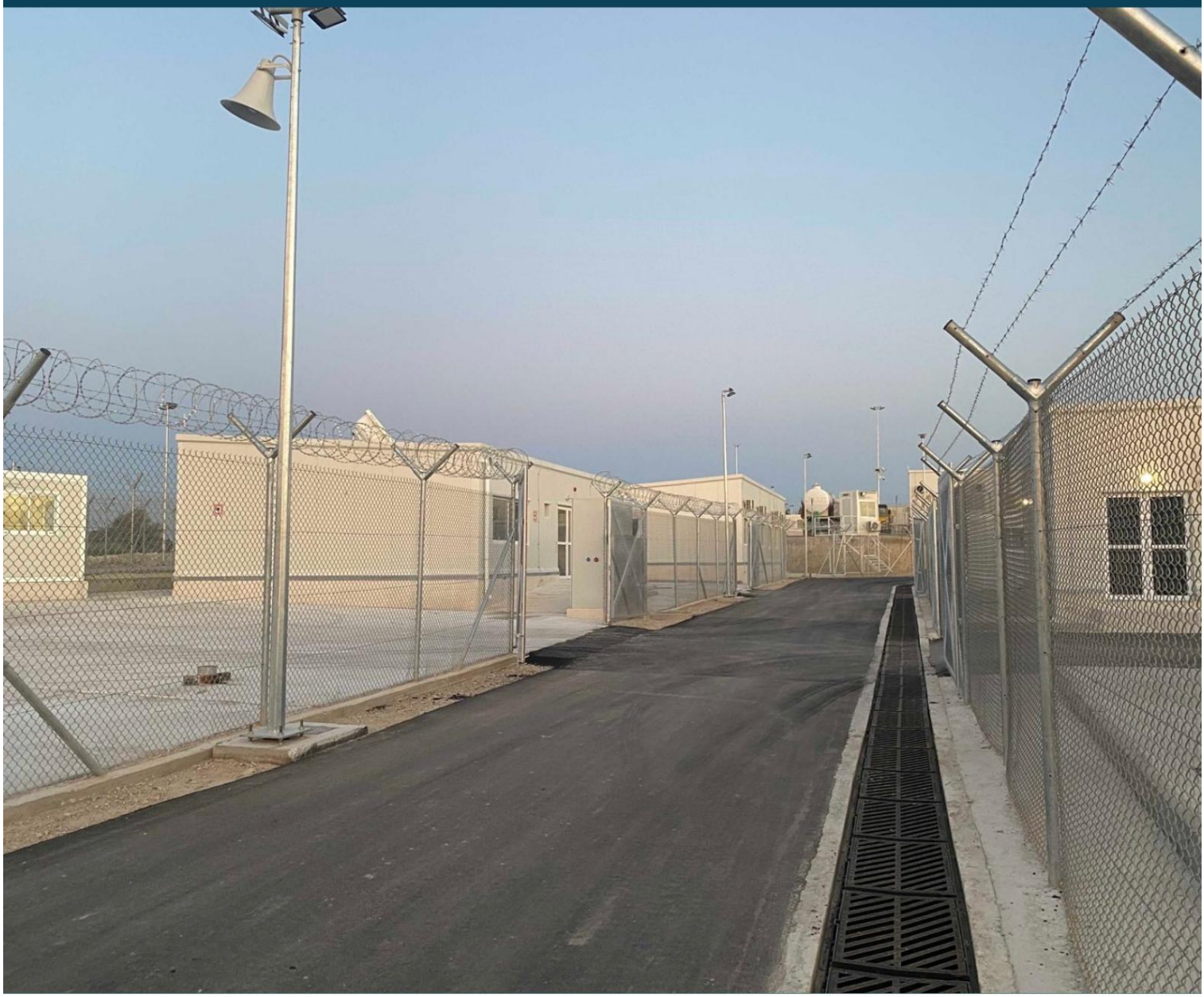
“They never tell us anything”

Ongoing Data Rights Violations in the Samos CCAC



I HAVE RIGHTS.

Homo Digitalis

Protect your rights

I Have Rights is a Samos-based human rights organisation. Since March 2022, I Have Rights has provided specialised legal support to more than 1,000 clients and legal information to nearly 2,000 people through its information hotline. I Have Rights documents human rights violations and hate crimes against people on the move, advocates for policy change and litigates against human rights violations. I Have Rights is a member of the Border Violence Monitoring Network.

Homo Digitalis is an Athens-based civil society organisation focusing on the promotion and protection of human rights in the digital age. Since 2018 and through the three pillars of their actions, namely, raising awareness, shaping policy decisions, and strategic legal interventions, Homo Digitalis aims to strengthen the protection of fundamental rights and freedoms, when new technologies are used by private or public entities. Homo Digitalis is a member of the European Digital Rigths (EDRi) network.

Acknowledgements

We extend our heartfelt gratitude to the respondents, who placed their trust in us and generously shared their experiences. Your openness was instrumental in shaping this research, and we are deeply appreciative of the time and insights you provided.

We also wish to express our sincere thanks to the Safe Passage Fund for their invaluable support and funding of this project. Their commitment to advancing migrant justice rights made this research possible.

To everyone who contributed, thank you.

Safe Passage Fund

CONTENTS

Safe Passage Fund

Researchers and authors: Eleftherios Chelioudakis, Charlotte Hutton, Magdalena Rassmann, Réka Rebeka Rósa and Dimitra Theotoki.

