

## **POLICY FOR VIDEO SURVEILLANCE IN LUKOIL NEFTOHIM BURGAS AD**

This Security Video Surveillance Policy ("Policy") has been prepared by LUKOIL Neftohim Burgas AD ("LUKOIL"/"Company"/"We") in order to provide all interested parties with an accessible and understandable information about the security video surveillance system (the "System") used, the conditions and manner of processing of the personal data generated as a result of the operation of the System, as well as the order according to which the natural persons whose personal data is processed can exercise their rights as per the personal data protection legislation.

### **1. Purpose and Scope of the Policy**

In order to provide for the security and safety of the employees, visitors, sites, property and information, the Company uses a security video surveillance system for the perimeter and in some areas of its sites. The Policy describes the security video surveillance system of the Company and the protection measures taken for protection of personal data, personal life inviolability and other main rules and legitimate interests of the natural persons that fall into the scope of the cameras.

### **2. Conformity with the Applicable Data Protection Texts**

#### **2.1. Reference**

The Company uses its security video surveillance system in accordance with Regulation (EC) 2016/679 concerning the protection of natural persons in terms of personal data processing and free movement of such data.

#### **2.2. Transparency**

This Policy is accessible in the public domain and is announced on the Internet site of LUKOIL Neftohim Burgas AD [neftochim.lukoil.com/bg](http://neftochim.lukoil.com/bg) - Company / Information Exacted for Publication.

#### **2.3. Periodic Inspections**

A periodic inspection of the System is made once a year for:

- evaluation of the adequacy of the System in terms of security provision;
- conformity of the System with the requirements of Regulation (EC) 2016/679.

#### **2.4. Personal Life Inviolability Protection**

In order to protect personal life inviolability, the Company applies the following principles and approaches in the video surveillance:

- indistinguishable image – masking (in order to obtain partially or fully indistinctive image as the case may be);
- limitation of the period for record storage in accordance with the requirements of the Private Security Activity Law;
- strict management of the rights of the operators of the System.

### **3. Areas under Surveillance**

The location of the cameras is reconsidered carefully in order to ensure that areas of no importance for the purposes pursued are included to the minimum. The surveillance outside the territory of the Company is brought to the minimum.

There is no surveillance in areas in which there are increased expectations for inviolability. As an exception, in case of duly justified security-related circumstances, cameras can also be installed in such areas and, in any case, this is done after evaluation of the impact and after a notification to the Data Protection Official of LUKOIL Neftohim Burgas AD. In such cases, a special, clearly visible notice is put on the premises.

In exceptional cases, when there is a duly justified and demonstrable security-related necessity, hidden cameras can be used in order to prevent and disclose violations. The use of hidden cameras is subject to a preliminary approval by the Chairman of the Board of Managers of the Company and to an orderly notification to the Data Protection Official within an official inspection for security purposes. The use of hidden cameras is always proportionate to the severity of the violation presumed. Any case of use of hidden cameras is documented in detail which includes:

- a clearly defined purpose which cannot be achieved by means of an alternative way of inspection which violates personal life inviolability to a lower degree;
- evaluation of the impact in terms of the area which is within the range of the hidden cameras and the people concerned;
- a strictly limited period of time;
- strictly limited locations;
- strict limitation of the users and clear definition of their identities;
- deletion of the records immediately after they are no longer necessary for the inspection purposes.

### **4. Personal Data Collection and Purpose of Collection**

#### **4.1. General**

Company's security video surveillance is a conventional and mostly static system. Digital images in the areas under surveillance are recorded together with the time, hour, and location. All cameras operate continuously. When advisable, image quality allows to identify the people within the camera range. Almost all cameras are stationary and very few of them can be used by the operators to enhance the image in a particular situation due to security reasons. Operators who are trained for that purpose observe the requirements in terms of personal life and access rights protection.

The Company does not use high-tech or intelligent technologies for video surveillance and sound-recording equipment or the so called talking CCTV.

#### **4.2. Surveillance Use Purpose**

The Company uses the security video surveillance system only for security and safety purposes. The system guarantees the security of Company's sites, the safety of the employees and visitors, as well as of the property and information which are located or stored on the territory.

When necessary, the security video surveillance complements the other physical security systems like the access control system and the physical infiltration control systems. It is a part of the measures which support the procedures applied in the Company in the field of security and contributes to prevent, restrain and, if necessary, make inspections for unsanctioned physical access, including to secure and protected premises, information infrastructure, and/or confidential information.

#### **4.3. Limitation of Purposes**

The system is not used for other purposes like surveillance of the work of the employees or the rest of the personnel or for keeping track of the presence. The system is used as an inspection or evidence tool within internal inspections or disciplinary proceedings, exclusively for the purposes of the inspection of incidents related to physical security. The inspections are always made within a specific mandate provided by the Chairman of the Board of Managers of the Company.

#### **4.4. Ad hoc Use of Video Systems**

In case of a duly justified, security-related need for ad hoc video surveillance, it can be provided and the activities are planned in advance, an evaluation of the impact is prepared and the Data Protection Official is informed.

#### **4.5. Web Cameras**

The Company does not use web cameras in the security video surveillance system.

#### **4.6. Special Data Categories**

Company's security video surveillance system does not aim at catching (for example, by enhancing an image or target guidance) or at otherwise processing (for example, indexing, profiling) images which disclose the so called "special data categories".

