Frontex and interoperable databases

Knowledge as power?

statewatch

About this report

Authors: Chris Jones, Romain Lanneau, Yasha Maccanico

Published by *Statewatch*, February 2023

This report is based on an analysis of relevant EU law, policy, other official documentation and open sources. It was produced as part of the project ‘Building the biometric state - EU agencies and interoperable databases’, supported by *Privacy International*.

Images:

- p.4: Not4rthur, CC BY-SA 2.0, https://www.flickr.com/photos/pierrotcarre/4450487354/
- p.6: Frontex
- p.21: Erica Fischer, CC BY 2.0, https://www.flickr.com/photos/walkingsf/8033247558/

About Statewatch

Statewatch produces and promotes critical research, policy analysis and investigative journalism to inform debates, movements and campaigns for civil liberties, human rights and democratic standards.

statewatch.org

(+44) (0) 203 393 8366

c/o MayDay Rooms
88 Fleet Street
London EC4Y 1DH
UK

Support our work: make a donation

Scan the QR code or visit: statewatch.org/donate

Join our mailing list

statewatch.org/about/mailing-list

Registered UK charity number: 1154784
Registered UK company number: 08480724
Registered company name: The Libertarian Research & Education Trust
Registered office: 88 Fleet Street, London EC4Y 1DH, UK.

Contents

1.Introduction

The European Border and Coast Guard Agency, Frontex, has been implicated in a number of serious scandals in recent years. Its involvement in brutal violations of fundamental rights at the Greek borders led to the resignation of the executive director, Fabrice Leggeri, and a catalogue of other serious violations has been documented.[1] An array of legal actions have been filed against the agency for violations of human rights in Greece, and a court ruling eventually forced it to halt most of its operations in Hungary.[2] It also stands accused of multiple procedural and administrative failings that undermine the rights of EU and non-EU citizens alike: there are nine open cases lodged with the European Ombudsman concerning Frontex, on top of 59 cases[3] in which decisions have already been taken.[4]

[1] Jennifer Rankin, Head of EU border agency Frontex resigns amid criticisms, 29 April 2022 The Guardian https://www.theguardian.com/world/2022/apr/29/head-of-eu-border-agency-frontex-resigns-amid-criticisms-fabrice-leggeri
Prakken d'Oliveira, EU agency Frontex charged with illegal pushbacks, 2021 https://www.prakkendoliveira.nl/en/news/news-2021/eu-agency-frontex-charged-with-illegal-pushbacks; 'Revealed: The OLAF report on Frontex',

[2] Frontex suspends operations in Hungary over asylum system, info migrants 28 January 2021: https://www.infomigrants.net/en/post/29917/frontex-suspends-operations-in-hungary-over-asylum-system. The decision to continue supporting return operations came in defiance of the opinion of the Fundamental Rights Officer expressed in a report that remained until now secret, cf. https://euobserver.com/migration/155320

[3] Figures obtained via the European Ombudsman's website, https://www.ombudsman.europa.eu/en/search-inquiries?docTypes=EODECISION&institutions=21

[4] 'EU: Legal action against Frontex's operations in Greece initiated at the European Court of Justice', *Statewatch*, 26 May 2021, https://www.statewatch.org/news/2021/may/eu-legal-action-against-frontex-s-operations-in-greece-initiated-at-the-european-court-of-justice/. The Ombudsman's investigations include one on "how the European Border and Coast Guard Agency assesses the

Many of these scandals have followed the vast expansion of the agency’s tasks and powers in 2019 that are seeing it establish a standing corps of 10,000 border guards, whilst acquiring its own surveillance equipment and vehicles. The extent of the malpractice has been so severe that the European Parliament refused to sign off Frontex’s 2020 budget.[5] Nevertheless, the agency continues to participate in human rights violations, for example through its partnership with the so-called Libyan Coast Guard. Frontex plays a direct role in assisting interception operations at sea by sharing surveillance imagery and information that leads to people being taken back to mistreatment and abuse in Libya.[6]

At the same time as the agency’s growing operational powers and exposure of its involvement in violence and violations have dominated headlines and political debate, the agency has quietly been assigned new powers to obtain, access and use personal data in its operations. These developments have not gone entirely unnoticed. The “Personal Data for Risk Analysis” (PeDRA) project, launched jointly with Europol, sought to use data collected by Frontex from “debriefing” interviews with migrants[7] to feed Europol’s databases and analyses. In the face of opposition from its own data protection officials, Frontex sought to gather genetic data and data on sexual orientation, and to gather information not just from people suspected of involvement in criminal activities, but from victims and witnesses as well.[8] Press coverage was followed by criticism from the European Data Protection Supervisor[9] and MEPs,[10] and the project was put on hold.[11]

It is also well-established that Frontex has considerable interest in developing and deploying new technologies. It has sponsored research on the use of artificial intelligence for border controls, “technology foresight on biometrics for the future of travel,” and “Weak Signals in

potential human rights risk and general impact before providing assistance to non-EU countries to develop surveillance capabilities.”

[5] Nikolaj Nielsen, 'Slap in the face': European Parliament refuses to endorse Frontex budget, EU Observer, 18 October 2022https://euobserver.com/migration/156299

[6] Arthur Carpentier, Marceau Bretonnier et Cellule Enquête vidéo, ‘Des appareils de surveillance de Frontex sont utilisés par les gardes-côtes libyens pour intercepter illégalement des migrants’, *Le Monde*, 23 November 2022, https://www.lemonde.fr/international/article/2022/11/23/enquete-comment-des-appareils-de-surveillance-de-frontex-sont-utilises-par-les-gardes-cotes-libyens-pour-intercepter-illegalement-des-migrants_6151323_3210.html; Matthias Monroy, ‘WhatsApp to Libya: How Frontex uses a trick to circumvent international law‘, *Security Architectures in the EU*, 8 October 2021, https://digit.site36.net/2021/10/08/whatsapp-to-libya-how-frontex-uses-a-trick-to-circumvent-international-law/

[7] Cova Bachiller López and Fran Morenilla, ‘Questioning the interviewers: Frontex’s covert interrogations at the Spanish southern border’, *Statewatch*, 3 August 2022, https://www.statewatch.org/analyses/2022/questioning-the-interviewers-frontex-s-covert-interrogations-at-the-spanish-southern-border/

[8] Statewatch, Document collection: Frontex and "operational personal data", https://www.statewatch.org/observatories/frontex/document-collection-frontex-and-operational-personal-data/

[9] ‘Exchange of personal data between Frontex and Europol - Wojciech Wiewiórowski’, 8 November 2022, https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/2022-11-08-exchange-personal-data-between-frontex-and-europol-wojciech-wiewiorowski_en

[10] Luděk Stavinoha, Apostolis Fotiadis and Giacomo Zandonini, ‘Frontex tripped in plan for intrusive surveillance of migrants’, Balkan Insight, 7 July 2022, https://balkaninsight.com/2022/07/07/eus-frontex-tripped-in-plan-for-intrusive-surveillance-of-migrants/

[11]Apostolis Fotiadis and Luděk Stavinoha, ‘European Parliament scrutinises Frontex surveillance programme after BIRN investigation’, Balkan Insight, 7 November 2022, https://balkaninsight.com/2022/11/07/european-parliament-scrutinises-frontex-surveillance-programme-after-birn-investigation/

Border Management and Surveillance Technologies", [12] as well as having a role in influencing EU security research priorities.[13] It is both politically committed and legally obliged[14] to ensure the use of advanced technologies for border surveillance and control.

Many of those technologies will rely upon novel ways to harvest and use the personal data of migrants, refugees and other people travelling to the EU, and many of them will be developed on the basis of existing databases and technical systems. This briefing elucidates those systems – in particular, the EU's large-scale policing and immigration databases – and explains the types of data they hold, what Frontex is able to access, the reasons for doing so, and what the agency can do with that data. It divides the agency's use of data into two forms (operational and statistical) and provides an overview of the agency's role in the EU's emerging "travel intelligence" architecture. It aims to inform understanding, analysis and critique of the agency and its role, with a view to making it possible to better understand, engage with and challenge future developments in this area.

