Biometrics, Surveillance and Control at the Border.

17 OCTOBER 2026

Laura Binetti



Photo by Michał Jakubowski on Unsplash

Schengen Mobility in the Age of the EES

On 10 April 2026, the European Union's Entry/Exit System (EES) became fully operational across the Schengen area, replacing passport stamps with fingerprints and facial scans (Wahl, 2026). Phased in from 12 October 2025, the EES is the most extensive biometric border system the EU has introduced so far. It records the entry, exit and biometric data of third-country nationals subject to the system who cross an external Schengen border for a short stay (Council of the European Union, 2025). However, the EES is not just a technical upgrade. Its introduction comes at a time when the EU is also trying to regulate the growing use of artificial intelligence through the AI Act, which treats biometric identification as a particularly sensitive area (European Commission, 2026a).

This creates an important tension. The EU presents itself as a global leader in regulating digital technologies while protecting fundamental rights. At the same time, it operates one of the world's largest biometric border systems. The Schengen area's foundational promise (that of free movement without systematic identity checks) was built for a paper-based world of passport stamps and visual inspection. Today, this system has to coexist with facial recognition, centralised biometric databases and interconnected information systems that can also be accessed for purposes of law enforcement.

The question is also timely. The EES became fully operational in April 2026, and the Pact on Migration and Asylum has applied since 12 June 2026 (Council of the European Union, 2026). ETIAS is not yet in operation (European Commission, 2025), and the AI Act's high-risk rules apply later. Biometric border management is therefore expanding before the surrounding legal framework is complete.

This paper asks whether these two developments can coexist: can the EU use biometric technologies at its external borders without weakening the promise of free movement at the heart of the Schengen area?

Schengen, Borders and Biometrics

The Schengen area is often described as a "borderless Europe", but in practice the system is more complex. Border controls between member states were removed, while controls at the common external borders were strengthened and increasingly managed at the European level (European Parliament, 2025).

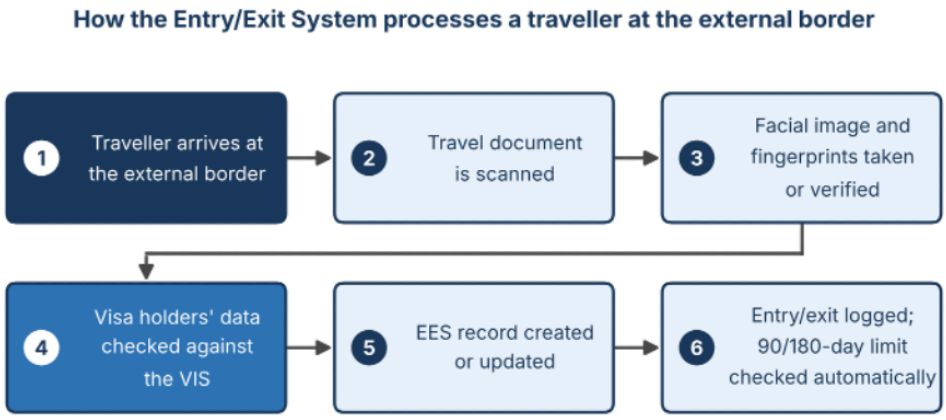
As internal border controls disappeared, member states invested more in managing the external borders, and biometric identification became increasingly important. EU biometric border systems mainly use two types of biometric data: facial images and fingerprints, collected from third-country nationals when they enter or leave the Schengen area. These systems are part of the EU's broader "smart borders" policy, developed to make external border checks faster, more automated and less dependent on manual document checks (European Commission, 2026, August 10).

The EES is the clearest example of this approach. Instead of simply stamping a passport, the system creates an electronic file for each third-country national it covers. Figure 1 shows how this works at the border. At a first crossing, the traveller's travel document is scanned, and a facial image and fingerprints are taken; at later crossings, these data are verified against the file. For visa holders, the data are also checked against the Visa Information System (VIS). Each entry and exit is recorded, and the system automatically calculates whether the traveller has exceeded the permitted 90-day stay in any 180-day period (Council of the European Union, 2025; European Union, 2017).

