Privatics team (models, architectures and tools for the protection of privacy in the information society) where he is conducting research in the areas of digital privacy protection and computer security. He is also the scientific director of the Chair on the Legal and Regulatory Implications of Artificial Intelligence at the University Grenoble Alpes and a member of the French Data Protection Agency (CNIL).*



Daniel LE MÉTAYER is an independent consultant. Until January 2022, he was Research Director at Inria in the team Privatics working in the area of privacy protection, in particular privacy by design, privacy risk analysis, accountability and transparency. He has also been a member of the Commission of the French National Assembly on the rights and freedoms in the digital society and chairman of the scientific committee of the CNIL-Inria Privacy Award.

Other Contributors bio

Alexandre LODIE has joined the Chair as a Research Fellow in September 2021. He has successfully defended a PhD thesis on the principle of non-interference in the context of the Cyberspace development in December 2021. He has also taught law at University Grenoble Alpes and University Savoie Mont-Blanc for four years (2017-2021).

Stephanie CELIS JUAREZ has joined the Chair as a Research Fellow in October 2021. She worked as a lawyer in diverse law branches (civil, administrative, constitutional) in her native country, Mexico. She is particularly interested in online political manipulation and international security and politics.

Coralie PISON HINDAWI has recently joined the Chair as a Research Fellow. Prior to that, she was for many years Associate Professor in International Politics at the American University of Beirut, where she focused on arms control as well as ethics in international affairs. She is associate editor of the journal *Critical Studies on Security*.

Anaïs TROTRY is currently a PhD candidate at University Grenoble Alpes (UGA). Under the supervision of Professor Christakis, her thesis focuses on the concept of risk and on its role in the regulation of new technologies (AI, cyber, access to data and data protection). She is affiliated with the Chair and she has been participating in its work since September 2020.

Acknowledgments and Disclaimers

This is the third report, in a series of six, of a research project that began in June 2021 and covers developments up to April 2022. The first report can be found [here](#) and the second [here](#).

The authors would like to thank all of those who have contributed ideas and comments over the various stages of this research project. Special thanks for their peer-review of a previous version of this report (all errors are ours): Professor Peter Fussey, University of Essex, Human Rights, Big Data and Technology Project; Irina Orssich, Head of Sector AI Policy, European Commission DG Communications Networks, Content and Technology; Isabelle Hupont-Torres and Emilia Gomez-Gutierrez, European Commission Joint Research Centre (JRC).

Many thanks also to Andy Brinded, copyeditor at Ableword (UK), for linguistic proof-reading, Gilles Esparbet for the composition of the cover and Jonathan Collin of Cerf à Lunettes for the images in our classification table. Thanks also to Mathias Becuywe and Maeva El Bouchikhi for their assistance during the initial stage of this project.

This work has been supported by MIAI@Grenoble Alpes, (ANR-19-P3IA-0003). It has also been supported by the Future of Privacy Forum.

The statements in this report are attributable to the authors only, and this publication does not necessarily reflect the views of the Future of Privacy Forum, the Multidisciplinary Institute of Artificial Intelligence, other members of the AI-Regulation Chair or any other partner organisation of the Chair or to which the authors are affiliated.

* The work presented in these reports started before Claude Castelluccia was nominated as a member of the CNIL in August 2021 and was performed at Inria and MIAI, independently of his activity at the CNIL. The views and opinions expressed in this document do not necessarily reflect the position of the CNIL.



HOW TO CITE THIS REPORT:

T. Christakis, K. Bannelier, C. Castelluccia, D. Le Métayer, "Mapping the Use of Facial Recognition in Public Spaces in Europe – Part 3: Facial Recognition for Authorisation Purposes", Report of the AI- Regulation Chair (AI-Regulation.Com), MIAI,

Mapping the Use of Facial Recognition in Public Spaces in Europe

Part 3

FACIAL RECOGNITION FOR AUTHORISATION PURPOSES

Authors:

Theodore CHRISTAKIS (project leader)

Karine BANNELIER

Claude CASTELLUCCIA

Daniel LE MÉTAYER

With contributions from:

Alexandre LODIE

Stephanie CELIS JUAREZ

Coralie PISON-HINDAWI

Anaïs TROTRY

TABLE OF CONTENTS

EXECUTIVE SUMMARY	1
INTRODUCTION	3
A TECHNOLOGY ON THE RISE	3
TWO DIFFERENT FACIAL RECOGNITION FUNCTIONS CAN BE USED FOR AUTHORISATION PURPOSES	5
TABLE 1. AUTHORISATION WITH FRT HAS BEEN PRACTICED IN EUROPE IN 3 DIFFERENT WAYS	6
OUR SEVEN USE CASES	7
TABLE 2. SEVEN USE CASES, DIFFERENT APPLICATIONS AND TECHNIQUES	7
OUTLINE OF THIS REPORT	8
I. LEGAL BASIS: BETWEEN CONSENT AND SUBSTANTIAL PUBLIC INTEREST	9
1. CONDITIONS FOR VALID CONSENT WITH REGARD TO THE USE OF FRT	9
1.1. FREE: AN IMBALANCE OF POWER AND THE ISSUE OF THE CONSENT OF MINORS	10
Invalidity of consent given by students for an FRT trial at the entrance to high schools in southern France ("PACA Schools" Case)	
The issue of consent in the UK Canteens Case	
Invalidity of consent in the Skelleftea School trial in Sweden	
1.2. "FREE": EXISTENCE OF ALTERNATIVE SOLUTIONS	12
Non-biometric gates used for authentication purposes in the Molenbeek Stadium trial	
The importance of an alternative non-biometric route in the case of the "MONA" trial in French airports	
1.3. RESPECT OF THE OTHER REQUIREMENTS FOR VALID CONSENT	14
2. THE USE OF THE "PUBLIC INTEREST" ARGUMENT BY PUBLIC AUTHORITIES	15
2.1. USE OF THE "SUBSTANTIAL PUBLIC INTEREST" EXCEPTION REQUIRES A "LAW"	16
"PARAFE": French Code of Internal Security authorises use of FRT for automated access control at French borders	
Belgian DPA on the need for "explicit" law	
2.2. RELATIONSHIP BETWEEN "CONSENT" AND A "VOLUNTARY" UNDERTAKING	17
II. NECESSITY AND PROPORTIONALITY	19
1. A BALANCING ACT THAT INCLUDES SEVERAL COMPONENTS	19
Disagreements between European DPAs about whether facial recognition is as a strong means of authentication or not	
Belgian DPA guidelines on how to navigate the balancing act	
Link between the proportionality test and the GDPR data processing principles	
Do not process the data of people who have not consented to it	
2. LESS INTRUSIVE MEANS	22
The Belgian DPA on "less intrusive means"	
The French DPA on the need to "demonstrate the inadequacy of other, less intrusive security means"	
When Facial Recognition is less intrusive than previous authentication techniques	
Acceptance of use of biometrics for pre-existing police access controls if there are "substantial guarantees" that ensure a high level of data protection	
Less intrusive means and a need for "comfort"	
"Certain uses are forbidden in our society". Facial recognition for authorisation in schools and the "less intrusive means" requirement	
Avoiding a "slippery slope" and the phenomenon of habituation: The case of the traveler's lounge	
III. RISK OF DIVERGENCE: DIFFERENT ASSESSMENTS OF THE "ONE ID" CONCEPT FOR AIR TRAVEL?	31
1. IATA: THE "ONE ID" CONCEPT	32
The "One ID" Concept's Objectives	
Improvements for Passengers According to the IATA	
Data Minimisation and Storage Limitation – the IATA's Position	
2. DPA'S TRADITIONAL HOSTILITY TO CENTRAL STORAGE OF BIOMETRIC DATA	36
EDPB: "Biometrics should preferably not be stored in a database"	

Belgian DPA: "Don't use biometric systems that store biometric reference data in a database"
AEPD and EDPB: Biometric identification/authentication systems are not safer for users
French DPA: "Keeping biometric data under the exclusive control of the passengers"

3. CNIL'S RESERVATIONS CONCERNING THE MONA CASE	38
Is Biometric Data Deleted Each Time a Plane Takes Off?	
CNIL's doubts about the compatibility of IATA's "One ID" Concept with the data minimisation and storage limitation principles of the GDPR	
4. DIVERGENCES? DEPLOYMENT OF "ONE ID" SOLUTIONS IN SPAIN, GERMANY, AND BEYOND	41
From AENA pilot projects to a generalisation of "One ID" applications in Spain?	
Star Alliance Biometrics in Germany	
5. POTENTIAL SOLUTIONS TO BRING ABOUT HARMONISATION	44
IV. ASSESSMENTS: FROM DPIAS TO EVALUATING ACCURACY AND EFFICIENCY	46
1. DATA PROTECTION IMPACT ASSESSMENTS	46
CNIL Recommends that a DPIA be carried out before the use of FRT for authorisation at an airport	
Belgian DPA: "Not carrying out a DPIA can only be justified in exceptional cases"	
2. EVALUATING ACCURACY AND EFFICIENCY	48
CONCLUSIONS AND RECOMMENDATIONS	51
1. RECOMMENDATIONS IN RELATION TO DATA CONTROLLERS	51
1.1. Data controllers should understand that they have the burden to prove that they meet all GDPR requirement	
1.2. Data controllers should understand the limits of the "cooperative" use of facial recognition for authorisation purposes	
1.3. Data controllers should conduct DPIAs and evaluation reports	
2. RECOMMENDATIONS IN RELATION TO DPAs AND THE EDPB	53
2.1. DPAs and the EDPB should ensure that there is harmonisation on issues such as the use databases, and principles relating to processing of personal data	
2.2. The EDPB could produce guidance on the approach to be followed both for DPIAs and evaluation reports of FRT authorisation applications	
3. RECOMMENDATIONS REGARDING POLICYMAKERS	54

EXECUTIVE SUMMARY

[Part 1](#) of our “MAPping the use of Facial Recognition in public spaces in Europe” (MAP-FRE) project reports explained in detail what “facial recognition” means, addressed the issues surrounding definitions, presented the political landscape and set out the exact material and geographical scope of the study. [Part 2](#) of our Reports presented, in the most accessible way possible, how facial recognition works and produced a “Classification Table” with illustrations, explanations and examples, detailing the uses of facial recognition/analysis in public spaces, in order to help avoid conflating the diverse ways in which facial recognition is used and to bring nuance and precision to the public debate.

This 3rd Report focuses on what is, undoubtedly, the most widespread way in which Facial Recognition Technologies (FRT) are used in public (and private) spaces: Facial Recognition for authorisation purposes.

Facial recognition is often used to authorise access to a space (e.g. access control) or to a service (e.g. to make a payment). Depending on the situation, both verification and identification functionalities (terms that are explained in our [2nd Report](#)) can be used. Millions of people use FRT to unlock their phones every day. Private entities (such as banks) or public authorities (such as the French government in terms of the now abandoned ALICEM project) increasingly envisage using FRT as a means of providing strong authentication in order to control access to private or public online services, such as e-banking, or administrative websites that concern income, health or other personal matters. FRT is increasingly being considered as a means of improving security when controlling and managing access to private areas (building entrances, goods warehouses, etc.).

In **public spaces**, FRT is being used as an authentication tool for automated international border controls (for example at airports) or to manage access in places as diverse as airports, stadiums or schools. Pre Covid-19, there were a lot of projects to use in the future FRT in order to “accelerate people flows”, “improve the customer experience”, “speed up operations” and “reduce queuing time” for users of different services (e.g. passengers boarding a plane or shopping) but the advent of the Covid-19 pandemic has further boosted calls for investment in FRTs in order to provide contactless services and reduce the risk of contamination. Supermarkets, such as Carrefour, which was involved in a pilot project in Romania, or transport utilities in “smart cities”, such as the EMT bus network in Madrid, which teamed with Mastercard to conduct a pilot project that enables users to pay on EMT buses using FRT, have implemented facial recognition payment systems that permit consumers to complete transactions by simply having their faces scanned. In Europe, similar pilot projects are currently being tested enabling the management of payments in restaurants, cafés and shops.

Despite this widespread existing use or projected use of FRT for authorisation purposes we are not aware of any detailed study that is focusing on this specific issue. We hope that the present analytic study will help fill this gap by focusing on the specific issue of the use of FRT for authorisation purposes in public spaces in Europe.

We have examined in detail seven “emblematic” cases of FRT being used for authorisation purposes in public spaces in Europe. We have reviewed the documents disseminated by data controllers concerning all of these cases (and several others). We have sought out the reactions of civil society and other actors. We have dived into EU and Member State laws. We have analysed a number of Data Protection Authority (DPA) opinions. We have identified Court decisions of relevance to this matter.

Our panoramic analysis enables the identification of convergences among EU Member States, but also the risks of divergence with regard to certain specific, important ways in which FRTs are used. It also permits an assessment of whether the GDPR, as interpreted by DPAs and Courts around Europe, is a sufficient means of regulating the use of FRT for authorisation purposes in public spaces in Europe – or whether new rules are needed.

What are the main issues in practice in terms of the legal basis invoked by data controllers? What is the difference between “consent” and “voluntary” in relation to the ways in which FRT is used? Are the “alternative (non-biometric) solutions” proposed satisfactory? What are the positions of DPAs and Courts around Europe on the important issues around necessity and proportionality, including the key “less intrusive means” criterion? What are the divergences among DPAs on these issues? Is harmonisation needed and if so, how is this to be achieved? What are the lessons learned concerning the issue of DPIAs and evaluations? These are some of the questions examined in this report.

Our study ends with a series of specific recommendations that we are making, in relation to data controllers, the EDPB as well as stakeholders making proposals for new FRT rules.

We make **three recommendations vis-à-vis those data controllers** wishing to use facial recognition applications for authorisation purposes:

- 1) Data controllers should understand that they have the burden of proof in terms of meeting all of the GDPR requirements, including understanding exactly how the necessity and proportionality principles as well as the principles relating to processing of personal data should be applied in this field.
- 2) Data controllers should understand the limits of the “cooperative” use of facial recognition when used for authorisation purposes. Deployments of FR systems for authorisation purposes in public spaces in Europe have almost always been based on consent or have been used in a “voluntary” way. However, this does not mean that consent is almighty. First, there are situations (such as the various failed attempts to introduce FRT in schools in Europe) where consent could not be justified as being “freely given” because of an imbalance of power between users and data controllers. Second, consensual and other “voluntary” uses of FRT imply the existence of alternative solutions which must be as available and as effective as those that involve the use of FRT.
- 3) Data controllers should conduct DPIAs and evaluation reports and publish them to the extent possible and compatible with industrial secrets and property rights. Our study found that there is a serious lack of information available on DPIAs and evaluations of the effectiveness of FRT systems. As we explain, this is regrettable for several reasons.

We make **two recommendations in relation to the EDPB**:

- 1) The EDPB should ensure that there is harmonization on issues such as the use of centralised databases, and those principles that relate to the processing of personal data. A diverging interpretation of the GDPR on issues such as the implementation of IATA’s “One ID” concept for air travel or “pay by face” applications in Europe could create legal tension and operational difficulties.
- 2) The EDPB could also produce guidance on the approach that should be followed both for DPIAs and evaluation reports where FRT authorisation applications are concerned.

Finally, a **recommendation regarding policy makers and other stakeholders formulating new legislative proposals**: there is often a great deal of confusion about the different proposals that concern the regulation of facial recognition. It is therefore important for all stakeholders to distinguish the numerous ways in which FRT is used for authorisation purposes from other use cases and to target their proposals accordingly. For instance, proposals calling for a broad ban on “biometric recognition in public spaces” are likely to result in all of the ways in which FRT is used for authorisation purposes being prohibited. Policy-makers should take this into consideration, and make sure that this is their intention, before they make such proposals.

INTRODUCTION

Part 1¹ of our “MAPping the use of Facial Recognition in public spaces in Europe” (MAPFRE) explained in detail what “facial recognition” means, addressed the issues surrounding definitions, presented the political landscape and set out the exact material and geographical scope of the study. Part 2² of our Reports presented, in the most accessible way possible, exactly how facial recognition and facial analysis work. We have endeavoured to produce a “**Classification Table**” with illustrations, explanations and examples, detailing the uses of facial recognition/analysis in public spaces, in order to help avoid conflating the diverse ways in which facial recognition is used and to bring nuance and precision to the public debate. This third Report focuses on what is, undoubtedly, **the most widespread way in which Facial Recognition Technologies (FRT) are used in public (and private) spaces**: Facial Recognition (FR) for authorisation purposes. FR is indeed often used to authorise access to a space (*e.g.* access control) or to a service (*e.g.* to make a payment). Depending on the situation, both verification and identification functionalities can be used. What are the main issues in practice in terms of the legal basis invoked by data controllers? What is the difference between “consent” and “voluntary” in relation to the ways in which FRT is used? Are the “alternative (non-biometric) solutions” proposed satisfactory? What are the positions of DPAs and Courts around Europe on the important issues around necessity and proportionality, including the key “less intrusive means” criterion? Are there divergences among DPAs on these issues? Is harmonisation needed and if so, how is this to be achieved? What are the lessons learned concerning the issue of DPIAs and evaluations? These are some of the questions examined in this report.

A Technology on the Rise

The use of Facial Recognition Technology (FRT) for authorisation purposes has become more and more widespread. Millions of people use FRT to unlock their phones or other electronic devices every day. Private entities (such as banks) or public authorities (such as the French government in terms of the ALICEM project³) increasingly envisage using FRT as a means of providing strong authentication in order to control access to private or public online services, such as e-banking, or administrative websites that concern income, health or other highly sensitive personal matters. FRT is increasingly being considered as a means of improving

¹ See T. Christakis, K. Bannelier, C. Castelluccia, D. Le Métayer, “[Mapping the Use of Facial Recognition in Public Spaces in Europe – Part 1: A Quest for Clarity: Unpicking the “Catch-All” Term](#)”, Report of the AI-Regulation Chair (AI-Regulation.Com), MIAI, May 2022.

