# *The Effects and Risks of Increased Usage of Biometric Data from Migrants and Refugees in the EU*

## 1 Executive Summary

**Biometric data is increasingly used to control and surveil migrants and refugees in the EU**. The technologies impact fundamental and data protection rights, are experimental and error-prone and criminalize asylum seekers even further. Severe consequences include the facilitation of deportation, rejection of asylum claims, and an increase in discriminatory treatment.

To counter these developments, regulatory bodies like EDPS or FRA should escalate the issue to court in order to implement their recommendations. They should commission research on migrants' knowledge about their data rights, while experts and civil society should continue to spread public awareness of the risks of biometric data.

## 2 Introduction

> In this scenario, the real game changer will be the great use of biometrics, as not only fingerprints, but also facial images, as biometrics, in my opinion, is the only key to perform an efficient identity management.[1]

These optimistic words by the Chair of the Eurodac Advisory Group Lorenzo Rinaldi perfectly encapsulate the spirit and ambition with which the European Union is approaching the usage of biometric data from migrants, asylum seekers, and refugees. However, biometric data is far from perfect and carries its distinct risks. For authorities, it is particularly attractive due to being universal, distinct, and permanent.[2] Types of biometric data include fingerprints, facial images, DNA, voices, etc. The data in itself is not

[1] Lorenzo Rinaldi, *Contribution to the panel "EU-LISA TODAY: THE DIGITAL AGENCY FOR EU HOME AFFAIRS", "10 years as the Digital Heart of Schengen"* (Talinn/Online, 2022) quoted in Matthias Wienroth and Nina Amelung, "Crisis, Control and Circulation: Biometric Surveillance in the Policing of the 'Crimmigrant Other,'" *International Journal of Police Science & Management* 25, no. 3 (2023): 306.

[2] Niovi Vavoula, "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, no. 4 (2021): 475.

problematic, however, issues arise in terms of how it is obtained and weaponized against vulnerable groups.

This policy brief aims to shed light on how migrants and refugees are impacted by the EU's investments in biometric technologies and why it is important to act on those expansions.

# 3 Background

The main reasons to use biometric data is for **identification** and **verification** purposes. One prominent example is Eurodac, a biometric database launched to determine the responsible member state where an asylum seeker could apply, following the Dublin regulation and to prevent "asylum shopping" - migrants applying for asylum in multiple member states.[3] Utilizing biometric data also promises speed, in the form of faster processing and more efficient migration management.[4] Especially in contrast to when migrants' documents are not available or not intelligible to authorities, biometric data is inherent to the body and difficult to alter.

Salvaging data from human bodies in this way is not new: Already in the transatlantic slave trade, features of the marginalized have been used for control and surveillance.[5] One current development that reignited the debate is the **New Pact on Migration and Asylum** which was recently passed in 2024. Amongst other regulations, it included the extension of the Eurodac system by including facial images next to fingerprints as well as lowering the age of people who need to give their data from originally 14 to six years old.[6]

Alongside Eurodac **other systems operating on EU-level** exist, such as the Schengen Information System SIS or the Visa Information System VIS that contain biometric data too, specifically fingerprints and/or facial images.[7] An overarching integration of all those databases is in planning, called shared Biometric Matching Service sBMS. It is supposed to become "one of the largest biometric systems globally."[8]

---

[3] Nina Amelung, ""Crimmigration Control" across Borders," *Historical Social Research/Historische Sozialforschung* 46, no. 3 (2021): 153.

[4] Simon Sontowski, "Speed, Timing and Duration: Contested Temporalities, Techno-Political Controversies and the Emergence of the EU's Smart Border," Journal of Ethnic and Migration Studies 44, no. 16 (2018): 2730–2746.

[5] Simone Browne, *Dark Matters: On the Surveillance of Blackness* (Durham: Duke University Press, 2015), 2–29.

[6] Bianca-Ioana Marcu, "Eurodac: Biometrics, Facial Recognition, and the Fundamental Rights of Minors," *European Law Blog*, April 2021, https://doi.org/10.21428/9885764c.1fc6d748.