Interview team: Bela Abeln, Hamida Ahmadi, Alexandros Avramis, Salomé Brun, Lara Edtmüller, Charlotte Hutton, Rafka Ibrahim, Ali Karimi, Dalia Noureldeen, Éilis McCarthy, Zainab Omer Hamid Zain Elabdin, Magdalena Rassmann, Réka Rebeka Rósa, Khoshy Salaam, Raed Shaaban, Candice Schmitz, Georgia Sotiraki and Dimitra Theodoki.

I HAVE RIGHTS.

Homo Digitalis
Protect your rights

1 Introduction

The use of border surveillance technology proliferated in recent years with millions of funds poured into increasingly sophisticated high-tech surveillance to monitor, control and prevent movement of racialized people at European borders. This trend is particularly evident in Greece, acting as a "testing ground" for new technologies.[1]

A prominent example for the increased use of surveillance technology on the European external borders is the Samos Closed Control Access Centre (CCAC). The Samos CCAC is an EU-funded "pilot" reception facility located in the remote, north-western area of the Greek island Samos.[2] At least four IT systems - Centaur, Hyperion, Rea, and Alkioni II - deployed in the centre form "an EU-funded, AI-led surveillance ecosystem."[3]

Ever since its opening in September 2021, the "dystopian nightmare"[4] of the Samos CCAC has faced widespread criticism from national and international organisations and the people held in the facility. There have been frequent and consistent comparisons of the CCAC to "prison"[5], condemnations of its regime of blanket *de facto* detention[6] and concerns about prevalent inadequate living conditions[7] and the "intense surveillance and tracking infrastructure."[8] Alarmingly, to this day serious concerns about rights violations in the Samos CCAC persist.[9]

A positive step toward state accountability for rights violations against people held in the Samos CCAC emerged in April 2024 with a historic ruling by the Hellenic Data

---

[1] Petra Molnar. 2020. Technological testing grounds: Migration management experiments and reflections from the ground up. Available here.
[2] I Have Rights. 2025. Controlled and Confined: Unveiling the Impact of Technology in the Samos Closed Controlled Access Centre. Available here.
[3] Eleftherios Chelioudakis. 2024. Unpacking AI-enabled border management technologies in Greece: To what extent their development and deployment are transparent and respect data protection rules? Available here. Page 4.
[4] Amnesty International. 2024. People seeking asylum detained in EU-funded "pilot" refugee camp on Samos. Available here.
[5] Ever since its opening, people on the move have referred to the Samos CCAC as a "prison". More information on this from 2021, 2022, 2023 and 2024.
[6] I Have Rights. 2023. The EU-Funded Closed Controlled Access Centre - the De Facto Detention of People Seeking Safety on Samos. Available here.
[7] Border Violence Monitoring Network. 2024. Monthly Report: Illegal pushbacks and border violence reports. November 2024. Available here; Amnesty International. 2025. Samos: Unlawful detention and sub-standard conditions must not become a blueprint for the EU Migration Pact. Available here.
[8] UN Special Rapporteur on Trafficking in Persons. 2024. AL GRC 3/2024. Available here. Page 8.
[9] Amnesty International. 2025. Samos: Unlawful detention and sub-standard conditions must not become a blueprint for the EU Migration Pact. Available here.

Protection Authority (HDPA)[10] against the Hellenic Ministry of Migration (MoMA).[11] Following a complaint by Homo Digitalis, the Hellenic League for Human Rights, HIAS Greece and academic Prof. Niovi Vavoula in 2022,[12] the HDPA imposed with 175,000 Euro the largest penalty ever on a public Greek body. This was a response to several significant violations of the General Data Protection Regulation (GDPR) through the use of surveillance technology in reception facilities for migrants and asylum seekers on the Aegean islands (Lesvos, Chios, Samos, Leros, and Kos). The HDPA found data processing practices were unclear, mandatory Data Protection Impact Assessments lacked coherence, and found serious transparency issues concerning the implementation of the Centaur and Hyperion systems. Along with the substantive fine, the HDPA issued a compliance order for the MoMA to comply with its GDPR obligations by July 2024.[13]

This decision was significant not only because of the substantive fine imposed. It also marked an important step in protecting the rights of "data subjects"— people on the move, migrants and asylum seekers — who face structural obstacles and have fewer economic resources to defend their rights. With the compliance order passed since July 2024, this report aims to assess *whether the ruling has been effectively implemented.* Thereby, it aims to counter trends where the use of technology in migration 'management' is legitimized to control and surveil mobile populations, often unchallenged and driven by weak state accountability.[14] Resisting the invasive and expansive use of border surveillance technology is crucial: Its proliferation both reflects and contributes to broader trends and racist narratives of border securitization, border enforcement, and border externalisation, deliberately designed to control and curtail the mobility of people on the move.

Based on 27 semi-structured interviews conducted between July 2024 and March 2025 and a legal analysis, the report finds that the *MoMA did not comply with the HDPA implementation order, in violation with data protection rights of people held in the Samos CCAC.* The report will present this argument in the following way: It will introduce the use of surveillance technology in the Samos CCAC, followed by an overview of the HDPA compliance order. It will then analyse to what extent the compliance order was

[10] The Hellenic Data Protection Authority is an independent public body, tasked with overseeing the implementation of the General Data Protection Regulation (GDPR), national laws, and other regulations aimed at protecting individuals from the misuse of their personal data.
[11] Homo Digitalis. 2024. The Hellenic Data Protection Authority fines the Ministry of Migration and Asylum for the "Centaurus" and "Hyperion" systems with the largest penalty ever imposed to a Greek public body. Available here.
[12] Homo Digitalis. 2022. The Hellenic DPA is requested to take action against the deployment of ICT systems IPERION & KENTAUROS in facilities hosting asylum seekers in Greece. Available here.
[13] Homo Digitalis. 2024. The Hellenic Data Protection Authority fines the Ministry of Migration and Asylum for the "Centaurus" and "Hyperion" systems with the largest penalty ever imposed to a Greek public body. Available here.
[14] Petra Molnar. 2020. Technological testing grounds: Migration management experiments and reflections from the ground up. Available here.

implemented, contextualise the analysis in broader developments on surveillance technology and conclude with a summary.

