

# **PREVENTAI AB**

## **COMPLIANCE GUIDE**

### **AI Act | DPIA | FRIA**

---



## Table of Contents

|                                                          |           |
|----------------------------------------------------------|-----------|
| <b>Assessment according to the AI Act.....</b>           | <b>3</b>  |
| General information about the AI Act.....                | 3         |
| Preventai's solution .....                               | 3         |
| Executive summary.....                                   | 4         |
| Background.....                                          | 5         |
| Assessment .....                                         | 6         |
| Conclusions .....                                        | 10        |
| <b>DPIA (Data Protection Impact Assessment) .....</b>    | <b>13</b> |
| General information about DPIA:s .....                   | 13        |
| Data controller.....                                     | 13        |
| Elevated risk activities .....                           | 13        |
| Purpose of the processing .....                          | 15        |
| Legal basis of the processing .....                      | 16        |
| Data processed.....                                      | 17        |
| Scope of data processed.....                             | 17        |
| Collection of data.....                                  | 17        |
| Security of personal data.....                           | 19        |
| Data subjects' rights.....                               | 19        |
| Proportionality of interests.....                        | 20        |
| <b>FRIA (Fundamental Rights Impact Assessment) .....</b> | <b>23</b> |
| General information about fundamental rights.....        | 23        |
| Background and scope.....                                | 23        |
| Description of the processes of the Deployer.....        | 23        |
| Time period and frequency .....                          | 24        |
| Categories of registered individuals .....               | 24        |
| Specific risks of harm .....                             | 24        |
| Measures for human oversight.....                        | 26        |

## Assessment according to the AI Act

### General information about the AI Act

The European Union's Artificial Intelligence Act<sup>1</sup> (the “**AI Act**”) introduces a risk-based framework governing the development and use of AI systems within the EU. AI systems are categorized into four levels of risk, each with corresponding obligations:

- (i) **Prohibited AI:** Certain AI systems are not allowed due to unacceptable risk, such as systems that manipulate behaviour or enable social scoring.
- (ii) **High-Risk AI:** AI systems used in critical contexts are considered high-risk and are subject to strict regulatory requirements. These include systems used in areas such as critical infrastructure, employment, law enforcement, and biometric identification.
- (iii) **Limited-Risk AI:** These systems are subject to transparency obligations, such as informing users that AI is being used.
- (iv) **Minimal or No-Risk AI:** Most AI systems fall into this category and are subject to limited or no regulatory requirements.

The classification of an AI system depends on its intended purpose, functionality, and deployment context.

### Preventai's solution

Preventai provides an AI-based video analysis solution designed to transform existing camera infrastructure into intelligent, real-time sensing systems (the “**Solution**”). The Solution connects directly to existing cameras, enabling deployment across different types of operations. At the core of the Solution is a proprietary video language model, which allows users to define detection capabilities using natural language.

This enables flexible configuration of the Solution based on operational needs. The Solution continuously analyses video streams to detect certain actions and operational events. When such events are identified, alerts are generated to support timely response by on-site personnel. The Solution is designed as a decision-support tool, enhancing situational awareness while ensuring that all actions are taken by human operators.

---

<sup>1</sup> Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (the “**AI Act**”).

## Executive summary

This assessment sets out preventai's analysis of the classification and regulatory position of its AI-powered video analytics system under the AI Act (the "**Assessment**"). The Solution connects to existing camera infrastructure in selected environments and uses artificial intelligence to detect events indicative of, for example, shoplifting or other loss-prevention-relevant events in real time, sending notifications to personnel for assessment at their discretion. All images are automatically and irreversibly anonymised and the Solution does not perform emotion recognition or biometric identification.

Preventai has assessed the Solution against each layer of the AI Act's risk-based framework and concludes the following:

- (i) **Prohibited practices (Article 5):** The Solution does not fall within the scope of any prohibited AI practice. It does not perform emotion recognition, does not constitute a real-time remote biometric identification system for law enforcement, and does not engage in social scoring.
- (ii) **High-risk classification (Article 6):** The Solution is not classified as high-risk. It does not fall within the scope of the EU harmonisation legislation listed in Annex I, and it is not referred to in any of the use-case areas listed in Annex III.
- (iii) **Transparency obligations (Article 50):** Some transparency obligations under Article 50 apply to the Solution.
- (iv) **Applicable obligations:** The Solution is subject to the general provisions of the AI Act applicable to all AI systems, including the AI literacy obligation under Article 4. No conformity assessment, EU declaration of conformity, CE marking, or registration in the EU database for high-risk AI systems is required.

Notwithstanding this classification, preventai has elected to voluntarily comply with the key substantive requirements applicable to high-risk AI systems under Chapter III, Section 2 of the AI Act – covering risk management, data governance and bias mitigation, transparency and instructions for use, human oversight, and accuracy, robustness and cybersecurity – in recognition of the fundamental rights implications of AI-powered event monitoring in publicly accessible spaces.

The above conclusions are contingent on the Solution being deployed and used in accordance with its intended purpose of loss prevention, operational security and efficiency and risk detection. Use of the Solution outside this scope – including for employee monitoring, law enforcement, or the systematic sharing of outputs with law enforcement authorities – may alter its classification under the AI Act.

This Assessment should be read in conjunction with the separate Data Protection Impact Assessment ("**DPIA**") and Fundamental Rights Impact Assessment ("**FRIA**") provided by preventai.

## Background

This Assessment sets out preventai's analysis of the classification of the Solution under the AI Act and documents the measures taken to ensure compliance. It is provided to deployers and prospective deployers (within the meaning of Article 3(4) of the AI Act) to enable them to understand the Solution's regulatory position and to support them in meeting their own obligations under the AI Act, including, where applicable, the fundamental rights impact assessment obligation under Article 27.

This Assessment is based on the AI Act as published in the Official Journal of the European Union and on guidance available as of its date. As no enforcement practice, delegated or implementing acts, harmonised standards, or case law has yet developed in relation to the questions addressed herein, certain aspects of the analysis necessarily involve interpretive judgments.

### The Provider

Preventai ("**preventai**" or the "**Provider**") is the developer and provider, within the meaning of Article 3(3) of the AI Act, of the Solution described below.

### The Solution

Preventai provides an AI-powered video analytics system designed for deployment in many different types of operations. The Solution connects to existing camera infrastructure and processes video feeds in real time to detect events indicative of, for example, shoplifting or other loss-prevention-relevant events, sending notifications to personnel to assess and respond at their discretion.

The Solution incorporates the following design characteristics that are material to its classification under the AI Act:

- (i) **Automatic anonymisation:** All images processed by the Solution are automatically and irreversibly anonymised. The Solution does not identify, or seek to identify, any natural person.
- (ii) **No emotion recognition:** The Solution does not detect, analyse, infer, or otherwise process emotional states. It operates exclusively at the level of action detection, identifying observable physical actions (such as concealment of merchandise or bypassing of point-of-sale infrastructure) rather than inferring psychological or emotional states.
- (iii) **No biometric identification:** The Solution does not compare biometric data against any reference database, watchlist, or repository of biometric templates. It does not perform facial recognition or any other form of remote biometric identification.

- (iv) **Human-in-the-loop design:** The Solution does not take autonomous action. It sends notifications to personnel, who retain full discretion as to whether and how to respond. The Solution does not trigger automated interventions such as locking mechanisms, direct alerts to law enforcement, or any other measure producing legal or similarly significant effects without human intervention.

The Solution's intended purpose is exclusively loss prevention, operational security and efficiency and risk detection. It is not intended or designed for use in law enforcement, border control, employee monitoring, or any other purpose outside this scope.

## Assessment

### Prohibited AI practices (Article 5)

Article 5 of the AI Act prohibits AI practices posing an unacceptable risk. These provisions have applied since 2 February 2025. Preventai has assessed the Solution against each prohibited practice under Article 5(1) and concludes that none applies. The most relevant prohibitions are analysed below.

- (i) **Emotion recognition in the workplace and educational institutions (Article 5(1)(f)):** Article 5(1)(f) prohibits AI systems that infer emotions of natural persons in workplace and educational settings, except for medical or safety purposes. As described above, the Solution does not detect, analyse, or infer emotional states.
- (ii) **Real-time remote biometric identification for law enforcement (Article 5(1)(h)):** Article 5(1)(h) prohibits real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes, subject to narrow exceptions. This requires three cumulative conditions: (i) the system must constitute a real-time remote biometric identification system; (ii) it must be used in publicly accessible spaces; and (iii) it must be used for law enforcement. While the Solution is deployed in publicly accessible spaces, it does not constitute a remote biometric identification system as defined in Article 3(41), as it does not identify natural persons by comparing biometric data against a reference database. Furthermore, it is operated by private entities for loss prevention, operational security and efficiency and risk detection, not by or on behalf of law enforcement. Accordingly, Article 5(1)(h) does not apply.
- (iii) **Social scoring (Article 5(1)(c)):** Article 5(1)(c) prohibits AI systems that evaluate or classify natural persons based on social behaviour or personal characteristics, leading to unjustified or disproportionate detrimental treatment. The Solution does not evaluate, score, or classify natural persons over time or across contexts. It detects discrete events in real time and does not maintain

behavioural profiles, cumulative risk scores, or records attributable to identified or identifiable individuals.

The Solution does not fall within the scope of any of the prohibited AI practices under Article 5 of the AI Act.

### **High-risk classification (Articles 6 and Annex III)**

Under Article 6, an AI system is classified as high-risk if it falls within the scope of the legislation listed in Annex I and requires a third-party conformity assessment, or if it is referred to in the use-case areas listed in Annex III.

The Solution is not a product, nor a safety component of a product, falling within the scope of any legislation listed in Annex I.

Furthermore, preventai has assessed the Solution against each Annex III use-case area:

- (i) **Point 1(a) – Remote biometric identification systems:** Annex III, Point 1(a) covers AI systems intended for remote biometric identification, excluding biometric verification systems whose sole purpose is to confirm a person's claimed identity. The Solution does not identify natural persons, does not compare biometric data against any reference database, and does not perform facial recognition. Point 1(a) does not apply.
- (ii) **Point 1(b) – Biometric categorisation systems:** Annex III, Point 1(b) covers AI systems intended for biometric categorisation according to sensitive or protected attributes based on inference. The Solution does not categorise natural persons on the basis of any sensitive or protected attribute. Point 1(b) does not apply.
- (iii) **Point 4 – Employment, workers management and access to self-employment:** Annex III, Point 4 covers AI systems intended for monitoring and evaluating the performance and behaviour of persons in work-related contractual relationships. The Solution's intended purpose is exclusively loss prevention; it is not designed or intended for employee monitoring. The instructions for use expressly prohibit such use. Point 4 does not apply.
- (iv) **Point 6 – Law enforcement:** Annex III, Point 6 covers AI systems intended for use by or on behalf of law enforcement authorities, including for predicting criminal offences (Point 6(d)), profiling in criminal proceedings (Point 6(e)), and crime analytics (Point 6(f)). The Solution is operated by private businesses for commercial loss prevention, not by or on behalf of law enforcement. Point 6 does not apply.
- (v) **Remaining Annex III categories:** Preventai has assessed the Solution against the remaining Annex III categories, including Point 2 (critical infrastructure),

Point 3 (education and vocational training), Point 5 (essential private and public services), Point 7 (migration, asylum and border control), and Point 8 (administration of justice and democratic processes). None applies given the Solution's intended purpose of loss prevention in commercial environments.

For completeness, even if the Solution were considered to fall within an Annex III category, Article 6(3) provides that such a system shall not be considered high-risk if it does not pose a significant risk of harm to health, safety, or fundamental rights, provided it does not, among other things, perform profiling. Preventai considers the Solution would qualify for this exception but maintains that no Annex III category is triggered in the first place.

The Solution is not classified as high-risk under Article 6. It does not fall within Annex I or any Annex III use-case area. This conclusion is based on the Solution's technical architecture and intended purpose as described above and is contingent on deployment in accordance with that intended purpose.

### **Specific transparency obligations (Article 50)**

Article 50 imposes specific transparency obligations on providers of certain AI systems, regardless of high-risk classification. Preventai has assessed the Solution against each obligation under Article 50.

- (i) **Article 50(1) – AI systems intended to directly interact with natural persons:** This provision requires that natural persons are informed when interacting with an AI system. The Solution interacts with personnel through notifications and processes video footage of natural persons by means of AI. Therefore, the Provider recommends that deployers should ensure that natural persons present in monitored premises are informed that AI-powered video analytics are in operation, both as good practice and to comply with this transparency obligation as well as the transparency obligations under Articles 12–14 GDPR<sup>2</sup>.
- (ii) **Article 50(2) – AI-generated or manipulated content:** This provision applies to AI systems generating synthetic content. The Solution does not generate synthetic content; Article 50(2) does not apply.
- (iii) **Article 50(3) – Emotion recognition and biometric categorisation systems:** This provision requires deployers of such systems to inform exposed natural persons. The Solution does not perform emotion recognition or biometric categorisation; Article 50(3) does not apply.

---

<sup>2</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

### **Overall classification**

Based on the analysis above, the Solution is not classified as high-risk under Article 6, as it does not fall within any Annex I or Annex III category. The Solution does however trigger some transparency obligations under Article 50. It is furthermore subject to the general provisions applicable to all AI systems, including the AI literacy obligation under Article 4.

### **Voluntary compliance measures**

Notwithstanding the above classification, preventai recognises that the Solution operates in a context – real-time camera surveillance in publicly accessible spaces – engaging fundamental rights including privacy, data protection, and non-discrimination. Preventai has therefore elected to voluntarily comply with the key requirements applicable to high-risk AI systems under Chapter III, Section 2 of the AI Act, as summarised below.

- (i) **Risk management (Article 9):** Preventai maintains a risk management system covering the Solution's entire lifecycle, comprising identification, analysis, estimation, and evaluation of risks to health, safety, and fundamental rights arising from intended use and reasonably foreseeable misuse. Appropriate mitigation measures have been implemented, including the design features described above.
- (ii) **Data governance and bias (Article 10):** Training, validation, and testing data sets have been subject to appropriate governance and management practices. Preventai has taken measures to identify and mitigate bias risk, including testing for differential accuracy across demographic groups. The detection mechanism is based on observable physical actions rather than appearance-based features, reducing the risk of discriminatory outcomes.
- (iii) **Transparency and instructions for use (Article 13):** preventai provides deployers with instructions covering the Solution's intended purpose, capabilities, known limitations, accuracy levels, foreseeable risks, and required human oversight measures. The instructions expressly prohibit use for employee monitoring or any purpose outside the defined intended purpose.
- (iv) **Human oversight (Article 14):** As described above, the Solution does not take autonomous action. All notifications are directed to personnel who retain full discretion in determining whether and how to respond. Staff are informed that notifications are probabilistic and do not constitute a definitive determination that an offence has occurred.
- (v) **Accuracy, robustness and cybersecurity (Article 15):** The Solution has been designed to achieve an appropriate level of accuracy, robustness, and cybersecurity throughout its lifecycle. Preventai has established processes for monitoring performance and addressing errors, faults, or inconsistencies.

### **Obligations of the deployer**

While the Solution is not classified as high-risk, preventai draws deployers' attention to the following obligations and recommended actions under applicable law:

- (i) **AI literacy (Article 4):** Deployers must ensure that staff and other persons operating the Solution on their behalf have a sufficient level of AI literacy, taking into account their technical knowledge, experience, training, and the context of use.
- (ii) **Data protection (GDPR):** The Solution processes video footage constituting personal data under the GDPR until effective anonymisation. Deployers, acting as data controllers, must ensure a valid legal basis for processing, are likely required to carry out a DPIA under Article 35(3)(c) GDPR (systematic monitoring of a publicly accessible area on a large scale), and must comply with all applicable GDPR obligations. The separate DPIA provided by preventai is intended to assist deployers in this regard.
- (iii) **Fundamental rights impact assessment (Article 27):** Deployers that are public bodies or private entities providing public services and that use high-risk AI systems must perform a FRIA under Article 27. While the Solution is not classified as high-risk, such deployers should assess whether the obligation is nonetheless applicable to them. The separate FRIA provided by preventai is intended to assist in this regard.
- (iv) **Transparency to natural persons:** Preventai recommends that deployers inform natural persons present in monitored premises that AI-powered video analytics are in operation.
- (v) **Use within intended purpose:** The Solution's classification under this Assessment is contingent on deployment in accordance with its intended purpose as described above. Deployers must not use the Solution outside this scope, including for employee monitoring, law enforcement, or systematic sharing of outputs with law enforcement authorities. Such use may alter the Solution's classification and give rise to additional obligations or prohibitions.

### **Conclusions**

Based on this Assessment, preventai draws the following conclusions regarding the Solution's classification under the AI Act.

- (i) The Solution does not fall within any prohibited AI practice under Article 5. It does not perform emotion recognition, does not constitute a real-time remote biometric identification system for law enforcement, and does not engage in social scoring.
- (ii) The Solution is not classified as high-risk under Article 6. It does not fall within Annex I or any Annex III use-case area.

- (iii) The Solution triggers transparency obligations under Article 50, as it interacts directly with staff receiving notifications and indirectly by processing video material of natural persons.
- (iv) The Solution is subject to the general provisions applicable to all AI systems, including the AI literacy obligation under Article 4.
- (v) Notwithstanding the above, preventai has elected to voluntarily comply with the key requirements applicable to high-risk AI systems under Chapter III, Section 2 of the AI Act – covering risk management, data governance and bias mitigation, transparency and instructions for use, human oversight, and accuracy, robustness and cybersecurity – in recognition of the fundamental rights implications of AI-powered event monitoring in publicly accessible spaces, and to provide deployers with the assurance they may need to meet their own obligations.

These conclusions are contingent on the Solution being deployed in accordance with its intended purpose. Use outside that scope – including for employee monitoring, law enforcement, or systematic sharing of outputs with law enforcement authorities – may alter the Solution’s classification and give rise to additional obligations or prohibitions. Deployers are responsible for ensuring use remains within the intended purpose.

This Assessment should be read in conjunction with the DPIA and the FRIA, which together provide deployers with a comprehensive view of the regulatory framework applicable to the Solution and support them in meeting their compliance obligations.

**DPIA**



## DPIA (Data Protection Impact Assessment)

### General information about DPIA:s

Article 35 of the GDPR<sup>3</sup> requires data controllers to carry out a data protection impact assessment (“**DPIA**”) where a type of processing, in particular using new technologies, is likely to result in a high risk to the rights and freedoms of natural persons. A DPIA is mandatory where the processing meets any of the criteria set out in Article 35(3), including systematic monitoring of a publicly accessible area on a large scale (Article 35(3)(c)). The European Data Protection Board has further identified categories of processing that generally require a DPIA, including large-scale processing of data concerning vulnerable data subjects, and systematic monitoring. Given that preventai’s solution (the “**Solution**”) involves AI-powered real-time analysis of video feeds from camera infrastructure in publicly accessible environments, a DPIA is considered necessary. This assessment identifies and evaluates the risks to data subjects arising from the processing and sets out the measures adopted to address those risks. Furthermore, this assessment is aimed at supporting the entity employing the Solution in carrying out their own evaluation of the Solution in their specific use cases and to carry out their respective DPIA.

### Data controller

Preventai’s customers (the “**Controllers**”) will determine the purposes and means of the processing and will therefore act as data controllers for the relevant processing activities.

### Elevated risk activities

| Question                                     | Answer                                                                                                                                                                                             |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Does the processing include:</b>          |                                                                                                                                                                                                    |
| Evaluation or scoring (including profiling)? | No. Profiling within the meaning of Article 4(4) GDPR and the AI Act requires automated processing of personal data to evaluate personal aspects relating to an identified or identifiable natural |

<sup>3</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

|                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                     | <p>person. The Solution does not constitute profiling because the Solution does not maintain persistent profiles, cumulative scores, or behavioural histories linked to specific individuals over time or across contexts. Furthermore, detection operates exclusively at the level of observable physical actions rather than evaluating personal characteristics or predicting future behaviour. Moreover, the Solution does not compare data against any reference database or external data source and the Solution does not make autonomous decisions.</p> <p>The processing therefore consists of automated real-time analysis and classification of observed actions in video feeds to identify unusual or suspicious conduct and to analyse the flow of persons through designated areas, without any element of personal evaluation or prediction based on one's profile or appearance.</p> |
| Automated decision making with legal or similar significant effect? | No. The Solution only generates alerts and explanatory information. Any intervention or decision concerning an individual is made following human review. The Solution shall be viewed as a support tool rather than an autonomous decision-maker. Alerts are triggered exclusively by the detection of objective, observable physical actions – such as concealment of merchandise or bypassing of point-of-sale infrastructure – and not by any form of emotion recognition or intent detection.                                                                                                                                                                                                                                                                                                                                                                                                   |
| Systematic monitoring in a publicly accessible area?                | Yes. The processing entails ongoing observation and analysis of individuals in a publicly accessible environment. Camera surveillance involving personal data is typically regarded as systematic monitoring, and publicly accessible places are to be interpreted broadly.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Sensitive data or data of a highly personal nature?                 | Yes. Although the solution does not use facial recognition or biometric identification and does not intentionally process special category data, the video material may incidentally capture information that could reveal health-related circumstances (for example, crutches or wheelchairs) or information regarding religion (for example, religious clothing). However, the images are, as mentioned, subject to irreversible facial blurring/anonymisation, which reduces the privacy risk.                                                                                                                                                                                                                                                                                                                                                                                                    |

|                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data processed on a large scale?                                                                              | Yes. The solution is deployed in settings with material customer footfall. Large-scale processing is assessed by reference to the number of data subjects, the volume and variety of data, the duration, and the geographical extent of the processing.                                                                                                                                                                              |
| Matching or combining datasets?                                                                               | No.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Data concerning vulnerable data subjects?                                                                     | Yes. The processing may concern vulnerable data subjects, in particular children and employees present in the monitored environment. It may also concern, for example, elderly persons or persons with mental illness. Employees may be considered vulnerable due to the imbalance in the employment relationship, and children and other vulnerable individuals may have limited ability to understand or object to the processing. |
| New technology such as processing of biometric data for the purpose of identifying a natural person?          | No.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Processing which in itself “prevents data subjects from exercising a right or using a service or a contract”? | No.                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Purpose of the processing

| Question                               | Answer                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| What is the purpose of the processing? | Personal data collected via the Solution is processed for the purpose of providing video analytics services in connection with existing camera infrastructure and converting camera-based input into actionable operational information. Personal data derived from video streams is first anonymised and thereafter processed to detect, classify, analyse and assess events, actions and other circumstances relevant to the applicable use case, and to generate alerts, analyses, recommendations and other operational outputs. The processing is also carried out where necessary for implementation, configuration, testing, validation, maintenance, support, |

|                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                               | <p>security, incident handling, troubleshooting, performance monitoring and documentation related to the provision of the service.</p> <p>Contact information is also stored for the purpose of providing access to the Solution.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Describe why the processing is necessary to achieve the purpose.                              | The processing is necessary to detect, classify, analyse and assess events, conditions and other circumstances relevant to the applicable use case, and to generate operational outputs. It is also necessary for the implementation, configuration, maintenance, support, security, troubleshooting and performance monitoring required to provide the service effectively.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Describe less intrusive alternatives and why they haven't been chosen to achieve the purpose. | Less intrusive alternatives include not using video analytics, relying solely on manual monitoring or limiting processing to static images or heavily filtered footage. These alternatives have not been chosen because they would not achieve the purpose of the service, which depends on the interpretation of continuous video data, including its temporal and contextual information. Manual monitoring alone would not provide the same consistency, scalability or real-time output, and may require broader human access to the footage.                                                                                                                                                                                                                                                                                             |
| Is the processing limited to what is needed to achieve the purpose?                           | Yes. Only personal data relevant to the applicable use case and required to analyse video streams, generate operational outputs, and maintain the Solution is processed. Faces of natural persons are blurred to reduce intrusiveness. Access is restricted to individuals who need it to perform their duties, and data is processed only for the purposes for which it was collected. Personal data is retained only for as long as necessary in light of the processing purpose, contractual requirements and legal obligations, and is protected by technical and organisational measures against unauthorised access, misuse, alteration and unnecessary retention. Personal data deriving from video material is processed in real time and is not stored unless the Solution detects an action which triggers a notification to users. |

## Legal basis of the processing

| Question                                    | Answer                           |
|---------------------------------------------|----------------------------------|
| What is the legal basis for the processing? | Legitimate interest. For further |

information, see the section on “Proportionality of Interests” below.

## Data processed

| Question                          | Answer                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| What types of data are processed? | <p>Video material of natural persons. IP addresses and limited contact information may also be processed for access to and administration of the services.</p> <p>As such, the following categories of personal data may be processed:</p> <ul style="list-style-type: none"> <li>(i) IP addresses.</li> <li>(ii) Contact information.</li> <li>(iii) Images containing individuals.</li> </ul> |

## Scope of data processed

| Question                                            | Answer                                                                                                                                                      |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| How many data subjects are expected to be affected? | A large number of data subjects may be affected, as the processing may capture all individuals who enter the cameras’ field of view within monitored areas. |

## Collection of data

| Question | Answer |
|----------|--------|
|----------|--------|

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>What is the source of the data?</p>  | <p>Personal data is collected primarily from the Controller’s existing camera infrastructure through real-time video feeds covering monitored areas. In addition, limited contact information and IP addresses are collected from the Controller or its authorised users for access to and administration of the services.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <p>To whom is the data transferred?</p> | <p>Only those individuals at the Controller, or where applicable at preventai as processor, who need access to personal data in order to perform their duties will have access to it.</p> <p>Personal data deriving from video material can only be transferred to a third party in an anonymised form (i.e. individual frames or notifications provided through use of the Solution).</p> <p>Other personal data may be shared with selected recipients where necessary, on the basis of the same purposes and legal bases for which the data was originally collected, and subject to appropriate technical and organisational measures.</p> <p>Categories of recipients may include:</p> <ul style="list-style-type: none"> <li>(i) Suppliers and subcontractors, including service providers supporting technical operations, IT systems, maintenance, support and related business functions.</li> <li>(ii) The Controller’s authorised personnel and, where relevant, other entities acting as independent data controllers, to the extent necessary for the relevant processing activity.</li> <li>(iii) Courts, supervisory authorities, law enforcement authorities and other public bodies, where disclosure is required by applicable law, regulation, government decision or court order, or where disclosure is necessary to establish, exercise or defend legal claims.</li> <li>(iv) A buyer, investor or other third party in connection with a merger, restructuring, sale or transfer of all or part of the Controller’s or preventai’s shares, assets or business, subject to appropriate safeguards and consistent processing by the recipient.</li> </ul> |

## Security of personal data

| Question                                                     | Answer                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Who will have access to the data and why?                    | Access to the data should, to the greatest extent possible, be allocated by the customer and limited on a strict need-to-know basis.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| What technical and organisational measures protect the data? | <p>Technical and organisational measures include:</p> <ul style="list-style-type: none"> <li>(i) Regular security scans of the codebase are conducted.</li> <li>(ii) Identity and access management controls.</li> <li>(iii) All employees undergo recurring data security training.</li> <li>(iv) All security procedures are regularly assessed and evaluated.</li> <li>(v) All activities on our servers are logged to identify potential suspicious traffic and unauthorised access.</li> <li>(vi) All statistical output is anonymised.</li> <li>(vii) All employees work on dedicated encrypted workstations with private access, secured by multi-factor authentication.</li> <li>(viii) Personal data is processed only in secure physical locations with restricted access.</li> <li>(ix) Remote access to internal systems is restricted to authorised users and devices via an encrypted VPN connection, using identity-based authentication as well as deny-by-default and least-privilege access policies.</li> </ul> |

## Data subjects' rights

| Question                                       | Answer                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| What information is provided to data subjects? | <p>In connection with the camera surveillance, data subjects should be provided with clear information regarding the surveillance by the Controller. Preventai will, according to agreements entered into between preventai and the Controller, assist the Controller in fulfilling data subjects' rights. Information provided to the data subjects by the Controller should include, as applicable:</p> <ul style="list-style-type: none"> <li>(i) The purpose of the camera surveillance.</li> </ul> |

|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <ul style="list-style-type: none"> <li>(ii) The identity of the Controller.</li> <li>(iii) Contact details of the Controller.</li> <li>(iv) Information that data subjects have rights under the GDPR.</li> <li>(v) Any circumstances that may be unexpected for the data subject, such as audio recording or storage of surveillance material outside the EU/EEA.</li> <li>(vi) How long surveillance material is stored, or the criteria used to determine the retention period.</li> <li>(vii) Where data subjects can turn to obtain additional information about the surveillance.</li> <li>(viii) The legal basis relied upon for the surveillance, usually legitimate interests.</li> <li>(ix) If the legal basis is legitimate interests, information on why camera surveillance is necessary and how the balancing test has been carried out.</li> <li>(x) Whether recorded material will be shared with any third party, such as an alarm company or similar recipient.</li> <li>(xi) The rights available to data subjects in relation to the processing, including the right to request erasure and the right to access surveillance material in which they appear.</li> <li>(xii) Information that data subjects may lodge a complaint with the relevant data protection supervisory authority if they consider the surveillance to be unlawful.</li> </ul> |
|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Proportionality of interests

| Question                                                              | Answer                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| What is the expected attitude of the data subjects to the processing? | The expected attitude from data subjects is likely to be broadly neutral to cautiously accepting, provided that clear information is made available about the processing. The technology is an extension of already widely used camera surveillance and is intended to support security-related purposes. In addition, the impact on most data subjects is limited, since individuals are anonymised through facial blurring, personal data related to processed video is not stored, and no action is taken in relation to almost all data subjects. |

|                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Is the processing to be expected by the data subjects?</p>                                                            | <p>Yes. The processing should generally be expected by data subjects, as it is carried out in connection with camera surveillance in monitored areas and clear information is to be provided by the Controller and, where applicable, specific information relating to the camera surveillance. In addition, the processing is an extension of already commonly used camera technology. That said, data subjects should be clearly informed that AI-based real-time analysis is used, as this may not otherwise be apparent to them.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <p>Explain why the purpose of the processing is proportional to the protection of the integrity of the data subject.</p> | <p>The processing is proportionate because it serves a legitimate purpose – supporting security, loss prevention and operational awareness – while measures have been implemented to reduce the impact on data subjects' privacy. Less intrusive alternatives have been assessed but found insufficient to achieve the same operational purpose.</p> <p>The impact is further mitigated by irreversible facial blurring, the absence of facial recognition or personal identification, no connection to external databases, and no storage of personal data from real-time analysis. Any action taken in response to alerts remains subject to human assessment.</p> <p>Access to personal data is restricted on a need-to-know basis and protected by technical and organisational measures. Data subjects are informed through the Controller and camera surveillance notices and are advised of their rights, including access, erasure, objection and restriction.</p> |

**FRIA**



## FRIA (Fundamental Rights Impact Assessment)

### General information about fundamental rights

A Fundamental Rights Impact Assessment (“**FRIA**”), according to the European Union’s Artificial Intelligence Act<sup>4</sup> (“**AI Act**”) evaluates how a system may affect individuals’ rights and freedoms, even in cases where specific regulatory classifications do not require formal high-risk treatment. The purpose of such an assessment is to identify, analyse, and mitigate potential impacts arising from the deployment and use of the system, particularly in environments where individuals may be subject to monitoring.

### Background and scope

Preventai provides an AI-based video analysis solution designed to transform existing camera infrastructure into intelligent, real-time sensing systems (the “**Solution**”) to its customers (the “**Deployers**”). Based on the assessment that the Solution does not classify as a high-risk AI according to the AI Act (provided in the separate “Assessment according to the AI Act”), there is no obligation for the Deployer of the Solution to carry out a FRIA. However, preventai still provides a FRIA based on the key provisions of Article 27 of the AI Act to enable the Deployer to carry out an assessment of the Solution’s impact on fundamental rights.

This FRIA is based on the AI Act as published in the Official Journal of the European Union and on the guidance and interpretive materials available as of the date of this FRIA. As the AI Act is a new instrument and no enforcement practice, delegated or implementing acts, harmonised standards, or case law have yet developed in relation to the specific questions addressed herein, certain aspects of the classification analysis necessarily involve interpretive judgments.

### Description of the processes of the Deployer

The Solution connects to existing video surveillance infrastructure in certain environments and uses artificial intelligence to detect events indicative of, for example, shoplifting or other loss-prevention-relevant events in real time, sending notifications to personnel for assessment at their discretion. All images and video material are automatically and irreversibly anonymised, making re-identification from the Solution’s output impossible. The Solution does not process the emotional states of any natural person. It operates exclusively at the level of action detection,

---

<sup>4</sup> Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (the “**AI Act**”).

identifying observable physical actions (such as concealment of merchandise or bypassing of point-of-sale infrastructure), rather than inferring psychological or emotional states or profiling.

### Time period and frequency

From the first day of deployment, the Solution will operate continuously during all hours, analysing camera footage to detect actions indicative of shoplifting or other loss-prevention-relevant events.

The number of classification outputs generated during this period will depend on the number of individuals present within the range of the camera surveillance system. As such, the exact number of registered individuals cannot be estimated without considering in which type of location the cameras are put to use.

### Categories of registered individuals

As set out above, the Solution analyses all video material from connected cameras in real time. The categories of affected individuals include all persons present within the range of the camera systems, as identified below.

#### Categories of registered individuals

Visitors in the surveyed area.

Particularly vulnerable groups among customers or visitors to the surveyed areas include, for example, elderly persons, children, and individuals whose appearance may reveal, for example, information regarding religion.

Employees and other personnel present during surveyed hours.

Third parties temporarily present in the surveyed area, for example, third party security personnel.

### Specific risks of harm

Article 27(1)(d) of the AI Act requires that the FRIA specifically identify the risks of harm that the use of the AI system is likely to pose to affected individuals. In this context, risk shall be understood as the combination of the likelihood of harm occurring and the severity of that harm. A compilation is set out in the table below:

| Category of individuals                                                     | Description of the specific risk                                                                                   | Fundamental right affected                                                                                                               | Likelihood of occurrence                                                                     | Severity of impact                                   | Risk of cumulative impact                                      |
|-----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|------------------------------------------------------|----------------------------------------------------------------|
| Customers and visitors.                                                     | Continuous recording and analysis of the individuals without the individual's knowledge.                           | The right to privacy and the protection of personal data (Articles 7 and 8 of the EU Charter of Fundamental Rights).                     | High. The system is active throughout the periods during which the individuals are surveyed. | Low.                                                 | None.                                                          |
| Employees and other personnel.                                              | Constant surveillance during working hours.                                                                        | The right to privacy and the protection of personal data (Articles 7 and 8 of the EU Charter of Fundamental Rights) and workers' rights. | High. Employees and other personnel are likely continuously within the surveyed range.       | Low.                                                 | None.                                                          |
| Third parties temporarily present on the premises, such as security guards. | Third parties temporarily present on the premises are exposed to the Solution's continuous recording and analysis. | The right to privacy and the protection of personal data (Articles 7 and 8 of the EU Charter of Fundamental Rights).                     | High.                                                                                        | Low.                                                 | None.                                                          |
| Other individuals who are not present within the surveyed area but who      | The use of a camera-based AI system with an operational range extending                                            | The right to privacy and the protection of personal data (Articles 7 and 8 of the EU Charter                                             | Low. Requires that the Deployer angles surveillance cameras in a                             | Medium, following a possible expectation of privacy. | Yes, in cases of wrongful continuous exposure where the camera |

|                                             |                                                                                                                                                                                              |                         |                  |  |                       |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|------------------|--|-----------------------|
| move within the outer range of the cameras. | beyond the premises may produce an indirect effect on the freedom of assembly and movement of individuals present in the surrounding public space if the cameras are angled in a faulty way. | of Fundamental Rights). | wrongful manner. |  | covers a public area. |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|------------------|--|-----------------------|

### Measures for human oversight

The Solution does not take autonomous action in response to detected events. It sends notifications to users, who retain full discretion as to how, or whether, to respond. The Solution does not trigger automated interventions such as locking mechanisms, direct alerts to law enforcement, or any other measure that would produce legal or similarly significant effects on natural persons without human intervention.

To use the Solution, it is required to have knowledge of how to use it correctly. The users must also follow internal procedures on how to manage situations involving suspected theft, damage to property, and similar conduct. In those situations that have been identified due to the Solution, any potential measure and the rationale for the measure shall be documented in writing in an appropriate manner.