The system was introduced gradually over six months. At least ten per cent of estimated border crossings were covered after the first month, with all eligible travellers registered by April 2026. A gradual rollout was chosen because introducing the system everywhere at the same time could have created problems for the system and passenger flows (European Union, 2025).

What used to be a simple border check now involves collecting and storing personal data in a centralised EU database. The scale is considerable: in its first six months, the EES registered over 66 million entries and exits and 32,000 refusals of entry (European Commission, 2026b). These figures count crossings, not travellers, and cover a phased rollout, so they are not an annual total. This change raises important legal and political questions, which the rest of this paper will examine.

The first months of the EES have not been without problems. Some airports reported long queues after the full launch, and nine member states asked the EU to extend a temporary measure allowing border guards to suspend biometric checks during busy periods (Banks, 2026).



Source: Council of the European Union (2025); European Union (2017), Art. 8

Figure 1. How the Entry/Exit System processes a traveller at the external border.

The Legal Framework

The EU did not build the EES in a legal vacuum. Since 2024, it has had in place the AI Act, the world's first comprehensive attempt to regulate artificial intelligence through a general and cross-sectoral law rather than through voluntary guidelines (European Commission, 2026a). The Act follows a risk-based approach, dividing AI systems into four levels of risk: unacceptable, high, limited and minimal (Figure 2). Some uses of biometric identification are considered particularly sensitive and are therefore either prohibited or subject to stricter rules.

Article 5 of the AI Act prohibits certain uses of biometric identification. In particular, it generally prohibits real-time remote biometric identification in public spaces for law enforcement purposes. However, three exceptions are allowed: searching for victims of abduction, trafficking or sexual exploitation and for missing persons; preventing a specific and imminent threat to life or a terrorist attack; and identifying or locating suspects of certain serious crimes. These exceptions concern law enforcement use in public spaces under the AI Act and are not functions of the EES. Together, the restrictions show that the EU considers real-time biometric identification particularly sensitive.

The EES itself is not a high-risk AI system, but mainly a large-scale information system. Instead, the AI Act classifies specific AI tools used in migration, asylum and border control as high-risk. Annex III includes systems used to assess risks or to detect, recognise or identify individuals, while systems used only to verify travel documents are excluded. When these high-risk AI tools are used at the border, they must follow specific requirements on human oversight, accuracy, record-keeping and assessment.

However, these rules do not all apply immediately. The Digital Omnibus (Regulation (EU) 2026/1744), in force since 27 July 2026, postponed the main obligations for high-risk AI systems listed in Annex III until 2 December 2027 (European Union, 2026). There is an even longer transition period for AI systems that are part of large-scale EU border databases, including the EES. Under Article 111 of the AI Act, systems introduced before 2 August 2027 have until 31 December 2030 to comply (European Union, 2024; Vavoula, 2024). Figure 2 shows where border biometric tools sit in this classification and which deadlines apply to them. The border infrastructure is therefore already operating while some of the AI Act rules applying to its AI components will only become fully applicable later.

The EES is also subject to data protection oversight. The European Data Protection Supervisor (EDPS) works with national data protection authorities through the Coordinated Supervision Committee to monitor the system at both EU and national levels (European Data Protection Supervisor, 2025). The EDPS has stressed that personal data protection is a fundamental right and fully applies to the EES.

Taken together, the AI Act's risk classification and the EDPS's supervisory mandate show that EU law already treats biometric border tools as a distinct category requiring heightened scrutiny. The open question is whether this legal structure is enough to contain the practical risks the EES and its companion systems create. This is the subject of the next section.