2 Surveillance Technology in the Samos CCAC

The Samos CCAC is equipped with at least four IT systems: Centaur, Hyperion, Rea[15] and Alkioni II.[16] As the HDPA decision focuses on the EU-funded systems Centaur and Hyperion, this report limits its scope to these tools.[17]

Centaur deploys motion analysis algorithms and transmits CCTV and drone footage to a control room at the MoMA.[18] At least three Greek and two Israeli companies have been involved in the system since 2021: ESA Security, Space Hellas, Adaptit, ViiSights[19] and Octopus.[20] The Israeli firms supply military-grade surveillance technology, likely developed on Palestinians, and now reused as part of the EU's border enforcement infrastructure.[21] This is not only the case on Samos: Israeli technology developed "to control the Palestinian people is made available for Israeli and international tech

[15] Rea is an internet infrastructure system, allowing access to high-speed internet. Through Rea, personnel of the Asylum Service will have access to the Alkioni II system from all facilities. Additionally, free Wi-Fi will be made available to asylum seekers, exclusively through the use of a Mobile Application that will be developed with the Hyperion system. Finally, the system will allow for the transmission of video and audio from the facilities to the new Operations Center of the Ministry, as well as to related agencies (Hellenic Police, Hellenic National Defence General Staff, Coast Guard, etc.) via the Centaur system. More information here. Also, see more about the surveillance challenges that arise from this here.

[16] Alkioni II aims to incorporate existing systems of the Hellenic Police, such as the Information System for Mapping the Traffic of Foreigners as well as systems of international organisations, such as systems of the United Nations High Commissioner for Refugees (UNHCR) and the United Nations Relief and Works Agency for Palestine Refugees in the Near East (UNRWA). The project is funded by the EU's Internal Security Fund and will offer multilingual digital services for asylum seekers who have completed the initial registration and interview process. Through Alkioni II, users will be able to submit supplementary or updated documents, apply for family reunification, file an appeal, withdraw their asylum application, report lost or stolen documents or apply to renew documents. See more here.

[17] For more information on the use of technology in the Samos CCAC, and potential rights implications please read: I Have Rights. 2025. Controlled and Confined: Unveiling the Impact of Technology in the Samos Closed Controlled Access Centre. Available here.

[18] Stavros Malichudis. 2022. Asylum Surveillance Systems Launched in Greece without Data Safeguards. Available here.

[19] IHR learnt about the involvement of ViiSights in Centaur through submitting Data Subject Access Requests to obtain video footage. The footage obtained was marked with "ViiSIGHTS" and is similar to examples of camera feeds featured on ViiSight's website. Available here. ViiSights website details that they work in "refugee camps in Greece". Available here.
In January 2025, a Computer Weekly article indicated that Viisights was undergoing insolvency proceedings, casting uncertainty over its future involvement in its operations in the Samos CCAC. See here.

[20] Lydia Emmanouilidou uncovered the involvement of Octopus following an in person visit to the control centre in the Ministry of Migration and Asylum.

[21] Anas Ambri. 2025. Stephen Harper's firm behind spy tech used in 'dystopian' Greek refugee camps. Available here.

companies to scale up and export to other countries for repressive purposes."[22] This global circulation of militarized surveillance infrastructure illustrates how technologies of control are deployed from settler-colonial contexts to new sites of border violence and enforcement.

Hyperion meanwhile uses biometric data to monitor movement in and out of the Samos CCAC.[23] People held in the Samos CCAC are required to scan their fingerprints and biometric ID card to enter, exit and sometimes to move through the facility.[24] This is incredibly time-consuming, often leading to long queues at the gates, with people reportedly having to wait up to more than one hour to enter and exit the CCAC. This practice is not only undignified, requiring people to wait outside in adverse weather conditions, but does not take into consideration varying accessibility requirements. What is presented as a tool for "digitalisation of the migration and asylum system"[25] thus becomes another layer of control, restricting the freedom of movement of people. This adds additional obstacles to accessing basic services and necessities such as legal aid.

Data received through a Freedom of Information request also reveals that due to malfunctioning of the Hyperion system, that from October 2024 to at least January 2025 the catering company in the Samos CCAC had to scan every ID card when giving out food to avoid double shows. Due to this practice and frequent overcrowding people reportedly may queue for hours to receive meals,[26] further undermining dignified treatment.