² See T. Christakis, K. Bannelier, C. Castelluccia, D. Le Métayer, “[Mapping the Use of Facial Recognition in Public Spaces in Europe – Part 2: Classification](#)”, Report of the AI-Regulation Chair (AI-Regulation.Com), MIAI, May 2022.

³ The French ALICEM system (a project that was not implemented in the end), worked by comparing a “selfie” and a video taken in real time by the user with a photograph stored in the electronic component of the biometric passport or residence permit belonging to the same person. This process offered a way of creating a digital identity using a mobile app (smartphone, tablet...) which could then be used to securely access online administrative services. For an analysis, and the French DPA’s, CNIL, positions on this project, see Marc Rees, “[ALICEM : la biométrie de l’identité numérique sur mobile fait tiquer la CNIL](#)”, NextInPact, May 16, 2019.

security when controlling and managing access to private areas (building entrances, goods warehouses, etc.). In public spaces, FRT is being used as an effective authentication tool for automated international border controls or to manage access in places as diverse as airports, stadiums or schools.

Pre Covid-19, there were a lot of projects for using FRT in order to “accelerate people flows”, “improve the customer’s experience”, “speed up operations” and “reduce queuing time” for users of different services (*e.g.* passengers boarding a plane or shopping) but the advent of the Covid-19 pandemic has further boosted calls for investment in FRTs in order to provide contactless services and reduce the risk of contamination. Supermarkets, in countries such as South Korea⁴ or in a pilot project by Carrefour in Romania,⁵ or transport utilities in “smart cities”, such as the pilot project of Mastercard intending to allow users to pay on EMT buses in Madrid using facial recognition,⁶ have implemented facial recognition payment systems that permit consumers to complete transactions by simply having their faces scanned. Similar pilot projects are currently being tested, or it appears are already being used, in Europe for payments in restaurants, cafés and other shops.⁷ A very similar system has also been used, as we will see, in the “UK School Canteens” case discussed below. A recent study, conducted jointly by AI.Regulation.Com and Skopai, focusing on 130 start-ups around the world that develop facial recognition technologies, found that 68% of them are working on products designed to be used for authentication purposes.⁸

Despite this widespread existing or projected use of FRT for authorisation purposes we are not aware of any detailed study that is focusing on this specific issue. We hope that the present study will help fill this gap by focusing on the specific issue of the use of FRT for authorisation purposes in public spaces in Europe. We have examined in detail seven “emblematic” use cases of FRT being used for authorisation purposes in public spaces in Europe. We have reviewed the documents disseminated by data controllers concerning all these cases. We have sought out the reactions of civil society or other actors. We have dived into EU and Member State laws. We have analysed a number of Data Protection Authority (DPA) opinions. We have identified Court decisions of relevance to this matter.

⁴ Consumers are simply required to stand in front of the device and briefly look into the camera, and their facial features are automatically captured without cashiers manually having to enter the information for that person. Once the person’s identity has been matched with the platform database, the shopping bill is deducted from the linked bank account. See : [“Telpo Facial Payment Device Boost Supermarket Operation”](#), March 2, 2022.

⁵ See for instance [“Carrefour Romania Offers Biometric Payments on Top of single Digital Portal”](#), March 2019.

⁶ According to the description of the project: “users of Madrid buses will simply have to download an EMT mobile application in which they will enter their payment details and take a photograph of their face to start using biometric payment. From then on, once inside the bus, they will show their face to a recognition camera that will allow them to validate, at the same time, identification and authentication, i.e. the purchase of a ticket and payment in a single gesture. For more information see [here](#). It [seems](#) that Madrid’s city council suspended this pilot project in 2020 during the Covid-19 pandemic claiming that the system [had not been perfected to recognise individuals wearing a mask](#) (rendered compulsory during that year in public transport in Spain). It also seems that the Madrid City Council has not continued with this biometric project and has replaced it instead with one called “Madrid Mobility 360” that allows users to pay using instead a QR code associated with their account. See: [“Madrid Mobility 360 es la App de movilidad inteligente para moverse por Madrid”](#).

⁷ See for instance the pilot projects related to the [“Face to Pay” Application](#), developed by Payment Innovation Hub, “a joint venture from CaixaBank, Global Payments Inc, Visa, Samsung, and Arval that jointly promotes R&D projects on new payment and commerce solutions”.

⁸ See Becuywe, M., Beliaeva, T., Beltran Gautron, S., Christakis T., El Bouchikhi, M., Guerraz, A. [“Landscape of start-ups developing facial recognition. Analysis and legal considerations”](#), AI- Regulation.com, Skopai.com, January 2022, at 10-12.

Our panoramic analysis enables the identification of convergences among EU Member States, but also the risks of divergence with regard to certain specific, important ways in which FRTs are used. It also permits an assessment of whether the GDPR, as interpreted by DPAs and Courts around Europe, is a sufficient means of regulating the use of FRT for authorisation purposes in public spaces in Europe – or whether new rules are needed.

Two Different Facial Recognition Functions Can Be Used for Authorisation Purposes

It is very important to emphasise something that we have already tried to show in our classification table.⁹ When a data controller wishes to use facial recognition for authorisation purposes in a specific context, he/she can opt between **two different biometric functions**, *i.e.* either using the “*verification*” function or the “*identification*” function. As we will see in this report the choice between the two functionalities is not without consequences on the data protection regime.

The first functionality that can be used is “**verification**”, which involves, as we have seen in Part 2 of these Reports, a 1-1 comparison, between a single captured facial image of a user (for instance taken at an eGate at the border) and the biometric photo stored in a biometric token (for instance a passport) or an index. Verification is most often considered as a synonym to “**authentication**”.¹⁰ Authentication is the process of verifying the purported identity of a person (or any given entity). The International Organization for Standardization (ISO) defined “authentication” in 2005 in the following way:

*“Authentication: Provision of assurance of the claimed identity of an entity. In case of user authentication, users are identified either by knowledge (e.g., password), by possession (e.g., token) or by a personal characteristic (biometrics). Strong authentication is either based on strong mechanisms (e.g., biometrics) or makes use of at least two of these factors (so-called multi-factor authentication)”.*¹¹

Similarly, the Article 29 Working Party explained in 2003 that:

*“To perform authentication, three different methods may be used jointly – based on something an individual knows (password, PIN, etc.), something an individual owns (token, CAD key, smart card, etc.) and something an individual is (a biometric feature)”.*¹²

While the things that an individual “knows” or “owns” can be stolen (a password can be hacked, a token can be stolen...), biometric characteristics are generally perceived as a much more secure means of authentication.

⁹ See : T. Christakis, et al., “[Mapping the Use of Facial Recognition in Public Spaces in Europe – Part 2: Classification](#)”, Report of the AI- Regulation Chair (AI-Regulation.Com), MIAI, May 2022.

¹⁰ However, as we have already noted in [Part 2](#) of these series, the Belgian DPA has argued that “in the particular context of biometrics, the definition of verification has a specific meaning *that is totally distinct from the notion of authentication*. Indeed, authentication (*i.e.* the process of identity verification) can be achieved by both biometric functions, *i.e.* either by the identification function or by the verification function”. [Own-initiative opinion on the processing of biometric data for the authentication of persons \(A/2008/017\)](#), April 9, 2008, at 5.

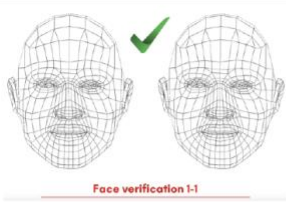
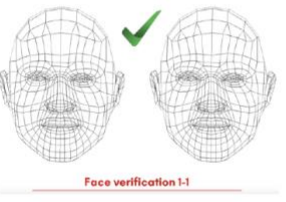
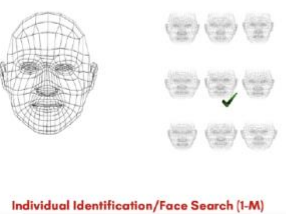
¹¹ ISO/IEC 18028-4: 2005.

¹² Article 29 Working Party Biometrics Working Paper, WG80, adopted August 1, 2003, p.3.

Authentication is generally used as a means of granting rights that are normally reserved for specific people (access to a space or to a specific service, etc.).

The second functionality that can be used is “**identification**”. As we have explained in Part 2 of these Reports, the identification function consists of comparing a single captured facial image of a user (for instance an image taken at a checkpoint of a person who wishes to board a plane or to make a payment) with the reference facial images of users authorised to use this service appearing in a database (1-M or “one-to-many” comparison). This function will first identify the user among all the registered persons, and can then be used to authorise the use of a specific service by the user.

Table 1. Authorisation with FRT has been practiced in 3 different ways

Functionality	Application	Captured Faces	Reference Faces	Explanation	Examples
	Authorisation using a biometric token	1	1	Compares a single face against a reference image stored in a biometric token of the user (e.g. a passport). Face recognition is used to confirm that there is indeed a match between the two images. This may be used in security access control protocols.	PARAFE Automated Passport control at the border (FR)
	Authorisation using an ID token	1	1 (in M)	Compares a single face against a single reference indexed in a database. A token stores an identifier of the user. The token can be in the form of a badge, QR code in a smartphone, etc. It is provided as an input by a person and links to his/her specific images stored in this database “1 (in M)”. Face recognition is used to confirm that there is indeed a match between the two images. This may be used for instance in access controls in a closed space (e.g a school).	PACA Schools Access Control in High schools in the South of France
	Authorisation without using a token	1	M	Authorises a user by searching if his faceprint appears in a database of authorised users.	Molenbeek Stadium (BE) MONA System in Airports (FR) IBERIA (ES) Payments in School Canteens (UK) (...)

Our Seven Use Cases

The use of facial recognition for authorisation purposes is, by far, the most widespread way in which facial recognition techniques (FRT) are used in public (and private) spaces. Indeed, we have been able to identify a considerable number of such cases in public spaces. Some of these cases concern permanent deployments of facial recognition. Others concern past, ongoing or future pilot projects. And a few others concern aborted projects (such as those that involve the use of FRT in schools) that started but had to be terminated following strong criticism and the intervention of DPAs or Courts.

Among several of the cases that we have identified, we have selected and

Facial Recognition for Authorisation Purposes

analysed in detail seven cases, based on a number of criteria that we have presented in the first report in the MAPFRE series.¹³

Table 2. Seven Use Cases, Different Applications and Techniques

Name	Description/Objectives	Captured Faces	Reference Faces	Functionality & Application
Parafe (FR)	FRT automated system used by the French Government to authenticate, on a voluntary basis, European passengers in airports and stations. Main objective: to make police controls at external borders more fluid.	1 (Image of a passenger captured at the eGate)	1 Image appearing in the biometric passport scanned by the passenger at the eGate.	VERIFICATION (Authorisation using a biometric token)
PACA Schools (FR)	Experimental Use of FRT at the entrance to two high schools in the French PACA Region. Main objectives: - to provide assistance to the agents in charge of access control; - to facilitate and reduce the duration of controls; - to fight against identity theft.	1 (Image of a student captured at the entrance eGate)	1 (in M) The processing consists of correlating a digital identity (QR code affixed to a document, badge, smartphone) with a facial identity. The experimental system consists of 2 databases created for the experiment: - An "identity" database: Last name, First name, Digital identifier (of choice), NFC or QR Code; - A biometric database containing: Digital identifier, biometric templates (collected during the enrolment of volunteers within the school (students, teachers, ...)); this second database can only be accessed in order to be read by conducting the comparison process. No administrator has access to it. The student presents an ID token at the entrance. The systems' software then reads the digital identifier on the reader (NFC or QR Code), detects the face thanks to the cameras coupled to the reader, extracts a template and compares it on the fly with the reference template corresponding to the digital identifier.	VERIFICATION (Authorisation using an ID token)
Payment in School Canteens (UK)	FRT solution used in canteens to implement a cashless payment solution in 9 schools in North Ayrshire. Main objectives: - remove the need for pupils to bring cash and cheques to school making all school purchases cashless; - make payment in school canteens faster - Reduce the risk of spreading Covid by means of contactless payments	1 (Image captured when the child looks at the Canteen's camera)	M Pupils who have consented to uploading an identity photo via an application. A specific database is then created with the biometric templates of all the children who have consented to this procedure. Then, when the child looks at the canteen's camera, the software reads their key features (distance between facial features) and compares this against the database of registered users. When it finds a match it automatically opens their cashless canteen account allowing the operator to complete the sale of their school meal.	INDIVIDUAL IDENTIFICATION (Authorisation without using a token)
Molenbeek Stadium (BE)	Offers season ticket holders a 'fast lane' in which they are only required to show their face. This "will save precious minutes, for example, when you arrive just before kick-off".	1 (Image of a season ticket holder captured at the entrance)	M Fans who order their season tickets online can upload an identity photo via an application. A specific database is created comprising all those who have bought season tickets who consent to the use of FRT. Then a special "fast lane" gate is created for them and the FR system captures their images as they pass by, compares them to the database of people who have been authorised to use this service, and if there is a match, the gate will open.	INDIVIDUAL IDENTIFICATION (Authorisation without using a token)
MONA (FR)	FRT system tested at Lyon Airport allowing passengers to go through check in, security and boarding controls by having their faces scanned. Main objectives: - make the traveler's journey through the airport more fluid; - improve the customer experience - increase the level of security	1 (Image of a passenger captured at the various checkpoints in the airport)	M Passengers who consent to the use of the "MONA" application before they travel must enter their name/telephone number, scan their identity card and boarding pass, and take a photograph of their face. A specific database is then created comprising the biometric templates of all the passengers of a specific flight. Once at the airport, passengers go through the MONA process by having their faces scanned at the various gates or kiosks equipped with FRT devices. Each candidate face template is compared with the M biometric templates stored in the database. The question "Who am I?" is therefore answered by finding the closest match to the candidate in a set of templates, allowing the passenger to continue their journey.	INDIVIDUAL IDENTIFICATION (Authorisation without using a biometric token)

¹³ See T. Christakis, et al, "[Mapping the Use of Facial Recognition in Public Spaces in Europe – Part 1: A Quest for Clarity: Unpicking the "Catch-All" Term](#)", op.cit.

Aena/Iberia (ES)	FRT system tested in three airports and involving three airlines in Spain, allowing passengers to go through check in, security and boarding controls by having their faces scanned	1 (Image of a passenger captured at the various checkpoints in the airport)	M The system works in a way similar to MONA (although the implementation is different).	INDIVIDUAL IDENTIFICATION (Authorisation without using a token)
Star Alliance (DE/AT)	FRT system tested by three airlines in three airports in Germany and one in Austria allowing passengers to go through check in, security and boarding controls by having their faces scanned	1 (Image of a passenger captured at the various checkpoints in the airport)	M The system works in a way similar to MONA (although the implementation is different).	INDIVIDUAL IDENTIFICATION (Authorisation without using a token)

Outline of this Report

We invite readers to read our detailed analysis of these use cases, which is to be published soon.¹⁴ In this report we focus solely on certain very important issues and key takeaways that have resulted from our analysis.

Part I of this report focuses on the issue of the legal basis used for the deployment of facial recognition for authorisation purposes in public spaces in Europe.

Part II discusses extensively the major issue of necessity and proportionality.

Part III compares a number of case studies concerning the commercial use of FRT for authorisation purposes in airports in order to assess whether there is a risk of divergence between DPAs in Europe concerning the interpretation of the necessity and proportionality principles. We also discuss how this risk could be mitigated.

Part IV examines whether the deployment of facial recognition for authorisation purposes in public spaces in Europe, has been preceded by the conclusion of Data Protection Impact Assessments (DPIA) and has been followed by the drafting of evaluation reports, assessing the accuracy and the overall efficiency of the deployment, *i.e.* the capacity of FRT to meet the overall objectives.

We end this report with a series of conclusions and recommendations.

¹⁴ See T. Christakis, et al, “Mapping the Use of Facial Recognition in Public Spaces in Europe – 25 Selected Case Studies”, Report of the AI- Regulation Chair (AI-Regulation.Com), MIAI, forthcoming.

I. LEGAL BASIS: BETWEEN CONSENT AND SUBSTANTIAL PUBLIC INTEREST

All facial recognition systems used for authorisation purposes in public spaces in the EU and the UK that we have examined have been based on two GDPR-related legal bases:¹⁵

- “Explicit consent” under Article 9(2)(a) of the GDPR, which is the first exception¹⁶ to the prohibition of processing of biometric data posed by Art. 9(1) of the GDPR **(1)**; and
- “Processing necessary for reasons of substantial public interest”, under Article 9(2)(g) of the GDPR¹⁷ **(2)**.

We will now examine these two legal bases, and the way in which FRT is used accordingly.

1. Conditions for valid consent with regard to the use of FRT

While inapplicable where the Law Enforcement Directive is concerned,¹⁸ explicit consent is, under several conditions, a very common legal basis for the use of FRT within the scope of the GDPR. In 2008, in an Opinion on the use of FRT for authentication purposes, the Belgian DPA had already noted that “consent certainly allows these new technologies to be socially accepted by the users”. This was confirmed by the survey “on the public attitudes to facial recognition technology” conducted in 2019 by the Ada Lovelace Institute which emphasised that “people place considerable importance on being able to consent to, or opt out

¹⁵ As the EDPB stressed, if a data controller processes biometric data, the data controller must identify **both** an exception for processing special categories of data under Article 9 (i.e. an exemption from the general rule that one should not process special categories of data) **and** a legal basis under Article 6. See EDPB, [Guidelines 3/2019 on processing of personal data through video devices](#), January 29, 2020 p. 17.

