ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Μετανάστευσης & Ασύλου

CENTAUR & HYPERION SYSTEMS IN THE RECEPTION AND IDENTIFICATION CENTRES
FUNDAMENTAL RIGHTS IMPACT ASSESSMENT (FRIA)

Versioning:

Initial version 11 January 2022

updated version 11 January 2024

Οργανισμός	
Νομική Οντότητα	HELLENIC REPUBLIC - MINISTRY OF IMMIGRATION AND ASYLUM
Υπεύθυνος συμπλήρωσης DPIA	IOANNIS GIANNAKAKIS
Επιχειρησιακή Μονάδα	General Secretariat for the Reception of Asylum Seekers
Στοιχεία επικοινωνίας	Gen. Secr. for the Reception of Asylum Seekers, 196-198 Thivon Avenue
Υπεύθυνος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα - "Data Protection Officer"	Euroaxes Consultants S.A.
Στοιχεία επικοινωνίας	https://migration.gov.gr/epikoinonia/
	fro-complaints@migration.gov.gr
Συμβουλή υπευθύνου προστασίας δεδομένων προσωπικού χαρακτήρα	dpo@migration.gov.gr
Επικύρωση (ημερομηνία)	Versioning:
	Initial version 11 January 2022 updated version 11 January 2024

Έργο / Εφαρμογή	
Τίτλος	Centaur & Hyperion Systems in Reception and Identification Centres
Hosting type (π.χ. εντός ή εκτός υποδομής Εταιρείας)	Centaur & Hyperion Systems belongs to Ministry's infrastructure
Σκοπός επεξεργασίας/ Σύντομη περιγραφή	Fundamental rights encompass rights such as human dignity and non-discrimination, as well as rights in relation to data protection and privacy. Prior to self-assessing Centaur & Hyperion Systems, a fundamental rights impact assessment (FRIA) should be performed. A FRIA could include questions such as the following – drawing on specific articles in the Charter and the European Convention on Human Rights (ECHR) its protocols and the European Social Charter.

Fundamental Rights Impact Assessment

Fundamental Rights Impact Assessment	
Name	
Organisation/Position	Ministry of Migration and Asylum
Date	
Contributors	
Systems assessed	Centaur System - Hyperion System
Detailed description of the technology and input data	Centaur System - Hyperion System (The project includes CCTV, x-rays, magnetic gates, loudspeakers, one control room per camp and one drone per camp)
Detailed description of the purposes and context of use	Centaur CCTV: Is a CCTV system installed in common areas, the perimeter and the corridors in the buildings, NOT in the rooms, NOT for beds and wc/showers Hyperion: X-rays and magnetic gates: they are installed in the main entrance Loudspeakers: they are installed in multiple places in the camp, NOT in the rooms.The usage of the drone will be for monitoring from above in case of emergency and for inspecting the perimetrical fence to detect any violation of it
Centaur System	The Centaur CCTV system is a digital electronic and physical security management system around and inside the facilities, using cameras and behavioral analysis algorithms (Artificial Intelligence Behavioral Analytics). It includes Signaling of perimeter breach alarms using cameras and motion analysis algorithms, signaling of illegal behavior alarms of individuals or groups of individuals in assembly areas inside the facility, and using unmanned aircraft systems to assess incidents inside the facility without human intervention, among other functions .
Hyperion System	The Hyperion system is the asylum seeker management system, regarding all the needs of the Reception and Identification Service. It includes a detailed record of the data of asylum seekers and will interoperate with the ALKYONI II system regarding the asylum application.In addition, it is the basic tool for the operation of the facilities and hospitality structures as it is responsible for access control (entrance - exit through security turnstiles, with presentation of an individual immigrant, NGO member, employee card and simultaneous use of a fingerprint), of monitoring benefits per asylum seeker using an individual card (food, clothing supplies, etc.) and movements between facilities and hospitality structures.

1. Presumption of innocence and right to an effective remedy and to a fair trial

Everyone charged with a criminal offence must be presumed innocent until proved guilty according to law.
Everyone whose rights and freedoms are violated has the right to an effective remedy before a tribunal.
Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law, including rights:
❖ to be informed promptly of the nature and cause of the accusation;
❖ to bring their arguments and evidence as well as scrutinise and counteract the evidence presented against them; and
to obtain an adequately reasoned and accessible decision.

Challenge	Evaluation	Estimated impact level
1.1 The AI system does not communicate that a decision/advice or outcome is the result of an algorithmic decision	NEGATIVE. Human oversight is active and involved, with the human retaining full control and the AI technologies in Centaur and Hyperion only providing recommendations or input. Decisions cannot be exercised without affirmative actions by the human, such as a human command to proceed with a given decision.	LOW
1.2 The AI system does not provide percentages or other indication on the degree of likelihood that the outcome is correct/incorrect, prejudicing the user that there is no possibility of error and therefore that the outcome is undoubtedly incriminating	NEGATIVE. The AI technologies in Centaur and Hyperion do not communicate any percentages or other indication or the likelihood of the output and it is impossible for the System User to establish it.	LOW
1.3 The AI system produces an outcome that forces a reversal of burden of proof upon the suspect, by presenting itself as an absolute truth, practically depriving the defence of any chance to counter it	NEGATIVE. When the AI technologies in Centaur and Hyperion flags an individual (data subject), a further investigation against the individual is possible to get started, even in the absence of other evidence incriminating the data subject	LOW
1.4 There is no explanation of reasons and criteria behind a certain output of the AI system that the user can understand	AFFIRMATIVE. The AI technologies in Centaur and Hyperion does not communicate to the User a certain output and/or the reasons and criteria behind any of the output reached and the User cannot understand them with or any other means.	LOW
1.5 There is no indication of the extent to which the AI system influences the overall decision-making process	AFFIRMATIVE. There is no indication of the AI technologies in Centaur and Hyperion weight of the output influences in the overall decision-making process	LOW
1.6 There is no set of measures that allow for redress in case of the occurrence of any harm or adverse impact	Data subject can file a complaint to the Ministry's Fundamental Rights Protection Officer and/or the DPO who work in collaboration with the Special Committee for Compliance with Fundamental Rights which was recently established in collaboration with the European Commission and whose purpose will be to monitor the procedures and implementation of national, EU and international legislation in areas of border protection and the granting of international protection.	-

2. Right to equality and non-discrimination

Everyone is equal before the law.
Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a
Everyone should be protected against discriminatory decisions or policies, including automated decision-making based on sensitive data.