3 Overview of HDPA Recommendations

The EU-funded "new generation" CCACs in the Aegean that employ pervasive technology systems are only expected to serve as the beginning and the blueprint for the development of similar facilities and tech systems all over Europe and its borders. As the EU moves forward with implementing the New Pact on Migration and Asylum,[27]

[22] Apoorva PG. 2023. Seeing The World Like A Palestinian. Intersectional Struggles Against Big Tech and Israeli Apartheid. Available here.
[23] Stavros Malichudis. 2022. Asylum Surveillance Systems Launched in Greece without Data Safeguards. Available here.
[24] I Have Rights. 2025. Controlled and Confined: Unveiling the Impact of Technology in the Samos Closed Controlled Access Centre. Available here.
[25] This is under Greece's 2014-2020 National Programme. European Commission. 2022. Answer given by Ms Johansson on behalf of the European Commission on 22 December 2022. E-003094/2022. Available here.
[26] European Commission. 08.01.2025. Weekly update on the migratory situation in Greece (islands and mainland) 08/01/2025 - Ares (2025) 143701. Received through a Freedom of Information Request.
[27] According to article 78 of the Treaty on the Functioning of the EU, the EU shall develop a common policy on asylum, subsidiary protection and temporary protection, known as the Common European Asylum System. Within this context, the Pact on Migration and Asylum was adopted which entered into force on 11 June 2024, but will enter into application after 2 years.

there is a significant risk that the data protection and human rights violations identified in these centres could be replicated on a broader scale. The data protection violations found by the HDPA in the CCACs include:

1. The HDPA found a violation of the principles of lawfulness, fairness and transparency as enshrined in article 5(1)(a) GDPR in a twofold manner: *Firstly*, the MoMA did not adequately explain the legal basis employed for data processing. *Secondly*, the authorities failed to provide any information regarding the automated functions of Centaur, which possesses behavioural analytics algorithms, and thus to properly justify the lawfulness of this processing. The HDPA noted confusion and inconsistency regarding the legal basis for the processing conducted by both the Hyperion and Centaur system, as the authorities used multiple legal bases alternatively.[28] Initially, the authorities invoked their "legitimate interests"[29] even though these are specifically excluded by GDPR provisions in cases of processing conducted by public authorities in the performance of their tasks.[30] To address concerns expressed by the HDPA, the authorities eventually referred to the consent of "data subject", migrants and asylum seekers, obtained via a document signed during registration.[31] However, the HDPA rejected this argument, finding that the consent did not meet the GDPR standards for valid consent.[32] According to the HDPA, the authorities also omitted to substantiate the legal basis in accordance with data subject category.[33] Lastly, the HDPA could not safely conclude that sensitive data, e.g. ethnic origin or religious convictions, are not being processed.[34] As a result, the HDPA ordered the MoMA to identify and justify the appropriate legal basis for any data processing conducted by Centaur and Hyperion, mentioning specific guarantees for sensitive data processing and for specific data subject categories.[35]

2. According to the HDPA ruling, the authorities violated subjects', migrants and asylum seekers', rights to transparent information, as established by articles 12, 13 and 14 of the GDPR. Information on data processing by both Centaur and Hyperion is allegedly provided to people in the CCACs by a special document in English and Greek.[36] However, this practice does not meet GDPR transparency requirements, particularly

[28] Hellenic Data Protection Authority. 2024. Decision 13/2024. Available (in Greek) here. Page 33, para 16.
[29] Hellenic Data Protection Authority. 2024. Decision 13/2024. Available (in Greek) here. Page 8.
[30] EU Regulation 2016/679 (GDPR), Article 6 Para 1(f); Hellenic Data Protection Authority. 2024. Decision 13/2024. Available (in Greek) here. Page 33, para 16.
[31] Hellenic Data Protection Authority. 2024. Decision 13/2024. Available (in Greek) here. Page 8.
[32] Hellenic Data Protection Authority. 2024. Decision 13/2024. Available (in Greek) here. Pages 20-22 and 33, paras 6 and 16.
[33] Hellenic Data Protection Authority. 2024. Decision 13/2024. Available (in Greek) here. Page 34, para 16.
[34] *Ibid.*
[35] Hellenic Data Protection Authority. 2024. Decision 13/2024. Available (in Greek) here. Pages 33 and 37, paras 16 and 20.
[36] Hellenic Data Protection Authority. 2024. Decision 13/2024. Available (in Greek) here. Pages 11 and 35, para 18.

considering the data subjects', people on the move, migrants and asylum seekers', profile as people with systematically-induced vulnerabilities.[37] The information is presented solely in languages many may not understand and includes technical and legal terminology, while lacking essential information regarding the nature and scope of the data processing that according to GDPR provisions should be provided to the data subjects.[38] Similarly, the HDPA questioned the accessibility and transparency of the privacy policies conducted by the MoMA exclusively in Greek, which were not in conformity with the requirement for clear and simple wording and accessible language.[39] Lastly, the authorities claimed having adhered to their obligation to provide transparent information by invoking the CCTV warning signs placed within the CCAC facilities.[40] However, these were found by the HDPA to contain incomplete or inaccurate information. Indicatively, the HDPA mentioned the use of an improper legal basis and the denial of third-party data transfer.[41] In response, the HDPA requested the MoMA to proceed to the necessary additions through appropriate means and understandable language of all necessary information, including the categories of data recipients.[42]

3. The HDPA also identified multiple violations of the general obligations of the MoMA in *its* capacity as data controller. Specifically, the HDPA found lack of systematic and comprehensive impact assessments,[43] a lack of written contracts between all processing actors,[44] lack of an activity record prior to the processing,[45] and shortcomings regarding the appointment and functions of the Data Protection Officer.[46] As a result of the intransparency of the MoMA with regards to essential information which made it impossible for the HDPA to conclude on the legality of the data processing, the HDPA imposed the administrative fine of 75,000 euros.[47] It additionally imposed the administrative fine of 100,000 euros for the non-conduct of complete data

