Advanced Digital Technologies in Migration Management

Data Protection and Fundamental Rights Concerns

10.02.2025

As migration management systems across the globe increasingly adopt advanced digital technologies, new challenges emerge at the intersection of technological innovations, human rights, and data protection. From artificial intelligence (dataAI) and large-scale surveillance systems to health data monitoring tools, these technologies are transforming migration governance. While they promise efficiency and enhanced capabilities for managing complex migration dynamics, their deployment raises serious concerns about compliance with human rights and refugee law, as well as data protection standards stemming from international and EU law frameworks. This blog symposium stems from the discussions and debates held during the Workshop on *Advanced Digital Technologies in Migration Management: Data Protection and Fundamental Rights Concerns,* organized on 4 September 2024 at the 2024 ESIL Annual Conference in Vilnius, by the Interest Group on Migration and Refugee Law of the European Society of International Law (ESIL), in partnership with the Human Rights Research League (HRRL) and the CoSME (Community Sponsorship for Migrants in Europe) Project. It seeks to explore these pressing issues through contributions that critically examine specific technologies, their regulatory frameworks, and the potential risks they pose to the rights of migrants and protection seekers.

More specifically, this symposium highlights the impact of new technologies on the protection of the rights of people on the move, shedding light on the delicate balance between harnessing innovation to achieve efficiency and safeguarding human rights. By focusing on specific regulatory frameworks, the contributions in this series unpack the legal and practical challenges that arise when digital tools are integrated into migration management systems. As these technologies often operate in complex transnational and multi-stakeholder environments, the potential for rights violations – whether through biased algorithms, unlawful data processing, or inadequate safeguards – demands urgent attention. Against this background, the symposium's contributions reflect on how we can ensure that the digitalization of migration management aligns with international legal standards while fostering a regulatory environment that respects, fulfills, and protects the human rights of people on the move.

Agnese Palazzi kicks off the symposium by exploring the use of AI in asylum procedures. In particular, her contribution warns that the involvement of AI in asylum procedures, particularly in initial phases, such as the credibility assessment, may give rise to human rights and refugee law violations. From the angle of the European Union's AI Act, the author also considers the suitability of this legal instrument to protect the rights of asylum-seekers and offers some preliminary (but critical) reflections on the effectiveness of the safeguards it provides.

Irene Baceiredo-Macho then highlights the data protection concerns underpinning the European Border Surveillance System (EUROSUR), the framework for data exchange and the cooperation between Frontex and the EU Member States. This blogpost explains the key components of EUROSUR. It showcases how the exchange of information under EUROSUR and the defined purposes of the system may lead to the unlawful processing of personal data.

Finally, Francesca Tassinari concludes the symposium with an analysis of the European Travel Information and Authorisation System (ETIAS) and the concerns raised by its assessment of the high epidemic risks posed by visa-exempt third-country nationals in the EU. This post clarifies how ETIAS processes the health

data of third-country nationals and criticizes the lack of specific safeguards to protect the rights of data subjects under Article 8 of the EU Charter of Fundamental Rights.

Striking a fair balance between efficiency and protection is crucial to ensure that technological innovations make a positive contribution to migration management. But can this balance be struck without compromising the fundamental human rights protection of people on the move, particularly those crossing borders to seek asylum? This question lies at the heart of ongoing debates on the integration of advanced digital technologies in migration management. While these tools hold the promise to streamline asylum or visa procedures and enhance decision-making, they also risk reinforcing structural inequalities, perpetuating discriminatory practices, and undermining the rights of people in vulnerable situations, such as asylum seekers. Taken together, these contributions provide valuable and critical insights into the pressing legal issues surrounding the use of advanced digital technologies in migration management and invite further debate on the future of human rights and refugee law in this context.

Cite as
Sissy Katsoni, Daniela Vitiello, Giulia Raimondo & Sara Arapiles, Advanced Digital Technologies in Migration Management: Data Protection and Fundamental Rights Concerns, *Völkerrechtsblog,* 10.02.2025.

AI and Asylum in the EU Legal Framework

A Liaison Dangéreuse?

10.02.2025

In recent years, the European Union's asylum system has seen the gradual integration of AI tools aimed at streamlining certain processes optimizing workflows. Since the stakes in asylum cases are high and involve fundamental rights, careful scrutiny of AI's role in this highly sensitive area is necessary.