[7] Evelien Brouwer, "The Use of Biometrics at the Borders: A European Policy and Law Perspective," in *Innovating Government: Normative, Policy and Technological Dimensions of Modern Government* (2011): 231–249.

[8] Wienroth and Amelung, "'Crisis', control and circulation," 303.

# 4 The Problem

## Asylum seekers' fundamental rights and data protection rights are infringed and disregarded

The General Data Protection Regulation **GDPR** in the EU is the strongest data protection framework in the world.[9] However, migration is seemingly a case where regulations are loosened, in order to enforce security. The European Data Protection Supervisor EDPS, a regulatory body, has criticized the far-reaching consequences of Eurodac, speaking of "an extensive intrusion in the rights of individuals constituting a vulnerable group in need of higher protection because they flee from persecution."[10]

Some key principles of the GDPR have been neglected, one of which is **purpose limitation**. With further developments of Eurodac, it extended the usage of biometric data beyond its original purpose ("function creep"). Hereby the functionalities of the data increase - providing law enforcement authorities access widens the scope of mere migration management. Even for future scenarios, the data is collected "just in case."[11] Other data protection principles of **proportionality** and **necessity**[12] must be considered, especially when it comes to fundamental rights violations. In a report, the Fundamental Rights Agency FRA analyzes how rights like the right to information, the right to human dignity, and the right to protection of personal data are potentially at risk when dealing with biometric data.[13][14]

As with any data collection, there usually needs to be **consent**, which is supposed to be obtained in a voluntary and informed way.[15] Nevertheless, there is no data available on to which extent migrants are informed about their rights and purposes.[16] In **accounts of violence**, people were detained when they refused to give their fingerprints, or when they had mutilated them. In Italy, in order to achieve a high coverage of registered fingerprints,

[9] "What is GDPR, the EU's new data protection law?", *GDPR.eu*, accessed November 19, 2024, https://gdpr.eu/what-is-gdpr/.

[10] Hustinx, "EDPS" (2009), quoted in Brouwer, "The Use of Biometrics at the Borders", 247.

[11] Wienroth and Amelung, "'Crisis', control and circulation," 307.

[12] Brouwer, "The Use of Biometrics at the Borders", 248.

[13] European Union Agency for Fundamental Rights, *Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights* (Luxembourg: Publications Office of the European Union, 2018), 9-18.

[14] Christoph Busch et al., "Facilitating Free Travel in the Schengen Area—A Position Paper by the European Association for Biometrics," *IET Biometrics* 12, no. 2 (2023): 114.

[15] "Consent," *GDPR-info.eu*, accessed November 19, 2024, https://gdpr-info.eu/issues/consent/.

[16] Amelung, "Crimmigration Control," 153.

there were even “stories of abuse and torture”;[17] whereas the FRA condemns the use of “physical or psychological force”[18] in these situations.

By lowering the age from 14 to six years old, even **children** are now subject to recording their fingerprints in the Eurodac database. Again fundamental rights, such as the right to human dignity or the rights of the child, are at risk; the experience could leave children traumatized.[19] There is also skepticism about the usefulness of this extension since children’s faces still evolve and change, and their fingerprints are not necessarily machine-readable,[20] undermining the argument of stability and permanence when using biometric data.

The intrusive character of biometric data collection can also be explained by how **sensitive its information** is. Generally, biometric features can reveal identity markers such as gender, and race, or even contain health information.[2122] Therefore they cannot be considered neutral data points, but are under the GDPR actually classified as sensitive personal data, affording extra safeguards.[23]

## Questionable technical efficiency of systems has severe consequences for migrants

Despite the marketing of biometric data as infallible, several studies have pointed out the experimental character of technologies: **Fingerprints** still perform on probabilistics, and the matches can be inconclusive.[24] There is also a shift towards biometric identification using **facial recognition technology**. In this AI-based tool, insufficient data quality and biases create false hits. People may be wrongly identified and flagged as security risks in an automated way.[25] Even if the error rate is low, it can still have an impact on hundreds of

[17] Georgios Glouftsios and Anna Casaglia, "Epidermal Politics: Control, Violence and Dissent at the Biometric Border," *Environment and Planning C: Politics and Space* 41, no. 3 (2023): 573.