---

[37] Hellenic Data Protection Authority. 2024. Decision 13/2024. Available (in Greek) here. Page 35, para 19.
[38] Articles 13 and 14 of the GDPR require data controllers to provide specific information to data subjects. This includes the identity and the contact details of the controller, the contact details of the data protection officer, the purposes of the processing for which the personal data are intended and the legal basis for the processing, and the recipients of the personal data.
[39] Hellenic Data Protection Authority. 2024. Decision 13/2024. Available (in Greek) here. Page 37, para 19.
[40] Hellenic Data Protection Authority. 2024. Decision 13/2024. Available (in Greek) here. Page 11.
[41] Hellenic Data Protection Authority. 2024. Decision 13/2024. Available (in Greek) here. Page 37, para 19.
[42] Hellenic Data Protection Authority. 2024. Decision 13/2024. Available (in Greek) here. Page 37, para 20.
[43] Hellenic Data Protection Authority. 2024. Decision 13/2024. Available (in Greek) here. Pages 40-41, para 23.
[44] Hellenic Data Protection Authority. 2024. Decision 13/2024. Available (in Greek) here. Pages 37-39, para 21.
[45] Hellenic Data Protection Authority. 2024. Decision 13/2024. Available (in Greek) here. Page 40, para 22.
[46] Hellenic Data Protection Authority. 2024. Decision 13/2024. Available (in Greek) here. Pages 42-43, para 25.
[47] Hellenic Data Protection Authority. 2024. Decision 13/2024. Available (in Greek) here. Page 48.

protection impact assessments prior to the implementation of the Centaur and Hyperion systems.[48]

4. Lastly, the HDPA found a violation of the principle of cooperation with the supervisory authority due to the MoMA's refusal to adhere to *its* obligation under article 31 GDPR to provide full, precise, and clear data to justify the legality of its actions within the frame of the data processing activities under Centaur and Hyperion. Thus, the MoMA did not justify its compliance with GDPR according to the principle of accountability as enshrined in article 5(2).[49]

5. Under article 58(2)(d) GDPR, the HDPA issued a compliance order to the MoMA to proceed to all necessary actions with the purpose of complying fully with *its* obligations as data controller, as these were described within the body of the decision, within three months.[50]

4 Implementation Analysis

The following chapter will assess whether the MoMA is effectively complying with this order. It will focus on key areas of concern: the insufficiency of transparency to "data subjects", the lack of a clear legal basis for data processing, the absence of written agreements between data processors, and the failure to conduct a systematic and comprehensive data protection impact assessment.

At the core of this analysis is the issue of inadequate information provided to people on the move. Thereby, the analysis seeks to center their voices and experiences, highlighting how opaque surveillance systems and bureaucratic obstacles further marginalize people in the already restrictive environment of the Samos CCAC. This is compounded by the overall lack of transparency in Greece's asylum procedure.

4.1 Insufficient Information Provided

4.1.1 Information Provided on Centaur

In order to comply with the HDPA ruling, the MoMA is required to provide information on the use of CCTV cameras to people held in the CCAC in a manner that is "*concise*, *transparent*, *intelligible and easily accessible*, *using clear and plain language*" in accordance with Article 12(1) and Recital 39 of the GDPR. However, this obligation is not met in practice, in violation of the data protection rights of people held in the CCAC. A significant 82% of respondents reported that they had not received any information from the authorities regarding the use of CCTV cameras within the Samos CCAC. As one

[48] Hellenic Data Protection Authority. 2024. Decision 13/2024. Available (in Greek) here. Page 47.
[49] Hellenic Data Protection Authority. 2024. Decision 13/2024. Available (in Greek) here. Pages 43-44, para 26.
[50] Hellenic Data Protection Authority. 2024. Decision 13/2024. Available (in Greek) here. Page 48.

respondent stated, "*they (the authorities) never told me about cameras.*" Another noted, "*my friends told me, not the authorities.*"

Out of the 27 people interviewed, only five reported having received any information about the presence or use of surveillance cameras in the Samos CCAC. According to one of them, "*when we arrived to the camp, they informed us that the camp had surveillance cameras all around.*"

This limited and inconsistent provision of information suggests that the authorities are not systematically informing people held in the CCAC about the surveillance practices with CCTV cameras. Rather than a blanket policy, the authorities seem to provide information on the use of CCTV cameras only partially, in clear violation of GDPR standards and the HDPA's ruling.

In addition to mandating transparency about CCTV usage, the HDPA ruling specifically requires that warning signs informing individuals about the presence of CCTV cameras include all pertinent and essential information.[51] These signs must be clearly displayed within the Samos CCAC premises in a format that is accessible to all individuals, regardless of language proficiency or literacy levels.

However, the interview data indicates a significant gap between this requirement and actual implementation. 76% of respondents indicated that they did not see any signs informing about the use of CCTV cameras within the Samos CCAC. Only 14% of respondents recalled seeing warning signs. One respondent mentioned noticing "*many signs of cameras next to the exit of the camp*" but noted that these were only available in Greek and English. Another respondent stated that the signs partially used symbols and included "*not a lot of text*" further raising concerns about their adequacy under GDPR standards.

CCTV warning signs may technically be present within the Samos CCAC. However, the low number of respondents who reported noticing them suggests that these signs are not sufficiently visible or prominent to meet the standards set by GDPR. Moreover, the signs that have been installed do not appear to comply with the HDPA's requirements for accessibility and clarity.