Challenge	Evaluation	Estimated impact level
2.1 The AI system targets members of a specific social group	AI system learn from data which may be unbalanced and/or reflect discrimination, they may produce outputs which have discriminatory effects on people based on their gender, race, age, health, religion, disability, sexual orientation or other characteristics. The fact that AI systems learn from data does not guarantee that their outputs will not lead to discriminatory effects, however human oversight is active and involved, with the human retaining full control and the AI technologies in Centaur and Hyperion	MODERATE
2.2 There are no mechanisms to flag and correct issues related to bias, discrimination, or poor performance	The pillars of performance and associated measures and mechanisms for addressing bias, discrimination, or poor performance are: (i) regulatory framework addressing regulations and codes of ethics and codes of conduct, (ii) operational management for addressing racism and racial discrimination at the individual level, inclusive of intrapersonal and interpersonal forms of discrimination and (iii) enhancing organizational resilience, agility and adaptability, providing adequate and appropriate resources and capacities, enhancing governance and accountability, enhancing the empowerment of personnel and the development of networks for safe space and supporting organizations in managing change	-
2.3 The AI system does not consider the diversity and representativeness for specific population or problematic use cases	Diversity and inclusion (D&I) considerations are significantly neglected in AI systems design, development, and deployment. Ignoring D&I in AI systems can cause digital redlining, discrimination, and algorithmic oppression, leading to AI systems being perceived as untrustworthy and unfair	-

3. Freedom of expression and information

Everyone has the right to freedom of expression, including freedom to hold opinions, communicate and acquire information
❖ State negative obligation not to interfere and positive obligation to facilitate the exercise of the right

Challenge	Evaluation	Estimated impact level
3.1 There is no mechanism to limit the deployment of the AI system to suspected individuals	AI's three biggest limitations are (1) AI can only be as smart or effective as the quality of data you provide it, (2) algorithmic bias and (3) its "black box" nature.	-
3.2 The data stored, recorded, and produced are not easily accessible to concerned individuals	The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data, as well as other supplementary information	-
4. Right to respect for private and family life and right to protection of personal data Everyone has the right to respect for their private and family life, home and communications. ❖ Self-development without state interference. ❖ Everyone has the right to the protection of personal data concerning them. ❖ Personal data must be processed fairly for specified purposes and on a legitimate basis. ❖ Rights of access and rectification. ❖ Independent oversight.		
Challenge	Evaluation	Estimated impact level
4.1 There are no mechanisms for the user to exercise control over the processing of personal data	One major mechanism for responsible compatibility-based processing of personal data compels the Ministry to make a thorough assessment of the processing activities involved and of both the interests of the data subject and the Ministry, and it forces the Ministry to be transparent about the processing activities that are employed.	-
4.2 There are no measures to ensure the lawfulness of the processing of personal data	In this case, the processing is carried out in the public interest on the legal basis in EU or national law. Its purpose is determined in that legal basis or be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller. Therefore, this legal basis is relevant, in particular, for processing operations by public authorities for the purpose of carrying out their tasks.	-
4.3 There are no procedures to limit the access to personal data and to the extent and amount necessary for those purposes	In particular, the specific purposes for which personal data are processed are explicitly and legitimately and determined at the time of the collection of the personal data. However, further processing for archiving purposes in the public interest, scientific, or historical research purposes or statistical purposes (in accordance with Article 89(1) GDPR) is not considered to be incompatible with the initial purposes.	-
4.4 There is no mechanism allowing to comply with the exercise of data subject's rights (access, rectification and erasure of data relating to a specific individual)	Modalities are provided for facilitating the exercise of the data subject's rights, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The Ministry also provides means for requests to be made electronically, especially where personal data are processed by electronic means. The Ministry responds to requests from the data subject without undue delay and at the latest within one month and to give reasons where the Ministry does not intend to comply with any such requests.	-
4.5 There are no specific measures in place to enhance the security of the processing of personal data (via encryption, anonymisation and aggregation)	(i) determine the existing or planned measures to address each risk (e.g. access control, backups, traceability, premises security, encryption); (ii) estimate the severity and likelihood of the risks, based on the above elements (example of a scale that can be used for the estimate: negligible, moderate, significant, maximum); (iii) implement and verify planned measures if existing and planned measures are deemed appropriate, ensure that they are implemented and monitored; (iv) conduct periodic security audits: each audit should result in an action plan whose implementation should be monitored at the highest level of the organisation.	-
4.6 There is no procedure to conduct a data protection impact assessment	A DPIA has been conducted for the Centaur-Hyperion Systems	-

System Governance

System Governance	
Name	
Organisation/Position	Ministry of Migration and Asylum
Date	
Contributors	
Systems assessed	Centaur System - Hyperion System
Detailed description of the technology and input data	Centaur System - Hyperion System (The project includes CCTV, x-rays, magnetic gates, loudspeakers, one control room per camp and one drone per camp)
Detailed description of the purposes and context of use	

1. Human autonomy								
Component	Minimum standards to be achieved	Initial impact estimate		Additional mitigation measures implemented	Final assessment		Responsible department	Timeline
		Challenge no.	Impact level		Final estimated impact level	Further actions		
Human agency	The task allocation between the AI system and the user allows meaningful interactions	[1.2]	Low	The AI System reveals the likelihood of the output, so that the User can take an informed decision on the follow up	Low	Performance monitoring (particularly for	IT Department	January 2024
		[1.5]	Low	The User can play an active role in the decision making process, by modifying the parameters informing the decision of	Low	implementing a mechanism to allow the User	IT and legal departments	January 2024
	There are procedures to describe the level of human involvement and the moments for human interventions	[1.5]	Low	The weight of the output of the AI System in the decision making processess of the organization is concretely evaluated. The results are made known to the users, who are tasked to take an informed decision on the follow up actions	Low	Testing and validating	IT and legal departments	January 2024
		[2.2]	Low	Human intervention to aid in data collection, annotation, and validation helps improve the performance of AI	Low	Ethics and rule of law by design (X-by-design)	IT and legal departments	January 2024
		[4.1]	Low	The User ensures that the development, deployment and use of AI systems meets the seven key requirements for trustworthy AI: (1) human agency and	Low	Architectures for trustworthy AI	IT and legal departments	January 2024
	The AI system does not affect human autonomy by interfering with the user decision-making process	[1.2]	Low	Comply with Article 14 (Human oversight) of EU AI Act. For every incomplete or inaccurate data and unsecured “protected” data, there is Data-quality metrics and assurance measures and Privacy protections	Low	Consider the task allocation between the AI system and humans for meaningful interactions and appropriate human oversight and control. The AI system enhance or augment human capabilities; Take safeguards to prevent overconfidence in or overreliance on the AI system for work processes;	IT Department	January 2024
		[1.3]	Low	Comply with Article 14 (Human oversight) of EU AI Act. In case of Nonrepresentative data, Biased or discriminatory model outcomes and Model instability or performance degradation, the User should apply Transparency and explainability requirements, Fairness review, Real-time performance analysis, Model testing and validation.	Low	Consider the appropriate level of human control for the particular AI system and use case. Describe the level of human control or involvement; Put in place mechanisms and measures to ensure human control or oversight; Take measures to enable audit and to remedy issues related to governing AI autonomy;	IT Department	January 2024