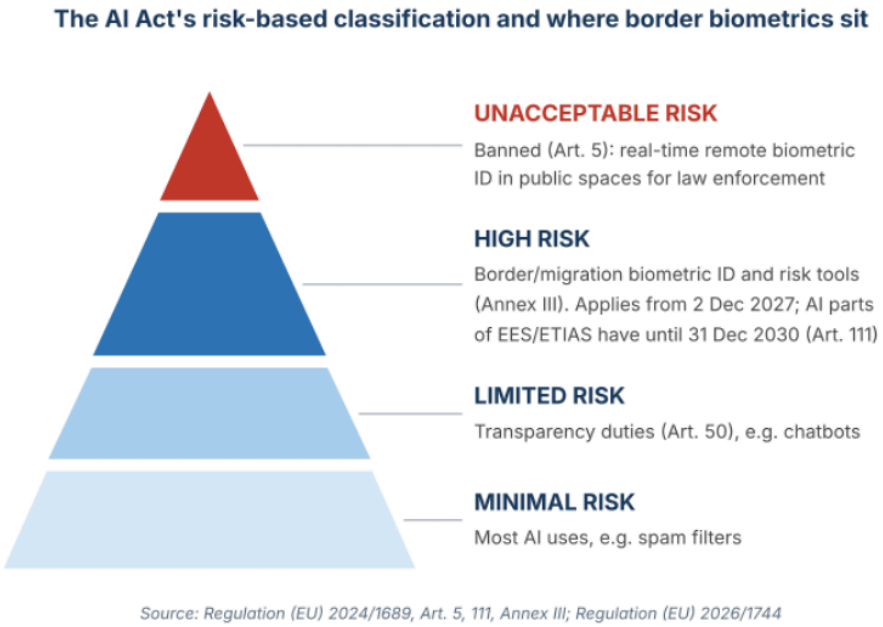


Figure 2. The AI Act's risk-based classification and where border biometrics sit.

Main Concerns

Three main concerns appear in the literature on EU biometric border systems: function creep, the risks created by interoperability and the impact of biometric controls on the idea of open mobility within Schengen.

Function creep means that data collected for one purpose is later used for another. A common example is Eurodac, the EU fingerprint database originally created to determine which member state is responsible for an asylum claim under the Dublin Regulation. It was later opened to police and law enforcement authorities for investigative purposes (Tsormpatzoudi et al., 2015). This is concerning because it challenges the principle of purpose limitation, a core rule of EU data protection law: personal data should be collected for specified purposes and not used in ways that are incompatible with them. It also affects the rights to private life and to the protection of personal data in Articles 7 and 8 of the EU Charter of Fundamental Rights (European Union, 2012). Each new use of the data is an additional interference with these rights, and it must be necessary and proportionate (European Union, 2012, Art. 52(1)). The risk is greater for third-country nationals, who provided their data as travellers or asylum seekers, not as suspects, and who have little practical ability to object. Once large amounts of biometric data are stored in a centralised system, pressure to use them for purposes beyond those for which they were collected may grow.

The second concern is interoperability. The EES is connected to a wider network of EU information systems. These include the Visa Information System (VIS), the Schengen Information System (SIS), the European Travel

Information and Authorisation System (ETIAS), which is not yet in operation (European Commission, 2025), and the European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN). Regulations (EU) 2019/817 and 2019/818 support this interoperability through tools such as a shared search portal and a common identity repository (European Union, 2019a, 2019b). Statewatch argues that linking these systems is creating a de facto centralised EU database containing biometric and personal data on non-EU nationals (Bunyan, 2018). The EU Fundamental Rights Agency has also raised concerns about the position of people whose data is stored in these systems, particularly migrants and asylum seekers. They may find it difficult to understand how their data is being used, correct inaccurate information or exercise their rights of access (European Union Agency for Fundamental Rights, 2018). Interoperability can make border systems more efficient, but it also allows identity and biometric data to be searched across different systems, within the access rules established by EU law. This can also increase the possibilities for profiling and algorithmic risk assessment (Derave et al., 2022; Vavoula, 2021).

The third concern is how biometric controls can change the experience of crossing a Schengen border. Providing fingerprints and a facial image is different from simply having a passport checked and stamped by a border guard. Even when privacy rules are respected, the growing use of biometric registration can make border crossings feel more controlled and less open. This creates a tension with the idea of Schengen as an area of free and easy movement.

Legal and Political Implications

These concerns are not only technical issues that can be solved by improving how the system works. They also raise important legal and political questions about individual rights and trust in public institutions.

From a legal perspective, biometric border systems can affect several rights protected by the EU Charter of Fundamental Rights, including privacy, personal data protection, non-discrimination and the right to an effective remedy. The Open Society Foundations raised similar concerns when the EES was first proposed in 2013. It argued that creating such a system mainly to identify "overstayers" could be disproportionate, especially given its limited ability to actually locate them (Butler, 2013). Now that the EES is fully operational, its impact and proportionality can be assessed in practice rather than only in theory.