¹⁶ Consent is one of six lawful bases for the processing of personal data, as listed in Article 6 of the GDPR, and one of the ten exceptions to the prohibition of the processing of biometric data posed by Art. 9(1) of the GDPR.

¹⁷ It is interesting to note that the corresponding legal basis in Article 6 for all personal data is processing “necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller” Article 6(1)(e). In other terms the “public interest” must be “**substantial**” when processing biometric data. Both Articles 6(1)(e) and 9(2)(g) require the existence of a specific provision to that effect in EU or Member State law.

¹⁸ Under recital 35 of the LED: “The performance of the tasks of preventing, investigating, detecting or prosecuting criminal offences institutionally conferred by law to the competent authorities allows them to require or order natural persons to comply with requests made. In such a case, the consent of the data subject, as defined in Regulation (EU) 2016/679, should not provide a legal ground for processing personal data by competent authorities. Where the data subject is required to comply with a legal obligation, the data subject has no genuine and free choice, so the reaction of the data subject could not be considered to be a freely given indication of his or her wishes”.

of, facial recognition technologies”.¹⁹ However, despite its importance, consent in the context of the use of FRT is subject to several important conditions and restrictions. The practice that we have examined in our MAPFRE project confirms, indeed, that in certain situations data controllers are not able to rely on consent, while in other situations they need to take care of a number of elements if they want to ensure that consent will still be valid under the GDPR requirements.

As a matter of fact, under Article 9(2)(a) of the GDPR, the prohibition of processing of biometric data shall not apply when:

“the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject”.

Article 4(11) of the GDPR defines consent as:

“any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”.

This definition includes the different constitutive elements that make up valid consent.²⁰ Let's now examine the main issues that have emerged in relation to these elements in practice, with regard to the use of facial recognition for authorisation purposes in public spaces in Europe.

1.1. “Free”: An Imbalance of power and the issue of the consent of minors

European DPAs have insisted constantly since 2011 that the “free” element implies that data subjects have authentic choice and control. This means that if the data subject is not afforded authentic choice, feels compelled to consent or endures negative consequences as a result of not consenting, then consent is not valid.²¹ The DPAs describe this as a situation whereby there is an “imbalance of power” and have often given the example of the “employment context”, explaining that “given the dependency that results from the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal”.²² In terms of the existing practice of the use of facial recognition in public spaces in Europe, however, the “imbalance of power” concerns another scenario, namely minors giving their consent when facial recognition is used for authorisation purposes in schools.

¹⁹ [“Beyond face value: public attitudes to facial recognition technology”](#), Report, Ada Lovelace institute, September 2, 2019, at 6.

²⁰ See also EDPB, [Guidelines 05/2020 on consent under Regulation 2016/679](#), May 4, 2020 (“EDPB 2020 Guidelines on Consent”).

²¹ See Article 29 WP, [Opinion 15/2011 on the definition of consent \(WP187\)](#), p.12 and EDPB 2020 Guidelines on Consent, p. 7.

²² EDPB 2020 Guidelines on Consent, p. 9.

Invalidity of consent given by students for an FRT trial at the entrance to high schools in southern France (“PACA Schools” Case)

The PACA region (located in southern France) voted to experiment with facial recognition in two high schools in the region. The main aim was to manage access to the schools by biometric means (authorisation of students who consent to the trial). The data controllers claimed in their “trial convention” that consent would be free by arguing the following:

“[p]articipation in this experiment is optional, and based on the individual consent of the students, and their legal representative if they are minors. Each person concerned is free to accept or refuse to participate in this experiment and to authorise the processing of their personal data. His/her refusal does not entail any consequences as regards his/her rights and duties with regard to the school. If he/she wishes to refuse to participate in this experiment and not to authorise the processing of his/her personal data, it is sufficient for him/her not to sign the consent form.”²³

However, the project was never implemented since both the French DPA and, later, a French Court considered that such an experiment would have been unlawful as regards the GDPR provisions. One of the main arguments was that pupils could not freely provide consent since the High Schools Board of directors have authority over the pupils – at least some of which were minors at the time of the trial. In its decision of February 27, 2020²⁴, the Administrative Court of Marseille stated the following:

“It is clear from the documents in the file that the PACA region intended to legally justify the processing of the biometric data in question based on the prior consent of the high school students concerned or, in the case of minors, that of their legal representatives. However, by merely providing that this consent would be obtained by signing a form, when those in charge of the public education establishments concerned have authority over the public concerned, the region cannot justify that they have provided sufficient guarantees in terms of obtaining consent from the pupils or their legal representatives for the collection of their personal data in a free and informed manner.”²⁵

The issue of consent in the UK Canteens Case

North Ayrshire Council decided in October 2021 to deploy an FRT system in canteens as a means of implementing a cashless payment solution in nine schools. The purpose of this system was to make payments in school canteens faster, but also to engender a safer environment, as it was also intended to reduce the risk of the spread of Covid. The FRT authorisation system was based on consent. Facial Recognition forms were emailed to the children’s families. As reported in a press article, “North Ayrshire council claims that 97 percent of children or parents consented to be enrolled”. The use of consent as a legal basis has been disputed by critics who claimed that “although UK data protection law specifies that children aged 13 and over can consent to the processing of their personal data, this doesn’t mean they fully understand the implications”. In reaction to this case the UK DPA, the ICO, emphasised that

²³ “Convention d’expérimentation”, Région PROVENCE-ALPES-CÔTE D’AZUR – CISCO – LYCEE. Our translation.

²⁴ See CHRISTAKIS (T.), “[First Ever Decision of a French Court Applying GDPR to Facial Recognition](#)”, *AI-Regulation.com*, February 27, 2020.

²⁵ Tribunal administratif de Marseille, 27 février 2020, n° 1901249. Our translation

“data protection law provides additional protections for children”. However, in contrast to the position of the French DPA and Court in the PACA case, the ICO did not claim publicly that consent in this case was invalid. Instead, it challenged the use of FRT in the North Ayrshire school canteens on the basis of the argument that it did not meet the requirements of necessity and proportionality, and that less intrusive means should be considered (see below).

While the following is not technically a case that involves the use of FRT for “authorisation” purposes²⁶, it is also worth mentioning the position of the Swedish DPA in the case of the trial at Skelleftea school:

Invalidity of consent in the Skelleftea School trial in Sweden

The board of a Swedish school in the town of Skelleftea decided to conduct an experiment with FRT to monitor pupils’ attendance in class. The Swedish DPA stopped the trial however, when it found that the two legal bases for processing biometric data invoked by the school to justify it were not valid. More specifically, one of the arguments used by the DPA was that the consent of the pupils sought by the school could not be used as a legal basis as there was an imbalance in the relationship between the pupils and the school’s board. The DPA noted that:

*“the assessment of whether consent has been freely given should be based not only on the prevailing freedom of choice, but also on the relationship that exists between the data subject and the controller. The scope for voluntary consent within the public sphere is therefore limited. As regards the school sector, it is clear that the students are in a position of dependence with respect to the school both as regards grades, student grants and loans and education, and therefore also as regards the scope to obtain employment in the future or to continue further education. [...] In the case of attendance monitoring, the students are in a position of dependence which results in a substantial imbalance. The Swedish Data Protection Authority therefore believes that consent cannot constitute a legal basis for the processing operations which this supervision regards”.*²⁷

In this case, the Swedish DPA fined the municipality 200 000 SEK (approximately 20 000 euros).

1.2. “Free”: Existence of alternative solutions

The “free” element of consent implies that there must be a genuine choice for the data subject with regard to accepting or declining the use of facial recognition for authorisation purposes. As a general rule, if the data subject does not have a genuine choice, feels obliged to give consent or risks being disadvantaged by not

²⁶ As we will see in a subsequent report, in this case the objective was not to authorise access to the school premises, but to monitor attendance of pupils within the school premises. Each time the students entered the classroom, they were recognized by a camera, which meant that the teacher did not have to make any notes about attendance.

²⁷ Swedish Data Protection Authority, [“Supervision pursuant to the General Data Protection Regulation \(EU\) 2016/679 – facial recognition used to monitor the attendance of students”](#), n°DI-2019-2221, August 20, 2019, at p. 4. Our translation.

giving consent, then the consent given cannot be considered as valid under the GDPR. As the EDPB explained:

*“In other words and notably when the biometric processing is used for authentication purpose, the data controller must offer an alternative solution that does not involve biometric processing – without restraints or additional cost for the data subject. This alternative solution is also needed for persons who do not meet the constraints of the biometric device (enrolment or reading of the biometric data impossible, disability situation making it difficult to use, etc.) and in anticipation of unavailability of the biometric device (such as a malfunction of the device), a “back-up solution” must be implemented to ensure continuity of the proposed service”.*²⁸

Data controllers appear to have taken this important requirement into account in practice. In **all** the cases that we have examined, data controllers went to great lengths in their implementation of FRT systems to convince the authorities that they have put in place adequate alternative solutions.

Non-biometric gates used for authentication purposes in the Molenbeek Stadium trial

The RWDM football club implemented an FRT trial during the 2019-2020 Belgian football season to authenticate season tickets holders as they approach the entrance gates. The purpose of this experiment was to create a ‘fast lane’ and to give season ticket holders easier and faster access to the stadium. The legal basis for the experiment was consent, so only volunteers had their biometric data processed. People who did not consent to the trial could access the stadium using other gates where there were no facial recognition devices. Season ticket holders could access the stadium using other gates, but they had to produce their tickets.

To our knowledge, today no case exists whereby an FRT system used for authorisation purposes in public spaces has been stopped due to the absence of adequate alternative solutions.²⁹ However, taking into consideration the fact that data controllers may wish to use FRT systems for authorisation purposes as a cheaper means of managing access than human control, one cannot ignore the risk that data controllers may in future neglect “alternative”, non-biometric, solutions. This is why, for instance, the French DPA has heavily insisted on the importance of such efficient alternative solutions as a condition for “free” consent:

²⁸ EDPB, [Guidelines 3/2019 on processing of personal data through video devices](#), January 29, 2020 p. 20.

²⁹ It is interesting to note, however, that in its [October 2018 Opinion concerning the “ALICEM” system involving online authentication](#) (see *supra*, note 3) the CNIL considered that “the creation of an ALICEM digital identity is subject to a facial recognition process without any other equivalent alternative being provided to enable the issue of a digital identity by this application” and, as a result, “consent to the processing of biometric data cannot be regarded as free and as therefore likely to lift the prohibition laid down in Article 9(1) of the GDPR”. However, in [a decision published on November 4, 2020](#), the Council of State, France’s highest administrative tribunal, rejected CNIL’s argument considering that there was, effectively, an alternative way to connect to the service without having to use facial recognition – and therefore consent was freely given.

The importance of an alternative non-biometric route in the case of the “MONA” trial in French airports

MONA is a facial recognition system, which is currently being tested at Lyon Saint-Exupéry Airport. The project aims to “make the passenger experience more fluid and secure”. The passengers who decide to opt in to MONA’s service can access a variety of services, and go through check in, security and boarding via those designated gates equipped with FRT. Having accepted consent as a legal basis, the French DPA (CNIL) stated:

“[E]ach experimental project clearly states that the biometric device is optional and that passengers can take a conventional route at any time. Moreover, even if they have given their consent, passengers can withdraw their consent and choose to take the alternative, non-biometric route at any stage of the journey. It must be remembered that this choice must not be hindered by any major inconvenience imposed on the passenger.”³⁰

1.3. Respect of the other requirements for valid consent

In all the cases that we have examined, data controllers tried to convince the authorities that the other GDPR requirements for valid consent were present.

- **“Informed”**. They insisted, for instance, that they had provided all the necessary information to users, and been sufficiently transparent, to make the consent “informed”, which implies that the person giving consent must fully understand what they are consenting to and for what purposes. However, compliance with this requirement has been challenged in the UK School Canteens case where critics argued that children could not “fully understand the implications” of the use of FRT and that “children, parents and guardians should be provided with nothing less than full information, couched in language children can easily understand”.³¹ Going beyond the issue of children, another consent-related issue concerns foreseeability. It could be difficult sometimes for subjects to know exactly what they are consenting to given the complexity of the technology and the eventual opacity of how data is managed. This applies to adults as well as children. In some of the cases that we have examined (for instance the Star Alliance Biometrics program) data controllers have tried to overcome these difficulties by providing very clear information and FAQs in their website.
- **“Specific”, “explicit” and “unambiguous”**. In a similar way, data controllers argued in all cases that the ways in which consent was given ensured that it was “specific”, “explicit” and “unambiguous”. In the case of the “MONA” trial, for instance, the French DPA noted that: “the

³⁰ CNIL, “[Communication présentée en séance plénière le 28 mai 2020 relative à la mise en œuvre d’expérimentations de dispositifs de reconnaissance faciale au sein de plusieurs aéroports aux fins de fluidification et de sécurisation du parcours passager](#)”, p. 14. Our translation.

³¹ LAU (P-L.), “Facial recognition in schools: here are the risks to children”, *The Conversation*, Online, October 27th, 2021, available at: <https://theconversation.com/facial-recognition-in-schools-here-are-the-risks-to-children-170341> (emphasis added), last accessed on March 30, 2022.

consent of each volunteer passenger will be collected at the time of enrolment by means of a box to be ticked before any data collection, in a way that is distinct from any other data processing (in the case of the project by Aéroports de Lyon, it will be distinguished from the consent obtained for the possible collection of geolocation data or for the sending of notifications)".³² The data controller in this case also specified that "the text associated with the box that has to be checked when creating a MONA account at a MONA kiosk at the airport or on the mobile application is "I accept facial recognition with MONA to make my journey easier" and that "the camera will not switch on if the passenger does not accept the terms".³³

- **Withdraw of consent.** Finally, in all the cases that we have examined the data controllers insisted that users could withdraw consent at any time without experiencing any adverse consequences.

2. The use of the "public interest" argument by public authorities

Another GDPR legal basis that has been put forward in the context of the use of FRT for authorisation purposes is that which appears in Article 9(2)(g) of the GDPR³⁴, according to which the prohibition of processing of biometric data shall not apply when:

"processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".

The "substantial public interest" exception could play an important role when the FRT system is deployed, especially when it is applied for access control purposes, by a public authority which, for one reason or another, does not wish to rely on "explicit consent" or when, due to the existence of an imbalance of power between the controller and the data subject, the conditions for explicit consent according to Article 9(2)(a) of the GDPR cannot be fulfilled.

Two important observations can be made in relation to this legal basis.

³² CNIL, "[Communication présentée en séance plénière le 28 mai 2020 relative à la mise en oeuvre d'expérimentations de dispositifs de reconnaissance faciale au sein de plusieurs aéroports aux fins de fluidification et de sécurisation du parcours passager](#)", pp. 13-14. Our translation.

³³ Annexe 2 of the Communication présentée en séance plénière le 28 mai 2020 relative à la mise en oeuvre d'expérimentations de dispositifs de reconnaissance faciale au sein de plusieurs aéroports aux fins de fluidification et de sécurisation du parcours passager". Our translation.

³⁴ For the relation between Articles 6(1)(e) and 9(2)(g) GDPR see *supra* notes 15 and 17.

2.1. Use of the “substantial public interest” exception requires a “Law”

As made clear by the text of Article 9(2)(g) of the GDPR, the “substantial public interest” exception *cannot* be used in relation to the use of FRT systems for authorisation (or other) purposes when there is no “law” authorising such use at the EU or the Member State level. Furthermore, according to Article 36(5) GDPR, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest. This is the case, for instance, in France, where the French DPA, CNIL, gave several successive opinions on the decrees authorizing the use of facial recognition for Automated Border Control (ABC) gates.

“PARAFE”: French Code of Internal Security authorises use of FRT for automated access control at French borders

PARAFE is a program used by the French Government to authenticate European passengers crossing the French borders at airports and stations, and involves automated processing of biometric data (fingerprints since 2007 and facial recognition since 2016). The use of FRT within this program has elicited a number of opinions from the French DPA, the CNIL, who have found that it complies with European and French data protection law. PARAFE finds its legal basis in the French Code of International Security and in diverse administrative acts. Articles 232-6 to 232-11 of the French Code of Internal Security (CSI), in the “regulatory section”, provides that:

Art. R. 232-6: *“The Minister of the Interior and the Minister in charge of Immigration are authorised to implement an automated system for processing personal data called “PARAFE” (rapid passage at external borders) and this is intended, for voluntary air, sea and rail travellers, to improve and facilitate police controls at external borders.*

The PARAFE system is open to adults and minors over the age of 12 who are citizens of the European Union or nationals of another State party to the Agreement on the European Economic Area or of the Swiss Confederation, or nationals of the United States, Andorra, Australia, the United Kingdom, Canada, South Korea, Japan, Monaco, New Zealand, San Marino and Singapore. To benefit from PARAFE processing, applicants must hold a travel document containing biometric data and equipped with a machine-readable zone...”³⁵

The implementation of the system has been authorised by successive decrees adopted by various French Prime Ministers since 2005. In 2016, a decree authorising the replacement of fingerprint analysis with facial recognition in relation to PARAFE was adopted. On this occasion, in an opinion published on January 2016 the French DPA acknowledged that while the draft decree indicated that the system would be used for a limited time, it provided a permanent legal basis for the processing of biometric data (face matching). More recently, in a deliberation adopted on November 2020, the DPA (CNIL) stated:

“The CNIL considers that the PARAFE processing operation, which is intended to facilitate police checks at external borders, falls within the scope of Regulation

³⁵ [Code de la Sécurité Intérieure](#). Our translation.