[12] 'Artificial intelligence-based capabilities for the European Border and Coast Guard', 26 March 2021, https://frontex.europa.eu/media-centre/news/news-release/artificial-intelligence-based-capabilities-for-european-border-and-coast-guard-1Dczge; 'Frontex publishes technology foresight on biometrics for the future of travel', 21 October 2022, https://frontex.europa.eu/future-of-border-control/eu-research/news-and-events/frontex-publishes-technology-foresight-on-biometrics-for-the-future-of-travel-us6C6v; 'Weak Signals in Border Management and Surveillance Technologies', 2022 https://publications.jrc.ec.europa.eu/repository/handle/JRC128871

[13] Frontex, 'Frontex to provide border security expertise to European Commission's research projects', 6 February 2020, https://frontex.europa.eu/media-centre/news/news-release/frontex-to-provide-border-security-expertise-to-european-commission-s-research-projects-ZrCBoM

[14] Article 3(1)(j), Regulation (EU) 2019/1896, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32019R1896

2.Interoperable EU databases

While EU institutions have been discussing the possibility of “interoperability” between justice and home affairs databases since the early years of the 21st century,[15] it was not until 2016 that concrete plans were put in motion. The European Commission framed a series of terrorist attacks and the arrival of over one million refugees as security threats that required the creation of a comprehensive digital identity architecture for non-EU nationals.[16] This was to be achieved by interconnecting existing databases and setting up new ones, to close “information gaps” and “blind spots”[17] – a framing that provides a continual justification for expanding surveillance and data collection schemes. Nearly seven years later, those plans are in full swing and new elements are continuously being added,[18] demonstrating that the

[15] European Commission, ‘Communication on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs’, Council document 5122/05, 29 November 2005, https://www.statewatch.org/media/documents/interoperability/interoperability/Unsorted/council/eu-council-interoperability-15122-05.pdf

[16] “In the past three years, the EU has experienced an increase in irregular border crossings into the EU, and an evolving and ongoing threat to internal security as demonstrated by a series of terrorist attacks.” See: European Commission, COM(2017) 794 final, 12 December 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0794

[17] European Commission, ‘Stronger and Smarter Information Systems for Borders and Security’, COM(2016) 205 final, 6 April 2016, https://www.statewatch.org/media/documents/interoperability/interoperability/commission/eu-com-205-communication-on-stronger-and-smart-borders-06-04-16.pdf

[18] ‘European police facial recognition system must be halted, warns new paper’, *Statewatch*¸ 7 September 2022, https://www.statewatch.org/news/2022/september/european-police-facial-recognition-system-must-be-halted-warns-new-paper/; ‘EU: Tracking the Pact: Access to criminal records for “screening” of migrants’, *Statewatch*¸ 26 July 2022,

existing architecture is not an end in itself but a building block for more comprehensive systems of surveillance and control.

The core elements of the EU's interoperability architecture are:

- the **European Search Portal** (ESP, granting a user the ability to make simultaneous searches of any database(s) to which they have access);
- the **Shared Biometric Matching System** (sBMS, facilitating biometric searches across the interconnected systems);
- the **Multiple Identity Detector** (MID, which will be used for the automated detection of suspected false or fraudulent identities, through the large-scale comparison of "identity data"); and
- the **Common Identity Repository** (CIR, a new centralised database that will hold "identity data" from each of the underlying systems, bar the Schengen Information System: identity data consists of name, nationality, date of birth, sex/gender, fingerprints, facial image, and travel document information).

These are to be used to interconnect data from, and facilitate access to:

- the **Entry/Exit System**: to monitor the dates, places and times at which temporary visitors (e.g. tourists, businesspeople or visa holders) enter and exit the Schengen area. The system will automatically calculate the amount of time they are permitted to stay and issue automatic alerts to national authorities on individuals who stay longer than permitted, with the aim of having them removed from the Schengen area;
- **Eurodac**: established as a database of asylum-seekers' fingerprints and used for determining the EU member state responsible for an asylum application, it is now being turned into "a common European database to support EU policies on asylum, resettlement and irregular migration";
- the **European Criminal Records Information System on Third-Country Nationals** (ECRIS-TCN): contains information on non-EU nationals who have been convicted in one or more EU member states, in order to make it easier for national authorities to find information on convictions handed down elsewhere in the EU;
- the **European Travel Information and Authorisation System** (ETIAS): to ensure the vetting of citizens of countries who do not currently require a visa to enter the Schengen area - for example the UK, USA, Canada, Japan, multiple Latin American states, Ukraine and others;
- the **Schengen Information System** (SIS): a database containing alerts on third-country nationals refused entry into or stay in the Schengen area, individuals subject to deportation, and persons or objects sought for police or judicial purposes; and
- the **Visa Information System** (VIS): aids implementation of the common visa policy by storing data on all short-stay Schengen visa applicants, as well as long-stay visas and residence permits that have been issued.

A further crucial element in the interoperability architecture is the new **Central Repository for Reporting and Statistics** (CRRS), which is discussed in more detail below.

https://www.statewatch.org/news/2022/july/eu-tracking-the-pact-access-to-criminal-records-for-screening-of-migrants/

3.Frontex and interoperable databases

Increasing efforts to digitise the EU's borders have come at the same time as Frontex has been granted extended powers and tasks, including through access to databases. This access comes in two forms: operational and statistical.

Its operational access to data concerns the access needed by the agency to carry out operational tasks. Access to large-scale EU databases makes it possible for members of Frontex "teams" (see further below) to carry out border control or deportation tasks: for example, checking the validity of a person's visa at a border crossing (the Visa Information System), or establishing whether a removal notice has been handed down against an individual by national authorities (the Schengen Information System).

The law governing the agency has long included general provisions that require member states hosting operations to ensure Frontex team members have access to EU and national databases. In recent years, with the adoption of a swathe of new laws to create and upgrade EU policing and immigration systems, some specific legal provisions have been introduced governing Frontex's operational access to data. The agency is also responsible for operating the Central Unit of the European Travel Information and Authorisation System (ETIAS), giving it a key role in the EU's emerging "travel intelligence" architecture.

While the potential effects of the agency's operational use of data are fairly obvious (approval or denial of entry, enactment of deportation, and so on), the effects of the use of statistical data are more obscured, yet at the same time potentially further-reaching. Since its very inception, one of Frontex's key tasks has been "risk analysis".[19] In the words of the agency itself:

> *"Risk analysis is the starting point for all Frontex activities, from high level strategic decision-making to planning and implementation of operational activities… The agency's risk analysis is used to advise high level decision-making as well for daily coordination of joint operations."*[20]

This is presented as a relatively scientific, neutral activity. A "wide range of data" is collected to help identify "risks" to EU border security,[21] including on border crossings, visa applications, asylum proceedings and so on. This data is subsequently analysed in order to decide upon an appropriate response to different migratory dynamics. This response may come from Frontex itself, or the agency may make recommendations to national or EU policy-makers and officials. It is therefore important to understand what is considered a risk (and what is not), and the ways those risks are then analysed and understood. In recent years, a growing critical academic literature has pointed to the gendered, racialized and militarised underpinnings of Frontex's risk analysis process.[22] Through access to statistical data from large-scale EU databases, the agency will have access to vast new pools of information to be used in this process.

It should be noted that EU rules on data protection apply to Frontex,[23] and the law governing the agency includes a number of more specific measures.[24] Evidently, Frontex's desire to be seen as a crime-fighting agency has led it to try to circumvent those rules, making clear the need for stringent internal and external supervision of the agency's personal data processing.[25] The increasingly extensive use of data handed over by travellers, and received from national authorities, Europol and potentially non-EU states raises serious issues in relation to privacy, data protection, the right to claim asylum and a host other rights, in particular in light of the declared aim to deploy AI 'solutions' at the EU's borders. At the same time, many of the data processing powers granted to the agency in recent years clearly fit squarely within the law. The issue in that case, then, is not what the law forbids, but what it permits.