Politically, the issue also matters for the EU's credibility as a setter of global standards. During the AI Act era, the EU has presented itself as a model for regulating digital technologies while protecting fundamental rights. However, Vavoula argues that important gaps remain in how the AI Act applies to EU border systems. For example, anonymised statistical data used within the interoperability system falls outside EU data protection law

(Vavoula, 2024). This could raise doubts about whether the EU applies the same standards to its own systems that it expects from other actors.

Another point worth considering is whether the EU has benefited from the system. The Commission reports 32,000 refusals of entry in the first six months (European Commission, 2026b) and, by 10 April 2026, over 700 people identified as posing a security risk (European Commission, 2026c). These figures show that the system is being used, but a refusal is not the same as a criminal being stopped, and they say nothing about proportionality. No independent evaluation of cost savings or security gains appears to be available yet, while reported difficulties include long queues at some airports (Banks, 2026).

Possible Safeguards

These concerns do not mean that biometric border management should be abandoned, but they show the importance of having strong safeguards in place.

First, the principle of purpose limitation needs to be strictly applied. Data collected by the EES to manage entries of short-stay and exits should not be used for broader law enforcement purposes without a clear legal basis and a specific justification. The development of Eurodac shows how biometric data collected for one purpose can later be used for others, and critics have raised similar concerns about the EU's wider interoperability system (Tsormpatzoudi et al., 2015; Bunyan, 2018).

Second, oversight bodies need enough resources to effectively monitor a system as large as the EES. The EDPS and the Coordinated Supervision Committee already have a formal role in supervising the system (European Data Protection Supervisor, 2025). Strong oversight is especially important during the first years of the EES, as problems can become more difficult to address once the system is fully integrated into border operations across 29 countries.

Third, greater transparency towards travellers is needed. Data protection rights are only effective if people understand how their personal and biometric data is used and know how to exercise their rights. The EDPS has also stressed the importance of transparency and of informing travellers about their rights. However, this information should be provided in a clear and consistent way across all Schengen border crossing points.

None of these safeguards requires abandoning biometric border management altogether. Instead, they require the EU to actively enforce the rules and oversight mechanisms that are already in place, including the AI Act and the role of the EDPS.

Conclusion

The Entry/Exit System's transition from proposal to fully operational infrastructure marks a genuine turning point in how the EU manages its external

border, and by extension, in what Schengen's promise of free movement actually means in practice. There is a clear tension between the growing use of biometric controls for security purposes and the idea of Schengen as an open area of free movement. The fact that the AI Act recognises the risks of biometric technologies does not remove this tension.

The main risks identified in this paper show that the expansion of biometric border management is not only a question of efficiency or security. It also raises questions about how personal data may be used over time, particularly as EU information systems become increasingly interconnected. Early figures suggest that the system is producing results, but its benefits have not yet been independently assessed.

For Schengen to remain an area that is both open and respectful of rights, biometric border systems need strong safeguards. Purpose limitation must be respected, oversight bodies need sufficient resources, and greater transparency towards travellers is necessary. These safeguards must be applied continuously in practice, rather than simply included in EU legislation.

References

Banks, M. (2026, August 10). *EU could extend flexibility on EES border checks amid fears of further travel disruption*. Travel Tomorrow. https://traveltomorrow.com/eu-could-extend-flexibility-on-ees-border-checks-amid-fears-of-further-travel-disruption/

Bunyan, T. (2018). *Briefing: The interoperability of Justice and Home Affairs databases*. Statewatch. https://statewatch.org/analyses/2018/briefing-the-interoperability-of-justice-and-home-affairs-databases/

Butler, I. (2013, April 23). *No good reason for a Schengen entry/exit system*. Open Society Foundations. https://www.opensocietyfoundations.org/voices/no-good-reason-schengen-entryexit-system

Council of the European Union. (2026). *Pact on migration and asylum*. https://www.consilium.europa.eu/en/policies/eu-migration-policy/eu-migration-asylum-reform-pact/

Council of the European Union. (2025, October 11). *With start of operation of new EES border control system the EU will strengthen border security and increase efficiency for travellers* [Press release]. https://www.consilium.europa.eu/en/press/press-releases/2025/10/11/with-start-of-operation-of-new-ees-border-control-system-the-eu-will-strengthen-border-security-and-increase-efficiency-for-travellers/