The fact that the signs remain reportedly only in Greek and English renders them inaccessible to the majority of people held in the Samos CCAC, many of whom do not speak or understand these languages. Additionally, reports that the signs contain "*not a lot of text*" raise doubts on whether all information required by GDPR is being communicated to the people, even after the compliance order imposed the obligation

[51] Articles 13 and 14 of the GDPR require data controllers to provide specific information to data subjects. This includes the identity and the contact details of the controller, the contact details of the data protection officer, the purposes of the processing for which the personal data are intended and the legal basis for the processing, and the recipients of the personal data. Hellenic Data Protection Authority. 2024. Decision 13/2024. Available (in Greek) here. Page 37, para 19.

on the MoMA to make amendments and additions. This lack of sufficient, accessible signage reflects a failure to comply with legal obligations concerning transparency in surveillance practices. It underscores the authorities' ongoing shortcoming to ensure that information about the use of surveillance cameras is not only visible, but also understandable and accessible to all people held in the Samos CCAC, regardless of their language proficiency or literacy levels.

4.1.2 Information Provided on Hyperion

In order to comply with the HDPA ruling, the authorities must clearly inform individuals about the different purposes for which their biometric data, such as fingerprints, are collected, the legal basis for each purpose, and any transfers of this data to other stakeholders, such as law enforcement or other state authorities. However, this does not appear to be happening in practice.

75% of respondents reported that they had not received any information regarding why their fingerprints were being taken. One individual recalled being told simply to "*sit and wait*" for several hours without explanation. Another stated "*No, no one explains it. They only take fingerprints and take us from one place to another, and we do it without knowing why. There is no person to explain what is happening*". This lack of information given was confirmed by another respondent saying: "*When they want to take fingerprints, the police officers they just bring the people in, they don't talk*".

Even among those who did receive some form of information, the explanations were vague and unlikely to meet the HDPA's requirements. Respondents reported being told that fingerprinting was "*for us to be in the system*", or "*it was procedure*". These generic justifications fall short of GDPR standards, which require information to be provided in a concise, transparent, intelligible, and easily accessible form, indicating clear and specific purposes for data processing.

The widespread lack of meaningful information not only undermines informed consent and transparency but also signals ongoing non-compliance with the HDPA decision and EU data protection standards.

4.2 Lack of Appropriate Legal Basis for Data Processing

In its 2024 revised Privacy Policy concerning the Centaur surveillance system, the MoMA invokes Article 6(1)(e) GDPR as the legal basis for processing personal data, asserting that such processing is carried out in the public interest under the Dublin III Regulation and the Immigration Code. The policy also identifies the CCACs as "critical infrastructures of the State." However, the MoMA fails to meet its obligations as a data controller, as Article 6(1)(e) GDPR requires a clear justification that the data processing activity is strictly necessary for the exercise of official authority. The MoMA does not

provide any explanation as to why the deployment of video surveillance systems is necessary in this specific context, and necessity cannot be presumed solely based on institutional authority. With regard to biometric data, the MoMA refers to Article 9(2)(g) GDPR, citing "substantial public interest" as the legal basis for processing. Nevertheless, this provision mandates that such processing must be grounded in specific Union or Member State law, be proportionate to the intended purpose, and incorporate appropriate safeguards to protect fundamental rights. Policy of the MoMA lacks any explicit reference to a concrete legal instrument authorizing biometric surveillance, instead relying on general references such as the Dublin III Regulation. This falls short of GDPR requirements. There is no demonstration of proportionality or mention of safeguards. Consequently, the MoMA has not sufficiently justified the legality or necessity of either standard or biometric data processing within the Centaur system.

Similar issues of GDPR compliance arise in the context of the Hyperion system. To begin with, the only available document referencing Hyperion's data processing activities addresses solely the processing of biometric data, making no mention of the processing of non-special categories of personal data (such as biographical data). As a result, the legal basis for such processing remains entirely undefined. With respect to biometric data, the policy presents a vague and internally inconsistent legal rationale. The MoMA simultaneously cites Article 6 GDPR—which is inapplicable to special categories of data—and Article 9(2)(g) GDPR, asserting that the processing is justified on grounds of substantial public interest under the Dublin III Regulation or the Immigration Code. However, within the same paragraph, the policy also asserts that no special category data is processed under either the Hyperion system, thereby contradicting its earlier claim. Moreover, as mentioned before, Article 9(2)(g) GDPR requires that such processing be clearly grounded in specific Union or Member State legislation and accompanied by appropriate and tailored safeguards. As with the Centaur system, the MoMA once again fails to reference any concrete legal instrument that would authorize the use of biometric authentication for entry/exit systems in the CCACs. Additionally, the policy lacks any assessment of necessity and proportionality or the inclusion of specific measures to protect the fundamental rights and interests of data subjects, including staff and other non-residents entering the CCACs.

4.3 Written Contracts between Processing Factors

The implementation of the Centaur and Hyperion systems by the MoMA raises serious concerns regarding GDPR compliance, particularly in relation to transparency, data sharing, and the existence of adequate data processing agreements. According to the findings of the HDPA in relation to the Centaur system, the contracts submitted for review lack specific provisions outlining the data processing responsibilities of the system operators. More critically, there is no Data Processing Agreement (DPA) or any equivalent legal framework in place between the MoMA and the Hellenic Police, despite clear indications that data sharing occurs between the two entities. For example, the

document titled “Centaur Privacy Policy – Video Surveillance & Security Camera System in the MMA’s Accommodation Facilities”[52] explicitly states in Article 2.5 that the Centaur system is interconnected with the Hellenic Police, thereby allowing for the potential processing of special categories of personal data for law enforcement purposes. This processing is justified by the MoMA under Article 6(1)(c) GDPR, referring to legal obligations to cooperate with law enforcement authorities. However, the lack of a formalized agreement with the police raises significant concerns regarding the legality and safeguards surrounding such data transfers. Additionally, Article 6.5 of the same privacy policy references a “transfer policy” designed to document and assess all disclosures of personal data. Yet, it remains unclear whether data subjects have access to this policy or whether they have been adequately informed of such transfers, particularly those involving the Hellenic Police or other third parties. Moreover, the “Privacy Policy for the Processing of Biometric Data” states in Article 12 that data transfers may occur if the data subject has been informed and does not object[53]—an assertion that necessitates verification and appropriate documentation to ensure compliance.