[18] European Union Agency for Fundamental Rights, *Under Watchful Eyes*, 11.

[19] Marcu, "Eurodac," April 2021.

[20] Irma van der Ploeg, "Normative Assumptions in Biometrics: On Bodily Differences and Automated Classifications," in *Innovating Government: Normative, Policy and Technological Dimensions of Modern Government* (2011): 31.

[21] Lindsey N. Kingston, "Biometric Identification, Displacement, and Protection Gaps," in *Digital Lifeline? ICTs for Refugees and Displaced Persons*, ed. Carleen F. Maitland (Cambridge, MA: MIT Press, 2018): 45..

[22] Busch et al., "Facilitating Free Travel," 123.

[23] Marcu, "Eurodac," April 2021.

[24] Brouwer, “The Use of Biometrics at the Borders”, 248.

[25] Vavoula, "Artificial Intelligence at Schengen Borders," 479.

people, e.g. leading to further checks and discriminatory treatment.[26] The technology performs particularly worse when it comes to children's images.[27] Additionally, it is likely that the causal low-quality data will even deteriorate in the future: The increasing investment in the interoperability of several databases results in "an increasingly complex and opaque ecosystem."[28]

Yet, another case to exemplify the technical inefficiency is the **lie detection system iBorderCtrl**. The application is supposed to determine if migrants are lying based on micro-gestures, with the ultimate goal of speeding up processes at the borders.[29] Even though the technology handles "biomarkers of deceit"[30] and not biometrics per se, it still illustrates the EU's fixation on the migrant's body. Much of the system's algorithm is not available to the public, however after studying the limited accessible information, it was concluded that "even in the most favourable case for iBorderCtrl it is very unlikely that the tool can work in practice."[31] The system was trained with only 30 people in a non-representative sample, fueling concerns about racial and gender biases.

These inefficiencies have **extensive, real consequences** on affected populations: Automated structures make it harder for asylum seekers to contest decisions. The fate of vulnerable persons essentially lies in the hands of experimental technologies with significant error rates. A false hit can be a reason for faster deportation,[32] less protection, or rejection of asylum claims.

On a technical level, the **aspect of security** needs to be ensured as well. Naturally, databases can be targets of data breaches and the FRA urges to not share personal data with third countries.[33] Privacy International emphasizes permanence: "Biometric data can identify a person for their entire lifetime. This makes the creation of a biometric database problematic, as they have to anticipate risks far into the future."[34] Persecuted migrants are in continuous danger in case political contexts shift or regimes change.

---

[26] Ibid.

[27] Ibid., 480.

[28] Marcu, "Eurodac," April 2021.

[29] Javier Sánchez-Monedero and Lina Dencik, "The Politics of Deceptive Borders: 'Biomarkers of Deceit' and the Case of iBorderCtrl," *Information, Communication & Society* 25, no. 3 (2022): 416.

[30] Ibid.

[31] Ibid., 426.

[32] Nanna Dahler, "Biometrics as Imperialism: Age Assessments of Young Asylum Seekers in Denmark," *Race & Class* 62, no. 1 (2020): 31.

[33] European Union Agency for Fundamental Rights, *Under Watchful Eyes*, 14.

[34] "Biometrics," *Privacy International*, accessed November 19, 2024, https://privacyinternational.org/learn/biometrics.