Derave, C., Genicot, N., & Hetmanska, N. (2022). The risks of trustworthy artificial intelligence: The case of the European Travel Information and Authorisation System. *European Journal of Risk Regulation, 13*(3), 389–420. https://doi.org/10.1017/err.2022.5

European Commission. (2026, August 10). *Entry/Exit System (EES)*. https://home-affairs.ec.europa.eu/policies/schengen/smart-borders/entry-exit-system_en

European Commission. (2025, October 6). *European Travel Information and Authorisation System (ETIAS)*. https://home-affairs.ec.europa.eu/policies/schengen/smart-borders/european-travel-information-authorisation-system_en

European Commission. (2026a, August 3). *AI Act*. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

European Commission. (2026b, May 18). *Commission report shows Schengen area continues to be resilient and ready for future challenges* [News]. https://luxembourg.representation.ec.europa.eu/actualites-et-evenements/actualites/commission-report-shows-schengen-area-continues-be-resilient-and-ready-future-challenges-2026-05-18_en

European Commission. (2026c, April 10). *Entry/Exit System (EES) is fully operational* [News]. https://home-affairs.ec.europa.eu/news/entryexit-system-ees-fully-operational-2026-04-10_en

European Data Protection Supervisor. (2025, October 24). *Supervising the entry into operations of the Entry/Exit System* [Press release]. https://www.edps.europa.eu/system/files/2025-10/2025_10_Supervising_EU_Entry_Exit_System_EN.pdf

European Union. (2012). *Charter of Fundamental Rights of the European Union*. *Official Journal of the European Union, C 326*, 391–407. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

European Parliament. (2025). *Free movement of persons*. Fact Sheets on the European Union. https://www.europarl.europa.eu/factsheets/en/sheet/147/free-movement-of-persons

European Union. (2017). Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011. *Official Journal of the European Union, L 327*, 20–82. https://eur-lex.europa.eu/eli/reg/2017/2226/oj

European Union. (2019a). Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 establishing a framework for interoperability between EU information systems in the field of borders and visa. *Official Journal of the European Union, L 135*, 27–84. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0817

European Union. (2019b). Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration. *Official Journal of the European Union, L 135*, 85–135. https://eur-lex.europa.eu/eli/reg/2019/818/oj

European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union, L 2024/1689*. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

European Union. (2025). Regulation (EU) 2025/1534 of the European Parliament and of the Council of 18 July 2025 on temporary derogations from certain provisions of Regulations (EU) 2017/2226 and (EU) 2016/399 as regards the progressive start of operations of the Entry/Exit System. *Official Journal of the European Union, L 2025/1534*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32025R1534

European Union. (2026). Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of har-

monised rules on artificial intelligence (Digital Omnibus on AI). *Official Journal of the European Union, L 2026/1744*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32026R1744

European Union Agency for Fundamental Rights. (2018). *Under watchful eyes: Biometrics, EU IT systems and fundamental rights*. Publications Office of the European Union. https://op.europa.eu/en/publication-detail/-/publication/abefeb05-387b-11e8-b5fe-01aa75ed71a1/language-en

Tsormpatzoudi, P., Dimitrova, D., Schroers, J., & Kindt, E. (2015). Privacy by design: The case of automated border control. In *Privacy and identity management for the future internet in the age of globalisation* (Vol. 457, pp. 139–152). Springer. https://doi.org/10.1007/978-3-319-18621-4_10

Vavoula, N. (2021). Artificial intelligence (AI) at Schengen borders: Automated processing, algorithmic profiling and facial recognition in the era of techno-solutionism. *European Journal of Migration and Law, 23*(4), 457–484. https://doi.org/10.1163/15718166-12340114

Vavoula, N. (2024, December 13). *Regulating AI at Europe's borders: Where the AI Act falls short*. Verfassungsblog. https://doi.org/10.59704/10a27137a898fa42

Wahl, T. (2026, April 15). *Entry/Exit System (EES) fully operational since 10 April 2026*. eucrim. https://eucrim.eu/news/entryexit-system-ees-fully-operational-since-10-april-2026/

EPIS