*(EU) 2016/679 of 27 April 2016 (hereinafter GDPR). Insofar as it is implemented on behalf of the State, acting in the exercise of its prerogatives as a public authority, and that it concerns biometric data necessary for the authentication or control of the identity of persons, its modification must be the subject of a decree by the Council of State, issued after the opinion of the CNIL...*³⁶

Belgian DPA on the need for “explicit” law

The Belgian DPA observed recently that “unlike several of our neighbours, the Belgian legislator has not opted for a general legal basis authorising the processing of biometric data in the context of the identification or unique authentication of a person for security purposes”. The DPA also noted, in an interesting way, that it:

“considers that a generally formulated legal obligation on the part of the controller to ‘take adequate security measures’ cannot be considered as a justification for the use of biometric data. Although ... the processing of biometric data for the identification or authentication of persons may be justified in certain cases, there must always be a legal provision (general or sectoral) that explicitly authorises the processing of biometric data, in view of Article 9(2)(g) of the GDPR”.

³⁷

2.2. Relationship between “consent” and a “voluntary” undertaking

As noted above, the PARAFE system which uses FRT for border controls in French airports, despite being based on the “substantial public interest” exception and being authorised by French Law, is only used by data subjects on a voluntary basis. The French Code of Internal Security clearly indicates that “The Minister of the Interior and the Minister in charge of Immigration are authorised to implement an automated system for processing personal data called “PARAFE” (rapid passage at external borders) and this is intended, **for voluntary air, sea and rail travellers**, to improve and facilitate police controls at external borders”.³⁸ Eligible passengers can indeed choose in an entirely voluntary way to be assessed in the traditional way by police officers at the border or to pass through the biometric authorisation gates.

This raises the interesting question of the difference between a “voluntary” FRT authorisation system based on “substantial public interest”, and an equivalent authorisation system based on “explicit consent” (such as all the others that we have analysed previously in our report). As a matter of fact, despite the fact that in both cases, use of the FRT authorisation system depends on the data subject exercising their free will, there at least two fundamental differences.

³⁶ CNIL, [“Délibération n°2020-114 du 26 novembre 2020 portant avis sur un projet de décret portant diverses dispositions relatives au traitement automatisé de données à caractère personnel dénommé PARAFE \(demande d’avis n°20010013\)”](#), December 30, 2020. Our translation.

³⁷ Autorité de protection des données, [“Recommandation relative au traitement de données biométriques”](#), December 1st, 2021, p. 26. Our translation.

³⁸ Art. R. 232-6, emphasis added. Our translation.

First, a “voluntary” (but not “consensual”) system such as PARAFE, does not require data controllers to obtain the “explicit consent” of the data subjects or to meet all the other formal and substantive requirements of consent. In other words, the data controller is under no obligation to demonstrate that the choice of a passenger to use the PARAFE authentication system is based on a “freely given”, “specific”, “informed”, “explicit” and “unambiguous” consent.

Second, the fact that a system such as PARAFE is based on Member State law (that can be modified using the procedure that the French DPA has indicated), means that the French Government could theoretically, at any time, amend this legal basis in order to render the PARAFE system compulsory for eligible passengers. While the removal of the “voluntary” basis would undoubtedly be something to take into consideration when conducting the necessity and proportionality assessment, the “substantial public interest” exception definitely and theoretically authorises use of an FRT authentication system that would be mandatory for all data subjects concerned.

II. NECESSITY AND PROPORTIONALITY

Neither the existence of consent nor the introduction of a legal provision enabling a reliance on the “substantial public interest” exception relieve the data controller of his obligation to demonstrate the necessity and proportionality of the data processing. Indeed, the necessity and proportionality tests are absolutely essential for all FRT deployments.

In this section we will present some key takeaways about the practice of using facial recognition for authorisation purposes. We will start with some general considerations about the “balancing act” that a data controller must undertake before such use **(1)**. We will then focus on the more specific criterion of “less intrusive means” **(2)**.

1. A balancing act that includes several components

The necessity and proportionality test is an essential but complex operation that must precede any FRT deployment. It involves taking into consideration a series of parameters. The question whether facial recognition is a strong means of authentication is one of them.

Disagreements between European DPAs about whether facial recognition is as a strong means of authentication or not!

In an Opinion on the processing of biometric data for the authentication of persons (A/2008/017) published in 2008 the Belgian DPA stressed that the data controller could cite the advantage of using the biometric system for security, in addition to other advantages such as cost reduction or ease of use:

“[T]he specific advantage of using a biometric system is certainly the improved security in many cases. Indeed, the biometric system is considered to be a strong means of authentication”.

Indeed, the Belgian DPA referred to the definition of authentication provided by ISO according to which: “Strong authentication is either based on strong mechanisms (e.g. biometrics) or makes use of at least two (...) factors (so-called multi-factor authentication)”. (ISO/IEC 18028-4: 2005).³⁹

However, in a 2020 joint Opinion, the Spanish DPA, AEPD, as well as the European Data Protection Supervisor (EDPS), seem to challenge this. They argued that the statement “biometric authentication is strong” is one of... “14 misunderstandings with regard to biometric data”.

They explained:

³⁹ Autorité de protection des données, “[Avis d’initiative relatif aux traitements de données biométriques dans le cadre de l’authentification de personnes \(A/2008/017\)](#)”, April 9, 2008, §43. Our translation.

“By definition, using only biometric data is a weak authentication process, while using an access card and a password is strong. Although biometric authentication often requires a previous process of enrolment or identification in which, for example, in facial recognition, it is necessary to compare with the photo in the ID, if, after the identification process, the authentication process is only biometric, it remains a weak system”.⁴⁰

Fifteen scholars published a response to this joint AEPD/EDPS paper and they... challenged the previous statement, arguing among other things:

“Both knowledge-based and token-based authentication factors have the intrinsic disadvantage that any given security policy can be violated, when the knowledge or the token is forwarded to an unauthorised data subject. On the contrary, biometrics is the only authentication scheme that can establish a secure and unique link between the data subject and the enrolment record”.⁴¹

Despite the divergences on these issues, agreement exists between European DPAs that any advantages for the data controller need to be balanced with other important interests.

Belgian DPA guidelines on how to navigate the balancing act

In its Recommendations on the processing of biometric data published on December 2021 the Belgian DPA stated the following on how the data controller should proceed with the “balancing” act:

“It will always be necessary to balance the (important) interests pursued against the risks for the rights and freedoms of the data subjects. This can be done, for example, by checking how the proposed processing operation affects society, both 'in depth' (the extent of the benefit or harm experienced as a result of the processing operation) and 'in breadth' (the number of people who receive a benefit or harm)”.

The Belgian DPA gave the example of a shoe shop which was [condemned by an Amsterdam court](#) on 12 August 2019 for requiring from employees to use a checkout system that involved a biometric authorisation (fingerprint scan). The shop concerned argued that this was permitted under Article 9(2.g) of the GDPR, as the use of a fingerprint scan authorisation system was necessary for securing sensitive information, namely financial information and the personal data of both employees and customers. Furthermore, such a system was supposed to prevent fraud in relation to cash registers. The judge rejected these arguments considering that the use of biometric authentication in this case did not pass the proportionality test. The Belgian DPA explained that:

“[I]n the above example, we are dealing with a relatively large harm (the mandatory use of fingerprints) for a (proportionately) large group of affected persons (all employees of the shoe shop) that is not proportionate to the benefit perceived by one person (the owner of the shop). Compare this to the use of biometric authentication to grant access to the premises of a nuclear power plant. The perceived harm to the employees (proportionally a relatively small group of people involved) does not outweigh the benefit to the general population (the security of a critical infrastructure)”.

⁴⁰ AEPD/EDPS Joint Paper, “[14 Misunderstandings with regard to Biometric Data](#)”, June 2020.

⁴¹ Busch et al., “[A response to the European Data Protection Supervisor 'Misunderstandings in Biometrics' by the European Association for Biometrics](#)”, IET Biometrics, May 2021, p. 81.

The Belgian DPA added that:

*“[T]he controller must always consider whether the processing activities he or she envisages are (1) appropriate (is the measure relevant for the achievement of the purposes?), (2) necessary (is the measure necessary for the achievement of the purposes?) and (3) not excessive (does the measure go beyond what is necessary for the achievement of the purposes)”.*⁴²

It is also important to note that in all the cases that we have examined it is very clear that respect for GDPR data processing principles is not only considered an autonomous requirement in addition to the necessity and proportionality test, but also a part of this test.

Link between the proportionality test and the GDPR data processing principles

In its Opinion of December 2021 the Belgian DPA unambiguously formulated the link between proportionality and data processing principles. It stressed that:

*“[T]he mandatory proportionality test is part of the compliance with the obligations imposed by the GDPR. Only when the controller can effectively demonstrate that all data protection principles have been respected can we speak of lawful and therefore proportionate data processing”.*⁴³

For instance, respect for data minimisation, purpose or storage limitation are not only considered as conditions per se imposed by the GDPR for any lawful use of facial recognition for authorisation (or other) purposes, but also as part of the proportionality assessment. We will discuss below in Part III the “traditional” position of the Belgian (and other) DPAs in Europe according to which it is important, for this proportionality assessment, “not to use biometric systems that store biometric reference data in a database”⁴⁴ – and how this criterion fits in with the new practices in several European airports.

Do not process the data of people who have not consented to it

The fundamental importance of respecting data processing principles with regard to using FRT for authorisation purposes can also be seen when one examines how European DPAs have insisted that techniques be used that guarantee that people who *have not consented* to the use of FRT will not have their biometric data processed.

The EDPB, for instance, stressed in 2020 that:

“The check points with facial recognition need to be clearly separated, e. g. the system must be installed within a gantry so that the biometric templates of non-consenting persons will not be captured. Only the passengers, who will have

⁴² Autorité de protection des données, [“Recommandation relative au traitement de données biométriques”](#), December 1st, 2021, at 27 and 31. Our translation.

⁴³ Ibid.

⁴⁴ Autorité de protection des données, [“Avis d’initiative relatif aux traitements de données biométriques dans le cadre de l’authentification de personnes \(A/2008/017\)”](#), April 9, 2008, p.14. Our translation.

previously given their consent and proceeded with their enrolment, will use the gantry equipped with the biometric system”.⁴⁵

Similarly, in terms of the commercial use of facial recognition by airports and airlines in France (the continuation of the MONA pilot project) the French DPA emphasised that:

“Technical and organisational measures must also be implemented to ensure that the facial recognition device only processes the data of persons who have given their prior consent, for example facial recognition cameras only activating after the passenger concerned has taken a particular action, a technical configuration that blurs the faces of passengers in the background, display panels and floor markings that distinguish facial recognition control areas from conventional control areas, etc”.⁴⁶

2. “Less Intrusive Means”

One of the main elements in the assessment of whether an FRT system deployed for authorisation purposes meets the necessity and proportionality requirements is whether less intrusive means exist to accomplish the same objectives. Indeed, Recital 39 of the GDPR states that:

“Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means”.

Several DPAs across Europe have emphasised the fundamental importance of the “less intrusive means” assessment when it comes to the processing of biometric data, which are considered to be particularly sensitive as far as European data protection law is concerned.

The Belgian DPA on “less intrusive means”

In 2008, the Belgian DPA had already stated the following with regard to the use of biometrics for authorisation purposes:

“The data controller must therefore make a concrete balance of the different processing systems available to him in order to obtain the desired result and favour those that are more respectful of privacy and generally accepted by civil society. The controller should therefore make a comparison of the different authentication systems and check whether the same result could not be obtained with a less privacy-intrusive system, such as visual recognition (comparison with the photo on a card or badge).

Biometrics is a strong means of authentication and should be reserved for situations requiring this level of security”.⁴⁷

⁴⁵ EDPB, [Guidelines 3/2019 on processing of personal data through video devices](#), January 29, 2020, at 20.

⁴⁶ CNIL, [“Reconnaissance faciale dans les aéroports : quels enjeux et quels grands principes à respecter?”](#), October 9, 2020. Our translation.

⁴⁷ Autorité de protection des données, [“Avis d’initiative relatif aux traitements de données biométriques dans le cadre de l’authentification de personnes \(A/2008/017\)”](#), April 9, 2008, §68-69. Our translation

The French DPA on the need to “demonstrate the inadequacy of other, less intrusive security means”

In a general position on biometrics published in 2019 the French CNIL seemed to suggest that there is a “strict necessity” requirement:

“The principles of the legitimacy of the aims pursued and the strict necessity of implementing such biometric processing are indeed indispensable requirements. Facial recognition cannot be lawfully used – even on an experimental basis – unless it is grounded in a specific requirement to ensure a high level of reliability in the authentication or identification of data subjects and without demonstrating the inadequacy of other, less intrusive security means”.⁴⁸

In a subsequent opinion on the use of FRT for authorisation purposes in French airports, issued in 2020, the CNIL put emphasis on:

“[T]he general principle that the processing of data must be proportionate, in terms of its impact on the rights and freedoms of individuals, to the purpose for which it is being carried out and must only involve data that is ‘necessary’ to achieve that purpose”.⁴⁹

We will discuss later the application of the “strict necessity” requirement in cases involving the commercial use of FRT by airlines and airports in order to offer dematerialized and contactless travel to passengers.

Interestingly, the “less intrusive means” test has in some rare cases led DPAs to consider that the implementation of certain specific authentication techniques using FRT for authorisation purposes can be less intrusive than other means that have previously been used.

When Facial Recognition is less intrusive than previous authentication techniques

In 2003 the EDPB’s predecessor had already stated that:

“For access control purposes (authentication/verification), the Working Party is of the opinion that biometric systems related to physical characteristics which do not leave traces [...] create less risks for the protection of fundamental rights and freedoms of individuals”.⁵⁰

The Belgian DPA endorsed this position in an opinion published in 2008 stating that:

“It should be noted that privacy risks may vary depending on the type of biometric data used. For example, biometric systems referring to physical features that do not leave traces create less privacy risks than systems using physical features that leave traces”.⁵¹

During its assessment of the evolution of the PARAFE border control system in France, the French DPA concluded that the introduction of facial

⁴⁸ CNIL, “[Facial Recognition: For a Debate Living up to the Challenges](#)”, November 15, 2019.

⁴⁹ CNIL, “[Communication présentée en séance plénière relative à la mise en oeuvre d’expérimentations de dispositifs de reconnaissance faciale au sein de plusieurs aéroports aux fins de fluidification et de sécurisation du parcours passager](#)”, May 28, 2020, p. 13. Our translation.

⁵⁰ [Article 29 Working Party Biometrics Working Paper, WG80](#), adopted August 1, 2003, p. 6.

⁵¹ Autorité de protection des données, “[Avis d’initiative relatif aux traitements de données biométriques dans le cadre de l’authentification de personnes \(A/2008/017\)](#)”, April 9, 2008, §48. Our translation.

recognition based on a 1-1 comparison between the image captured at the eGate and the photo of the user in his/her biometric passport, was an improvement on, and a “less intrusive means” than, the previous fingerprint recognition-based technique that involved using a centralised database. The CNIL noted that the use of FRT reduces the risks of infringements with regard to personal data and individual freedoms:

*“The Commission takes note of the abolition of the enrolment process and thus welcomes the fact that the corresponding central database containing fingerprints was completely purged by April 2, 2020. Indeed, as the Commission has pointed out in numerous deliberations and in particular in its previous opinions on the conditions for implementing this processing and on the substantial guarantees that must surround the “PARAFE” system in order to ensure a high level of protection for the data subjects, **the processing of biometric data such as fingerprints in an automated and centralised form, generates more risks from the point of view of personal data protection**, taking into account the characteristics of the physical identification element retained, the possible uses of such processing and the resulting risks of serious infringements of privacy and individual freedoms.”⁵².*

Even when other, less intrusive means of authentication exist, DPAs seem to agree to the use of facial recognition when the controls are necessary for security, the FRT provides a significant improvement and its use is surrounded by “substantial guarantees”. This is especially the case when facial recognition is used in “e-Gates” for automated border police controls in European international airports, as shown by the positions of the French DPA concerning the PARAFE system being used in France.

Acceptance of use of biometrics for pre-existing police access controls if there are “substantial guarantees” that ensure a high level of data protection

In its first opinion of 2007, concerning the use of biometrics (which was produced via fingerprint recognition at that time) in French airports, the French DPA found that the system met the proportionality test, based on the following reasoning:

“While each of the purposes assigned to PARAFE processing - to improve border police control of air travellers and to facilitate rapid passage through the external borders of the States party to the Schengen Convention - is legitimate, the commission notes that the main objective is indeed to speed up border crossing, on a voluntary basis, for “certain passengers who present little risk from the point of view of security”, as the report to the Prime Minister accompanying the draft decree states, with a view to greater comfort for the travellers concerned, a better image of the airports and the attractiveness of France in international business relations. This should also result in productivity gains for the border police. [...] [T]he commission considers that such a system, based on voluntary participation, concerning a limited number of people and implemented in particular to improve the comfort of passengers by speeding up border controls, is the appropriate framework for implementing techniques for recognising the identity of individuals that are more

⁵² CNIL, [“Délibération no 2020-114 du 26 novembre 2020 portant avis sur un projet de décret portant diverses dispositions relatives au traitement automatisé de données à caractère personnel dénommé PARAFE \(demande d’avis no 20010013\)”](#), (Our translation, emphasis added).

protective of personal data than the establishment of a centralised database of fingerprints”⁵³.

The evolution of PARAFE to incorporate facial recognition technology for authentication purposes, was approved by the CNIL in an Opinion released on April 8, 2016, taking into account the following considerations:

“[T]he commission considers that the implementation, on behalf of the State, of a facial recognition system for the purpose of authenticating travellers and facilitating police checks at external borders must be surrounded by substantial guarantees to ensure a high level of data protection for the persons concerned. In this respect, it notes that the planned system is surrounded by the following guarantees.