With respect to the Hyperion system, these issues are exacerbated by a pronounced lack of transparency. The MoMA submitted only partial documentation to the HDPA, citing secrecy concerns. As noted in the HDPA Decision, the incomplete documentation prevented the Authority from verifying whether the requirements of Article 28 GDPR—particularly the existence of valid contracts with data processors—had been met.

4.4 Lack of Systematic and Comprehensive Impact Assessments (DPIAs – Article 35 GDPR)

The MoMA has not published a DPIA on its website. While the MoMA, as the data controller, is not legally required to publish a DPIA, it has instead chosen to make a Fundamental Rights Impact Assessment (FRIA) – dated January 2024 – publicly available online. Under Article 5 of Law 4961/2022, the MoMA is obligated to carry out a FRIA; however, there is no requirement for such an assessment to be published. This raises questions about the rationale behind the MoMA’s decision to disclose the FRIA while withholding the DPIA.

The section of the FRIA that addresses personal data protection is limited, merely stating that a DPIA had already been conducted prior to the FRIA’s publication (i.e., before January 2024), without offering any further detail. As a result, there is no publicly

[52] Hellenic Ministry of Migration. 2024. Centaur Privacy Policy – Video Surveillance & Security Camera System in the MMA's Accommodation Facilities. Available here.
[53] Hellenic Ministry of Migration. 2024. Privacy Policy for the Processing of Biometric Data. Available here. Page 8.

available information confirming whether the MoMA has updated its DPIA in accordance with the HDPA April 2024 decision. The only known reference to the DPIA remains the one included in the FRIA from January 2024.

Moreover, there is a complete lack of information regarding any consultations with MoMA's Data Protection Officer (DPO) concerning the revision of the DPIA. This absence of transparency further complicates the assessment of whether MoMA has fulfilled its obligations under the GDPR and the relevant national legal framework.

4.5 General Trend Analysis

The analysis shows that the MoMA is falling short in implementing the compliance order issued by the HDPA with regards to the three-part principles of lawfulness, fairness, and transparency. It further underscores MoMA's continued failure to adequately demonstrate compliance with its legal obligations, thereby breaching the principle of accountability.

Beyond this, the use of invasive technologies against racialized individuals appears to further contribute to problematic developments ultimately reinforcing colonial logics within contemporary border regimes. To contextualize this analysis, the following section will examine how surveillance technologies more broadly function to enforce racialized governance and border regimes. It will then explore how these dynamics are materialising within the Samos CCAC, contributing to the securitization of migration, the dehumanization of people on the move, and the increasing control over movement and mobility.

4.5.1 Surveillance as Border Logic of Racialized Control

From Occupied Palestine, to the US-Mexican border, to the EU borders, as key sites of control and differentiation in human mobility, borders are deeply connected with expanding surveillance and monitoring practices.[54] In particular, biometric technologies, like fingerprinting, facial recognition, or iris scans, increasingly serve as tools for border enforcement. Facilitating tracking and control of racialised people and people on the move,[55] these technologies reinforce systems of exclusion and discrimination. Scholars have argued that biometric security has long been connected to processes of racialisation, constructing racialized identities and people on the move as a security threat.[56] In an environment of "spiralling securitisation"[57] and increasing criminalisation of movement, people on the move are "presupposed to be criminals unless proven

[54] Peter Adey. 2012. Borders, identification and surveillance. New regimes of border controls. Available here.
[55] Weaving Liberation. Digital Policing Harms. Available here.
[56] Mark Maguire. 2012. Biopower, racialization and new security technology. Available here.
[57] Sarah Léonard and Christian Kaunert. 2022. The securitisation of migration in the European Union: Frontex and its evolving security practices. Available here.

otherwise."[58] This presumption is reinforced by the fact that biometric technologies were historically reserved for criminal investigations.[59] When applied to people on the move, these tools render movement in itself as a criminal act "that must be surveilled and managed".[60] This construction is used to justify the expansive use of technology and border control, contributing to xenophobia.

Sachseder et al. argue that using racialized bodies of people on the move for data gathering and enhancing racialized constructions of movement as a 'threat' and 'crime', "reaffirms the need for colonial ordering of chaotic, unknown 'Otherness'."[61] In that sense, postcolonial scholarship traces the origins of surveillance to colonial governance, where data collection and surveillance were not only used to construct racialized distinctions between colonizers and the colonized but also to justify physical intrusions and control.[62] In (post)-colonial contexts contemporary monitoring practices serve to regulate and control (formerly) colonized populations.[63] Much like borders, surveillance thereby serves to maintain colonial and social hierarchies - "keeping 'others' out."[64]

Therefore, modern surveillance extends historical patterns of racialized governance, further embedding colonial logics into contemporary border regimes and serving to justify increasingly hostile migration policies and border enforcement.