In response to the proliferation of AI, the European Union (EU) adopted its first legally binding AI regulation, the EU AI Act. The Act seeks to ensure that AI respects fundamental rights while promoting innovation through a risk-based approach. However, the Act leaves key questions unresolved and contains exceptions that may undermine the protection of fundamental rights in this context.

This blog post argues that the use of AI in asylum procedures, particularly in phases like credibility assessment, can disrupt the delicate procedural balance that has been carefully constructed through legal frameworks. Furthermore, it questions whether the EU AI Act, with its inherent flexibility and discretionary allowances, is the best regulatory tool to safeguard the fundamental rights of asylum seekers. This way, the contribution highlights the critical concerns raised by AI's involvement in asylum procedures and offers preliminary considerations regarding the effectiveness of the safeguards provided by the EU AI Act.

AI in EU Asylum Procedures: Enhancing or Disrupting the Procedural Balance?

The asylum procedure in the EU is complex and it is grounded in international law and European legal frameworks, including EU's constitutional law. These frameworks create a system that seeks to balance the thorough evaluation of asylum claims with the vulnerability of applicants, many of whom lack documentary evidence to support their claims.

The asylum process comprises several key stages: registering the application, conducting interviews to assess the claim's grounds, assessing available evidence, and issuing a decision. At each stage, specific legal principles are designed to create a fair and thorough process where the position of the applicant is balanced against the need for accurate decision-making. For example, the shared burden of proof between applicants and authorities [Directive 2011/95/EU Article 4(1)] ensures that decision-makers consider the inherent difficulties faced by asylum seekers. Similarly, the principle of the "benefit of the doubt" allows for flexibility when applicants cannot provide adequate documentation.

Central to this process is the interview phase, where applicants provide their personal testimonies regarding their need for international protection. Credibility assessments during this stage are critical, as asylum claims often rely heavily on personal accounts due to the lack of physical evidence. If the applicant's statements are deemed credible and aligned with the legal criteria for international protection, they may be granted refugee status or other forms of protection. As such, the assessment of credibility is a delicate and highly important aspect of the asylum process.

Despite this complexity, AI tools are increasingly being used to "enhance" specific phases of the asylum process in several EU Member States. For instance, in Germany, a Dialect Identification Assistance System (DIAS) has been in operation since 2017. DIAS analyzes phonetic patterns in applicants' speech to provide a probabilistic determination of their country or region of origin. This tool is used to supplement other

evidence in the asylum process, particularly when applicants lack identification documents. The German authorities argue that DIAS helps identify fraudulent narratives, optimizes decision-making, and facilitates the return of rejected asylum seekers.

While AI tools like DIAS offer practical benefits, their deployment in such sensitive phases of the asylum process raises significant concerns. The AI-generated analysis of dialects contributes directly to the credibility assessment, which can have profound implications for the outcome of the asylum claim. If authorities rely too heavily on AI outputs, they may undervalue other evidence or ignore the "benefit of the doubt" principle that is essential in cases where documentary proof is lacking.

Additionally, the use of AI in this context can undermine the procedural balance of the asylum system. Even without altering existing laws, AI tools like DIAS can create outcomes that shift the decision-making process toward a more data-driven, and possibly less human-centered, approach. This shift is concerning because AI systems, while advanced, are not infallible. Errors in data analysis or interpretation could result in incorrect conclusions about an applicant's origin, leading to unfair decisions with potentially life-threatening consequences for the individual concerned.

Given the impact of AI on these delicate procedures, it is imperative to ensure that AI tools deployed in asylum cases meet the highest standards of accuracy and fairness. This is where the EU AI Act comes into play, offering an opportunity to regulate the use of AI in such high-stakes environments.

To Be High-Risk, or Not to Be? Classifying AI Systems in Asylum under the EU AI Act

The EU AI Act, adopted in 2024, represents a major step forward in the regulation of AI within the EU, which had been left regulated. The Act employs a risk-based approach, classifying AI systems into four categories based on their potential harm: unacceptable risk, high risk, limited risk, and minimal risk. AI systems considered unacceptable are outright prohibited, while high-risk systems, which include those used in asylum, migration, and border management, are subject to strict regulatory requirements (Annex III, point 7). These include mandatory risk management processes, transparency measures, human oversight, and fundamental rights impact assessments.

However, the EU AI Act contains several exceptions and loopholes that could limit the effectiveness of these safeguards, depending on the classification of a system as high-risk on the one hand and, on the other hand, concerning asylum matters.