Firstly, the commission notes that the operation of this new system, which aims to compare the photograph contained in the biometric passport chip with several facial images taken within the airlock, will not require the creation of a central database. The images taken in the airlock and the portrait read from the contactless component of the passport will not be stored in the processing.

This system is thus in line with the Commission's constant position on the matter, which considers that the use of biometric recognition systems based on the storage of data in a medium for the exclusive use of the person, such as a biometric passport, to verify the identity of a person, is likely to ensure better protection of the privacy of individuals than the creation of a central database.

Secondly, this functionality will be based, like the other biometric devices currently implemented in PARAFE, on the voluntary participation of travellers. Travellers will therefore have the choice between passing through the traditional booths and passing through the PARAFE airlocks.”⁵⁴

The respect of data processing principles and the existence of such “substantial guarantees” to ensure a high level of data protection, occupies such an important place in the proportionality assessment of some European DPAs that they seem to be ready to accept the use of FRT for authorisation purposes even in circumstances where, clearly, less intrusive means exist (and were the only means used in the past). For instance, despite their strong above-mentioned general statements on the matter, both the French and the Belgian DPAs seem to accept that a need for “comfort” could sometimes meet the necessity criterion if the implementation of FRT for commercial purposes respects all of the data processing principles.

Less intrusive means and a need for “comfort”

As we have seen earlier, the Belgian DPA has adopted strong positions on the importance of the “less intrusive means” criterion for the necessity/proportionality assessment, clearly stating that:

⁵³ CNIL, “Délibération no 2007-094 du 3 mai 2007 portant avis sur un projet de décret portant création d'un traitement automatisé de données à caractère personnel relatives à des passagers des aéroports français franchissant les frontières extérieures des Etats parties à la convention signée à Schengen le 19 juin 1990 (demande d'avis no 1205636)”, *op. cit.* Our translation.

⁵⁴ CNIL, “[Délibération n° 2016-012 du 28 janvier 2016 portant avis sur un projet de décret portant modification d'un traitement automatisé de données à caractère personnel dénommé PARAFE](#)”, April 8, 2016. In its deliberation No. 2019-028 of March 14, 2019 on a draft decree extending PARAFE to British nationals, the Commission recalled that it considers “*the use of biometric recognition devices to verify a person's identity to be legitimate, as long as the biometric data are stored on a medium for the exclusive use of the person, as is the case for the biometric passport.*” Our translations.

*“it must be checked whether there are less radical solutions (the processing of biometric data should always be the final solution)”.*⁵⁵

However, the very same DPA did not oppose Racing White Daring Molenbeek’s FRT trial during the 2019-2020 Belgian football season which consisted of using FRT to identify season ticket holders as they approached the entrance gates. The purpose of this experiment was to create a ‘fast lane’ and to make season ticket holders’ access to the stadium easier and faster. The arguments of the data controller, that the system was based on consent, was designed to be “privacy compliant and reliable” and that introducing FRT, to replace the previous traditional ticket management system, “*will save precious minutes, for example, when you arrive just before kick-off*”⁵⁶, were deemed sufficient reasons not to oppose the trial. However, it must be emphasised that this was just a trial that was intended to test the system, and the Belgian DPA has not published, to our knowledge, any specific opinion concerning the use of FRT for authorisation purposes in similar contexts in stadiums in Belgium.

Similarly, the French DPA agreed to a trial of the “MONA” FR system in French airports, which aims to dematerialize documentary and identity checks (at check in, baggage drop-off, security and boarding) by means of a facial recognition system. Here also it was evident that “less intrusive means” (the traditional controls used in the past) existed. However, the data controllers argued that the introduction of the FRT authorisation system would be quicker, would “improve the customer experience” and would “increase the level of security through a more reliable identification of passengers”. The French DPA seemed to accept the idea that a mere need for “comfort” would meet the necessity test as long as the necessary safeguards in terms of data processing were in place, the system was based on consent and alternative solutions existed. It stated the following:

“Generally speaking, the use of biometric devices to meet these purposes raises questions about their necessity and proportionality. The necessity criterion must be assessed with particular vigilance in the case of biometric data processing, which is particularly intrusive and involves sensitive data, especially when it is conducted via facial recognition. [...]

[W]hile the Commission has always considered that, in order to be implemented, biometric data processing must meet a specific need, it has never made an assessment of what this ‘specific need’ should be. Thus, biometric devices that meet a specific need, even if it is similar to a need for ‘comfort’, and that are based on the consent of the data subjects, appear to meet the necessity criterion.

The Commission was able to rule in favor of the PARAFE facial recognition system, which was designed solely to facilitate traffic flow.

*While the need for these systems in principle cannot be questioned, particularly insofar as they are based on the participation of willing and consenting passengers, the need for their deployment at certain stages of the airport journey appears more problematic”*⁵⁷.

The French DPA therefore agreed to the use of MONA on an experimental basis – while rejecting some of its applications (see our focus on “The Case of the Traveler’s Lounge” below). Furthermore, a thorough analysis of the

⁵⁵ Autorité de protection des données, [“Recommandation relative au traitement de données biométriques”](#), December 1st, 2021, p. 31. Our translation.

⁵⁶ SCHMITZ (B.), [“Le RWDM comme laboratoire pour une technologie de reconnaissance faciale”](#), RTBF, September 5th, 2018. Our translation.

⁵⁷ CNIL, [“Communication présentée en séance plénière le 28 mai 2020 relative à la mise en oeuvre d’expérimentations de dispositifs de reconnaissance faciale au sein de plusieurs aéroports aux fins de fluidification et de sécurisation du parcours passager”](#), May 28, 2020, p. 12-13. Our translation.

current DPA positions on the permanent use of MONA seem to indicate that the CNIL has not yet opposed the use of the system *as such* or the need for “comfort” it tries to serve, but rather the *modalities* of its deployment in relation to certain important data processing principles – in particular, data minimisation and storage limitation. We will discuss this issue extensively below in Section 3, where we will also see that similar FRT systems seem to have been deployed in Spain (see our “AENA case”) and in Germany (through the “Star Alliance Biometrics” program) without any known opposition by the relevant DPAs.

At the other side of the spectrum, DPAs and Courts around Europe have found that in certain specific cases and contexts, the necessity and proportionality test could not be passed when FRT has been introduced for authorisation purposes. This has especially been the case when facial recognition has been used for authorisation purposes in schools.

**“Certain uses are forbidden in our society”.
Facial recognition for authorisation in schools and the “less
intrusive means” requirement**

As mentioned earlier, (I (1.1)) projects intended to introduce facial recognition to schools in France, the UK and Sweden have repeatedly been considered illegal because of the lack of a valid legal basis, and more specifically because of the impossibility of being able to rely on consent due to the imbalance of power between the data controllers (schools) and the children under their authority. However, Courts and DPAs in these cases have also used the additional argument that the use of FRT for authorisation purposes was disproportionate.

In the French PACA high school case, discussed above, which concerned an FRT trial that aimed to ensure access control of students by biometric means, the French DPA stated the following:

*“the objectives of security and the fluidity of entry to these schools can be achieved by means that are much less intrusive in terms of privacy and individual freedoms, such as control by badge. The Commission recalled that the processing of biometric data is a particularly sensitive issue, justifying enhanced protection for individuals. In particular, facial recognition devices are particularly intrusive and present major risks of infringement of the privacy and personal freedoms of the persons concerned. They are also likely to create a feeling of increased surveillance. [...] In this context, and in the presence of alternative, less intrusive means, such as badge control, the use of a facial recognition device to control access to a school appears disproportionate”.*⁵⁸

In another, more general opinion on facial recognition, published two weeks later, the French DPA described its position in even stronger terms and talked about using FRT in ways that are “forbidden in our society”:

“The CNIL has also already pointed out that certain uses are forbidden in our society. It has recently made this clear with regard to implementing facial recognition authentication systems for children for the purpose of controlling access to schools – when the aims of securing and facilitating entry to schools can be

⁵⁸ CNIL, [“Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position”](#), October 29th 2019. Our translation.

*achieved by equally effective but much less intrusive means in terms of privacy and individual freedoms, taking into account the special protection that children must be afforded”.*⁵⁹

In its decision of February 27, 2020 concerning the PACA Schools case, the Administrative Court of Marseille stressed the need to strictly assess the proportionality of the processing and followed the CNIL’s interpretation of the “less intrusive means” requirement. The Court considered that the PACA Region had not demonstrated why access control using a badge/ID card, possibly coupled with video surveillance, was insufficient to achieve the purposes of the processing operation (access control). It concluded that the FRT trial undertaken by the Region violated Article 9 of the GDPR and could not be justified by the exceptions announced in para. 2 of this Article.⁶⁰

In contrast with these developments in France, the UK DPA did not issue an official opinion or talk about “prohibition” in relation to the “UK School Canteens” case discussed above. However, an ICO spokesperson echoed its French counterpart in insisting that organisations which use facial recognition technology must comply with data protection law including the principles of necessity and proportionality and the “less intrusive means” requirement. As the ICO spokesperson declared:

*“Data protection law provides additional protections for children, and organisations need to carefully consider the necessity and proportionality of collecting biometric data before they do so. Organisations should consider using a different approach if the same goal can be achieved in a less intrusive manner. We are aware of the [case], and will be making inquiries with North Ayrshire council”.*⁶¹

However, this was not necessary as North Ayrshire Council put an end to this trial.

Another argument often put forward by DPAs is the risk of a “slippery slope”⁶² and, more specifically, of “normalizing” the use of FRT and creating a “phenomenon of habituation” by introducing biometric authentication or identification in situations where, clearly, there is no need for it. The “case of the traveler’s lounge” in French airports is emblematic of this.

⁵⁹ CNIL, “[Facial Recognition: For a Debate Living up to the Challenges](#)”, December 19, 2019. Emphasis by the CNIL.

⁶⁰ See CHRISTAKIS (T.), “[First Ever Decision of a French Court Applying GDPR to Facial Recognition](#)”, *AI-Regulation.com*, February 27, 2020.

⁶¹ WEALE (S.), “ICO to step in after schools use facial recognition to speed up lunch queue”, *The Guardian*, Online, October 18, 2021, available at : <https://www.theguardian.com/education/2021/oct/18/privacy-fears-as-schools-use-facial-recognition-to-speed-up-lunch-queue-ayrshire-technology-payments-uk>, last accessed on March 30, 2022.

⁶² In the case of the UK School Canteens case, critics said that they were “sceptical about the benefits that implementing facial recognition in schools could bring” and believed that “the ulterior motive behind it is financial”. “Tech companies want to make more money”, said Paul Bernal, professor of information technology at the University of East Anglia. “Then they have a foot in the door, and can sell the same tech to more places, and apply it to more situations. It’s a classic ‘slippery slope’”. He added that: “there are many ways to deal with serving school meals that can bypass the ‘queues at the till’ problem without the need for facial recognition. These could include having children paying for their meals in advance. Use a payment model that isn’t item-by-item, but meal by meal, and there’s no need for tech”, he concluded. LAGO (C.), “[Facial recognition in schools is here: Are we ready for it?](#)”, *Tech Monitor*, Online, October 18, 2021.

Avoiding a “slippery slope” and the phenomenon of habituation: The case of the traveler’s lounge

The Belgian DPA noted in December 2021 that even *“if the proportionality of authentication with a biometric system is established, the application of such a system should be limited to those areas/services that justify these particular measures”*.⁶³

The French DPA, CNIL, seemed to follow exactly the same logic in its assessment of the “MONA” trial in French airports. While the CNIL accepted in principle the legality and proportionality of this experimental system, which aimed to “make the passenger experience more fluid and secure”, it considered that its extension to the airports’ VIP Lounge was disproportionate. As the CNIL explained:

“One of the novelties presented by the experimental projects planned at Lyon Airports and [...] is the extension of the scope of facial recognition solutions to the entrance of the traveler’s lounge. The purpose of the biometric devices implemented in this area of the airport is always claimed to be to improve the flow and experience of travelers. [...] “However, access to a passenger lounge does not seem to have the same requirements for managing passenger flows as other control points in an airport. The collection and processing of biometric data to control access therefore appears excessive in relation to the purposes, which are based more on improving the passenger’s experience”. [...]

In this case, the processing of particularly sensitive biometric data for the sole purpose of facilitating access to a passenger lounge does not appear proportionate.

Thus, the processing of biometric data at the level of the passenger lounge, even if it were implemented only for consenting passengers, does not seem to meet the principles of necessity and proportionality set forth by the GDPR. Indeed, less intrusive means, such as automated kiosks, seem perfectly capable of meeting the objectives of simplification and fluidity sought. Moreover, the implementation of a dematerialized identification process at each stage of the passenger’s journey through the airport, including optional or comfort stages, would lead to increased traceability of the passenger’s comings and goings, creating a phenomenon of habituation, which has certainly been accepted, but which carries risks for rights and freedoms on a larger scale”.⁶⁴

To conclude, while the French DPA considers that the use of FRT for authorisation purposes to access the passenger lounge is disproportionate, due to the above-mentioned arguments, it is interesting to note that the **Germany**-based company Star Alliance, which produces a system that is almost identical to MONA (Star Alliance Biometrics), has announced on its website that:

“in the near future the range of process points will be gradually expanded – for example to [...] lounge access”.⁶⁵

Despite our efforts we have not found any positions of German DPAs concerning this project.

⁶³ Autorité de protection des données, [“Recommandation relative au traitement de données biométriques”](#), December 1st, 2021, at 32. Our translation.

⁶⁴ CNIL, [“Communication présentée en séance plénière le 28 mai 2020 relative à la mise en oeuvre d’expérimentations de dispositifs de reconnaissance faciale au sein de plusieurs aéroports aux fins de fluidification et de sécurisation du parcours passager”](#), May 28, 2020. Our translation.

⁶⁵ See [What is Star Alliance Biometrics?](#).

This last observation shows that, despite the existence of GDPR rules and an impressive corpus of opinions and interpretative work by European DPAs, there exists a risk of divergence with regard to the assessment of the necessity and proportionality vis-à-vis the deployment of FRT for authorisation purposes. In the following section we will focus specifically on one of the areas where divergence could appear in the future and discuss the ways in which a harmonized interpretation could be achieved concerning these issues in Europe.

III. RISK OF DIVERGENCE: DIFFERENT ASSESSMENTS OF THE “ONE ID” CONCEPT FOR AIR TRAVEL?

The interpretation of elements such as the necessity and the proportionality principles, the “less intrusive means” test, or the question of how exactly data processing principles should apply in the field of FRT for authorisation purposes, leave a lot of room for different interpretations – especially when one takes into consideration the industrial and financial interests at stake. This, in turn, creates the risk of divergent interpretations of the GDPR by European DPAs and therefore of different approaches on very similar issues in European States. We will try to illustrate this problem by focusing on an important issue that was analysed during our research, namely the use of facial recognition for authorisation purposes by airlines and airports across Europe to offer “seamless and contactless” travel to those passengers who opt into such programs.

Tech-driven changes based on biometrics are coming “fast and furiously to airports”.⁶⁶ Within an airport, facial recognition can be used to automate the various control stages (such as check-in, baggage drop-off, security or boarding) by replacing the control of travel and identity documents, with the aim of making the traveller’s journey more fluid and improving his or her experience by reducing waiting times. We are currently observing widespread use of biometric facial recognition devices in airports around the world. According to the “[Air Transport IT Insights 2021](#)” report by the international aeronautical telecommunication company (SITA), 22% of airlines and 24% of airports have already implemented self-boarding gates using biometrics only, and 62% plan to do so by 2024. According to the same report, self-boarding and biometrics remain a fundamental part of future airline strategy around passenger identity management and a key focus for airports hoping to provide a faster, touchless journey through the airport, with the majority of airport CIOs planning to invest in biometric identity management solutions for passengers. Indeed, investment in such biometrics-based authorisation solutions is constantly increasing; airlines and airports around the world argue that improving the security and travel experience is essential as passenger numbers are set to double by 2034, according to the International Air Transport Association (IATA).

As we will see, in Europe several airlines and airports have implemented such biometrics-based authorisation solutions, either on an experimental basis or on what seems to be a permanent basis (for instance Spain and Germany).⁶⁷ In practice, in all these systems, the photograph of the passenger’s face on his or her identity document is compared via facial recognition with the facial image captured during the passenger’s passage through the airport’s checkpoints. Despite data controllers’ claims that these new applications and biometric

⁶⁶ Elaine Glusac, “[Your Face Is, or Will Be, Your Boarding Pass](#)”, New York Times, December 7, 2021.

⁶⁷ For other examples see *infra* footnotes 89-93.

systems are based on “privacy by design” and “privacy by default” principles,⁶⁸ important questions seem to remain unsolved and some divergences seem to exist between European DPAs on this topic – which raises the question of how to eventually achieve harmonization in Europe on these important issues.

In this section we will present the different issues in turn, using the IATA’s “One ID” Concept for Air Travel as a starting point.

1. IATA: The “One ID” Concept

The International Air Transport Association initiated development in this field by introducing, a few years ago, its “One ID” Concept, the objective of which is to bring about, through the introduction of facial recognition, a “seamless” and “efficient” passenger experience while at the same time improving border, aviation and airport infrastructure security. This is how IATA describes the “One ID” Concept and its “benefits”:

The “One ID” Concept’s Objectives

In a “Fact Sheet” published in November 2020, the IATA starts by explaining that:

“Over the past decade, limited airport physical infrastructure and enhanced security requirements have resulted in a complicated and at times unpleasant passenger experience. Individual stakeholders, such as airlines, border control, customs and screening authorities, have designed their processes around their own obligations and requirements, with little or no coordination between them. This has resulted in repetitive processes for the passenger, such as having to present travel tokens (boarding passes, passports, etc.) to many different stakeholders for different purposes across the end-to-end passenger experience. This is inefficient and not sustainable in the long-term”.