3.1. Operational data

[19] Article 2(1)(c), Regulation 2007/2004, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004R2007

[20] 'Situational awareness and monitoring', *Frontex*, undated, https://frontex.europa.eu/we-know/situational-awareness-and-monitoring/monitoring-risk-analysis/

[21] Ibid.

[22] Saskia Stachowitsch and Julia Sachseder, 'The gendered and racialized politics of risk analysis. The case of Frontex', Critical Studies on Security, 7(2), 31 July 2019, https://www.tandfonline.com/doi/full/10.1080/21624887.2019.1644050

[23] Regulation (EU) 2018/1725, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32018R1725

[24] 'SECTION 2 – Processing of personal data by the European Border and Coast Guard', Regulation (EU) 2019/1896, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32019R1896#d1e6181-1-1

[25] 'Document collection: Frontex and "operational personal data"', *Statewatch*, https://www.statewatch.org/observatories/frontex/document-collection-frontex-and-operational-personal-data/

Frontex is able to deploy three types of "team" that have access, through various means, to information held in the EU's large-scale policing and immigration databases. These are made up of staff that are part of its "standing corps" of border guards:

- Border management teams are "deployed during joint operations at the external borders and rapid border interventions in Member States and third countries";[26]
- Migration management support teams are "teams of experts which provide technical and operational reinforcement to Member States, including at hotspot areas, composed of operational staff, experts from the European Asylum Support Office (EASO) [now the EU Agency for Asylum, EUAA] and Europol and, where relevant, experts from the European Union Agency for Fundamental Rights (FRA), other Union bodies, offices and agencies and Member States";[27]
- Return teams are "deployed during return operations, return interventions in Member States or other operational activities linked to the implementation of return-related tasks".[28]

As well as the activities specified in the legislation (such as "return interventions"), teams can also be deployed in "any other relevant operational activities in the Member States or in third countries."[29] Wherever and however they are deployed, they may be given access to EU and national databases.

3.1.1. Entry/Exit System

The Entry/Exit System (EES) will be used to monitor the dates, places and times at which temporary visitors (e.g. tourists or businesspeople) enter and exit the Schengen area. The system will automatically calculate the amount of time an individual is allowed to stay in the Schengen area and issue automatic alerts to national authorities on individuals who stay longer than permitted, with the aim of having them removed from the Schengen area (whether via deportation or "voluntary return").

The EES legislation does not specifically regulate operational access to data by Frontex teams. However, the Frontex Regulation stipulates that those teams may be granted access to national and EU databases as deemed necessary:

> *"...the host Member State shall authorise members of the teams to consult Union databases, the consultation of which is necessary for fulfilling operational aims specified in the operational plan on border checks, border surveillance and return, through their national interfaces or another form of access provided in the Union legal acts establishing such databases, as applicable. The host Member State may also authorise members of the teams to consult its national databases where necessary for the same purpose."*[30]

[26] Article 2(18), Regulation 2019/1986

[27] Article 2(19), Regulation 2019/1896

[28] Article 2(29), Regulation 2019/1896

[29] Article 54(2), Regulation 2019/1896

[30] Article 82, Regulation 2019/1896

3.1.2. Eurodac

Eurodac was established as a database of asylum-seekers' fingerprints, used for determining the state responsible for an asylum application. For example, if an individual had their fingerprints taken in Italy, but then left the country and was later apprehended by the French authorities, they could face removal to Italy to have their asylum application processed.

A proposal currently under negotiation will expand the system's purpose and thus the number of individuals whose data is stored, turning Eurodac into "a common European database to support EU policies on asylum, resettlement and irregular migration."[31] More specifically, the revamped Eurodac will be used to store data on undocumented individuals apprehended by the authorities, with the aim of facilitating their deportation. The age limit for data storage will also be lowered (from 14 to six) and the amount of data to be stored will be increased massively: whereas at the moment the system only holds an individual's fingerprints, in the future it will also be used to store facial images, names, nationality, travel document information (where available) and more.

Eurodac is used to process data on the following groups:

- individuals who have lodged an application for international protection in the member states (data is stored in the database);
- individuals apprehended in connection with irregular border-crossings (data is stored in the database);
- third-country nationals or stateless persons found irregularly staying in a Member State (currently, data is compared against the database, but not stored – under the new proposal, this data will be stored); and
- individuals disembarked following a search and rescue operation (a new category introduced by the 2020 proposal).

Currently, the legislation governing Eurodac does not specifically mention access by Frontex or members of its teams, although they may be granted access via a host member state in accordance with the Frontex Regulation. The 2020 Eurodac proposal, which is still under negotiation, contains specific provisions allowing members of Frontex teams to take biometric data from applicants for international protection[32] and "individuals apprehended in connection with the irregular crossing of an external border,"[33] and to transmit that data to the Eurodac Central System.

3.1.3. European Travel Information and Authorisation System (ETIAS)

Once the ETIAS enters into operation, citizens of countries who do not currently require a visa to enter the Schengen area - for example the UK, USA, Canada, Japan, multiple Latin American states, Ukraine and others - will have to pay a fee and file a digital "travel authorisation" application to do so. That application will be stored at the ETIAS Central Unit,

[31] 'Amended proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the establishment of 'Eurodac' for the comparison of biometric data', COM(2020) 614 final, 23 September 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0614

[32] COM(2020) 614 final, Article 10

[33] COM(2020) 614 final, Article 13

operated by Frontex, and may also be viewed by officials in one of the member states, each of which will operate an ETIAS National Unit.

Frontex has a key role in the functioning of ETIAS, through responsibility for the Central Unit (see section 4), but the legislation does not specifically govern access by the agency for use in border checks or other tasks carried out by Frontex teams. However, as with Eurodac, access may be granted by a host member state in accordance with a given operational plan.

3.1.4. Schengen Information System

The SIS contains millions of alerts on missing and stolen objects, wanted persons, individuals subject to discreet surveillance and checks, and individuals barred from entering the Schengen area.[34] It is the world's largest law enforcement database and under legislation agreed in 2018 it is set to get even larger.

The 2018 rules expand the types of information that will be held in the system (to include all deportation decisions issued by national authorities), the types of check that can be carried out by officials (new "inquiry checks" provide a basis for the questioning of individuals) as well as the types of data to be held in the system (for example, DNA profiles on "missing persons who need to be placed under protection" can now be stored[35]). Europol also now has the power to propose that member states add "information alerts" to the system, based on data received from non-EU states' police or intelligence agencies.[36]

Data stored in the SIS can be accessed by Frontex teams "insofar it is necessary for the performance of their task and as required by the operational plan for a specific operation. Access to data in SIS shall not be extended to any other team members."[37] Due to the EU's convoluted legal architecture, the legislation on the database is governed by three separate sets of rules, covering border checks, return, and police and judicial cooperation. Access by Frontex teams is regulated by provisions in each of the three regulations. Alerts for police and judicial cooperation purposes are checked at the EU's borders along with those on refusal of entry and stay (covered by the border checks rules) and deportation (return).

To access the SIS, Frontex is obliged to establish a "technical interface" that "shall allow direct connection to Central SIS." In April 2021, the agency awarded a €5 million contract to establish the interface, known as 'A2SISII', to two companies that have had extensive dealings with the EU's digital infrastructure for policing and immigration: *Sopra Steria* and *Idemia Identity and Security*.[38] The contract award notice foresees access to the SIS for Frontex team members via a web or mobile application, and notes that the contractors should "provide changes to its [A2SISII's] functionalities and to the underlying technical

[34] eu-LISA, 'SIS II 2021 annual statistics', March 2022, https://www.eulisa.europa.eu/Publications/Reports/SIS%20II%20-%202021%20Statistics.pdf

[35] Article 32(1)(a), Regulation (EU) 2018/1862, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1862

[36] 'New Europol rules massively expand police powers and reduce rights protections', *Statewatch*, 10 November 2022, https://www.statewatch.org/news/2022/november/new-europol-rules-massively-expand-police-powers-and-reduce-rights-protections/

[37] Article 50(1), Regulation (EU) 2018/1862, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1862

[38] 'Funds for Fortress Europe: spending by Frontex and eu-Lisa', *Statewatch*, 28 January 2022, https://www.statewatch.org/analyses/2022/funds-for-fortress-europe-spending-by-frontex-and-eu-lisa/

infrastructure in response to changing legal, political, organizational or technical environments."[39]

Any search in the SIS by a member of a team that "reveals the existence of an alert" should be notified to the member state that issued the alert, and team members "shall only act in response to an alert in SIS under instructions from and, as a general rule, in the presence of border guards or staff involved in return-related tasks of the host Member State in which they are operating." However, team members can be authorised to act on behalf of the host member state.