## Increased focus on biometrics subject migrants and refugees to criminalization, general suspicion, and extended (border) surveillance

Underlying all of the aforementioned systems is a pronounced distrust towards people on the move. The lie detection system is based on the belief that migrants lie and cannot be trusted. Developments in Eurodac, namely increased collaboration with law enforcement, are underscoring the perception of the "bad migrant" and drive the convergence of migration and crime, coined "**crimmigration**."[35] Migrants and refugees therefore experience a culture of disbelief, encounter distrustful authorities, and find themselves under general suspicion by default.[36] The mere development of technologies using biometric data is only possible on the premise that asylum seekers are considered less than EU citizens, being "used as a testing ground for experimentation."[37]

There is a case in Denmark that shows that not even sophisticated algorithms are needed to weaponize biometrics: **Age assessments** are conducted on migrant teenagers based on bone density, teeth examinations, and wrist size. The purpose is to identify the person's age, to determine whether they are entitled to child support. Interestingly, the age assessed would often be 19, deeming teenagers just outside of eligibility.[38] Similar procedures exist in other member states where biometrics are also instrumentalized to repel asylum seekers and refrain from helping.

Another effect consists of the transformation of the typical **physical border** into not only a digital but an internal one: "Biometrics was seen as a way to transpose Europe's diminished borders onto migrants' bodies so that the border encounter would become ubiquitous and independent from the space of the physical border."[39] This phenomenon could recreate "invisible borders with the risk of constant surveillance."[40] It is not a one-time crossing of borders either, since whenever migrants and refugees deal with the state, "they leave back digital, epidermal traces that are stored, processed and matched to reconstruct their past, thus rendering them biometrically controllable and deportable in the future."[41]

---

[35] Amelung, "Crimmigration Control."

[36] Ibid., 157.

[37] Daniel Leix Palumbo, "13. The Weaponization of Datafied Sound: The Case of Voice Biometrics in German Asylum Procedures," in *Doing Digital Migration Studies*, 305.

[38] Dahler, "Biometrics as Imperialism," 35.

[39] Romm Lewkowicz, "Capturing the Spirit of Bureaucratic Images: Photo IDs, Biometrics, and Passing in Border-Free Europe," *Visual Anthropology Review* 39, no. 1 (2023): 255.

[40] Busch et al., "Facilitating Free Travel," 123.

[41] Glouftsios and Casaglia, "Epidermal Politics," 573.

To give a short glance outside of Europe, biometric technologies are further used by the EU to **externalize borders** and gain more control, even over populations in non-EU countries. For the EU-project WAPIS, citizens in West African countries are urged to give their biometric data, with the aim to support law enforcement and fight crime.[42] Using biometric data, surveillance can even be extended outside of the EU, criminalizing whole populations and putting them under scrutiny even before any European border is crossed.

# 5 Opportunities for change: recommendations

The following recommendations aim to be specific and are not to be understood as comprehensive.

### EDPS and FRA:
### Research migrants' knowledge of their data rights, use results to implement guardrails

As mentioned before, there is no substantial data on how informed migrants are about data rights.[43] Either EDPS or FRA should mandate research on this. The data from the study serves as a foundation to implement guardrails with the goal to improve the agency and the information flow to the affected groups, e.g. knowing how to file a complaint. If it is not possible to remove biometrics altogether, in this way at least some sense of data ownership is given back.

### EDPS and FRA:
### Escalate the issue to the European Court of Human Rights

EDPS and FRA as regulatory bodies give thorough analyses and useful suggestions, but EU institutions are not obliged to follow any. Reading their reports, they do not lack ideas or recommendations, one of which is assessing the impact of Eurodac and its potential rights infringements,[44] but the political power. They should escalate the case of biometrics to the European Court of Human Rights which itself expressed criticism towards the matter.[45] Perhaps their ruling provides the authority to implement EDPS or FRA recommendations to secure the rights of asylum seekers.

---

[42] Bruno Oliveira Martins, Kristoffer Lidén, and Maria Gabrielsen Jumbert, "Border Security and the Digitalisation of Sovereignty: Insights from EU Borderwork," *European Security* 31, no. 3 (2022): 482.

[43] Amelung, "Crimmigration Control," 170.

[44] Ibid., 168.

[45] Brouwer, "The Use of Biometrics at the Borders," 241ff.

### Experts and civil society organizations: Keep spreading public awareness, unravel complexity, and provide expertise

Lastly, the further engagement of experts, civil society organizations, scholars, activists, etc. is crucial in bringing public awareness and should not be underestimated. Especially in a technically complex context such as data politics, data literacy is needed for the discourse:[46] "The civil society has a very important role in the contestation of policy and regulatory developments promoting increased digitalisation, at the borders and beyond."[47]

*Word Count: 2052 words*

[46] Martins, Lidén, and Jumbert, "Border Security," 488f.