4.5.2 Samos CCAC: Surveillance, Confinement, and Dehumanization

Responses from the interviews highlight how the use of surveillance technologies in the Samos CCAC seems to contribute to, reproduce and reinforce problematic trends, namely securitization of migration and dehumanization of people on the move and the control of movement and mobility. This manifests in three ways:

1. **Framing movement as a threat:** One respondent reported that authorities stated they were taking their fingerprints "*for security reasons, because we are entering Greece.*" This logic is mirrored by the securitized architecture of the Samos CCAC, with barbed wire fences, high police presence and the use of airport style security checks at the

[58] Petra Molnar. 2020. Technological testing grounds: Migration management experiments and reflections from the ground up. Available here.
[59] Euro-Med Human Rights Monitor. 2022. The multiple threats of biometric technology at European borders. Available here.
[60] Petra Molnar. 2020. Technological testing grounds: Migration management experiments and reflections from the ground up. Available here.
[61] Julia Sachseder and Saskia Stachowitsch. 2019. The gendered and racialized politics of risk analysis. The case of Frontex. Available here.
[62] Tahu Kukutai and Donna Cormack. 2022. Indigenous Peoples, Data, and the Coloniality of Surveillance. Available here.
[63] Tahu Kukutai and Donna Cormack. 2019. 'Mana motuhake ā-raraunga: datafication and social science research in Aotearoa. Available here; Tahu Kukutai and Donna Cormack. 2022. Indigenous Peoples, Data, and the Coloniality of Surveillance. Available here.
[64] Alpa Parmar. 2020. Borders as Mirrors: Racial Hierarchies and Policing Migration. Critical Criminology. Available here.

entrance of the Samos CCAC.[65] The use of such tools rooted in suspicion and control, constructs people on the move as potential threats. These practices reproduce harmful and racist narratives that equate seeking asylum with danger and migration with criminality, justifying surveillance and repression as a response to racialized mobility.

2. **Objectification and dehumanization of people on the move:** Multiple respondents expressed that they never felt like they could refuse giving their fingerprints and that the "*they* (the authorities) *take us from one place to another*, *and we do it* (provide fingerprints) *without knowing why*." This suggests that people do not feel as though they have the right to question such practices and exercise their rights, through e.g. receiving information on data collection. People on the move are not positioned as individuals with rights and agency. Instead, they are treated as passive objects of control. This illustrates how surveillance practices contribute to the broader dehumanization of people on the move, reducing them to bodies to be monitored, rather than individuals entitled to dignity, transparency, and autonomy.

3. Surveillance as confinement: One respondent mentioned that the long queues caused by the biometric entry systems and airport-style security checks actively discouraged them from leaving the Samos CCAC. This suggests that even within Greek territory, surveillance technology contributes to in practice limiting the mobility of people on the move, maintaining spatial control and keeping people confined within the isolated environment of the Samos CCAC where people have no or only severely limited access to essential services.

5 Conclusion and Recommendations

This report has analysed at the implementation of the HDPA decision, finding that the MoMA has failed to implement the compliance order in four ways:

1. It has provided only limited and insufficient information on the use of the Centaur and Hyperion systems in the Samos CCAC, reinforcing problematic trends of border securitization, dehumanization of people on the movement and confinement of mobility.

2. It has failed to establish privacy policies that clearly articulate a valid legal basis for processing both standard and special categories of personal data in relation to the Centaur and Hyperion surveillance systems. Instead, it relies on vague references to the public interest, without demonstrating necessity,

[65] Airport security checks were intensified after the 9/11 attacks as part of global counter-terrorism efforts. Much like biometric data collection with its origins in criminal investigations, the use of such tools in spaces meant to accommodate asylum seekers contributes to framing this group as a security threat.

proportionality, or grounding in specific legal provisions—thereby falling short of GDPR requirements.

3. It has not provided documentation, confirming the existence of formal DPAs with key partners such as the Hellenic Police, despite evidence of active data sharing.

4. It has remained silent regarding any revisions to its Data Protection Impact Assessment (DPIA) for the Hyperion and Centaur systems. The only known reference dates back to January 2024—prior to the HDPA's ruling—and is not publicly accessible. This lack of transparency, including the absence of updates or evidence of consultation with the DPO, raises serious concerns about MoMA's compliance with the GDPR.

The ongoing non-compliance with data protection obligations further undermines the rights of individuals subjected to surveillance and control in the already rights-depriving environment of the Samos CCAC. It also sets a dangerous precedent for future reception facilities under the EU's New Pact on Migration and Asylum.

To address the ongoing non-compliance with data protection rights raised in this report and to foster the protection of fundamental rights, we call on the EU and Greek authorities to:

1. Transparency and Accountability
❖ Make the technical specifications, data sources, and operational methods of Centaur and Hyperion publicly available.
❖ Conduct and publish detailed fundamental rights impact assessments for all high-risk technologies used in CCACs.

2. Protection of Rights for People on the Move
❖ Provide clear, accessible information to people on the move and workers in the CCAC about the surveillance technologies in use, including their purpose, legal basis, and data processing methods.
❖ Replace invasive fingerprinting with less intrusive methods, such as ID cards, to facilitate entry and exit while respecting personal dignity.

3. Safeguards Against Discrimination
❖ Ensure that AI algorithms used in Centaur and other systems are free from bias by implementing comprehensive testing and external review processes.
❖ Publish regular reports assessing the impact of these technologies on vulnerable populations, including safeguards to prevent discrimination.