The legislation also includes specific data protection and security provisions that apply to Frontex. The agency is obliged to ensure logging of every access to and search of the SIS by team members, has to apply measures for data security, confidentiality and self-monitoring, and its use of the SIS should be monitored by the European Data Protection Supervisor. The Frontex Regulation also includes an explicit provision prohibiting the connection of any part of SIS:

> *"…to any system for data collection and processing operated by the teams referred to in paragraph 1 or by the European Border and Coast Guard Agency, nor shall the data in SIS to which those teams have access be transferred to such a system. No part of SIS shall be downloaded or copied."*[40]

3.1.5. Visa Information System

The Visa Information System (VIS) allows the storage and exchange of visa data between EU and Schengen member states. It holds data and decisions relating to applications for visas (short-stay and long-term) and residence permits for the Schengen Area. The system can perform biometric matching, (currently only of fingerprints) for identification and verification purposes.

Long-stay visas and residence permits were added to the system by amendments agreed in July 2021, which also introduced various other changes:

- the age limits for collecting biometric data from children have been lowered from 12 to six years of age;
- Visa applications will be automatically cross-checked against all other EU information systems, Europol data and Interpol data;
- an automated profiling system will be used for "screening" visa applicants to determine if they may pose a security, health or irregular immigration risk;
- visa applicants will be checked against the "watchlist" established via the ETIAS legislation;
- copies of the photo page of travel documents will be stored in the system; and
- law enforcement authorities will have more "structured" access to the VIS.

VIS is used to process data on the follow groups of people:

- individuals who have lodged an application for a short term visa;
- individuals who have lodged an application for a long-stay visa; and

[39] 'Poland-Warsaw: Framework Contract for the Development of ICT Software Solution for EBCG Team Members Access to Schengen Information System (A2SISII)', *TED*, 14 June 2021, https://ted.europa.eu/udl?uri=TED:NOTICE:295695-2021:TEXT:EN:HTML&src=0

[40] Article 40(7), Regulation 2019/1896

- individuals who have lodged an application for a residence permit.

Applications may also hold data on individuals related to the applicant (either by family, business or other ties) whose names are mentioned in the application form.

The most recent amendments to the VIS Regulation, approved in July 2021, add specific powers for members of Frontex teams to make use of the VIS for the purposes of:

- border checks, for the purposes of "verification at the external border crossing points";
- "verifying whether the conditions for entry to, stay or residence on the territory of the Member States are fulfilled"; and
- return, for "identifying any person that does not or no longer fulfils the conditions for the entry to, stay or residence on the territory of the Member States".[41]

The agency is required to "designate a specialised unit with duly empowered European Border and Coast Guard officials as the central access point" through which members of the teams can access VIS data. The central access point is responsible for ensuring that the conditions for access are fulfilled. Unlike with the SIS, it does not appear that any contractors have been brought in to establish a technical interface between Frontex and the VIS, although it may simply be that this process has not yet begun.

To access VIS data, members of the teams must submit a request to the central access point and cite the relevant operational plan. The member state hosting the team in question must have authorised members to consult the VIS "in order to fulfil the operational aims specified in the operational plan," and consultation of the VIS must be "necessary for performing the specific tasks entrusted to the team by the host Member State." As with other large-scale EU databases, members of the teams must only "act in response to information obtained from the VIS… under instructions from and, as a general rule, in the presence of border guards or staff involved in return-related tasks" of the host member state. However, team members can be authorised to act on behalf of the host member state.[42]

There is one particular type of data in the VIS that Frontex teams are prohibited from accessing: that concerning "persons who have held valid residence permits recorded in the VIS… for a period of 10 years or more without interruption."[43]

Provisions equivalent to those concerning the SIS are included with regard to informing the host member state when searches "reveal the existence of data recorded in the VIS"; the logging of data processing operations, access and searches; data security; and the requirement for Frontex not to connect the VIS to any other system that it operates, or to download data.[44] The European Data Protection Supervisor is responsible for external supervision of Frontex's use of the VIS.[45]

3.2. Statistical data

Statistics is the fundamental science of the state: the word 'statistics' comes from the word 'state', and was brought into popular usage in the mid-1700s by German political scientist Gottfried Aschenwall. By the 1770s it was considered to mean "science dealing with data

[41] Article 45f(5), Regulation 2021/1152

[42] Article 45f, Regulation 2021/1152

[43] Article 6(2f), Regulation 2021/1152

[44] Article 45f(6)-(10), Regulation 2021/1152, on logs see also Article 34.

[45] Article 42, Regulation 2021/1152

about the condition of a state or community," before today's more general interpretation became popularised in the 1820s.[46]

At root, then, statistics is about the collection of data by public authorities in order to better understand a given situation and, in response, to formulate or influence policies to better exercise control. The nature of statistical work also relies on the continuous production of categories and constituencies of people who are often hierarchically ordered, giving rise to the possibility of various discriminatory practices and effects. Alongside the operational data that is to be made available through the EU's interoperable databases, there will also be a vast increase in the amount of statistics that are generated.

In its proposal to expand the Eurodac database, the European Commission gave an explicit example of what new statistical powers could be used for. Knowing how many people holding a short-stay Schengen visa "proceeded to enter legally (and where) and then proceeded to apply for international protection (and where)" would make it possible to assess "the appropriate policy response."[47] It would not be unreasonable to assume that the "appropriate" response here would be restrictions on the issuance of visas to citizens of the country in question.

As for Frontex, its risk analysis work (like that of other EU agencies[48]) relies heavily upon the statistics and data. As noted above, the border agency describes risk analysis as "the starting point for all Frontex activities, from high level strategic decision-making to planning and implementation of operational activities."[49] One critical analysis of the process argues that it casts migrants as both "a security risk" seeking to exploit European welfare systems, at the same time as being in need of humanitarian assistance. However, this latter framing allows "Western authorities to present themselves as saviors [sic] of racialized women and children."[50] It may also be observed that its analyses serve to promote increases in the agency's own influence, resources, structures, competences and powers. Access to these vast troves of new statistical data is intended to reinforce the reach and influence of Frontex's risk analyses. There are, however, no plans in place to alter the biases underlying that work.

Statistical data is also used to inform the "vulnerability assessments" that Frontex is obliged to carry out. These are used "to assess the capacity and readiness of the Member States to face challenges at their external borders and to contribute to the [Frontex] standing corps and technical equipment pool." Where a member state does not meet recommendations made in a vulnerability assessment, they face the prospect of a disciplinary process launched by the Frontex executive director and potentially involving the Council of the EU and the European Commission.[51]

[46] 'Statistics', *Online Etymology Dictionary*, https://www.etymonline.com/word/statistics#etymonline_v_22020

[47] COM(2020) 614 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0614

[48] Joanna Parkin, 'EU Home Affairs Agencies and the Construction of EU Internal Security', *CEPS*, 21 December 2012, https://www.ceps.eu/ceps-publications/eu-home-affairs-agencies-and-construction-eu-internal-security/

[49] Frontex, 'Situational awareness and monitoring', undated, https://frontex.europa.eu/we-know/situational-awareness-and-monitoring/monitoring-risk-analysis/

[50] Saskia Stachowitsch and Julia Sachseder, 'The gendered and racialized politics of risk analysis. The case of Frontex', *Critical Studies on Security*, 7(2), 31 July 2019, https://www.tandfonline.com/doi/full/10.1080/21624887.2019.1644050