The IATA adds that:

“The 2020 Covid-19 pandemic and industry crisis has shown the urgent need to provide a contactless safe and seamless airport experience to passengers. One ID aims to contribute to the industry re-start and to provide a passenger-centric experience”.

The IATA then explains that its vision is:

“to lead the industry in delivering an end-to-end passenger experience that is secure, seamless and efficient. One ID seeks to introduce a collaborative identity management solution that spans all process steps and stakeholders in the end-to-end journey, from booking to arrival at destination and back, putting the passenger at the center. One ID will remove the repetitive processes of passengers having to present different travel tokens to many different stakeholders for different purposes across the end-to-end passenger experience.

The concept relies on early validation of the passengers’ identity, and controlled access to this information by the various public and private stakeholders on an authorized-to-know basis. This is done so that the passenger can be recognized and attended to in the most efficient way in subsequent process steps.

The concept involves the use of a trusted, digital identity, biometric recognition technology and a collaborative identity management platform. It will be supported by the development of a trust framework among the different stakeholders”.

⁶⁸ See for instance IATA, “[One ID. FAQs on PRIVACY](#)”, September 2019.

The “benefits” of One ID are described by the IATA as follows:

“Seamless”- improved passenger experience

- Elimination of repetitive processes and possible combination and reduction in the number of touchpoints, and thus shorter queues and reduced waiting times
- Ultimately, enable passengers to arrive at the airport ready to fly in nearly every travel scenario
- Translates into commercial opportunities for the industry
- It supports **contactless** process by limiting physical interaction with people and equipment and minimizing exchange of documents.

“Efficient” - improved productivity, capacity and cost savings

- Staffing efficiencies and increased capacity by reducing time spent on manual ID checks
- Improved space efficiency and opportunities to mitigate additional investment in airport infrastructure
- Improved real-time visibility of where passengers are in the airport process, possibly efficiently directing passengers to the appropriate process

“Secure” - improvements in border, aviation and airport infrastructure security

- Reduce possibilities for individuals to cross borders under a false identity, and thus help combat human trafficking and other cross-border criminal activities
- Contribute to elimination of queues and crowds in airport landside areas
- Enable possibility of risk-based assessment and differentiated handling at border and security checkpoints”.⁶⁹

The IATA’s ultimate objectives go even further. As the IATA explained:

“Ultimately, we expect to see the use of a digital identity allowing an individual to assert their identity, online or in person, to the required level and throughout the end-to-end process, entirely replacing the use of a physical passport.”⁷⁰

According to the IATA, passengers will benefit in a number of ways when one takes into account their current experience.

Improvements for Passengers According to the IATA

The following table,⁷¹ published by the IATA, describes how the “One ID” Concept fundamentally differs from the legacy process:

	Description	Legacy process	One ID
Ready to fly ¹	<ul style="list-style-type: none"> • Joe Bloggs commences his trip 	<ul style="list-style-type: none"> • Admissibility: is Joe Bloggs authorized to travel to destination? • Identity may be checked depending on location and travel scenario: is this Joe Bloggs? 	<ul style="list-style-type: none"> • Identity check: is this Joe Bloggs? • Admissibility: is Joe Bloggs authorized to travel to destination? • Store information for later use
Bag drop	<ul style="list-style-type: none"> • Joe Bloggs wants to check bags 	<ul style="list-style-type: none"> • Identity may be checked depending on location and travel scenario: is this Joe Bloggs? 	<ul style="list-style-type: none"> • This is Joe Bloggs; he is ready to check bags

⁶⁹ IATA, “[One ID - Fact Sheet](#)”, November 2020.

⁷⁰ IATA, “[Simplifying the Business](#)”, 2017.

⁷¹ IATA, “[One ID. Concept Paper](#)”, Version 1, January 2018.

Security screening and access to the security restricted area	<ul style="list-style-type: none"> Joe Bloggs wants to go through security and proceed to the security restricted area 	<ul style="list-style-type: none"> Admissibility: is Joe Bloggs authorized to enter? Identity may be checked depending on location and travel scenario: is this Joe Bloggs? 	<ul style="list-style-type: none"> This is Joe Bloggs; he is authorized to go through security and proceed to the security restricted area; please use security screening protocol "A"
Outbound border controls	<ul style="list-style-type: none"> Joe Bloggs wants to cross the border and leave the country 	<ul style="list-style-type: none"> Admissibility: is Joe Bloggs authorized to cross the border? Identity check: is this Joe Bloggs? 	<ul style="list-style-type: none"> This is Joe Bloggs; background checks have already been performed and he is authorized to cross the border and leave the country
Boarding	<ul style="list-style-type: none"> Joe Bloggs wants to board the aircraft 	<ul style="list-style-type: none"> Admissibility: is Joe Bloggs authorized to board? Identity may be checked depending on location and travel scenario: is this Joe Bloggs? 	<ul style="list-style-type: none"> This is Joe Bloggs; he is authorized to board the aircraft
Inbound border controls	<ul style="list-style-type: none"> Joe Bloggs wants to cross the border and enter the country 	<ul style="list-style-type: none"> Admissibility: is Joe Bloggs authorized to cross the border? Identity check: is this Joe Bloggs? 	<ul style="list-style-type: none"> This is Joe Bloggs; background checks have already been performed, and he is authorized to cross the border and enter the country
Return trip – ready to fly	<ul style="list-style-type: none"> Joe Bloggs is traveling back home 	<ul style="list-style-type: none"> Admissibility: is Joe Bloggs authorized to travel? Identity may be checked depending on location and travel scenario: is this Joe Bloggs? 	<ul style="list-style-type: none"> This is Joe Bloggs; he is authorized to travel

Given these benefits, IATA claims that a lot of passengers may choose to opt in for such biometric identification applications. In its recently released 2021 passenger survey, the IATA claims that 73 percent of passengers are willing to share their biometric data as a means of improving airport processes, up from 46 percent in 2019.⁷²

The IATA may also feel emboldened by the fact that such facial recognition identification systems seem extremely accurate. Indeed, in a recent study the US National Institute of Standards and Technology (NIST) found that several face recognition algorithms used for airline passenger identification are at least 99.5% accurate.⁷³

Despite the IATA’s efforts to show that the “One ID” Concept is based on a “privacy by design” approach, certain issues which relate to data minimisation and storage limitation are creating, as we will see, divergences in the approaches of EU States and DPAs. Before explaining these divergences, let’s have a look at the IATA’s approach to this.

⁷² <https://www.iata.org/en/pressroom/2021-releases/2021-11-15-01/>.

⁷³ NIST, “NIST Evaluates Face Recognition Software’s Accuracy for Flight Boarding”, July 13, 2021. It should be noted however that the tests conducted by the NIST are based on simulated environments. As stated by the NIST “Because airport environments differ, and because the cameras themselves operate in different ways, the report offers some guidance for tests that an airline or immigration authority could run to complement the NIST test results. Such tests would provide accuracy estimates that reflect the actual equipment and environment where it is used”.

Data Minimisation and Storage Limitation – the IATA’s Position

In its document on the privacy and data protection aspects of the “One ID” Concept, the IATA claims that its approach respects data minimisation and storage limitation requirements. It states, among other things, that:

“Following the principle of data minimization, only strictly necessary personal data shall be collected and only for the express purpose for which it is collected [...] The recommended practice is that all personal, identifying data is deleted by the industry stakeholder after the data has fulfilled its purpose”.⁷⁴

However, the IATA has at the same time argued on several occasions that in order for passengers to be able to use the systems for multiple trips, it would be necessary for their biometric data to be stored for a longer period.

The IATA therefore includes, as one of the concept’s “key principles”, to ‘the extent possible’, the option of using biometric enrolment “for multiple trips and for a reasonable period of time”.⁷⁵

In another document the IATA specifies that:

“to the extent possible, and with the passenger’s consent, biometric enrolment is persistent for a certain period of time and does not need to be repeated for every trip”.⁷⁶

The IATA adds that:

“The digital identity could be (temporarily) stored on a cloud-based digital platform. [...] Alternatively, the digital identity could be stored on a mobile device or physical token”.⁷⁷

However, for the IATA, the risk of such storage for future use would be limited, because what would be stored is the biometric template, not the photo of the passenger. The IATA explains that:

“[T]he original biometric is not stored, but rather it is converted into a template (string of multiple numbers) via a one-way process. Each time a new biometric is captured it too is converted into a template, and these unique templates are then compared against each other to confirm an ID. Because the original image is not stored, it means that even if someone gains access to the data, reconstructing the original image is extremely difficult”.⁷⁸

To put it in another way, the “One ID” Concept is based, as IATA explains, on a 1-M biometric recognition⁷⁹ - what we call in our classification table a case of “Individual Identification (Authorisation without using a token)”. The passenger’s photo (“1”), captured at the different touchpoints in the airport, is compared with the database (“M”) that comprises the photos of all the passengers who have opted in. In order to prevent passengers having to repeatedly upload a photo of themselves to the application before every flight, the only solution would be to ensure that the relevant database (“M”) contains a pre-existing biometric template of the passenger, which is stored somewhere and can be retrieved

⁷⁴ IATA, “[One ID, FAQs on PRIVACY](#)”, September 2019.

⁷⁵ IATA, “[One ID End State & Key Principles](#)”, December 14, 2018.

⁷⁶ IATA, “[One ID, Concept Paper](#)”, Version 1, January 2018.

⁷⁷ *Ibid.*

⁷⁸ *Ibid.*

⁷⁹ *Ibid.*

automatically by each new flight's database. This is exactly where it gets complicated for some European DPAs.

2. DPAs' Traditional Hostility to Central Storage of Biometric Data

In their general positions on biometrics and facial recognition, European DPAs have often showed a strong preference for techniques and implementations that *do not require* the creation of a database. This means that where facial recognition for authorisation purposes is concerned, European DPAs consider that systems based on 1-1 verification and involving a biometric token pose less risks to human rights than systems which, like IATA's "One ID" Concept, are based on a 1-M individual identification.

EDPB: "Biometrics should preferably not be stored in a database"

As early as 2003, the EDPB's predecessor, the Article 29 Working Party, in its Biometrics Working Paper, was already stating the following:

"For access control purposes (authentication/verification), the Working Party is of the opinion that biometric systems [that] do not rely on the memorisation of the data in the possession of someone other than the individual concerned (in other words, the data is not memorised in the control access device or in a central data base) create less risks for the protection for fundamental rights and freedoms of individuals. Several Data Protection Authorities have endorsed this view stating that biometrics should preferably not be stored in a database but rather only in an object exclusively available to the user, like a microchip card, a mobile phone, a bank card. In other words, authentication/verification applications which can be carried out without a central storage of biometric data should not implement excessive identification techniques".⁸⁰

The EDPB, 17 years later, stressed again that, in one way or another, biometric data should remain under the control of the data subject. More specifically the EDPB stated the following:

"Identification and authentication/verification are likely to require the storage of the template for use in a later comparison. The data controller must consider the most appropriate location for storage of the data. In an environment under control (delimited hallways or checkpoints), templates shall be stored on an individual device kept by the user and under his or her sole control (in a smartphone or the id card) or – when needed for specific purposes and in the presence of objective needs – stored in a centralized database in an encrypted form with a key/secret solely in the hands of the person to prevent unauthorised access to the template or storage location".⁸¹

⁸⁰ *Op. cit.*, p. 6.

⁸¹ EDPB, [Guidelines 3/2019 on processing of personal data through video devices](#), January 29, 2020 p. 21.

Belgian DPA: “Don’t use biometric systems that store biometric reference data in a database”

In a similar way, the Belgian DPA advised data controllers “not to use biometric systems that store biometric reference data in a database”. It wrote:

“Indeed, when using a biometric system for the authentication of persons, it is not necessary to collect the biometric reference information in a central database. This information should preferably be stored on a secure removable medium (such as a smart card) held by the data subject or, if applicable, in the device containing the biometric sensor (e.g. at the entrance to the building) which must be secure and only accessible locally (without the possibility of connection to other IT systems).

It is therefore appropriate to use the verification function of the biometric system (one-to-one comparison, [...]), and not the identification function (one-to-many comparison) which necessarily implies the use of a database.

*Centralized storage of biometric data increases the risk of reuse of the data for further incompatible purposes and the risk that the data will be used as a key to link different databases”.*⁸²

This hostility of European DPAs to the central storage of biometric data can be explained by the fear of security and data breaches which could have particularly important consequences for data as sensitive as biometric data.

**AEPD and EDPS:
Biometric identification/authentication systems are not safer for users**

The Spanish DPA, AEPD, and the EDPS stressed in their joint 2020 Opinion:

“Any of the multiple systems in which our biometric data are processed can suffer a security breach. Unauthorised access to our biometric data in a system would allow or facilitate (in the case of multiple authentication factors) access in the rest of the systems using such biometric data. It could have the same effect as using the same password on many different systems, so the scale in biometric deployment is a problem in itself. Moreover, unlike password-based systems, once biometric information has been compromised it cannot be modified or cancelled.

*If biometric information was previously stored in a few databases (mainly for public security or border control purposes), it is now stored in an increasing number of devices. This greatly increases the probability of a security breach leaking biometric data (during its collection, transmission, storage or processing)...”.*⁸³

The French DPA seems to agree with all this.

⁸² Autorité de protection des données, “[Avis d’initiative relatif aux traitements de données biométriques dans le cadre de l’authentification de personnes \(A/2008/017\)](#)”, April 9, 2008, §58-60.

⁸³ AEPD/EDPS Joint Paper, “[14 Misunderstandings with regard to Biometric Data](#)”, June 2020, p. 4.

French DPA: “Keeping biometric data under the exclusive control of the passengers”

In a similar way the CNIL, in a 2020 Opinion on the use of facial recognition for authorisation purposes in airports, stressed the following:

“With regard to biometric data, the CNIL has consistently emphasised the need to store them on a medium over which the individual has exclusive use and control. The aim is to limit the risk of hacking associated with the centralisation of biometric templates in a database.

Placing the biometric data under the exclusive control of the persons concerned mechanically reduces the risk of misuse, compromise or misappropriation. The compromise of a biometric database could create risks for many people, whereas the compromise of an individual medium will only impact the data of its holder.

In practice :

- either the biometric data is stored on an individual medium over which the passenger has exclusive control and use (on a secure mobile application on his or her mobile phone, on a badge, a card, etc.) ;*
- or the biometric data is stored in an encrypted form in the database, making it unusable without the passenger communicating an element or secret enabling it to be decrypted.*

In this way, the passenger is certain that his biometric data will only be used if he decides to do so, following an action on his part (by presenting the medium or communicating the secret enabling it to be used). The passenger can also choose the control steps for which he or she wishes to use biometric authentication or not. This also makes it possible to subject the passenger to biometric authentication at each stage of the journey and not to biometric identification, which guarantees greater reliability of the device by reducing the risk of errors (false positives or false negatives).

This principle of keeping the data under the exclusive control of the data subject thus meets the principles laid down by the RGPD, of data protection by default and by design and the principle of data minimisation”.⁸⁴

3. CNIL’s Reservations concerning the MONA Case

As we explained earlier, the French DPA CNIL considered that the experimental deployment of the MONA facial recognition system at Lyon Airport was compatible with GDPR requirements. However, the CNIL stressed that it only agreed to the trial due to specific circumstances and because certain data minimisation and storage limitation protections were adopted by the data controller.

⁸⁴ CNIL, [“Reconnaissance faciale dans les aéroports : quels enjeux et quels grands principes à respecter?”](#), October 9, 2020. Our translation.

Is Biometric Data Deleted Each Time a Plane Takes Off?

In the MONA case the French DPA explained that:

“the experiment foresees that the biometric templates of voluntary and consenting passengers would be stored:

- *on a secure, dedicated server (separate from boarding pass data) located within the airport;*
- *temporarily, from enrolment until (i) a request for deletion of the template by the passenger or (ii) automatic deletion of the template when the aircraft takes off (even if the passenger has enrolled and checked in but has not boarded) or (iii) automatic deletion of the template in the event of flight cancellation”.*

The CNIL then, reminded everyone about its “constant position” on the “need” for data controllers:

“to store biometric data on a medium that the individual has exclusive use and control of, in order to limit the systemic risk of hacking associated with the centralization of numerous biometric templates in a database. Unlike other personal data, biometric data is unique and, for the most part, permanent and can therefore be altered if compromised”.

On this basis, the French DPA agreed to the MONA trial but only due to the circumstances of the case. It stated:

“Consequently, the Commission insists that the method of storage of biometric data as envisaged by your company in the context of the experiment described can only be considered acceptable because of :

- *the local nature of the database (within the airport) and the temporary nature of the storage (the data is only kept until the flight takes off or is cancelled);*
- *the experimental and time-limited nature of the system”.*⁸⁵

The CNIL noted however in another opinion, that while it has succeeded in establishing certain guarantees with regard to the implementation of MONA as an “an isolated and time-limited experimental project”, the “almost certain” prospect of an expansion of the scope of these systems and their mass deployment on a permanent basis required the Commission to consolidate its position on this subject. While the CNIL has not yet definitively ruled on the continuation of MONA (the matter is currently under discussion, as we will see), its previous positions seem to express strong doubts about the compatibility of IATA’s “One ID” Concept with the data minimisation and storage limitation principles of the GDPR.

⁸⁵ CNIL, [Communication en date du 6 juillet 2020 entre la Présidente de la CNIL et le Directeur général des Aéroports de Lyon](#), Saisine n°20011104, N/Réf : /SA201130, p. 1. Our translation.