In fact, Article 6, paragraph 3, specifies that an AI system deemed high-risk should not be classified as such if it does not pose a significant risk of harm to the health, safety, or fundamental rights of individuals, including by not materially influencing the outcome of decision-making. This presumption applies where any of the three conditions established are met. Thus, when deploying an AI system within the asylum sector, it will be crucial to determine whether the system falls under the high-risk classification and, if so, to understand the ensuing impact. To do so, it will be extremely important to take into consideration the European Commission Guidelines that will be provided no later than 18 months from the date of entry into force of this Regulation after consulting the European Artificial Intelligence Board.

Moreover, the EU AI Act introduces exceptions to the strict rules for high-risk AI systems, particularly in areas like asylum, migration, and border management. Normally, providers and public authorities using high-risk systems must register them in an EU database to ensure transparency. This database is meant to be publicly accessible and easily understandable. However, for AI systems used in law enforcement, migration, asylum, and border control, the registration must be in a secure, non-public section, accessible only to the European Commission and relevant national authorities (Art. 49, par. 4, EU AI Act). This restricts transparency, with no clear reason for the limitation.

Additionally, high-risk AI systems in asylum are subject to relaxed human oversight requirements (Art.14, EU AI Act), with flexibility depending on the system's context and level of autonomy. In asylum cases, where the stakes are exceptionally high, exempting human oversight could lead to situations where AI tools operate with minimal human intervention, increasing the risk of errors or bias going unchecked.

This creates a troubling scenario where AI tools like DIAS – if classified as a high-risk system – could continue to operate without the highest standards of accountability and transparency, potentially affecting the

rights of asylum seekers. For applicants, the use of AI certainly adds an additional layer of complexity to an already complicated process, raising concerns about fairness and, more generally, about fundamental rights. If applicants are not fully informed about how AI systems are influencing decisions, they may find it difficult to challenge those decisions, further weakening their position within the asylum process and potentially challenging the right to an effective remedy and access to the right to asylum itself.

Concluding Remarks

The integration of AI into EU asylum procedures presents a double-edged sword. On the one hand, AI offers opportunities to streamline the asylum process and improve efficiency in managing large caseloads. On the other hand, the use of AI in sensitive phases like credibility assessments risks undermining the procedural balance designed to protect vulnerable individuals.

The EU AI Act is a significant regulatory step forward, but its application to asylum procedures remains fraught with uncertainty. The Act's exceptions and discretionary allowances may weaken the protection it offers, particularly concerning transparency and human oversight.

While the EU AI Act marks progress in regulating AI, its effectiveness in the asylum context will ultimately depend on how well these safeguards are enforced. Striking a balance between technological innovation and the protection of human rights is essential in ensuring that AI contributes positively to asylum procedures without compromising the fundamental rights of those seeking refuge in Europe.

Cite as
Agnese Palazzi, AI and Asylum in the EU Legal Framework: A Liaison Dangéreuse?, *Völkerrechtsblog,* 10.02.2025, doi: 10.17176/20250211-000815-0.

The Processing of Health-Related Data in the Incoming European Travel Information and Authorisation System

11.02.2025

The European Travel Information and Authorisation System (ETIAS) requires visa-exempt third-country nationals (TCNs) to complete an online application form to enter the Schengen Area for a short-stay visit. While applicants do not disclose their health status, the ETIAS is designed to assess the high epidemic risks posed by their presence in the European Union (EU). This post clarifies how the ETIAS processes TCN's health data and critiques the lack of specific safeguards to protect the data subjects' rights under Article 8 of the Charter of Fundamental Rights of the EU (CFREU).

Health Data and Its Protection under the GDPR

Health data is any personal data on an individual's physical or mental health, including past, present, and future health status. According to Article 4(15) of the General Data Protection Regulation (GDPR), data concerning health includes the information inferred from the data subject's state of health risk, irrespective of whether it is true, appropriate, or legitimate. Such information may be indirect or situational, and may include the place of residence, environment, lifestyle, work, and economic relationships. Under the GDPR Article 9(1), the processing of such data is prohibited as this might lead to stigmatisation and discrimination, notwithstanding the surrounding context and purposes pursued. In a nutshell, health data is a special category of personal data because of its inherent sensitivity, which justifies the provision of a tightened regulatory regime. However, Article 9(2) of the GDPR sets forth exceptional conditions under which this prohibition can be lifted. These exceptional conditions include public interest in the area of public health as long as the EU or national law *'provides for suitable and specific measures to safeguard the rights and freedoms of the data subject'* [let. i)]. Still, each Member State is free to provide for further conditions limiting its processing according to Article 9(4) of the GDPR.