### **5. Legal Grounds for Video Surveillance**

- Ordinance № 181 by the Council of Ministers dated 20.07.2009 on the determination of strategic sites and activities which are of national security importance
- Instructions № Із – 3025/21.12.2010 on the conditions and order for determination of strategic areas of strategic sites and areas related to performance of strategic activities which are of national security importance
- Instructions by State Agency for National Security (SANS) № І – 1068/26.08.2011 on the system of measures, methods and means for physical security of strategic sites and strategic areas
- Regulation on the conditions and order for achievement of security for vessels, ports and port areas. Passed by Ordinance by the Council of Ministers № 374 dated 25.11.2014, publ., State Gazette (SG), issue 99 of 2.12.2014.
- Regulation № ПД-02-20-6 dated 19.12.2016 on the technical requirements for physical security of construction sites
- National Anti-Terrorism Plan
- LAW on Private Security Activity
- Site Security Surveillance

## **6. Access to Personal Data Collected**

**6.1.** The access to video records and to the material that is being recorded at the moment is restricted to very few, strictly determined people based on the “need-to-know” principle.

**6.2.** The access to the records and/or the technical architecture of the video system is restricted to very few, strictly determined people based on the “need-to-know” principle. The Company clarifies the purpose and scope of their rights to access. Particularly, the Company determines who has the right to watch the camera recordings in real time; to watch the records; to copy, download, or delete a certain record.

**6.3.** All employees who have rights to access, including the guards hired by an external subcontractor, initially pass also through periodic trainings in confidentiality and get familiar with the applicable legal, by-law, and internal company rules referring to personal data protection.

**6.4.** After training, each employee signs a confidentiality declaration. Such declaration is also signed by all subcontractors and their personnel that perform activities related to repair, maintenance, and revamp of the security video surveillance system.

**6.5.** All cases of transfer and disclosure outside Company’s corporate security structure are documented and are subject to a strict evaluation of the need for such transfer and the compatibility of the transfer purposes with the initial, security-related processing purpose. The Data Protection Official can review the register of the information kept and the transfers.

The management and the employees who work in the human resources field are not granted access, except within disciplinary proceedings which are a direct result of an incident related to physical security and as per an instruction by the Chairman of the Board of Managers.

If necessary, for the purposes of the investigation or the punitive prosecution of a criminal act, access can be granted to bodies of the judicial power and the security and public order services.

Any violation of data security in terms of security video surveillance is entered in the inspection register and is communicated in timely manner to the Data Protection Official.

## **7. Personal Data Protection and Guarantee**

In order to provide for the security of the security video surveillance, including personal data, the following technical and organizational measures have been taken и:

- The servers on which the records are stored are located in secure rooms which are protected by physical security measures; network firewalls protect the logical parameter of the information infrastructure; the main computer systems which store the data have an additional security protection;
- The administrative measures include the obligation to make an individual inspection for reliability of all hired subcontractors which have access to the system (including equipment and system maintenance personnel);
- All employees (internal and external) sign information non-disclosure and confidentiality agreements;

- The access rights for the users are granted only for the resources which are absolutely necessary for the fulfillment of their obligations;
- Only an official especially assigned for that purpose by the Company can grant, modify, or deprive the access rights of the employees. Any granting, modification, or deprivation of access rights is made in writing and according to an established order and strict criteria;
- At any time, the Company keeps an updated list of all people who have access to the system and describes in detail their access rights.

## **8. Data Storage Period**

The images are kept for a period of 60 (sixty) days. After the expiry of such period, the images are deleted in the same sequence in which they were recorded in the system. In case of a security-related incident, the relevant record can be kept for a period longer than the usual one, as long as necessary for the further inspection of the incident. The keeping of such a record is strictly documented and the need for keeping is reconsidered periodically. The corporate security structure authorized and the Data Protection Official can review the register of the information kept and the transfers.

## **9. Information for the Public**

### **9.1. Multi-layer Approach**

The Company applies a multi-layer approach which includes the following:

- a detailed message with information about the use of video surveillance is put at each Gate
- there are messages with pictograms in the buildings with video surveillance in order to indicate that there is surveillance and to indicate the way to obtain an additional information
- application of the best available practices in the video surveillance field

### **9.2. Specific Individual Message**

Notwithstanding the rules applicable to the inspections, the people who are recorded by the cameras (for example, security guard people within an inspection for security purposes) receive an individual message in case at least one of the following circumstances occurs:

- their identities are entered in a dossier/record;
- the video record is used against the respective person, it is kept for a period longer than the usual one, or it is transferred outside the corporate security sub-division;
- the identity of the person is revealed to someone outside the authorized corporate security structure.

The sending of a message can be delayed if it is necessary for the prevention, investigation, discovery and legal prosecution of criminal acts.

In any such case, the Data Protection Official is consulted in order to guarantee the observation of the rights of the people concerned, except in cases of investigations.

### **9.3. Right of Natural Persons to Confirm, Modify, or Delete their Data**

The persons have the right to access the personal data we process for them and the right to correct and supplement such data. Any request for access, correction, blocking and/or deletion of personal data obtained as a result of the operation of the security video surveillance System shall be made to:

The Data Protection Official

E-mail: [dpo@neftochim.bg](mailto:dpo@neftochim.bg)

Telephone: +359 5511/3410

LUKOIL provides information about the actions undertaken in relation to a request to exercise the rights of the subjects within one month from the receipt of the request and in accordance with Personal Data Protection Policy of LUKOIL Neftohim Burgas AD published on the website of LUKOIL Neftohim Burgas AD [neftochim.lukoil.com/bg](http://neftochim.lukoil.com/bg) - Company / Information Exacted for Publication.

*This Policy has been approved by the Chairman of the Board of Managers of LUKOIL Neftohim Burgas AD by Order № 30Д-0150-02.08.18.*