Human oversight		[1.5]	Low	Comply with Article 14 (Human oversight) of EU AI Act. In case of Nonrepresentative data, Biased or discriminatory model outcomes and Model instability or performance degradation, the User should apply Transparency and explainability requirements, Fairness review, Real-time performance analysis, Model testing and validation.	Low	Allocating enough resources for regular human monitoring and corrective action-taking is one best practice. Keep decisions actionable to combat this, but ensure monitoring is in place to stay within regulatory requirements.	IT Department	January 2024
		[4.1]	Low	Comply with Article 14 (Human oversight) of EU AI Act. In case of Nonrepresentative data, Biased or discriminatory model outcomes and Model instability or performance degradation, the User should apply Transparency and explainability requirements, Fairness review, Real-time performance analysis, Model testing and validation.	Low	Allocating enough resources for regular human monitoring and corrective action-taking is one best practice. Keep decisions actionable to combat this, but ensure monitoring is in place to stay within regulatory requirements.	IT Department	January 2024
	There are mechanisms to prevent overconfidence or over-reliance in the results offered by the AI system	[1.1]	Low	Comply with Article 14 (Human oversight) of EU AI Act. When there is a situation of Technology-environment malfunction	Low	Allocating enough resources for	IT Department	January 2024
		[1.2]	Low	Comply with Article 14 (Human oversight) of EU AI Act. When there is a situation of Technology-environment malfunction	Low	Allocating enough resources for	IT Department	January 2024
	There are mechanisms to detect and correct wrong outputs	[1.6]	Low	Comply with Article 14 (Human oversight) of EU AI Act. When there is a situation of Technology-environment malfunction, Slow detection of/response to, performance issues, Cybersecurity threats, Failure at the human–machine interface, the User applies Performance monitoring (particularly for data flows), Access management and other cyberprotections, Capture and analysis of errors, near misses, and overrides	Low	Allocating enough resources for regular human monitoring and corrective action-taking is one best practice. Keep decisions actionable to combat this, but ensure monitoring is in place to stay within regulatory requirements.	IT Department	January 2024
		[2.2]	Low	Apply Article 14 (Human oversight) of EU AI Act. When there is a situation of Technology-environment malfunction, Slow detection of/response to, performance issues, Cybersecurity threats, Failure at the human–machine interface, the User applies Performance monitoring (particularly for data flows), Access management and other cyberprotections, Capture and analysis of errors, near misses, and overrides	Low	Allocating enough resources for regular human monitoring and corrective action-taking is one best practice. Keep decisions actionable to combat this, but ensure monitoring is in place to stay within regulatory requirements.	IT Department	January 2024

		[2.3]	Low	Comply with Article 14 (Human oversight) of EU AI Act. When there is a situation of Technology-environment malfunction, Slow detection of/response to, performance issues, Cybersecurity threats, Failure at the human–machine interface, the User applies Performance monitoring (particularly for data flows), Access management and other cyberprotections, Capture and analysis of errors, near misses, and overrides	Low	Allocating enough resources for regular human monitoring and corrective action-taking is one best practice. Keep decisions actionable to combat this, but ensure monitoring is in place to stay within regulatory requirements.	IT Department	January 2024
	There are mechanisms to safely abort an entire operation when needed			Ensure a stop button or procedure to safely abort an operation where needed. Procedure to abort the process entirely, in part, or delegate control to a human			IT Department	

2. Transparency								
Component	Minimum standards to be achieved	Initial impact estimate		Additional mitigation measures implemented	Final assessment		Responsible department	Timeline
		Challenge no.	Impact level		Final estimated impact level	Further actions		
Traceability	There are mechanisms to ensure the traceability of the input data used by the AI system and its outcomes			Comply with Article 13 (Transparency and provision of information to users) of EU AI Act. All human rights impacts are addressed. Where it is necessary to prioritise actions to address impacts, severity of human rights impacts is the core criterion. Addressing identified impacts follows the mitigation hierarchy of 'avoid-reduce-restore remediate'		Auditing and monitoring tools can help to identify potential problems with AI systems. They can also help to track the performance of AI systems and to identify areas where they need to be improved. This can help to identify potential biases in the system and to correct them.	IT and legal departments	January 2024
Explainability	It is possible for the user to understand and explain the reasons and criteria behind a certain output of the AI system	[1.4]	Low	Comply with Article 13 (Transparency and provision of information to users) of EU AI Act. Explainability, on the other hand, refers to the ability to explain the workings and decisions of an AI system in a way that is understandable to humans. This is especially important for complex AI models like neural networks, which can often behave like "black boxes," making decisions in ways that are not easily interpretable by humans. Explainability mechanisms help to ensure that AI decisions can be interrogated and understood, thereby facilitating accountability. In determining mitigation measures, are all efforts made to first avoid the impact altogether, and if this is not possible, to reduce, mitigate and remediate the impact	Low	Auditing and monitoring tools can help to identify potential problems with AI systems. They can also help to track the performance of AI systems and to identify areas where they need to be improved. This can help to identify potential biases in the system and to correct them.	IT and legal departments	January 2024

Communication	There are procedures enabling the user to communicate to the public that decisions are taken on the basis of an algorithmic process	[1.3]	Low	Comply with Article 13 (Transparency and provision of information to users) of EU AI Act. Impact assessment which identify ways of exercising leverage to address any impacts the business contributes or is directly linked to (e.g. through business relationships)? Where leverage does not exist, does impact mitigation include building leverage to address such impacts?	Low	Auditing and monitoring tools can help to identify potential problems with AI systems. They can also help to track the performance of AI systems and to identify areas where they need to be improved. This can help to identify potential biases in the system and to correct them.	IT and legal departments	January 2024
	There are procedures enabling the user to explain to the public the purposes, characteristics, limitations, and shortcomings of the AI system			Comply with Article 13 (Transparency and provision of information to users) of EU AI Act. Impacts are addressed according to the severity of their human rights consequences. This includes considering the scope, scale and irremediability ofparticular impacts, taking into account the views of rightsholders and/or their legitimate representatives.		Auditing and monitoring tools can help to identify potential problems with AI systems. They can also help to track the performance of AI systems and to identify areas where they need to be improved. This can help to identify potential biases in the system and to correct them.	IT and legal departments	January 2024
	There are procedures enabling the user to make the data stored, recorded, and produced available to concerned individuals	[3.2]	Low	Comply with Article 13 (Transparency and provision of information to users) of EU AI Act. The impact assessment process is as transparent as possible in order to adequately engage affected or potentially affected rightsholders, without causing any risk to security and wellbeing of rightsholders or other participants (such as NGOs and human rights defenders). Impact assessment findings are appropriately publicly communicated.	Low	Auditing and monitoring tools can help to identify potential problems with AI systems. They can also help to track the performance of AI systems and to identify areas where they need to be improved. This can help to identify potential biases in the system and to correct them.	IT and legal departments	January 2024

3. Diversity, non-discrimination and fairness								
Component	Minimum standards to be achieved	Initial impact estimate		Additional mitigation measures implemented	Final assessment		Responsible department	Timeline
		Challenge no.	Impact level		Final estimated impact level	Further actions		
	There are procedures to test and evaluate the diversity and representativeness of the used datasets, also for specific social group or use cases	[2.3]	Low	Comply with Article 52 (Transparency obligations for certain AI systems) of EU AI Act. Transparency and explainability requirements Fairness review Real-time performance analysis Model testing and validation	Low	The Ministry has formed ethical review committees to analyze AI initiatives, uncover any biases, and ensure fairness consisted by the Ministry's Fundamental Rights Protection Officer and the Special Committee for Compliance with Fundamental Rights.	IT and legal departments	January 2024

Unfair bias avoidance	There are procedures to test and evaluate the diversity and representativeness of the algorithm used, also for specific social groups or use cases	[2.3]	Low	Comply with Article 52 (Transparency obligations for certain AI systems) of EU AI Act. Transparency and explainability requirements Fairness review Real-time performance analysis Model testing and validation	Low	The Ministry has formed ethical review committees to analyze AI initiatives, uncover any biases, and ensure fairness consisted by the Ministry's Fundamental Rights Protection Officer and the Special Committee for Compliance with Fundamental Rights.	IT and legal departments	January 2024
	There are procedures to evaluate whether specific social groups are disproportionally affected by the AI system	[2.1]	Low	Comply with Article 52 (Transparency obligations for certain AI systems) of EU AI Act. Transparency and explainability requirements Fairness review Real-time performance analysis Model testing and validation	Low	The Ministry has formed ethical review committees to analyze AI initiatives, uncover any biases, and ensure fairness consisted by the Ministry's Fundamental Rights Protection Officer and the Special Committee for Compliance with Fundamental Rights.	IT and legal departments	January 2024
	There are mechanisms to flag and correct bias, discrimination or poor performance	[2.2]	Low	Comply with Article 52 (Transparency obligations for certain AI systems) of EU AI Act. Employ compliance, fairness, and system governance committees/teams to evaluate input variables. If working with an internal tech team, education and training can help ensure the responsible use of AI. If working with an external IT team, a stringent screening process must be in place to ensure compliance.	Low	The Ministry has formed ethical review committees to analyze AI initiatives, uncover any biases, and ensure fairness consisted by the Ministry's Fundamental Rights Protection Officer and the Special Committee for Compliance with Fundamental Rights.	IT and legal departments	January 2024

4. Democracy and societal wellbeing

Component	Minimum standards to be achieved	Initial impact estimate		Additional mitigation measures implemented	Final assessment		Responsible department	Timeline
		Challenge no.	Impact level		Final estimated impact level	Further actions		
Social impact	There are procedures to ensure that the social impacts of the AI systems are well understood by the public			Ministry's international collaboration and standardization efforts to establish global norms, standards, and best practices for AI development and deployment are critical for risk mitigation.		employ non-experts to review a sample of results from AI models to assess whether they are accurate, ethics compliant, and satisfactory.	Ministry's Fundamental Rights Protection Officer and the Special Committee for Compliance with Fundamental Rights	January 2024
Society and	There are procedures to assess the broad social impact of the AI system (e.g., chilling effect, power asymmetry, trust, …)			Ministry's international collaboration and standardization efforts to establish global norms, standards, and best practices for AI development and deployment are critical for risk mitigation.		employ non-experts to review a sample of results from AI models to assess whether they are accurate, ethics compliant, and satisfactory.	Ministry's Fundamental Rights Protection Officer and the Special Committee for Compliance with Fundamental Rights	January 2024

democracy	There are mechanisms to limit the deployment of the AI system to groups of individuals on the basis of suspicion/objective criteria	[3.1]	Low	Ministry's international collaboration and standardization efforts to establish global norms, standards, and best practices for AI development and deployment are critical for risk mitigation.	Low	employ non-experts to review a sample of results from AI models to assess whether they are accurate, ethics compliant, and satisfactory.	Ministry's Fundamental Rights Protection Officer and the Special Committee for Compliance with Fundamental Rights	January 2024
5. Privacy and data governance								
Component	Minimum standards to be achieved	Initial impact estimate		Additional mitigation measures implemented	Final assessment		Responsible department	Timeline
		Challenge no.	Impact Level		Final estimated impact level	Further actions		
Respect for privacy and data protection	There are mechanisms for the user to exercise control over the processing of personal data	[4.1]	Low	Comply with Article 10 (Data and data governance) of EU AI Act.		Comprehensive inventory of data that exists; Contextual data classification to identify sensitive data/confidential data; Compliance with regulations that apply to the data fed to the training model, including meeting data consent, residency, and retention requirements; Inventory of all AI models to which data is being fed via various data pipelines; Governance of entitlements to data through granular access controls, dynamic	IT and legal departments	January 2024
	There are measures to ensure the lawfulness of the processing of personal data	[4.2]	Low	Comply with Article 10 (Data and data governance) of EU AI Act.		Establish a Clear AI Data Governance Framework	IT and legal departments	January 2024
	There are measures to minimise the amount of personal data processed	[4.3]	Low	Comply with Article 10 (Data and data governance) of EU AI Act.		Implement Data Retention and Minimization Policies	IT and legal departments	January 2024
	There is a mechanism allowing to comply with data subjects' rights	[4.4]	Low	Affirmative			IT and legal departments	January 2024
Quality and integrity of data	There are specific measures to enhance the security of the processing of personal data (via encryption, anonymization and aggregation)	[4.5]	Low	Comply with Article 10 (Data and data governance) of EU AI Act.		Data-quality metrics and assurance measures Privacy protections	IT and legal departments	January 2024
	There are processes to ensure the quality and integrity of data			Comply with Article 10 (Data and data governance) of EU AI Act.		Data-quality metrics and assurance measures Privacy protections	IT and legal departments	January 2024
	The AI system is aligned with relevant standards (ISO, IEEE) for data security, management and governance			Comply with Article 10 (Data and data governance) of EU AI Act.		Data-quality metrics and assurance measures Privacy protections	IT and legal departments	January 2024
Access to data	There are procedures to limit the access to personal data	[4.3]	-	Comply with Article 10 (Data and data governance) of EU AI Act.		Access management and other cyberprotections	IT and legal departments	January 2024
Governance	There is a procedure to conduct a data protection impact assessment	[4.6]	-	Affirmative			IT and legal departments	January 2024
	A data protection officer has been appointed			Affirmative			IT and legal departments	January 2024
	There are mechanisms to allow reporting of processing activities to the supervisory body			Affirmative			IT and legal departments	January 2024
International data transfers	There are mechanisms to control the transfer of personal data to third countries			Affirmative			IT and legal departments	January 2024
6. Technical robustness and safety								
		Initial impact estimate			Final assessment			

Component	Minimum standards to be achieved	Challenge no.	Impact level	Additional mitigation measures implemented	Final estimated impact level	Further actions	Responsible department	Timeline
Security	The potential vulnerability of the AI system has been assessed			Comply with Article 15 (Accuracy, robustness and cybersecurity) of EU AI Act. Trusted Infrastructure: Investment in secure, robust, and interoperable data infrastructure that can facilitate information sharing. Analysis Infrastructure: Developing sophisticated AI-enabled tools and platforms that can assist in auditing and monitoring AI systems.		Ministry's Chief Information Security Officer (CISO) ensures that Generative AI systems are protected against security threats, including encrypting data, regularly updating security protocols, and monitoring unauthorized access.	IT Department	January 2024
	There are mechanisms to ensure the integrity and resilience of the AI system against potential cyberattacks			Comply with Article 15 (Accuracy, robustness and cybersecurity) of EU AI Act. Trusted Infrastructure: Investment in secure, robust, and interoperable data infrastructure that can facilitate information sharing. Analysis Infrastructure: Developing sophisticated AI-enabled tools and platforms that can assist in auditing and monitoring AI systems.		**Prompt Injection & Jailbreak:** analyze prompts for attempts to discover or override system instructions in order to have the model behave maliciously. **Sensitive Data Phishing:** analyze prompts for attempts to gain access to sensitive information. **Model Hijacking / Knowledge Phishing:** analyze prompts for attempts to use the model for unintended purposes, such as extracting information,	IT Department	January 2024
Fallback and general safety	There is a fallback plan for adversarial attacks or unexpected situations			Comply with Article 15 (Accuracy, robustness and cybersecurity) of EU AI Act. Trusted Infrastructure: Investment in secure, robust, and interoperable data infrastructure that can facilitate information sharing. Analysis Infrastructure: Developing sophisticated AI-enabled tools and platforms that can assist in auditing and monitoring AI systems.		The response plan encompasses processes for detecting and investigating breaches, timely notification of affected parties and regulatory authorities, and steps to include implementing detection mechanisms, promptly notifying affected individuals and authorities, immediate mitigation and remediation efforts, and developing communication plans for addressing media and customer concerns.	IT Department	January 2024
	There is an assessment of the level of accuracy required in relation to the envisaged use			Comply with Article 15 (Accuracy, robustness and cybersecurity) of EU AI Act			IT Department	January 2024

Accuracy	There are mechanisms to evaluate and ensure that the used datasets are comprehensive and up to date			Comply with Article 15 (Accuracy, robustness and cybersecurity) of EU AI Act		Ministry's Chief Information Security Officer (CISO) ensures that Generative AI systems are protected against security threats, including encrypting data, regularly updating security protocols, and monitoring unauthorized access.	IT Department	January 2024
Reliability and reproducibility	There are procedures to evaluate the reliability and reproducibility of the AI system's aspects (inputs and outputs), also in specific contexts			Comply with Article 15 (Accuracy, robustness and cybersecurity) of EU AI Act		Ministry's Chief Information Security Officer (CISO) ensures that Generative AI systems are protected against security threats, including encrypting data, regularly updating security protocols, and monitoring unauthorized access.	IT Department	January 2024
7. Accountability								
Component	Minimum standards to be achieved	Initial impact estimate		Additional mitigation measures implemented	Final assessment		Responsible department	Timeline
		Challenge no.	Impact level		Final estimated impact level	Further actions		
Competence	There are clear programs to provide information on the role of the operator, the competencies required to operate the AI system and the implications of operator error			**Collective risk mitigation:** By enforcing developers to consider and act against potential widespread harms during the system design and operation, accountability mechanisms can address collective risks. For instance, requiring an AI Impact Assessment or risk profile assessment before deployment can help identify potential collective harms. **Systemic risk mitigation:** Accountability mechanisms can mandate regular monitoring of deployed AI systems, enabling early detection and mitigation of systemic risks, especially in those systems which are deemed to have the potential to become an existential threat.		Supporting programs to train AI auditors and researchers, as well as initiatives to educate the public about AI accountability.	Ministry's Fundamental Rights Protection Officer and the Special Committee for Compliance with Fundamental Rights	January 2024
	There are safeguards against incompetent operation of the AI system			**Collective risk mitigation:** By enforcing developers to consider and act against potential widespread harms during the system design and operation, accountability mechanisms can address collective risks. For instance, requiring an AI Impact Assessment or risk profile assessment before deployment can help identify potential collective harms. **Systemic risk mitigation:** Accountability mechanisms can mandate regular monitoring of deployed AI systems, enabling early detection and mitigation of systemic risks, especially in those systems which are deemed to have the potential to become an existential threat.		Supporting programs to train AI auditors and researchers, as well as initiatives to educate the public about AI accountability.	Ministry's Fundamental Rights Protection Officer and the Special Committee for Compliance with Fundamental Rights	January 2024

Misuse awareness	There is an assessment of the likelihood of misuse of the AI system and of its possible outcomes			**Collective risk mitigation:** By enforcing developers to consider and act against potential widespread harms during the system design and operation, accountability mechanisms can address collective risks. For instance, requiring an AI Impact Assessment or risk profile assessment before deployment can help identify potential collective harms. **Systemic risk mitigation:** Accountability mechanisms can mandate regular monitoring of deployed AI systems, enabling early detection and mitigation of systemic risks, especially in those systems which are deemed to have the potential to become an existential threat.		Supporting programs to train AI auditors and researchers, as well as initiatives to educate the public about AI accountability.	Ministry's Fundamental Rights Protection Officer and the Special Committee for Compliance with Fundamental Rights	January 2024
	There are ethics education and security awareness programs to sensitise the users to the potential risk of misuse			**Collective risk mitigation:** By enforcing developers to consider and act against potential widespread harms during the system design and operation, accountability mechanisms can address collective risks. For instance, requiring an AI Impact Assessment or risk profile assessment before deployment can help identify potential collective harms. **Systemic risk mitigation:** Accountability mechanisms can mandate regular monitoring of deployed AI systems, enabling early detection and mitigation of systemic risks, especially in those systems which are deemed to have the potential to become an existential threat.		Research and Development: Funding research into AI safety, ethics, and accountability, including public-private partnerships.	Ministry's Fundamental Rights Protection Officer and the Special Committee for Compliance with Fundamental Rights	January 2024
Auditability	There are legged and traceable procedures to enable independent audit, also in order to remedy to identified issues in the AI system			**Collective risk mitigation:** By enforcing developers to consider and act against potential widespread harms during the system design and operation, accountability mechanisms can address collective risks. For instance, requiring an AI Impact Assessment or risk profile assessment before deployment can help identify potential collective harms. **Systemic risk mitigation:** Accountability mechanisms can mandate regular monitoring of deployed AI systems, enabling early detection and mitigation of systemic risks, especially in those systems which are deemed to have the potential to become an existential threat.		Supporting programs to train AI auditors and researchers, as well as initiatives to educate the public about AI accountability.	IT Department, DPO, Ministry's Fundamental Rights Protection Officer and the Special Committee for Compliance with Fundamental Rights	January 2024
Ability to redress	There are measures that allow redress in case of the occurrence of any harm or adverse impact	[1.6]	-	Data subject can file a complaint to the Ministry's Fundamental Rights Protection Officer and/or the DPO who work in collaboration with the Special Committee for Compliance with Fundamental Rights which was recently established in collaboration with the European Commission and whose purpose will be to monitor the procedures and implementation of national, EU and international legislation in areas of border protection and the granting of international protection.				January 2024
	There are procedures to provide information to affected parties about opportunity for redress			Affirmative				January 2024

Fundamental Rights Impact Assessment (FRIA) Questions

The purpose of this assessment is to confirm that privacy laws and information governance standards are being complied with, or highlights problems that need to be addressed. It also aims to prevent problems arising at a later stage which might impede the progress or success of the project.

Answering "Yes" to any of the screening questions above represents a potential IG risk factor please proceed and complete the Fundamental Rights Impact Assessment (FRIA) Questionnaire tab.

Please answer all the Questions in this section and provide additional information where necessary.

D1 **Describe the Data or Datasets that will be processed i.e collected, linked, shared, collated etc.**

Ref#	Question	Select Answer	
D1	**Does the Centaur & Hyperion Systems potentially negatively discriminate against people on the basis of any of the following grounds (non-exhaustively)?**		
	Sex	No	
	Race	No	
	Colour	No	
	Ethnic or social origin	No	
	Genetic features	No	
	Language	No	
	Religion or Belief	No	
	Political or any other opinion	No	
	national minority	No	
	Disability	No	
	Age or sexual orientation	No	
	Other Identifiers not listed above- *Please state the identifier(s)*	NA	
D2	**Does the Centaur & Hyperion Systems involve the use collection or sharing of the following special categories of data or what would be considered sensitive about individuals?**		
	Racial or Ethnic Origin	Yes	
	Political Opinion	No	
	Religious Beliefs	No	
	Trade Union Membership	No	
	Physical or Mental Health condition	Yes	
	Sexual Life	No	
	Commission or alleged commission of an offence	Yes	
	Safeguarding Adults	Yes	
	Child Protection	Yes	
	Proceedings for any offence committed or alleged	Yes	
	Biometrics; DNA profile, fingerprints	Yes	
	Other Identifiers not listed above- *Please state the identifier(s)*	NA	
D3	**Is human rights awareness and potential? Are there safegurds in place?**		
	Are any human rights impacted by the use of the Centaur & Hyperion Systems?	Yes	e.g. non-discrimination and data protection
	Is there in place any measures, processes or internal guidelines to protect the human rights affected by the use of the Centaur & Hyperion Systems?	Yes	There are limitations on the use of the system or ways to challenge results of the system
	Can the use of the Centaur & Hyperion Systems discriminate against individuals based on their gender, age, ethnic origin, sexual orientation or political opinion or any other reasons?	No	
	Do standards (including laws and non-binding guidelines) apply to the use of the Centaur & Hyperion Systems?	Yes	ISO, certification schemes or codes of conduct
	Do these standards include provisions which sufficiently safeguard fundamental rights when it comes to the use of the Centaur & Hyperion Systems?	Yes	
	Are there any gaps in the current laws and standards covering the Centaur & Hyperion Systems as described ?	No	
	Do you find the current laws and standards governing the use of the Centaur & Hyperion Systems to be clear enough?	Yes	
	Are the laws and standards related to the Centaur & Hyperion Systems sufficiently adapted to current technical developments?	Yes	
	Are there any security and audit measures implemented to secure access to and limit use of personal identifiable and/or sensitive information?	Yes	card based access to rooms, mechanisms for opening and closing building. Allocation of responsibility of the premises is in place
	Is there an ability to audit access to the information?	Yes	A planned process will need to be put in place.
	Are individuals informed about the proposed uses of their personal data? (if Yes how is this done?)	Yes	Fair Processing notice.
	Are arrangements in place for recognising and responding individual rights in accordance with the law?	Yes	A planned process will need to be put in place.
	Will individuals be asked for consent for their information to be processes in this way? *If no, list the reasons for not gaining consent.*	NA	

Ref#	Question	Select Answer	
D4	**Centaur System impacts on refugees human rights?**		
	Right to liberty and security - Art.6 of ECHR	No	
	Respect for private and family life - Art. 7 of ECHR	No	
	Protection of personal data - Art. 8 of ECHR	No	
	Freedom of thought, conscience and religion - Art. 10 of ECHR	No	
	Freedom of expression and information - Art. 11 of ECHR	No	
	Freedom of assembly and of association - Art.12 of ECHR	No	
	Could the data being processed be required for the defence of a legal claim?	NA	

Answer all the FRIA assessment list questions below for the assessing of the CENTAUR System	
Have you considered the extent to which the Centaur system may interfere with the rights and freedoms conferred under the European Convention on Human Rights?	We consider data protection, our focus tends to be upon the potential to interfere with the Article 8 right to respect for private and family life. Surveillance undertaken in accordance with the law could, however, interfere with other rights and freedoms such as those of conscience and religion (Article 9), expression (Article 10) or association (Article 11).The deployment of the Centaur system is not considered likely to have a negative impact on the rights and freedoms of people as conferred by the ECHR. The use of CCTV is considered to be proportionate and the surveillance will be no more intrusive than necessary to achieve its operational requirement to detect and investigate Crime & ASB in the area surveilled. All such surveillance will only permitted by the Council if it is satisfied that it is warranted and proportionate. The System's use will not interfere with people's rights and freedoms under Articles 9, 10 or 11, as described above.
Do any of these measures discriminate against any particular sections of the community?	We consider there will be no discriminatory or disproportionate impact on any section of the community arising from the installation of the Centaur System. Article 14 of the ECHR prohibits discrimination with respect to rights under the Convention. Detail whether the proposed surveillance will have a potential discriminatory or disproportionate impact on a section of the community. For example, establishing a surveillance system in an area with a high density of one particular religious or ethnic group.
Doea the use of the Centaur system take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified?	The Centaur system consists of static cameras in the residential Reception and Identification Centers and generally presents a lower risk than to a system that has multiple High Definition Pan Tilt and Zoom (PTZ) cameras. However, the CCTV DPIA has helped to identify any cameras (irrespective of the type) that may be directed at a more vulnerable area (e.g. a children's play area) and thus presenting a higher privacy risk. This approach allows the Ministry of Immigration and Asylum to document a generic and methodical approach to any intrusion into privacy, catalogue the cameras by type and location, and finally identify any cameras that present specific privacy risks and document any mitigation that has been taken. It also allows to consider the risks associated with any integrated surveillance technology such as automatic facial recognition systems, along with security measures against cyber disruption of the system.
Does the Centaur system potentially negatively discriminate against people on the basis of any of the following grounds (non-exhaustively): sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation?	The Centaur System it does not purposely discriminate. The Centaur system technology is 'race' neutral and amoral, independent of bias, and objective in it's endeavour to prevent crime and offending behaviour.
Are there in place processes to test and monitor for potential discrimination (bias) during the development, deployment and use phase of the Centaur system?	The Centaur system technology is 'race' neutral and amoral, independent of bias, and objective in it's endeavour to prevent crime and offending behaviour. There is scientific objectivity and technological ('race' and ethnic) neutrality.
Are there in place processes to address and rectify for potential discrimination (bias) in the Centaur system?	The Ministry of Immigration and Asylum aided by the National Transparency Authority performs regularly necessary checks and balances to ensure that the use of the Centaur system is proportinate and against bias.
Does the Centaur system respect human rights, for example with respect to child protection and taking the child's best interests into account?	Children's privacy should be protected at all times. The Centaur System helps the Ministry of Immigration and Asylum to take necessary proactive measures to prevent discrimination on the basis of sex, disability, socioeconomic background, ethnic or national origin, language or any other grounds, and discrimination against minority and indigenous children, asylum-seeking, refugee and migrant children, lesbian, gay, bisexual, transgender and intersex children and children in other vulnerable situations. Further measures will be required to close the gender-related digital divide for girls and to ensure that particular attention is given to access, digital literacy, privacy and online safety.
Are there in place processes to address and rectify for potential harm to children by the Centaur system?	The Ministry of Immigration and Asylum aided by the National Transparency Authority performs regularly necessary checks and balances to ensure that the use of the Centaur system is proportinate and against potential harm to children.
How National Transparency Autority is implicated in the process?	The National Transparency Authority is implicated as a Concerned Supervisory Authority (CSA). The National Transparency Authority has been delegated with the task of a human rights monitoring mechanism. A memorandum of cooperation is in effect between the Ministry of Immigration and Asylum and the National Transparency Authority. The purpose of the memorandum of cooperation is to improve the Internal Audit System as per the compliance with the applicable legal framework on human rights and privacy laws.
What is the aiding role of National Transparency Authority towards the Ministry of Immigration and Asylum?	The National Transparency Authority covers recommendations that encourage the Ministry to deploy international human rights approved procedures; to invite EU/UN Special Rapporteurs; to implement recommendations from treaty bodies' concluding observations; to implement comments or other relevant documents.
What is the aiding role of National Transparency Authority towards the Ministry of Immigration and Asylum as per urgent legislative requirements respective to the Centaur System?	The National Transparency Authority covers recommendations that approve or call for changes in legislation; changes to the legal framework; the repeal of certain legal provisions.
What is the aiding role of National Transparency Authority towards the Ministry of Immigration and Asylum as per cooperation (funding and technical assistance) respective to the Centaur System?	The National Transparency Authority covers recommendations that engage the international community, assistance, cooperation and funding, either by encouraging the Greek Government (via the Ministry of Immigration and Asylum) under review to seek assistance from other states, or by requesting the Greek Government under review to share its expertise in a particular human rights project under deployment.
What is the aiding role of National Transparency Authority towards the Ministry of Immigration and Asylum as per human rights policies and programmes adopted by the Ministry of Immigration and Asylum?	The National Transparency Authority covers recommendations concerned with the enforcement or implementation of human rights through policies, procedures, programmes, services or other facilities.
Does the Centaur system respect the freedom of expression or assembly?	Yes
Could the Centaur system potentially limit a person's freedom to openly express an opinion, partake in a peaceful demonstration or join a union?	No
Does the Centaur system protect the right to privacy, including personal data relating to individuals in line with GDPR?	Yes, surveillance is deployed only in public spaces and areas. There is ni surveillance inside housing blocks.
Has the Min. of Migration and Asylum put in place processes to assess in detail the need for a data protection impact assessment, including an assessment of the necessity and proportionality of the processing operations in relation to their purpose, with respect to the development, deployment and use phases of the Centaur system?	N/A - exisiting arrangements in place.
Has the Min. of Migration and Asylum put in place measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data with respect to the development, deployment and use phases of the Centaur system?	N/A - exisiting arrangements in place.
Where and how will this data be stored?	CCTV - operations - exisiting arrangements in place.
Who will be able to access identifiable data?	Only Authorized Staff
Will the data be linked with any other data collections?	NO
How is it ensured that the right to data portability can be respected? i.e. Data relating to particular people can be extracted for transfer to another Data Controller, at the request of the person to which it relates, subject to: · Receipt of written instructions from the person to which the data relates. · Including data used for any automated processing, - The transfer of the data has been made technically feasible.	N/A - existing arrangements in place
What security measures will be used to transfer the data?	Security service with contractual arrangement, physical security under centrally managed access. Existing role based access controls in place.
What confidentiality and security measures will be used to store the data?	N/A - exisiting arrangements in place.
How long will the data be retained in identifiable form? And how will it be de-identified? Or destroyed?	N/A - exisiting arrangements in place.
What governance measures are in place to oversee the confidentiality, security and appropriate use of the data and manage disclosures of data extracts to third parties to ensure identifiable data is not disclosed or is only disclosed with consent or another legal basis?	Policy document - existing requirement for third party to sign contract detailing the confidentiality and requirements to ensure overisght and report accordingly.
Is there functionality to respect objections/ withdrawals of consent?	N/A
Are there any plans to allow the information to be used elsewhere within the Reception and Identification Centres, wider or by a third party?	No external disclosures - only internal processes .
The data must be able to be easily separated from other datasets to enable data portability (see previous questions), audit of data relating to specific organisations and to facilitate any requirements for service transitions.	N/A - exisiting arrangements in place.
Does the Centaur system protect that all persons with a mental illness, or who are being treated as such persons, shall be treated with humanity and respect for the inherent dignity of the human person?	There are no automated procedures or algorithmic-based technologies and the System is humanly operated. Decision making by the System's Operators is based on transparency and balancing of interests (proportionality tests in the narrow sense).

Is there any discrimination on the grounds of mental illness? "Discrimination" means any distinction, exclusion or preference that has the effect of nullifying or impairing equal enjoyment of rights.	Special measures solely to protect the rights, or secure the advancement, of persons with mental illness shall not be deemed to be discriminatory.
Any decision that, by reason of his or her mental illness, a person lacks legal capacity, and any decision that, in consequence of such incapacity, a personal representative shall be appointed, shall be made only after a fair hearing by an independent and impartial tribunal established by domestic law. The person whose capacity is at issue is entitled to be represented?	Decisions regarding capacity and the need for a personal representative are being reviewed at reasonable intervals prescribed by domestic law. The person whose capacity is at issue, his or her personal representative, if any, and any other interested person has the right to appeal to a higher court against any such decision.
Is special care being given within the purposes of these personal data processings and within the context of domestic law relating to the protection of the rights of minors, including, if necessary, the appointment of a personal representative other than a family member?	Yes
The Centaur System shall not classify as person as having, or otherwise indicate that a person has, a mental illness except for purposes directly relating to mental illness or the consequences of mental illness.	Person is compelled to undergo medical examination with a view to determining whether or not he or she has a mental illness except in accordance with a procedure authorized by domestic law.
Are there any restrictions imposed directly to persons by the Centaur System?	No - Every person is treated in the least restrictive environment and with the least restrictive or intrusive surveillance appropriate to the person's mental health needs and the need to protect the physical safety of others. Every person has the right to full respect for his or her: (a) Recognition everywhere as a person before the law; (b) Privacy; (c) Freedom of communication
How consent is obtained by vulnerable persons or persons with mental illness?	Informed consent is consent obtained freely, without threats or improper inducements, after appropriate disclosure to the patient of adequate and understandable information in a form and language understood by the person. A person may request the presence of a person or persons of the person's choosing during the procedure for granting consent.
At which stage a person with mental illness is being informed over his rights and how to exercise them.	A person with mental illness is informed as soon as possible after admission, in a form and a language which the person understands, of all his or her rights in accordance with human rights fundamental rights and under domestic law, which information shall include an explanation of those rights and how to exercise them. If and for so long as a patient is unable to understand such information, the rights of the patient shall be communicated to the personal representative, if any and if appropriate, and to the person or persons best able to represent the patient's interests and willing to do so.
Are there procedural safeguards in place?	Every person has the right to make a complaint through procedures as specified by domestic law. The person is entitled to choose and appoint a counsel to represent the person as such, including representation in any complaint procedure or appeal. If the person does not secure such services, a counsel shall be made available without payment by the person to the extent that the person lacks sufficient means to pay.

Privacy Risks & Issues for Consideration		Impact	Privacy Risk Management Implication for Projects				
		Low; Moderate; High	Avoid	Treat	Accept	Implemented Countermeasures	Date
1	To ensure that the Centaur Systems Operations have appropriate process in place, placement assessed (Considering privacy of third parties) and process relating to data storage, security and access.	**Moderate**		**YES**		Policy document on CCTV, security measures, contractual relationship with service provider. Processes to honour individual rights in relation to privacy. Update fair processing notice to reflect. Signs to notify patients and the public.	20-01-2022
2	Personal data retained for longer than necessary or personal data collected and stored unnecessarily	**Moderate**		**YES**		Video images will be retained for 15 days unless the authority is notified before deletion that they are required by: a data subject, insurance company, the police or other investigation agency	20-01-2022
3	Disclosure of personal data to unauthorised persons or agencies	**Moderate**		**YES**		Footage will only be realeased where it is permitted to do so to law enforcement agencies, and those other agencies that have a lawful reason to be provided with access to the images. Legitimate access to recorded images is set out in the CCTV Operations Policy and Procedural Manual and all security staff are trained in them before they are allowed to work in the Control Room. The Control Room Command & Control equipment maintains a log of all access to and download of recorded images.	20-01-2022
4	Intrusive surveillance disproportionate	**Moderate**		**YES**		Due to the nature of CCTV in the public areas of the Reception and Indentification Centers there will always be a level of collateral intrusion. When necessary other subjects in the footage will have their identity obscured to maintain their privacy. The FRIA cosiders the option for less intrusive means for achieving the same or a similar aim but none available will meet the requirements set by fundamental rights laws.	20-01-2022
5	Unauthorised third party access to images	**Moderate**		**YES**		The Centaur System equipment, cameras and review and control equipment are password protected which markedly reduces the risk of unauthorised access. Members of the public can submit a right of access request and view or receive footage of themselves, in accordance with their rights; this is an important part of the necessary checks and balances to ensure that the use of the CCTV system is proportionate.	20-01-2022
6	Algorithmically driven identification technologies disproportionately mis-identify people from black and other minority ethnic groups	**High**		NA		The Centaur system technology is 'race' neutral, independent of bias, and objective in it's endeavour to prevent crime and offending behaviour. The presence of new technologies both assists and drives over-policing by providing law enforcement agencies with risk-making capabilities, alongside developing databases which contain racialised stereotypical assumptions of minority communities.	20-01-2022
7	The impact of new technologies to identify, surveil and analyse will be disproportionately felt by minority ethnic communities, as they are already over-policed.	**High**		NA		The Ministry of Immigration and Asylum aided by the National Transparency Autority endorses necessary checks and balances to ensure that the use of the Centaur system is proportionate.	20-01-2022

8	Predictive policing by the use of Centaur System. In case an innocent person is flagged to the police as a suspect may result to potentially humiliation, thus can be associated with discrimination.	**High**		NA		The Ministry of Immigration and Asylum endorses necessary checks and balances to ensure that the use of the Centaur system is proportionate. The balance is more accurate predictive policing can result in higher levels of arrests of suspects/offenders, and a reduced risk of individuals' crime victimisation.	20-01-2022