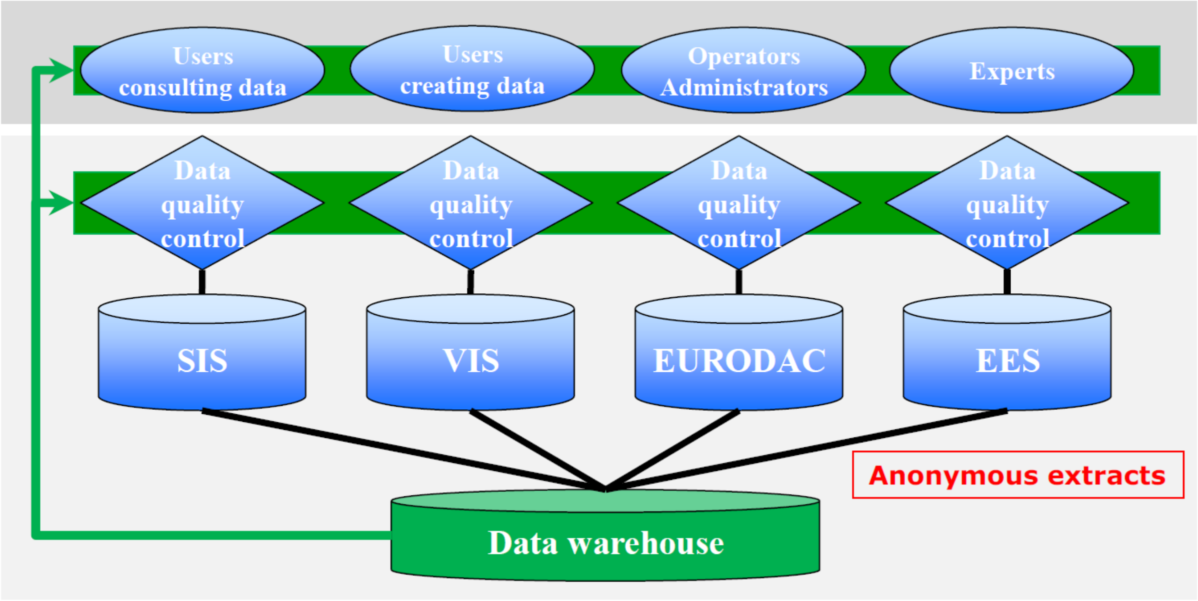
[51] Article 32, Regulation (EU) 2019/1896, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32019R1896

3.2.1. From data warehouse to central repository

One less-discussed aspect of the interoperability proposals is the establishment of a new Central Repository for Reporting and Statistics (CRRS). This was originally proposed as a "data warehouse" by the High-level expert group on information systems and interoperability, which said it would:

> *"…help Member States to make better use of the systems, including by taking informed decisions on EU policies in the area of migration and security. It would also provide valuable statistics for relevant agencies in these areas, to perform analytical reviews."*[52]

The High-Level Group provided examples of the kind of information that might be generated: the ability to profile Schengen visa "overstayers" by nationality and the EU state they first entered; the ability to work out "nationalities that enter in a different Member State than the one indicated in the visa application"; and "the distribution of fingerprint quality by Member State, authority and parent system."[53]



The "data warehouse", as envisaged by the high-level group. Source: Final report of the high-level group

The EU's agency for large-scale justice and home affairs IT systems, eu-Lisa, had in fact already been working to develop a data warehouse. In April 2016, it published a call for contractors to develop a new "Common Shared Infrastructure" that would include a data warehouse to "centralize all data from the different Core Business Systems"[54] (at that time,

[52] High-level expert group on information systems and interoperability, 'Final report', May 2017, p.12, https://www.statewatch.org/media/documents/news/2017/may/eu-com-hleg-info-systems-interoperability-final-report-5-17.pdf

[53] Ibid.

[54] eu-LISA, 'Common Shared Infrastructure – CSI (Restricted Call for tender No. LISA/2016/RP/01)', 6 April 2016, https://www.eulisa.europa.eu/Procurement/Tenders/LISA%202016%20RP%2001%20CSI/Invitation%20to%20submit%20candidatures%20LISA-2016-RP-01.pdf

Eurodac, the SIS and the VIS). The aim was to implement the system from 2017 onwards.[55] A "Central Repository for Reporting and Statistics focus group," hosted by eu-Lisa, started meeting in April 2018 after "the JHA Agencies group on Interoperability expressed particular interest in the future possibilities for improved statistical analysis that could be offered through interoperability."[56]

The Commission's initial interoperability proposals were published in December 2017. These called for "the establishment of a data warehouse (here presented as the central repository for reporting and statistics (CRRS))." It was described as:

> *"…necessary to enable the creation and sharing of reports with (anonymous) statistical data for policy, operational and data quality purposes. The current practice of gathering statistical data only on the individual information systems is detrimental to data security and performance and it does not enable the correlating of data across systems."*[57]

The plan duly made it into the final legislation, which was approved in May 2019.[58]

EU agencies are clearly excited about the opportunities that will be provided by the CRRS. The final report of the Europol-Frontex Future Group on travel intelligence[59] noted that Europol, Frontex and what is now the EU Asylum Agency[60] had "stressed repeatedly the importance of the future CRRS as a critical source of high-quality data for risk management."[61] Looking ahead, the report proposed the possibility of a "joint analysis capability" that:

> *"…could leverage the full potential of the CRRS as a data source for analytical purposes and develop appropriate analytical tools for risk assessment with the support of AI. The perspectives and information from other authorities such as customs, as well as public health authorities… could be taken into account and cooperation with analytical teams in Third Countries' National Targeting Centres would also be facilitated."*[62]

[55] 'eu-LISA, 'Single Programming Document 2017-2019', undated, 2016-110 REV 2, p.103, https://www.statewatch.org/media/documents/news/2017/mar/eu-lisa-single-programming-document-2017-2019.pdf

[56] eu-Lisa, 'First meeting of the Central Repository for Reporting and Statistics focus group', 24 April 2018, https://www.eulisa.europa.eu/Newsroom/News/Pages/Central-Repository-for-Reporting-and-Statistics.aspx

[57] European Commission, 'Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration)', COM(2017) 794 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0794

[58] Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32019R0817; Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32019R0818

[59] 'Final Report Future Group on Travel Intelligence and Border Management', 3 March 2022, https://www.statewatch.org/news/2022/august/eu-police-plans-for-the-future-of-travel-are-for-a-future-with-even-more-surveillance/

[60] At the time, it was the European Asylum Support Office.

[61] 'Final Report Future Group on Travel Intelligence and Border Management', Council document 6767/22, 3 March 2022, p.59, https://www.statewatch.org/news/2022/may/eu-agencies-propose-a-european-system-for-traveller-screening-that-could-include-ai-technology/

[62] Ibid., p.65

Furthermore, the report noted, the future collection of Passenger Name Record (PNR) and Advance Passenger Information (API) data through a single "EU Gateway" would generate further statistics "on travel to or from the Schengen area or the EU, which has an invaluable analytical potential."[63] Under current plans to expand the Prüm system[64] and the collection of API data,[65] eu-LISA will establish a "router" to serve as a one-stop interface for the collection and exchange of data, facilitating the future integration of other forms of data into the interoperability architecture and, thus, into the CRRS.

3.2.2. Content of and access to the CRRS

Implementing decisions approved in 2021 state that the data stored in the CRRS shall be "extracted from the underlying EU information systems and interoperability components" using a bespoke "technical solution".[66] Extraction will take place at least once a day and certain data items[67] must be automatically, irreversibly anonymised prior to storage in the CRRS.[68]

Alongside general reports on system availability, incidents, performance, biometric accuracy and data quality, a substantial set of more specific statistics and reports are to be produced using the CRRS with the aim of increasing the EU and member state authorities' ability to govern and control the Schengen area. While the lists detailing those statistics and reports are lengthy, they are included here to demonstrate the fine-tuned information that officials in the European Commission, EU agencies and national authorities are seeking.