[47] Ibid.

# Bibliography

Amelung, Nina. "“Crimmigration Control” across Borders." *Historical Social Research/Historische Sozialforschung* 46, no. 3 (2021): 151–177.

"Biometrics." *Privacy International*. Accessed November 19, 2024. https://privacyinternational.org/learn/biometrics.

Brouwer, Evelien. "The Use of Biometrics at the Borders: A European Policy and Law Perspective." In *Innovating Government: Normative, Policy and Technological Dimensions of Modern Government*, 231–249. 2011.

Browne, Simone. *Dark Matters: On the Surveillance of Blackness*. Durham: Duke University Press, 2015.

Busch, Christoph, et al. "Facilitating Free Travel in the Schengen Area—A Position Paper by the European Association for Biometrics." *IET Biometrics* 12, no. 2 (2023): 112–128.

Dahler, Nanna. "Biometrics as Imperialism: Age Assessments of Young Asylum Seekers in Denmark." *Race & Class* 62, no. 1 (2020): 24–45.

European Union Agency for Fundamental Rights. *Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights.* Luxembourg: Publications Office of the European Union, 2018.

GDPR.eu. "What Is GDPR, the EU’s New Data Protection Law?" Accessed November 19, 2024. https://gdpr.eu/what-is-gdpr/.

GDPR-info.eu. "Consent." Accessed November 19, 2024. https://gdpr-info.eu/issues/consent/.

Glouftsios, Georgios, and Casaglia, Anna. "Epidermal Politics: Control, Violence and Dissent at the Biometric Border." *Environment and Planning C: Politics and Space* 41, no. 3 (2023): 567–582.

Kingston, Lindsey N. "Biometric Identification, Displacement, and Protection Gaps." In *Digital Lifeline? ICTs for Refugees and Displaced Persons*, edited by Carleen F. Maitland, 35–53. Cambridge, MA: MIT Press, 2018.

Lewkowicz, Romm. "Capturing the Spirit of Bureaucratic Images: Photo IDs, Biometrics, and Passing in Border-Free Europe." *Visual Anthropology Review* 39, no. 1 (2023): 251–267.

Marcu, Bianca-Ioana. "Eurodac: Biometrics, Facial Recognition, and the Fundamental Rights of Minors." *European Law Blog*, April 2021. https://doi.org/10.21428/9885764c.1fc6d748.

Martins, Bruno Oliveira, Lidén, Kristoffer, and Jumbert, Maria Gabrielsen. "Border Security and the Digitalisation of Sovereignty: Insights from EU Borderwork." *European Security* 31, no. 3 (2022): 475–494.

Palumbo, Daniel Leix. "The Weaponization of Datafied Sound: The Case of Voice Biometrics in German Asylum Procedures." In *Doing Digital Migration Studies*, 303–322.

Sánchez-Monedero, Javier, and Lina Dencik. "The Politics of Deceptive Borders: 'Biomarkers of Deceit' and the Case of iBorderCtrl." *Information, Communication & Society* 25, no. 3 (2022): 413–430.

Sontowski, Simon. "Speed, Timing and Duration: Contested Temporalities, Techno-Political Controversies and the Emergence of the EU's Smart Border." *Journal of Ethnic and Migration Studies* 44, no. 16 (2018): 2730–2746.

Van der Ploeg, Irma. "Normative Assumptions in Biometrics: On Bodily Differences and Automated Classifications." In *Innovating Government: Normative, Policy and Technological Dimensions of Modern Government*, 29-40. 2011.

Vavoula, Niovi. "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, no. 4 (2021): 457–484.

Wienroth, Matthias, and Amelung, Nina. "Crisis, Control and Circulation: Biometric Surveillance in the Policing of the 'Crimmigrant Other.'" *International Journal of Police Science & Management* 25, no. 3 (2023): 297–312.