CNIL’s doubts about the compatibility of IATA’s “One ID” Concept with the data minimisation and storage limitation principles of the GDPR

In a “Communication” adopted in May 2020, the CNIL noted that the “One ID” initiative developed by the International Air Transport Association (IATA):

“is based on the retention of all identity and biometric data relating to the passenger and obtained at the time of enrolment, in order to enable the passenger to carry out all his or her travel in any airport in the world, without having to present a single document”.

The CNIL added that this “One ID” initiative aims to “generalize the substitution of existing passenger control systems in airports with facial recognition devices” to streamline and smooth passenger flow. One of its four elements is the creation of a “secure digital identity” that enables “validation of the passenger’s identity using enrolment via facial recognition on a mobile phone even before the passenger arrives at the airport”.

Following its preliminary analysis, the CNIL’s Rapporteur noted that:

“[T]his objective of almost permanently retaining the data of passengers appears to be incompatible with the principle of data minimisation laid down by the GDPR and the need to limit the duration of data retention”.

The CNIL added that:

“[T]he storage of this data, even if it were encrypted, appears disproportionate and excessive in relation to the purpose of their storage, particularly insofar as these data may be accessible to the controller”.

Recalling recital 39 of the GDPR (mentioned previously in our analysis), the CNIL noted that:

“[T]he copy of an identity document is a sensitive document and its quasi-permanent storage, without any reinforced security measures and with possible access by the controller, for the sole purpose of allowing the passenger not to have to photograph it again, does not seem justified”.

In conclusion, the CNIL explicitly specified, in its response to Lyon Airport, that:

“[T]he eventual continuation of the system will have to favour a storage method that allows the person concerned to control his or her biometric data”. [...] [I]n the context of a continuation of the envisaged system, the storage of biometric data within a centralized database cannot be considered as being in conformity with the principles of minimization and data protection by design and by default, as they are set by the RGPD”.⁸⁶

⁸⁶ CNIL, “[Communication présentée en séance plénière relative à la mise en oeuvre d’expérimentations de dispositifs de reconnaissance faciale au sein de plusieurs aéroports aux fins de fluidification et de sécurisation du parcours passager](#)”, May 28, 2020. Our translation.

Acknowledging the risk of divergences at the European level on this important issue, the CNIL emphasised in the conclusions of this very same “Communication” of May 2020,

*“the possibility of bringing the topic to the level of the EDPB in order to try to develop a harmonized position on the topic”.*⁸⁷

However, the EDPB has not yet published guidelines on this issue. The CNIL is now considering its final position on this matter, in relation to a request by MONA’s developers to render the application permanent and to eventually deploy their system in other French Airports.⁸⁸

4. Divergences? Deployment of “One ID” Solutions in Spain, Germany and Beyond

We have seen that, although the matter is currently under consideration, the CNIL has in the past expressed doubts about the compatibility of IATA’s “One ID” Concept with the data minimisation and storage limitation principles of the GDPR – and more specifically the possibility of storing - and making available to data controllers – the identity and biometric data of passengers for multiple journeys. This situation, which may render the permanent deployment of IATA’s “One ID” Concept problematic in France, seems to differ to that of other countries where airports and airlines have permanently implemented the “One ID” Concept without experiencing, according to our knowledge, any opposition from the relevant DPAs. During our research we have found similar experiments in several European countries such as Slovenia⁸⁹, Finland⁹⁰, The Netherlands⁹¹, Italy⁹² and the UK⁹³, but we have mainly focused on the situations in Spain and Germany/Austria.

From AENA pilot projects to a generalisation of “One ID” applications in Spain?

The airport management company “Aeropuertos Españoles y Navegación Aérea” (AENA) launched three pilot projects similar to the French “MONA” project in three different Spanish airports, which involved three different airlines.

The first pilot project was launched on March 29th, 2019, took place at Menorca airport, involved Air Europa and lasted a year. According to the information that we have gathered, the passengers’ biometric data were

⁸⁷ *Ibidem.*

⁸⁸ The CNIL [announced recently](#) that it is currently working on a « Communication relative à un projet de pérennisation d’un dispositif de reconnaissance faciale au sein de l’aéroport Lyon-Saint Exupéry aux fins de fluidification et de sécurisation du parcours passager ».

⁸⁹ See: “[Amadeus teams up with Ljubljana Airport, Adria Airways and LOT Polish Airlines for biometric boarding pilot](#)”, May 16, 2019.

⁹⁰ See Future of facial recognition: the Finland experiment - Future Airport; [Finnair, Finavia Test Facial Recognition Technology at Helsinki Airport | Travel Agent Central](#).

⁹¹ See [Schiphol Airport starts facial recognition boarding using Vision-Box platform](#).

⁹² See [Progetto Face Boarding | Milano Linate \(milanolinate-airport.com\)](#).

⁹³ See ICO, “[Regulatory Sandbox Final Report: Heathrow Airport Ltd](#)”, June 2020.

deleted following boarding, unless the passenger had given permission for their data to remain in a database for the whole period of the trial.⁹⁴

The second pilot project was launched on November 21st, 2019 at the Madrid-Barajas airport, and involved the Iberia airline.⁹⁵ According to the information that we have gathered, the personal data of users were not automatically erased after the plane's take off, in order to allow users to keep using the FRT option throughout the duration of the trial (one year) without having to enrol again. Iberia stated that registration on the system was valid for 1 year and that, in order to be removed from the database, individuals needed to send an e-mail to Aena's Central Data Protection Unit attaching a photo of their ID or passport and a recent photograph.⁹⁶ In a response to a written question from the Parliament, the Government stated that "*it is important to point out that this project complies at all times with current legislation on Data Protection*" and that "*once the pilot project is completed and its results are analysed, AENA will consider extending it to other airports in its network*".⁹⁷

The third pilot project, involving Vueling, was launched on December 1st, 2021 at the Josep Tarradellas Barcelona-El Prat airport, and was planned to be deployed for 6 months.⁹⁸ According to the information that we have been able to access, passengers have to ask Vueling to transfer their data to AENA and the data is kept for the duration of the trial.

It is unknown whether the Spanish DPA was involved in the planning of these pilot projects.

Star Alliance Biometrics in Germany

The facial recognition project launched by Star Alliance is by far the most important FR project in Europe as it already involves three European airlines (Lufthansa, Swiss and Austrian airlines) and four airports (in Frankfurt, Munich, Hamburg and Vienna) in two different countries, with the potential to expand to several other airlines and airports (Star Alliance is the world's largest airline group with 26 international operators). It permits 'Frequent Flyer' customers to use facial recognition at different stages of the airport and for boarding without having to show their ID or boarding pass. As the Star Alliance webpage explains⁹⁹:

"Star Alliance Biometrics is a voluntary Star Alliance product that allows customers to take advantage of facial recognition technology to pass through security and boarding gates in a touchless manner. In the near future the range of

⁹⁴ See GARCINUÑO (P.), "[Reconocimiento facial para embarcar sin necesidad de mostrar documentación](#)", *Innovaspain online*, April 3, 2019; & BRANDS (E.), "[El reconocimiento facial, pionero en un aeropuerto español: así funciona en Menorca](#)", *El Confidencial*, July 27, 2019; "[Tecnología punta para mejorar la experiencia del pasajero](#)", *El País*, May 3, 2019.

⁹⁵ See HERRANZ (A), "[Iberia te permitirá facturar 'por la cara': así está desplegando un sistema de reconocimiento facial que te reconoce hasta con mascarilla](#)", *Xataka*, February 16, 2021.

⁹⁶ "Registration on the programme is, in general, valid for 1 year. However, if you would like to unsubscribe at any time, you must send an email to the Aena Central Data Protection Unit (ocpd@aena.es) with a photocopy of your DNI/NIE/Passport and a recent photograph". See "[Hoy miramos más hacia el futuro. Embarcamos con reconocimiento facial](#)", *Iberia's official website*. Our translation.

⁹⁷ [Respuesta del Gobierno. 184/36403](#), March 31, 2021. Our translation.

⁹⁸ ORTEGA FIGUEIRAL (J.), "[Aeropuerto de Barcelona: pionero en 'volar por la cara'](#)", *The New Barcelona Post*, December 16, 2021.

⁹⁹ [FAQ - Star Alliance Biometrics](#).

process points will be gradually expanded – for example to baggage drop-off and lounge access.

When an enrolled customer travels through a participating airport and on a participating airline, Star Alliance Biometrics facial recognition technology matches the customer's live image to the boarding pass information and biometric profile, allowing the customer to effortlessly pass through security and boarding gates. [...]

"It is not required to remove the mask for the biometric identity check. The identification process works for passengers wearing masks".

With regard to the storage of personal data, the same website explains that:

"Star Alliance Biometrics stores the enrolled frequent flyer number, up to five pictures of the customer, the expiration date of the passport, and PIN as well as security questions. The customer's name is not stored". [...]

Star Alliance encrypts and stores your profile and data in a Microsoft Azure Cloud hosted in Europe. The data is subject to and protected by EU privacy laws. Airlines and airports will not have access to your biometric profile data".

The website clearly explains that passengers *do not need* to register before every flight. Christian Draeger, the VP of customer experience at Star Alliance, explained that a problem that he and his team wanted to solve was:

"avoiding customers having to re-enrol in the biometric programme each time they embarked on a trip. Before the partnership with NEC, Star Alliance passengers that could use biometric ID for travelling had to enrol in the programme for each new flight. Customers travelling from Atlanta on a Tuesday, for example, could use the biometric template only for that specific trip. If they came back the next day or a week after, they had to go through the enrolment process from scratch: That is where we said we want to have a programme where customers don't need to go through the same enrolment over and over again."

Draeger further explained that:

"The new service means customers in the Star Alliance 'frequent flyer' scheme can opt to enrol into the biometric programme for all their future trips through the company's app.

To use it, passengers take a selfie on their phones and scan a valid form of travel identification. The app then verifies the validity of the identification document against the selfie to prevent fraud. The passenger's photograph is encrypted, with the resulting biometric template stored in a central database in the Azure cloud. Star Alliance then matches the frequent flyer customer number against their reservations list and when the system detects that the customer is flying, the biometric template is made available for that specific date and airport only.

Once there has been a match with the identification, the biometric or facial recognition serves as the boarding pass and removes the need to show a physical document. If the customer, on a given day, comes to the airport, this gallery has been pre-created and if the customer now approaches one of the touchpoints (for example, the security gate or the departure gate), then there is a procedure where the picture taken at the touchpoint is compared to the biometric template that was stored in the day's gallery".¹⁰⁰

Draeger added that Star Alliance Biometrics:

"has the strictest security measures in place which offer "an extremely high level of assurance" to customers. [...]

The programme has a threefold strategy for data security. The first level is the

¹⁰⁰ <https://techmonitor.ai/emerging-tech/start-alliance-biometrics-lufthansa>.

principle of data minimisation, a term universalised by GDPR, which states that organisations should only collect and retain the minimum amount of personal data required to provide their services. In the case of Star Alliance’s biometric programme, this is the biometric template, which includes the frequent flyer customer number and the expiry date of their identity document. Biometric templates are encrypted and are not linked to the personal data of the customer, [...], so the frequent flyer number cannot be traced back.

Secondly, Star Alliance conducts a data protection assessment: “This is a tool where all aspects of security and data privacy are looked at in detail, identified by experts, and analysed so that they are sufficient and appropriately secure.

The third level of security involves transparency with the data protection authorities where the biometric service is launched. In the case of Frankfurt and Munich airports, Star Alliance has engaged with the German authorities at a federal level to ensure they are fully aware of how the biometric programme works and that it complies with GDPR.”¹⁰¹

Despite these clear declarations, according to which German DPAs have been involved in the deployment of Star Alliance Biometrics, we have been unable to find any published position by them on this topic, which would permit a comparison with the French DPA’s positions regarding MONA.

5. Potential Solutions to Bring About Harmonisation

As shown in this section there is a risk of divergent approaches by European Member States concerning the potential implementation of IATA’s “One ID” Concept for Air Travel. This raises the question of whether a harmonisation effort is necessary, in order to avoid differences in the interpretation of the GDPR in this field and airports and airlines in Europe being treated differently.

If such a harmonisation effort is deemed necessary by European authorities, then it could be achieved in two main ways.

The first, burdensome and complicated way, would be for EU legislators to take action in the future in order to clarify the rules in this area.

The second, and probably much more adequate solution, would be for the EDPB to issue guidance on this matter in order to ensure that the GDPR is being consistently applied. It is worth remembering that, according to Article 70 (1)(e) of the GDPR, one of the main tasks of the EDPB is to:

“examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation”.

As we have already seen, the French DPA stressed in a “Communication” published in May 2020:

“the possibility of bringing the topic to the level of the EDPB in

¹⁰¹ Ibid.

order to try to develop a harmonized position on the topic".¹⁰²

The EDPB guidance concerning the commercial use of FRT for authorisation purposes in EU Member State airports could indeed be very useful as a means of preventing discrepancies in this field. And to the extent that data controllers might plan to use similar facial recognition solutions in other user authorisation cases (such as stadiums) this guidance could also apply *mutatis mutandis* to such cases enabling a better understanding of the relationship between the different existing authorisation techniques that use facial recognition, based on the powerful legal basis of explicit consent, and the GDPR data processing principles.

¹⁰² *Op. cit.*

IV. ASSESSMENTS: FROM DPIAS TO EVALUATING ACCURACY AND EFFICIENCY

We will end this analysis with a few observations on the issue of how the use of FRT for authorisation purposes in public spaces in Europe is assessed. We will first discuss the question of whether Data Protection Impact Assessments (DPIAs) are required before the deployment of FRT for authorisation purposes in public spaces in Europe – and whether they are carried out in practice **(1)**; We will then turn to the issue of whether the posterior evaluation of both the accuracy of the systems and their efficiency more generally meet the proclaimed objectives **(2)**.

1. Data Protection Impact Assessments

According to Article 35 (1) of the GDPR:

“Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks”.

Article 35 (1) of the GDPR does not give precise details about the data processing situations that involve a “high risk to the rights and freedoms of natural persons”. Nevertheless, Article 35(3) provides some examples of when a processing operation is “likely to result in high risks”, citing among others:

“processing on a large scale of special categories of data referred to in Article 9(1) [...]; or a systematic monitoring of a publicly accessible area on a large scale”.

One could try to argue that none of the examples in Article 35(3) relate to the use of FRT for authorisation purposes in public spaces in Europe, as the types of facial processing involved (1-1 in the case of verification; 1-M in the case of individual identification) should not be considered as “large scale”.

On the other hand, even if the basic mechanism is characterised as 1-1 or 1-M, it can be applied repeatedly, and perhaps to a large number of people (*e.g.* all airports’ international passengers passing through a system like PARAFE). This should definitively be considered as meeting the requirements of Article 35 (1) of the GDPR. Indeed, according to recital 91 of the GDPR a data protection impact

assessment should be carried out by the controller prior to the processing in the case of operations which:

“aim to process a considerable amount of personal data [...] and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity”.

So despite the fact that neither Article 9 nor Article 35 (1) of the GDPR state that a DPIA is required each time there is processing of biometric data, and despite also the fact that, unfortunately, the Guidelines on Data Protection Impact Assessment¹⁰³ endorsed by the EDPB do not provide any supplementary guidance in this respect, one should conclude that such DPIAs are necessary in almost all facial recognition deployments.

This seems to be confirmed by National DPAs which constantly strongly recommend to data controllers to conduct a DPIA in all cases in which biometric data are processed.

CNIL Recommends that a DPIA be carried out before the use of FRT for authorisation at an airport

In its 2020 Opinion on the use of facial recognition for authorisation purposes in airports the French DPA stated the following:

“In the case of the implementation of a facial recognition system at an airport, and given the sensitivity of the data processed, the number of passengers potentially concerned and the risks inherent in this type of technology, the CNIL recommends that a DPIA be carried out before the processing is implemented, whether it is experimental or not.

*Within this DPIA, the data controller must determine the legal regime applicable to the data processing implemented. This determination presents essential challenges. Indeed, processing that falls within the framework of the so-called “Police-Justice” Directive or that is carried out on behalf of the State acting in its capacity as a public authority should be provided for by specific texts”.*¹⁰⁴

Belgian DPA: “Not carrying out a DPIA can only be justified in exceptional cases”

In its recent general Opinion on the processing of biometric data, the Belgian DPA seems to be enlarging on a previous position adopted in 2019, which already required that data controllers carry out DPIAs in all cases in which FRT is used for *identification* purposes. To be more precise, the Belgian DPA stated the following in its December 2021 Opinion:

“As stated in point 6 of Decision No 01/2019, a data protection impact assessment will always be required when the processing operation uses biometric data for the unique identification of data subjects in a public place or

¹⁰³ [Guidelines on Data Protection Impact Assessment \(DPIA\) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679](#), wp248rev.01.

¹⁰⁴ CNIL, [“Reconnaissance faciale dans les aéroports : quels enjeux et quels grands principes à respecter?”](#), October 9, 2020. Our translation.

in a private place accessible to the public. However, the Knowledge Centre would like to point out that the processing of biometric data for purposes other than those explicitly mentioned in the Decision is also subject to the obligation to carry out a data protection impact assessment. Moreover, in view of the inherently high risk for the rights and freedoms of the data subjects involved in the processing of biometric data, not carrying out a data protection impact assessment can only be justified in exceptional cases”.¹⁰⁵

During our research we realised that DPIAs were effectively carried out in at least three of the use cases examined (Parafe, PACA Schools and MONA) but we were unable to find out whether a DPIA had been conducted in the four other cases (Molenbeek Stadium; UK School Canteens; AENA; Star Alliance). In those cases where a DPIA was drafted, *not a single* DPIA was published – although in all cases it was communicated to the DPA and used for its assessment of the situation.