The legislation also gives EU agencies and national authorities the power to generate or request specific reports tailored to their own requirements. For example, Frontex will have direct access to data held in the CRRS that has been extracted from the SIS,[69] the EES[70] and the VIS.[71] The ETIAS Central Unit, which is operated by Frontex, will have access to data drawn from across the different databases, "to improve the assessment of the security, illegal immigration and high epidemic risks," enhance border checks and inform the

[63] Ibid., p.69

[64] 'European police facial recognition system must be halted, warns new paper', *Statewatch*, 7 September 2022, https://www.statewatch.org/news/2022/september/european-police-facial-recognition-system-must-be-halted-warns-new-paper/

[65] COM(2022) 719 final, 13 December 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0729; COM(2022) 731 final, 13 December 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0731

[66] Article 5, Commission Delegated Regulation (EU) 2021/2223 of 30 September 2021 supplementing Regulation (EU) 2019/817 of the European Parliament and of the Council with detailed rules on the operation of the central repository for reporting and statistics, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021R2223

[67] Those items are referred to as being "critical identity data", which "means any of the following data or a combination thereof, from which individuals can be identified: (a) name, first name, surname, family name, given names, alias of any person whose data may be stored in any EU information system; (b) number of travel document; (c) address (street name, house number); (d) telephone, IP address; (e) email addresses; (f) biometric data."

[68] Article 5, Commission Delegated Regulation (EU) 2021/2223

[69] Article 16 of Regulation (EU) 2018/1860 (deportations); Article 60, Regulation (EU) 2018/1861 (border checks); and Article 74 of Regulation (EU) 2018/1862 (police and judicial cooperation).

[70] Article 63, Regulation (EU) 2017/2226, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R2226

[71] Article 45a, Regulation (EU) 2021/1134, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021R1134

processing of travel authorisation applications.[72] Frontex will also have access to data on the use of the European Search Portal, Common Identity Repository, and Multiple Identity Detector, "for the purpose of carrying out risk analyses and vulnerability assessments".[73] Thus, the statistics and reports listed below are far from exhaustive.

Entry/Exit System

Statistics and reports on the EES will include:

- customisable reports and statistics on entries and exits, refusals of entry and overstays of third-country nationals;
- daily statistics on overstayers, third-country nationals who were refused entry, third-country nationals whose authorisation for stay was revoked or extended and third country nationals exempt from the requirement to give fingerprints;
- reports indicating abnormal rates of overstaying and refusals of entry for a specific group of travellers; and
- customisable reports and statistics on data quality and regular statistics to ensure monitoring by eu-LISA.

Eurodac

In keeping with the plan to repurpose Eurodac as a broader, more general "migration management" database, the 2020 proposal[74] sets out a vast set of statistics and reports to be drawn from Eurodac, covering:

- the number of applicants and the number of first-time applicants whose data is stored in linked datasets (datasets are to be "linked in a sequence" when a search with fingerprints leads to a 'hit' against another dataset(s), enabling the creation of timelines of individuals' movements and thus providing investigative capabilities);
- the number of applicants rejected due to the linking process;
- the number of data sets transmitted on applicants for international protection, third-country nationals or stateless persons apprehended in connection with irregular border crossing, "illegally" staying third-country nationals or stateless persons, and third-country nationals or stateless people disembarked following search and rescue operations;
- in relation to each of those groups, the number of hits related to persons:
    - for whom an application for international protection was registered who have subsequently lodged an application for international protection in the same or another member state;
    - who were apprehended in connection with the irregular crossing of an external border;
    - who were found illegally staying in a member state; and

[72] Article 84, Regulation (EU) 2018/1240, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32018R1240

[73] Article 62, Regulation (EU) 2019/818, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32019R0818

[74] Due to ongoing negotiations on the Eurodac Regulation at the time the interoperability rules were under negotiation, the interoperability rules do not yet cover the Eurodac database. The Eurodac proposal: Amended proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the establishment of 'Eurodac', https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0614

    - who were disembarked following a search and rescue operation;
- the number of fingerprint datasets that did not meet quality requirements and so had to be submitted to the Central System more than once;
- the number of data sets marked, unmarked, blocked and unblocked (e.g. when an individual has been granted international protection);
- the number of hits for persons granted international protection or who were "illegally" staying but were subsequently granted a residence permit for whom hits have been recorded regarding:
    - rejection on the basis of linked datasets;
    - who lodged an application for international protection after being apprehended in connection with an irregular border crossing;
    - who were apprehended in connection with an irregular border crossing and had previously lodged an application for international protection;
- the number of national law enforcement agency access requests and hits;
- the number of Europol access requests and hits;
- the number of requests made for access to, rectification and erasure of personal data; and
- the number of false fingerprint matches generated by the Central System.

European Travel Information and Authorisation System

The CRRS will produce statistics and reports on:

- daily statistics on the number and nationality of applicants whose travel authorisation was issued or refused, including the grounds for refusal, and of third-country nationals whose travel authorisation was annulled or revoked;
- customisable reports and statistics to improve the assessment of security, illegal immigration and high epidemic risks, to enhance the efficiency of border checks, to help the ETIAS Central Unit and the ETIAS National Units process travel authorisation applications and to support evidence-based Union migration policy-making;
- statistical data concerning the ETIAS watchlist;
- abnormal rates of refusal of travel authorisations due to a security, illegal immigration, or high epidemic risk associated with a specific group of travellers;
- reports indicating correlations between information collected through the ETIAS application form and overstaying by travellers or refusals of entry; and
- regular statistics to ensure monitoring by eu-LISA.

European Criminal Records Information System for Third Country-Nationals

Frontex currently has no access to the ECRIS-TCN, but its officers would do so were they tasked with carrying out security checks under the forthcoming Screening Regulation.[75] The CRRS will produce statistics and reports on:

[75] 'EU: Tracking the Pact: Access to criminal records for "screening" of migrants', *Statewatch*, 26 July 2022, https://www.statewatch.org/news/2022/july/eu-tracking-the-pact-access-to-criminal-records-for-screening-of-migrants/

- the recording, storage and exchange of information extracted from criminal records; and
- reports and statistics for the purposes of technical maintenance, data quality reporting and statistics.

Schengen Information System

Deportations (“returns”), border checks and police and judicial cooperation:

- daily, monthly and annual statistics showing the number of records per category of alerts, both for each Member State and in aggregate.

Border checks and police and judicial cooperation:

- annual reports on the number of hits per category of alert, how many times the Schengen Information System was searched and how many times it was accessed for the purpose of entering, updating or deleting an alert, both for each member state and in aggregate;
- at the request of the Commission, additional specific statistical reports, either on a regular or ad hoc basis, on the performance and the use of the Schengen Information System and on the exchange of supplementary information;
- at the request of the European Border and Coast Guard Agency, additional specific statistical reports, either on a regular or ad hoc basis, for the purpose of carrying out risk analyses and vulnerability assessments;
- reports and statistics for the purposes of technical maintenance, reporting, data quality reporting and statistics; and
- data quality reports.

Visa Information System

The CRRS is to store data extracted from the VIS on the following:

- status information;
- the authority with which the application has been lodged, including its location;
- sex, age and nationality or nationalities of the applicant;
- applicant country and city of residence (visas only);
- applicant occupation (visas only);
- member state of first entry and destination (visas only);
- date and place of the application and the decision concerning the application (issued, withdrawn, refused, annulled, revoked, renewed or extended);
- type of visa or residence permit applied for or issued;
- type of the travel document and the country of issue (visas only);
- decision on application and for the decision in case of refusal, withdrawal, annulment or revocation;
- hits resulting from queries of EU information systems, Europol data, Interpol databases, or the specific risk indicators and refusal decisions based on those hits;
- the competent authority that decided on the application and the date of the decision (visas only);
- the cases in which the same applicant applied for a visa from more than one visa authority;
- main purposes of the journey (visas only);

- visa applications processed in representation;
- the data entered in respect of any document withdrawn, annulled, revoked, renewed or extended;
- expiry date of the long-stay visa or residence permit;
- the number of persons exempt from the requirement to give fingerprints;
- the cases in which fingerprints could not be provided for legal or factual reasons, and the number of cases in which a person who could not provide fingerprints was refused a visa; and
- links to the previous application file on that applicant as well as links of the application files of the persons travelling together, only as regards visas.

There is also an obligation for eu-LISA to produce quarterly and annual reports on visas and residence permits applied for and the decisions on those applications.[76]

[76] Article 45a(4) and (5), Regulation (EU) 2021/1134, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R1134

4.‘Travel intelligence’: profiling and risk assessment

In 2013, Frontex noted that developments in technology were making it possible to undertake checks of travellers “partly or in full before their arrival to the physical border.”[77] That is, the EU’s borders – and the controls on entry that go with them – could be extended far beyond their physical boundaries.

This was hardly a new phenomenon. Individuals that need a visa to travel to the Schengen area (as well as many of the world’s rich states) have long been subject to forms of remote border control, through the need to apply for a visa in person (at a consulate or embassy) combined with carrier sanctions, through which travel companies can be fined for transporting a person who does not have the correct documentation. This of course encompasses the vast majority of the world’s asylum seekers.[78]

These forms of remote control are now both extending, through their application to a far wider group of people; and intensifying, through the increased use of personal data and new technologies to undertake the automated screening and profiling of travellers. In the case of the EU, the need for government “permission to travel”[79] is being extended to citizens from visa-exempt countries, who will soon need a “travel authorisation” to enter the Schengen area. Meanwhile, those subject to visa and travel authorisation requirements will have their

[77] Frontex, ‘Border Control in the Information Age’, 26 March 2013, https://frontex.europa.eu/media-centre/news/focus/border-control-in-the-information-age-udh57L

[78] The absurdity of such a system was laid bare when the UK’s Home Secretary, Suella Braverman, was questioned by fellow Conservative MP Tim Loughton in a parliamentary committee in November 2022. A video of the exchange is available in a tweet by Andrew Connolly, 23 November 2022, https://twitter.com/connellyandrew/status/1595376648261623810

[79] ‘Government permission to travel: “Authority to Transport”’, *Papers, Please!*, 8 February 2019, https://papersplease.org/wp/2019/02/08/government-permission-to-travel-authority-to-carry/

applications automatically assessed against "screening rules" and "risk indicators". It should be noted that the EU's proposed Artificial Intelligence Act seeks to exempt the EU's large-scale databases from the safeguards that would otherwise govern AI systems categorised as high-risk. This would allow the use of these technologies without sufficient guarantees for individual rights and liberties.[80]

4.1. Profiling HQ: the ETIAS Central Unit

In order to implement these new forms of control, Frontex will host the ETIAS Central Unit, the primary objective of which is to process travel authorisations and to define the "specific risk indicators" that will be used for the profiling of travel authorisation and visa applicants.[81] When a traveller submits an application for a visa or travel authorisation, the application will be sent to the Central Unit and automatically cross-checked against a variety of databases, run through a profiling tool and checked against a 'watchlist' of persons of interest. Any "hits" must be manually reviewed by a member state ETIAS National Unit for approval or refusal; Europol may also be involved in the assessment process, depending on the type of hit.

4.2. Automated checks of EU and international databases

Automated checks will rely on the "identity data" provided by the applicant: names, nationality, date of birth, travel document information, fingerprints and facial image. Through the European Search Portal, one of the components of the interoperability architecture,[82] applications will be compared to the records, files and/or alerts registered in an array of other EU and international databases:

- Schengen Information System (SIS);
- Entry/Exit System (EES);
- Eurodac;
- European Travel Information and Authorisation System (to check for previous applications);
- European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN);
- Visa Information System (to check for previous applications);
- Data held by Europol, the EU's policing agency;
- Interpol databases:
    - Stolen and Lost Travel Documents (SLTD); and
    - Travel Documents Associated With Notices (TDAWN).

This process opens up new possibilities for error and abuse in immigration procedures: firstly, because the EU's databases are known to be strewn with errors and omissions;[83]

[80] 'Joint statement: The EU Artifical Intelligence Act must protect people on the move', *Statewatch*, 6 December 2022, https://www.statewatch.org/news/2022/december/joint-statement-the-eu-artifical-intelligence-act-must-protect-people-on-the-move/

[81] Article 7, Regulation (EU) 2018/1240

[82] See 'European Search Portal' in the interactive map 'EU agencies and interoperable databases', https://www.statewatch.org/eu-agencies-and-interoperable-databases/

[83] Fundamental Rights Agency, 'Under watchful eyes', 2018, pp.81-98, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf

secondly, because both Interpol's databases and the EU's own systems are potential targets for abuse by repressive states wishing to pursue dissidents and opponents abroad.[84]

With regard to Interpol, the misuse of the SLTD database, in particular by the Turkish authorities, has been well-documented: officials report an individual's Turkish passport as lost or stolen, and when that individual attempts to travel using the document, they are prevented from doing so.[85] Interpol's 'red notice' system has also been misused by a variety of states across the globe.[86] The red notice system is not part of the EU's interoperability architecture, although it may be checked by states at border crossings.

Similar kinds of abuse may also take place via Europol and the SIS, due to new rules that came into force in June. Europol can now propose that member states create "information alerts on third-country nationals in the interests of the Union" in the SIS. These are to be based on data shared with Europol by third states, and should relate to individuals suspected of involvement in terrorism or serious crime.[87] This raises the possibility that third states could request the insertion of data on political opponents and dissidents, turning them into persons of interest for the EU authorities.[88] Rules under discussion to upgrade the Prüm network of national police databases raise a similar problem.[89] As Frontex's deployments grow in scale and scope, it is increasingly likely that it will be a Frontex officer refusing an individual entry to the EU on the basis of such alerts.

4.3. Automated profiling

Automated profiling of all visa and travel authorisation applications will take place via algorithms: the ETIAS screening rules[90] and the VIS screening rules.[91] Those rules will be drawn up based on a variety of statistics. For the ETIAS, these will be drawn from the EES and the ETIAS itself; and for the VIS, from the EES and the VIS. Both systems will also make use of "information substantiated by factual and evidence-based elements provided by Member States," and information on epidemic diseases provided by the European Centre for Disease Prevention and Control and the World Health Organization. The Commission is

[84] Ewelien Brouwer, 'Schengen Entry Bans for Political Reasons? The Case of Lyudmyla Kozlovska', Verfassungsblog, 30 August 2018, https://verfassungsblog.de/schengen-entry-bans-for-political-reasons-the-case-of-lyudmyla-kozlovska/; Edward Lemon, 'Weaponizing Interpol', Journal of Democracy, 30(2), April 2019, pp. 15-29; Romain Lanneau, 'How a Dutch Pacifist Activist Ended up on the Europol and Interpol Terrorism Lists', Politics Today, 6 December 2021, https://politicstoday.org/how-a-dutch-pacifist-activist-ended-up-on-the-europol-and-interpol-terrorism-lists/

[85] 'Turkey's Abuse of INTERPOL: How Erdoğan Weaponized the International Criminal Police Organization for Transnational Repression', Stockholm Center for Freedom, 24 August 2021, https://stockholmcf.org/turkeys-abuse-of-interpol-how-erdogan-weaponized-the-international-criminal-police-organization-for-transnational-repression/

[86] Fair Trials, 'INTERPOL', https://www.fairtrials.org/campaigns/interpol/

[87] 'CHAPTER IXa: Information alerts on third-country nationals in the interest of the Union', Regulation (EU) 2018/1862 (consolidated version), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02018R1862-20220801#tocId50

[88] 'Empowering the police, removing protections: the new Europol Regulation', *Statewatch*, November 2022, p.30, https://www.statewatch.org/media/3615/empowering-the-police-removing-protections-new-europol-regulation.pdf

[89] 'Empowering the police, removing protections', p.32

[90] 'CHAPTER V: THE ETIAS SCREENING RULES AND THE ETIAS WATCHLIST', Regulation (EU) 2018/1240, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32018R1240#d1e3365-1-1;

[91] Preamble para. 24, Regulation (EU) 2021/1134, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R1134

obliged to adopt delegated and implementing acts to define and specify the risks in question, although it has not yet done so.[92]

The ETIAS Central Unit will then draw up the "specific risk indicators", after having consulted the ETIAS Screening Board and the VIS Screening Board. These will be based on "a combination of data including one or several" of the factors set out in the table below.

Basis for the specific risk indicators	
ETIAS	**VIS**
age range, sex, nationality	age range, sex, nationality
country and city of residence	country and city of residence
current occupation (job group)	current occupation (job group)
	the Member States of destination
	the Member State of first entry
	purpose of travel
level of education (primary, secondary, higher or none)	

The two Screening Boards will be made up of representatives from Frontex, Europol and every ETIAS National Unit (in the case of the ETIAS) and every member state (in the case of the VIS). They are to be consulted by the Central Unit on "the definition, establishment, assessment ex ante, implementation, evaluation ex post, revision and deletion of the specific risk indicators," and will meet twice a year.[93] In doing so, they should also "take into consideration" the non-binding recommendations issued by the ETIAS Fundamental Rights Guidance Board and the VIS Fundamental Rights Guidance Board.[94]

Screening Boards	
ETIAS	**VIS**
Frontex representative	Frontex representative
Europol representative	Europol representative
Representative of every ETIAS National Unit	Representative of every member state

The Fundamental Rights Guidance Boards have an "advisory and appraisal function" and will be made up of Frontex's Fundamental Rights Officer, a member of the Frontex Consultative Forum on Fundamental Rights, and representatives from the European Data Protection Supervisor, the European Data Protection Board and the Fundamental Rights

[92] All the delegated acts adopted in relation to the ETIAS Regulation are available here: https://eur-lex.europa.eu/search.html?SUBDOM_INIT=ALL_ALL&DTS_SUBDOM=ALL_ALL&DTS_DOM=ALL&DB_DELEGATED=32018R1240&lang=en&type=advanced&qid=1673343289301. The related implementing acts are available here: https://eur-lex.europa.eu/search.html?SUBDOM_INIT=ALL_ALL&DTS_SUBDOM=ALL_ALL&DTS_DOM=ALL&lang=en&type=advanced&DB_IMPLEMENTING=32018R1240&qid=1673343118890

[93] Article 9, Regulation (EU) 2018/1240; Article 9k, Regulation (EU) 2021/1134

[94] Ibid.

Agency. A representative of each Fundamental Rights Guidance Board will be invited to attend meetings of the respective Screening Board "in an advisory capacity," and shall have access to the files of the respective Screening Board.[95]

The legislation on both the VIS and the ETIAS includes the following obligation:

> *"The specific risk indicators shall be targeted and proportionate. They shall, in no circumstances, be based solely on a person's sex or age or on information revealing a person's colour, race, ethnic or social origin, genetic features, language, political or any other opinion, religion or philosophical belief, trade union membership, membership of a national minority, property, birth, disability or sexual orientation."*

It will be up to the Central Unit, the Screening Boards and the Fundamental Rights Guidance Boards to determine whether the authorities uphold this obligation. However, as noted, the Fundamental Rights Guidance Boards have no binding powers.

4.4. The ETIAS watchlist

Despite the EU already operating an extensive digital infrastructure for keeping tabs on suspected criminals, terrorists and other persons of interest – in particular via the Schengen Information System and Europol's databases – the ETIAS legislation also establishes a new "watchlist", in keeping with an international trend for such practices.[96] All visa and travel authorisation applications will be checked against the watchlist, which aims at:

> *"…identifying connections between data in an application file and information related to persons who are suspected of having committed or having taken part in a terrorist offence or other serious criminal offence or regarding whom there are factual indications or reasonable grounds, based on an overall assessment of a person, to believe that they will commit a terrorist offence or other serious criminal offences."*[97]

Europol and the member states will be responsible for adding names to the watchlist,[98] which will be based on "information related to terrorist offences or other serious criminal offences." The legislation does not specify any particular sources of information, but it is noteworthy that the EU is making substantial efforts to make it simpler to receive information from non-EU states and insert it into EU-wide databases. In this context, the information that is used to make an "overall assessment of a person" may not be entirely reliable.

Before an individual's data is added to the watchlist, the authorities must check whether it corresponds to an alert in the SIS – and if so, they should not enter the data into the list. Here, the legislation indicates the reason for the list – as a way to keep tabs on individuals for whom there is insufficient justification to enter their data in the SIS: "Where the conditions for using the data to enter an alert in SIS are fulfilled, priority shall be given to entering an alert in SIS." If those conditions are not fulfilled, their name goes in the watchlist.[99]

[95] Article 10, Regulation (EU) 2018/1240; Article 9l, Regulation (EU) 2021/1134

[96] Ramzi Kassem, Rebecca Mignot-Mahdavi and Gavin Sullivan, 'Watchlisting the World: Digital Security Infrastructures, Informal Law, and the "Global War on Terror"', *Just Security*, 28 October 2021, https://www.justsecurity.org/78779/watchlisting-the-world-digital-security-infrastructures-informal-law-and-the-global-war-on-terror/

[97] Article 34(1), Regulation (EU) 2018/1240

[98] Article 20(4), Regulation (EU) 2018/1240, Article 9a(3)(c), Regulation (EU) 2021/1134

[99] Article 35(3), Regulation (EU) 2018/1240

Europol and the member states must review entries at least once per year and remove them if they are “obsolete or not up to date”.[100] While this looks efficient on paper, it has been noted that the necessity and efficacy of watchlisting “has not been reliably established and, in practice, [watchlisting] is extraordinarily difficult to challenge.”[101]

4.5. Towards an EU travel intelligence architecture

The new systems of surveillance control being established through the ETIAS and the changes to the VIS are part of a larger picture – the development of an EU “travel intelligence” architecture. While Frontex certainly has a role in this architecture, it appears that it is largely being propelled by Europol. The policing agency describes travel intelligence as relating to “PNR [Passenger Name Record], EES, ETIAS, VIS and other relevant information management initiatives on the movements of persons and goods.”[102]

Its current work programme notes that Europol will “work with the relevant EU agencies, the European Commission and the Member States to implement its roadmaps related to travel intelligence and to EU systems interoperability,”[103] which is intended to lead to “a fully-fledged European Travel Intelligence Centre (ETIC).”[104] The ETIC will provide “concrete operational and strategic products and services on the basis of travel information and intelligence to support the Member States,” interconnect national Passenger Information Units (PIUs, responsible for processing PNR data), and step up cooperation with “private partners relevant for the collection of travel intelligence,” including by using the new powers contained in the revamped Europol Regulation.[105,106]

More information on the travel intelligence plans can be found in the final report of the Europol-Frontex Future Group on Travel Intelligence, which was made public by *Statewatch* in May 2022. This outlined the possibility of a “European System for Traveller Screening” that would incorporate data from as many sources as possible to generate information on an individual across the “EU Border and Travel Continuum” – from an individual planning to travel to the EU, crossing the border, staying within the EU, and then departing. The Future Group report notes that this would require legal changes, and may see the further incorporation of artificial intelligence technologies into the EU’s border regime.[107]

[100] Article 45(4), Regulation (EU) 2018/1240

[101] Ramzi Kassem, Rebecca Mignot-Mahdavi and Gavin Sullivan, ‘Watchlisting the World: Digital Security Infrastructures, Informal Law, and the “Global War on Terror”’, *Just Security*, 28 October 2021, https://www.justsecurity.org/78779/watchlisting-the-world-digital-security-infrastructures-informal-law-and-the-global-war-on-terror/

[102] ‘Europol Programming Document 2023-25, p.41, https://www.europol.europa.eu/publications-events/publications/europol-programming-document

[103] Ibid., p.22

[104] Ibid., p.43

[105] Ibid., p.44

[106] ‘Empowering the police, removing protections: the new Europol Regulation’, *Statewatch*, 10 November 2022, https://www.statewatch.org/publications/reports-and-books/empowering-the-police-removing-protections-the-new-europol-regulation/

[107] ‘EU: Police plans for the “future of travel” are for “a future with even more surveillance”’, *Statewatch*, 30 August 2022, https://www.statewatch.org/news/2022/august/eu-police-plans-for-the-future-of-travel-are-for-a-future-with-even-more-surveillance/

statewatch