ETIAS Screening Rules and High Epidemic Risk Indicators

As the European Data Protection Supervisor (EDPS) spotted, health data are inferred throughout the ETIAS procedure indirectly. Two different stages are relevant: 1. to elaborate the high epidemic risk indicators and test the ETIAS screening rules and 2. when an application hits the high epidemic risk indicators stored in the ETIAS Central System (C-S), or the authorisation is annulled or revoked because the conditions for the issuing were not or are no longer met (e.g. false negative hits).

The European Border and Coast Guard Agency (*rectius* the ETIAS Central Unit) is establishing risk indicators of high epidemic, combining the information transferred by the World Health Organisation on disease outbreaks, the European Centre for Disease Prevention and Control on epidemiological surveillance and communicable diseases, and the Member States on high epidemic risks posing a serious cross-border threat to health, with known parameters (age range, sex, nationality, country and city of residence, level of education, and current occupation). As long as the data that the ETIAS Central Unit is using is not anonymised, their further use [which should undergo the compatibility test of Article 6(4) of the GDPR] interferes with the individuals' right to personal data protection, that is, the right to informational self-determination. Even though defining and testing the ETIAS screening rules could be research or innovation activities, the controller (the ETIAS Central Unit and eu-LISA) should apply appropriate safeguards like pseudonymisation in line with Article 89 of the GDPR.

The ETIAS risk indicators reveal a person's health status each time the comparison triggered by a new application suggests that they pose risks of high epidemic to the benefit of the community (e.g. Article 6 of Ley 41/2002). Following a first verification performed by the ETIAS Central Unit to scrap false positive hits, the ETIAS National Unit responsible for the application may ask for additional information, like hospital invoice(s) or health and vaccination certificate(s) or it may invite the applicant for an interview. The ETIAS National Unit must decide whether to grant or not the entry, which is recorded in the TCN's application file (Article 37 of the ETIAS regulation). In case the authorisation is issued, the ETIAS National Unit may annul or revoke it as long as the initial conditions are found to have never been met or are no longer met (Articles 40 and 41 of the ETIAS regulation). Such "indirect" information counts as (sensitive) personal data whose processing could not amount to a fully automated decision as per Article 22(4) of the GDPR, unless the ETIAS is found to underpin reasons of substantial public interest by virtue of its Article 9(2) let. g).

Data Subjects' Rights and ETIAS

According to the ETIAS regulation Article 64(1), TCNs whose data are stored in the ETIAS C-S are informed about the right to access, rectify, and erase personal data at the time of their collection. At this moment, the contact details of the European Border and Coast Guard Agency and the EDPS are given. The expression used, i.e. "collection", raises doubts on whether TCNs are aware of the fact that their health data are processed since these are not gathered from the application form, but inferred from the implementation (and eventually revision) of the ETIAS screening rules [Articles 14 and 23(1) let. e) of the GDPR]. In the specific case of granting the authorisation, TCNs are expected to be informed about the processing of health data during the assessment of which the ETIAS National Unit is competent (Articles 26-32 of the ETIAS regulation). Conversely, when the authorisation is refused, annulled, or revoked, the applicant is notified about the justification sustaining the negative decision, i.e. the fact that the TCN represents a high epidemic threat, and of the possibility of appealing it according to the national law of the responsible ETIAS National Unit [Articles 37(3), 43(3), and 41(3) of the ETIAS regulation]. In addition, the notification must state the procedures for exercising the right to access, rectify, and erase personal data before the ETIAS Central Unit or to the competent National Unit [Article 64(2) of the ETIAS regulation]. Overall, the exercise of this right is designed in view of the assessment or decision taken by the ETIAS National Unit, without regard to the ETIAS screening rules whose revision is performed by the European Commission every six months according to Article 33(3) of the ETIAS regulation.

Concluding Remarks

The lack of specific rules on the processing of health-related data in the ETIAS regulation confirms that the co-legislators have not provided enhanced safeguards to regulate the processing of such a special category of personal data, as it should be. This post holds that specific safeguards must be ensured for the whole data life cycle to safeguard the exercise of data subjects' rights as long as health data are processed in the ETIAS at different stages.

This post is part of the aid JDC2022-048217-I, funded by MCIN/AEI/10.13039/501100011033 and the European Union 'NextGenerationEU'/PRTR, and the 2024 Research Project 'Aproximación ético-jurídica al tratamiento de datos de salud de inmigrantes y refugiados para fines de salud pública en la UE' (DASIR-SP) funded by the Fundación Víctor Grífols i Lucas. The author is grateful to the Völkerrechtsblog team and Prof. Dr. Nicolás Jiménez for bringing significant recommendation to this study.
Cite as
Francesca Tassinari, The Processing of Health-Related Data in the Incoming European Travel Information and Authorisation System, *Völkerrechtsblog,* 11.02.2025, doi: 10.17176/20250212-000814-0.

Under EUROSUR's Watchful Eye

Exploring the Data Protection Concerns in European Border Surveillance

11.02.2025

The processing of migrants' personal data by FRONTEX has raised many concerns over the past years, prompting the European Data Protection Supervisor (EDPS) to investigate the matter on several occasions. The EDPS has noted that reports from debriefing interviews conducted by the Agency could lead to the identification of interviewees and, thus, it has stressed its serious doubts about these interviews' compliance with the principle of fair processing (Case 2022-0749). Moreover, it has observed that moving all of FRONTEX's services into the Microsoft cloud was in breach of the accountability principle (Case 2020-0584). However, little has been said about such processing in the context of the European Border Surveillance System (EUROSUR).

Regulation (EU) No 1052/2013 established EUROSUR as a framework for data exchange and for the cooperation between FRONTEX and the EU Member States, with the main purpose of detecting, preventing, and combating irregular migration and cross-border crime, as well as contributing to ensuring the protection and saving lives of migrants. In 2018, the European Commission concluded that EUROSUR was to be encompassed in the forthcoming FRONTEX Regulation in order to maximise the operational mandate of the Agency, as well as to expand the scope of the system so as to cover border checks at border crossing points and air border surveillance, along with the external land and sea borders. Against this background, this blogpost seeks to showcase how the basis for the exchange of information within the framework of EUROSUR, as well as the defined purposes of the system may lead to the unlawful processing of personal data.

Breaking Down EUROSUR: The System's Key Components Explained

EUROSUR is an intricate system. It comprises four main components that are interlinked in order to maintain a near-real-time picture of the external borders of the EU and to share information amongst actors involved in border management authorities.

The National Coordination Centres (NCCs) are established in each Member State, connecting all the national authorities that have competences in external border control, FRONTEX, and the NCCs of other Member States. The EUROSUR Fusion Services (EFS) constitute the component through which the Agency supplies the NCCs and itself with relevant information on the external borders and on the pre-frontier area, at the request of NCCs. Under EFS, FRONTEX cooperates with many EU Agencies and collects a wide variety of data, such as radar imagery or the deployment of aerial surveillance. The EUROSUR Communication Network (ECN) acts as the means of transfer of all the information collected in the system. Through ECN, sensitive non-classified and classified data is exchanged 'in a secure manner and in near-real-time with, and among the NCCs' [Article 14, 2019 European Border and Coast Guard (EBCG) Regulation].

Situational pictures are 'an aggregation of geo-referenced near-real-time data and information received from different authorities, sensors, platforms, and other sources' [Article 2(10), 2019 EBCG Regulation]. In other words, they are electronic maps that display the information gathered and disseminated by the relevant authorities and can be sorted into three types. First, National Situational Pictures are created by National Coordination Centres and relate to the external borders and pre-frontier area of each Member State. Second, the European Situational Picture is created by FRONTEX and contains the external borders and pre-frontier area of the EU, as well as all unauthorised secondary movements. Third, the Specific Situational Picture –

which was newly introduced by the 2019 EBCG Regulation – relates to specific operations carried out at the external borders, or aims at sharing information with third countries, international organisations, or other EU institutions, bodies, offices, and agencies.

It is the latter situational picture that raises more debate, given that information is shared with international organisations or third countries mainly on the basis of working arrangements. However, this raises two main concerns: first, most working arrangements concluded by FRONTEX lack adequate data protection and human rights safeguards; and second, the Regulation does not contain sufficient safeguards for the appropriate and lawful processing of personal data.

Data Protection Issues Within the Framework of EUROSUR

Although it has been claimed by FRONTEX that all working arrangements with external partners include 'specific fundamental rights safeguards', on most occasions, particularly with regard to the instruments concluded with third countries, these arrangements do not contain any safeguards, let alone specific provisions providing for the protection of fundamental rights. To highlight the relatively encouraging aspect first, the ratio of working arrangements concluded with IOs or other EU institutions, bodies, offices, or agencies that include fundamental/human rights protections is 44%. Except for the working arrangement with the European External Action Service (EEAS), which hardly states that the cooperation shall contribute to 'the streamlining and promotion of fundamental rights', those working arrangements contain quite specific safeguards.

In contrast, of the arrangements concluded between the Agency and third countries, only 40% contain a clause or a reference to the protection of fundamental/human rights and, in most cases, such references are extremely vague (e.g. clauses stating that the signing authority and the Agency should 'afford full respect for human rights' when cooperating). To date, the only working arrangement concluded with a third country that contains specific human rights protections is the one with the United Kingdom (UK), which provides for specific human rights obligations to both sides and for the monitoring of the FRONTEX Fundamental Rights Officer, amongst other measures.

The provisions concerning the protection of human rights contained in the UK working arrangement should be used by the Agency as inspiration for the (re)negotiation of future working arrangements with third countries. However, it cannot be forgotten that due to the non-legally binding nature of working arrangements, the inclusion of fundamental rights safeguards is not sufficient to mitigate the risk of human rights violations occurring, as stated by the EDPS in Case 2022-0647.

Data Protection Issues Stemming from the 2019 EBCG Regulation

Article 87 of the EBCG Regulation provides that FRONTEX may process personal data for the purposes of 'performing its tasks in the framework of EUROSUR in accordance with Article 89', which establishes the relevant rules. Article 89 allows for the Agency to process ship and aircraft identification numbers [89(2)], and to exceptionally process other types of personal data as long as the processing is limited 'to what is necessary for the purposes of EUROSUR in accordance with Article 18' [89(3)]. According to Article 18, the purposes of EUROSUR are the detection, prevention and fight against illegal immigration and cross-border crime and ensuring the protection and the saving of lives of migrants.

On the basis of Article 86(2), FRONTEX's Management Board adopted MB Decision 68/2021 on the processing of personal data by the Agency. In this regard, the EDPS adopted an Opinion where it established that there were certain aspects of the Regulation and MB Decision 68/2021 that did not provide for adequate safeguards. As regards EUROSUR, the EDPS established that Article 89 of the Regulation contained very few elements related to the processing of personal data, and that the MB Decision did not establish specific rules for processing such data within the EUROSUR framework.

Following this opinion, the Management Board adopted MB Decision 4/2024, which contained a more detailed set of rules for the processing of personal data concerning EUROSUR than Decision 69/2021. Although progress has been made in terms of developing a set of rules covering the specific situations where ship and aircraft identification numbers may be processed, there are nonetheless many gaps as regards the other kinds of personal data that, according to the Regulation, can be processed exceptionally for the purposes of EUROSUR. The only development in this regard is that Article 58 of the Decision – which

somewhat mimics Article 89 of the Regulation – explicitly includes the purposes for which personal data may be processed, instead of referring to Article 18. These purposes, however, are certainly very vague and, as pointed out by the Commission, leave a wide margin of interpretation [SWD(2024) 75], potentially resulting in the processing of personal data for other purposes such as for the prevention of arrival or pull-back practices, breaching the principle of purpose limitation. This principle requires that data must be collected only for specified, explicit and legitimate purposes and not processed in a way contrary to those purposes.

Concluding Remarks

As the main system for the surveillance of the EU's external borders, EUROSUR plays a key role in facilitating data-sharing among the Member States, FRONTEX and external actors. However, some key concerns remain about inadequate safeguards for the processing of personal data. Although the Agency's Management Board has taken a step forward in amending the data processing rules following Case 2022-0148, the Regulation remains unaltered. Moreover, MB Decision 4/2024 still leaves certain gaps, particularly with regard to the data that can be processed under Article 89(3) of the 2019 EBCG Regulation, triggering concerns about purpose limitation and the right to data protection under Article 8 of the Charter of Fundamental Rights of the EU.

Cite as
Irene Baceiredo-Macho, Under EUROSUR's Watchful Eye: Exploring the Data Protection Concerns in European Border Surveillance, *Völkerrechtsblog,* 11.02.2025, doi: 10.17176/20250212-000803-0.