2. Evaluating Accuracy and Efficiency

One of the important enquires in our “analytical framework” of use cases concerned the issue of whether an evaluation of the system had been conducted *after* its deployment in order to assess its accuracy, its potential impact on human rights (for instance problems of bias or discrimination) and, more broadly, its capacity to fulfil the declared objectives. The main conclusions of our research are as follows:

➤ We have been unable to find any published evaluation study concerning *specifically* any of the seven cases of the use of FRT for authorisation purposes in public spaces in Europe. In two of the cases examined (PACA Schools and UK School Canteens), the absence of such evaluation reports is to be expected, as the deployments of FRT were interrupted following the intervention of DPAs and Courts. In the other five cases it is possible that evaluations of their accuracy and efficiency were carried out, but the evaluation reports were not published. This is regrettable.

➤ Evaluation studies have been carried out sometimes in a more general way and for some authorization applications. Among the most important we have already mentioned the evaluations of the US National Institute of Standards and Technology (NIST) on “Face Recognition Software’s Accuracy for Flight Boarding”. NIST found that several facial recognition algorithms have an accuracy rate of “at least 99.5 percent”. A summary of the NIST study reads as follows:

“The most accurate face recognition algorithms have demonstrated the capability to confirm airline passenger identities while making very few errors, according to recent tests of the software conducted at the National Institute of Standards and Technology (NIST). The findings [...] focus on face recognition

¹⁰⁵ Autorité de protection des données, [“Recommandation relative au traitement de données biométriques”](#), December 1st, 2021, at 36-37. Our translation.

(FR) algorithms' performance under a particular set of simulated circumstances: matching images of travelers to previously obtained photos of those travelers stored in a database. This use of FR is currently part of the boarding process for international flights, both to confirm a passenger's identity for the airline's flight roster and also to record the passenger's official immigration exit from the United States. The results indicate that several of the FR algorithms NIST tested could perform the task using a single scan of a passenger's face with 99.5% accuracy or better — especially if the database contains several images of the passenger".¹⁰⁶

➤ These general evaluation studies do not only assess accuracy in general but also include other metrics, such as average transaction time, image processing failures, accuracy per demographics, percentage of customers satisfied, and effectiveness of providing positive identification in less than 20 seconds. Furthermore, institutions such as the U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) host periodically "Biometric Technology Rallies" which bring together "subject matter experts, technology vendors and volunteers to test new and emerging biometric technology systems".¹⁰⁷

➤ Our research has not permitted any specific problems to be identified in terms of the risk of bias/discrimination concerning FRT being used for authorisation purposes in public spaces in Europe. In none of the seven (or other) cases examined during our project have we found any claims that the systems were producing different results according to gender, age, ethnicity, or other distinctive criteria. However, the absence of independent evaluation reports means that no definitive conclusions can be arrived at in this field.

➤ With regard to the deployment of the PARAFE system at the French border we have been surprised not to have found any published detailed evaluation or other publicly available data on its accuracy.¹⁰⁸ Journalists had claimed in 2018 that "the technology [was] not yet completely reliable: the machine can mistakenly scan a face printed on a T-shirt or be disturbed by too much light".¹⁰⁹ Three years later, journalists report that the system "has a few bugs", while the attitude of some "impatient travellers" (who sometimes force their way through and create a situation where several people are left in the airlock) is also a

¹⁰⁶ NIST, "[NIST Evaluates Face Recognition Software's Accuracy for Flight Boarding](#)", July 13, 2021. See however *supra* note 73.

¹⁰⁷ See Department of Homeland Security, "[Biometric Technology Rally](#)".

¹⁰⁸ In 2012 three researchers noted that: "Very few independent studies exist that assess the reliability of automated facial recognition for border control". In their own evaluation study of the reliability of automated facial recognition for automatic border passage at Schiphol Airport, the authors concluded: "In spite of the critical analysis in this study, the prospects for automatic border passage using face recognition are very good. We expect that, provided that the quality of the live images acquired by the gates is improved and if possible the quality of the digital photographs stored on the passport, excellent recognition results can be obtained with Verification Rates (VR) of above 99% at a False Accept Rate (FAR) of 0.1% or even lower". SPREEUWERS (L.J.), HENDRIKSE (A.J.), GERRITSEN (K.J.), "[Evaluation of automatic face recognition for automatic border control on actual data recorded of travellers at Schiphol Airport](#)" 2012 BIOSIG - Proceedings of the International Conference of Biometrics Special Interest Group (BIOSIG), 2012, pp. 1-6.

¹⁰⁹ DAMOUR (P.), "[La vérité sur les sas Parafe dans les aéroports](#)", *Challenges*, September, 2018. BONTINCK, (J.), "[Aéroports de Roissy et d'Orly: des contrôles par reconnaissance faciale pour embarquer](#)", *Le Parisien*, June 29, 2018.

problem.¹¹⁰ However, the French group THALES, one of the companies which provide the system, claim on their website that it “offers outstanding operational efficiency”.¹¹¹ The same group claims that “today, an automatic facial recognition check takes 10 to 15 seconds, compared to 30 to 45 seconds for fingerprint checks”, the time that Parafe used to take.¹¹²

¹¹⁰ LICATO CARUSO (D.), “[Comment l’intelligence artificielle va fluidifier les passages de frontière dans les gares et aéroports](#)”, October 14, 2021.

¹¹¹ See <https://www.thalesgroup.com/fr/europe/france/dis/gouvernement/controle-aux-frontieres>.

¹¹² Ibid.

CONCLUSIONS AND RECOMMENDATIONS

In this paper we have tried to provide a detailed study of the use of facial recognition for authorisation purposes in public spaces in Europe. We gathered information for this analysis by selecting seven cases, beyond which there were a number of other similar cases¹¹³ or pilot projects. Arguments claiming that FRT will “increase security”, “provide for contactless solutions that will prevent the spread of Covid”, “accelerate users flows”, or simply “improve the customer experience”, increase the willingness of various actors to implement such solutions for authorisation purposes. We have dived into the opinions of Data Protection Authorities and we have analysed in detail existing law and all of the relevant documentation that we have been able to access. We have made a number of valuable findings. Here are some recommendations in relation to data controllers (1); the EDPB (2); and all the stakeholders making proposals for new FRT rules (3).

1) Recommendations in relation to data controllers

We make **three recommendations vis-à-vis those data controllers** wishing to use facial recognition applications for authorisation purposes.

1.1. Data controllers should understand that they have the burden to prove that they meet all GDPR requirements

The GDPR is king when it comes to the legal regime surrounding authorisation using FRT. As we have seen, until today, all the deployments of facial recognition for such purposes in public spaces in Europe have used as a legal basis either “explicit consent” (Article 9(2)(a) of the GDPR), or “processing necessary for reasons of substantial public interest” (Article 9(2)(g)).

The fact that these two legal bases constitute *exceptions* to the prohibition of processing of biometric data posed by Art. 9(1) of the GDPR means that **the burden of proof lies with data controllers**, who have to show that the use of FRT meets all the requirements of the GDPR. This involves a series of legal steps often linked to technical operations:

- making sure that the requirements for using a specific exception are met, either by respecting all the conditions that are required for consent, or making sure that a domestic “law” explicitly authorises the processing of biometric data under the “substantial public interest” exception;

¹¹³ Behind “PARAFE”, for instance, there are many similar uses of FRT for automated border controls (ABC) in many countries and airports.

- understanding exactly how the necessity and proportionality principles work in this field and ensuring that all required measures are taken to comply with these principles;
- complying with the other principles relating to processing of personal data (purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality) which, as we have seen, are frequently also taken into consideration by DPAs in their necessity and proportionality assessments.
- using the FRT solutions which are the most compatible with such principles relating to processing of personal data (for instance, and to the extent possible, FR systems that use verification functionality instead of identification).

1.2. Data controllers should understand the limits of the “cooperative” use of facial recognition for authorisation purposes

Deployments of facial recognition systems for authorisation purposes in public spaces in Europe have almost always been based on consent. In some rare cases (e.g. PARAFE), where the “substantial public interest” exception has been used instead, the relevant domestic legal provisions and practices enable users to “voluntarily” choose whether to select FRT or go with other solutions. This means that the use of FRT has always been undertaken “cooperatively” in Europe, based either on a consent that is freely given or on a “voluntary” choice. This is a field where consent and the exercising of free choice constitute powerful forces, permitting data controllers to try to “legitimize” the use of FRT.

However, **this does not mean that consent is almighty.**

First, there are situations (such as the various failed attempts to introduce FRT in schools in Europe) where consent could not be justified as being “freely given” because of an imbalance of power between users and data controllers.

Second, consensual and other “voluntary” uses of FRT imply the existence of **alternative solutions** which must be as available and as effective as those that involve the use of FRT. It should be noted, in this respect, that the *de facto* (e.g. the creation of major inconveniences for users of non-FRT solutions) or *de jure* (e.g. domestic laws which may render certain FRT authorisation techniques mandatory) removal of alternative solutions would not only affect consent as a legal basis, but could also influence the overall proportionality assessment.

1.3. Data controllers should conduct DPIAs and evaluation reports

We have seen that there is a serious lack of information available on DPIAs and evaluations of the effectiveness of FRT systems. This is regrettable for several reasons.

First, it is **difficult to have an informed debate about issues such as necessity and proportionality without a precise understanding of the real risks and benefits of these systems.** Each member State may obviously have its own, particular sensitivities about these issues, rooted in its own history and

culture, but different interpretations can also result from different perceptions of the risks and the benefits.

Second, is it important not only to demonstrate that the data controller, *before* implementing an FRT system, has calculated all the risks – and has adopted all of the necessary mitigation measures and safeguards, but also to demonstrate *post facto* that such systems are indeed capable of achieving their stated goals and **bring clear “added value” when compared with less-intrusive non-biometric systems.**

Last, but not least, conducting DPIAs and post-use evaluation reports, and publishing them to the extent possible, will **increase transparency**, something that will also be beneficial to data controllers and the promoters of these technologies (if indeed they deliver on their promises), since a lack of information typically fosters concern and mistrust – especially when it comes to technologies which are often depicted as potential threats to fundamental rights by their critics.

We therefore recommend not only **that DPIAs are always conducted for these systems** (which already seems to be the case, even if the results are not available), but also that they are published (or at least an outline of them) to the extent possible and compatible with industrial secrets and property rights.¹¹⁴ Such DPIAs should be complemented by mandatory assessments of the effectiveness of the systems following deployment. Such assessments should be **performed on the ground** rather than in laboratories since the effectiveness of these systems depends on many factors that go beyond the performance of the face recognition algorithms (the positions of the cameras, the light conditions, how the operators handle the equipment, how it is integrated within the overall organisation, etc.). It is also necessary to be able to **compare the effectiveness of the deployed FRT system with the one of traditional solutions** (that do not involve facial recognition).

2) Recommendations in relation to DPAs and the EDPB

We make two recommendations in relation to the EDPB.

2.1. DPAs and the EDPB should ensure that there is harmonisation on issues such as the use of centralised databases, and principles relating to processing of personal data

We possess, as of today, very rich, and **mostly convergent**, “case law” on the application of the GDPR in this field. However, as we have seen, interpretation of elements such as the **necessity and proportionality principles**, the **“less intrusive means” test**, or the question of exactly how **data processing principles**, such as data minimisation and storage limitation, apply when FRT is

¹¹⁴ In situations where publication would reveal trade secrets or jeopardize industrial property rights, a publication limited to an outline of the DPIA, without revealing such secrets or the strategies used by the provider to assess and mitigate the risks, could be possible (with only the DPA having access to the full version).

used for authorisation purposes, leave a lot of room for interpretation. This, in turn, creates the **risk of divergent interpretations** of the GDPR by European DPAs and, therefore, of different approaches to very similar issues in European States.

EU Member States have, of course, their own traditions and some may choose to have stricter and more protective regimes than others. Uniformity is not a necessity in *all* fields. However, a diverging interpretation of the GDPR could create legal tensions and operational difficulties. When it comes, for instance, to the implementation of IATA's "One ID" concept for air travel, French airports and airlines might not be able to understand why they might not be allowed to use such consent-based solutions in France, while their counterparts in Frankfurt, Munich and Vienna might be able to do so, relying on exactly the same legal text (the GDPR). To offer another theoretical example, would it be satisfactory for the unity of European data protection law if, for instance, the Spanish DPA decides that "pay by face" applications are compatible with the GDPR, while its counterparts in France or Belgium decide that they are disproportionate vis-à-vis the GDPR? There is **a risk here that European law could become fragmented**.

To avoid this risk, the EDPB should probably issue **guidance** on a number of issues, starting with the most pressing one, that of **how the principles of data minimisation and storage limitation should be interpreted**. European DPAs do converge in terms of their preference for using "verification by biometric token" techniques as a means of authorisation. But does this mean that other techniques, involving the use of databases, should be excluded? Could the introduction of strong protections and safeguards (including encryption) enable European operators to use 1-M authorisation techniques in consent-based FRT authorisation systems such as the "One ID" concept for air travel or "pay by face" applications? If so, according to which precise conditions? Aside from data processing principles, how can European DPAs create more legal certainty and visibility with regard to issues such as the interpretation of the "less intrusive means" requirement in this field?

2.2. The EDPB could produce guidance on the approach to be followed both for DPIAs and evaluation reports of FRT authorisation applications

This is less urgent and important, but the EDPB could eventually help data controllers implement our recommendation 1.3. above by producing precise recommendations on the approach to be followed both for the DPIAs and for the assessment of effectiveness of systems processing biometric data. This could help both their preparation by data controllers and their subsequent analysis by DPAs and all other stakeholders.

3) Recommendation regarding policymakers

As we have seen in Part 1 of our MAPFRE reports, there is **often a great deal of confusion** about the different proposals that concern the regulation of facial recognition. It is thus important for all stakeholders to **distinguish** the numerous

uses of facial recognition for authorization purposes from other use cases and to target their proposals accordingly.

This involves, first of all, to understand the relationship between FRT for authorisation purposes, the draft EU AI Act and calls for facial recognition “bans”.

The draft AI Regulation, as proposed by the European Commission, is unlikely to affect the use of FRT for authorisation purposes in public (or private) spaces. As we have seen in a previous segment of our MAPFRE series¹¹⁵, the Commission’s draft has only focused on “*remote biometric identification*” (“RBI”) systems. The Commission defines them as :“AI system(s) for the purpose of identifying natural persons at a distance [...] without prior knowledge of the user of the AI system whether the person will be present and can be identified”.¹¹⁶ Elements such as the word “remote” or “identification” or the absence of “prior knowledge” in this definition, **seem to indicate that the concept of “RBI” does not intend to cover the use of FRT systems for authorisation purposes.**¹¹⁷

As a result, even if the amendments to the draft AI Regulation, which have been proposed by certain lawmakers¹¹⁸, and aim to completely ban “*the use of remote biometric identification systems in publicly accessible spaces*”, are adopted, this should not affect the use of FRT for authorisation purposes – although it should certainly be better to say so.

If, on the other hand, other proposals, calling for a broad ban on “biometric recognition in public spaces”¹¹⁹ are ultimately successful, they are likely to result in all of the ways in which FRT is used for authorisation purposes being prohibited. **Policy-makers should take this into consideration, and make sure that this is their intention, before they make such proposals.**

¹¹⁵ See T. Christakis, K. Bannelier, C. Castelluccia, D. Le Métayer, “[Mapping the Use of Facial Recognition in Public Spaces in Europe – Part 1: A Quest for Clarity: Unpicking the “Catch-All” Term](#)”, Report of the AI-Regulation Chair (AI-Regulation.Com), MIAI, May 2022.

¹¹⁶ It is worth recalling here that the Commission’s AI regulation draft aims to prohibit the use of “real-time remote biometric identification systems” by law enforcement authorities – while at the same time introducing a number of exceptions. Nevertheless, the Commission’s proposals do not concern the use of “remote biometric identification systems” by private or public actors for purposes *other* than law enforcement.

¹¹⁷ This is clearly the case for FR authorization systems using verification function. But what about such systems (such as the ones presented in Part III of this Report) using the identification functionality? Are they less “remote” than other FR identification systems? Should we invent a category called “non-remote biometric identification” to cover such uses of facial identification for authorization purposes?

¹¹⁸ See T. Christakis, K. Bannelier, C. Castelluccia, D. Le Métayer, “[Mapping the Use of Facial Recognition in Public Spaces in Europe – Part 1: A Quest for Clarity: Unpicking the “Catch-All” Term](#)”, Report of the AI-Regulation Chair (AI-Regulation.Com), MIAI, May 2022.

¹¹⁹ For a few examples see *ibid.*



HOW TO CITE THIS REPORT:

T. Christakis, K. Bannelier, C. Castelluccia, D. Le Métayer, "Mapping the Use of Facial Recognition in Public Spaces in Europe – Part 3: Facial Recognition for Authorisation Purposes", Report of the AI- Regulation Chair (AI-Regulation.Com), MIAI, May 2022

The Chair on the Legal and Regulatory Implications of Artificial Intelligence

The Chair on the Legal and Regulatory Implications of Artificial Intelligence is part of the Multidisciplinary Institute in Artificial Intelligence (MIAI) established at Grenoble Alpes University in France. Its objective is to analyse the legal and regulatory questions raised by artificial intelligence and to contribute to the national, European and international debates on these issues.

The Chair has been built upon the highly successful interdisciplinary network created within the Grenoble Alpes Data and CyberSecurity Institutes. Its members are experts in law, economics, security, computer and data science, all actively working in the fields of data protection, privacy, cybersecurity and AI. They collaborate actively with and provide expert advice to major national, European and international institutions.

The Chair's work can be found on its website: AI-Regulation.Com.

THANKS TO THE FOLLOWING INSTITUTIONS FOR THEIR SUPPORT:

