 NIS БУДУЩНОСТ <small>GAZPROM NEFT</small> НА ДЕЛУ NIS PETROL EOOD	НИС ПЕТРОЛ ЕООД № 01/400/389 дата: 20.02.2020 гр.София Version 2.0
ECONOMIC SECURITY DEPARTMENT	
PERSONAL DATA PROTECTION POLICY	Regulation 2016/679 20.02.2020


APPROVE,
ALEXANDR MAKAREVICH
NIS PETROL EOOD MANAGER:



Owner: NIS PETROL EOOD	Date: 20.02.2020	Version 2.0
<p>NIS PETROL EOOD</p> <p>PERSONAL DATA PROTECTION POLICY</p> <p>REGULATION 2016/679</p> <p>Organization for the processing and protection of personal data</p> <p>Principles. Rules. Requirements. Protection measures</p>		

CONTENTS

I. GENERAL CONDITIONS	2
II. DEFINITIONS	2
III. PURPOSES FOR THE COLLECTION AND PROCESSING OF PERSONAL DATA	3
IV. DATA SUBJECTS' RIGHTS	3
V. PRINCIPLES FOR THE PROTECTION OF PERSONAL DATA	4
VI. MEASURES TO PROVIDE PERSONAL DATA PROTECTION	4
VII. BASIC RULES AND MEASURES FOR PROVIDING THE PROTECTION OF PERSONAL DATA IN COMPUTER PROCESSING	11
VIII. SUPPORTED REGISTERS WITH PERSONAL DATA AND THEIR MANAGEMENT	12
IX. RIGHTS AND OBLIGATIONS OF PROCESSORS	13
X. ADDITIONAL PROVISIONS	14

 NIS БУДУЩНОСТ <small>GAZPROM NEFT</small> НА ДЕЛУ NIS PETROL EOOD	Version 2.0
ECONOMIC SECURITY DEPARTMENT	
PERSONAL DATA PROTECTION POLICY	Regulation 2016/679 20.02.2020

I. GENERAL CONDITIONS

Art. 1. (1) NIS PETROL EOOD (NIS PETROL) is a legal entity that carries out activities related to trading of fuels and petroleum products.

(2) NIS PETROL is a legal entity with its registered office and management address in Sofia, 51A Nikola J. Vaptsarov Blvd.

(3) NIS PETROL is a personal data controller within the meaning of Art. 4, item 7 of the General Data Protection Regulation (EU) 2016/679

(4) As a data controller, NIS PETROL complies with the data protection principles laid down in the General Data Protection Regulation (EU) 2016/679 and the legislation of the European Union and the Republic of Bulgaria when processing personal data.

(5) As a legal entity established under the law, NIS PETROL carries out the activities described in the Internal Regulation on Labor Rules.

(6) NIS PETROL processes personal data in connection with its activity and determines the purposes and means for its processing in accordance with the requirements laid down in the relevant laws, regulations and normative acts. In this case, NIS PETROL acts as a data controller. In some of these cases NIS PETROL works with third parties who are processing personal data with which they have agreements, in accordance with the requirements of Art. 24 of the General Regulation.

(7) In the cases where NIS PETROL processes personal data for purposes determined independently by a third party or the purposes are jointly determined by NIS PETROL and a third party, NIS PETROL has the position of either a personal data processor (if the purposes are determined by the person, who assigned the processing) or of a joint controller.


Art. 2. (1) This NIS PETROL Personal Data Protection Policy governs the organization of the processing and protection of personal data of employees, including applicants for NIS PETROL jobs, of NIS PETROL's contractors and partners, and of all other groups of individuals with whom NIS PETROL enters into relations in the conduct of its activity. An integral part of this Policy is the Instruction on Technical Measures for Personal Data Protection, approved by the Manager of NIS PETROL.

(2) In accordance with the requirements of Art. 37, § 7 of the Regulation (EU) 2016/679 in NIS PETROL by an Order of the Manager has been designated a Data Protection Officer.

II. DEFINITIONS

Art. 3. (1) "Personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

(2) "Processing of personal data" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

 NIS БУДУЋНОСТ <small>GAZPROM NEFT</small> НА ДЕЛУ			
NIS PETROL EOOD		Version 2.0	
ECONOMIC SECURITY DEPARTMENT			
PERSONAL DATA PROTECTION POLICY		Regulation 2016/679	20.02.2020

(3) "Personal data register" means any structured set of personal data, regardless of type and medium, access to which is carried out according to certain criteria, whether centralized, decentralized or distributed according to functional or geographical principle.

III. PURPOSES FOR THE COLLECTION AND PROCESSING OF PERSONAL DATA

Art. 4. (1) Personal data shall be collected for specific, precisely defined by law purposes, the applicable normative acts and regulations applied by NIS PETROL. Personal data is processed lawfully and in good faith and cannot be further processed in a manner incompatible with these purposes.

(2) If the specific purpose or purposes for which personal data is processed by NIS PETROL do not require or no longer require identification of the data subject, NIS PETROL is not obliged to maintain, obtain or process additional information in order to identify the data subject for the sole purpose of proving compliance with the requirements of Regulation 2016/679.

(3) The grounds for the lawfulness of the processing of personal data by NIS PETROL pursuant to Article 6 of the Regulation are:

- (a) *the data subject has given consent to the processing of his or her personal data for one or more specific purposes;*
- (b) *processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*
- (c) *processing is necessary for compliance with a legal obligation to which the controller is subject;*
- (d) *processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*
- (e) *processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*


In such cases, NIS PETROL shall inform the data subjects of all aspects of the processing of their personal data, including, but not limited to, their rights as required by the General Regulation.

In cases where NIS PETROL processes personal data of the subjects on the grounds of Art. 6 paragraph 1, letter a) of the General Regulation, NIS PETROL requires the prior consent of the subjects and informs them in advance of all aspects of the processing of their personal data, including, but not limited to, their rights as required by the General Regulation

IV. DATA SUBJECTS' RIGHTS

Art. 5. (1) Everyone who provides personal data has the following rights:

1. To give explicit consent or disagreement to the processing of his/her personal data;
2. To receive information about the processing of personal data;
3. To have access to his/her personal data stored;
4. To request that incorrect, inaccurate or incomplete personal data be rectified;

 NIS БУДУЋНОСТ <small>GAZPROM NEFT</small> НА ДЕЛУ NIS PETROL EOOD	Version 2.0	
ECONOMIC SECURITY DEPARTMENT		
PERSONAL DATA PROTECTION POLICY	Regulation 2016/679	20.02.2020

5. To request that personal data be erased when it is no longer needed or if its processing is illegal;
6. To object to the processing of his/her personal data on grounds relating to a particular situation;
7. To request the restriction of the processing of personal data in specific cases;
8. To receive his/her personal data in a machine-readable format and send it to another controller ("data portability");
9. To demand that decisions based on automated processing and based on the personal data of their holder and which significantly affect the subject should be made by individuals, not just computers. The holder is also entitled in this case to express his or her personal point of view and to challenge the decision.

V. PRINCIPLES FOR THE PROTECTION OF PERSONAL DATA


Art. 6. (1) The principles for protection of personal data are:

1. **Lawfulness, fairness and transparency** - processing in the presence of a legal basis, taking due care and informing the data subject.
2. **Purpose limitation** - collecting data for specific, explicitly stated and legitimate purposes and prohibiting further processing in a manner incompatible with those purposes;
3. **Data minimization** - be adequate, relevant, and limited to what is necessary for processing purposes;
4. **Accuracy** - keeping up-to-date and taking all reasonable steps to ensure the timely erasure or rectification of inaccurate data, taking into account the purposes of processing;
5. **Storage limitation** - data should be processed for a minimum duration according to the purpose. Long-term preservation is permissible for purposes of archiving in the public interest, for scientific or historical research or for statistical purposes, provided that appropriate technical and organizational measures are applied;
6. **Integrity and confidentiality** - processed in a manner that guarantees an adequate level of security of personal data, applying appropriate technical and organizational measures for data security;
7. **Accountability** - the controller is responsible and must be able to demonstrate compliance with all principles regarding the processing of personal data.

VI. MEASURES TO PROVIDE PERSONAL DATA PROTECTION

Art. 7. NIS PETROL organizes and takes measures for protection of personal data from accidental or unlawful destruction, from unauthorized access, from alteration or distribution, as well as from other illegal forms of processing of personal data. Measures taken shall take into account current technological developments and the risks associated with the nature of the data to be protected and in accordance with the specified levels of impact.

Art. 8 (1) NIS PETROL applies adequate protection of personal data, which includes:

 NIS БУДУЋНОСТ <small>GAZPROM NEFT</small> НА ДЕЛУ NIS PETROL EOOD	Version 2.0	
ECONOMIC SECURITY DEPARTMENT		
PERSONAL DATA PROTECTION POLICY	Regulation 2016/679	20.02.2020

1. Physical protection;
2. Personal protection;
3. Documentary protection;
4. Protection of information systems and networks;
5. Cryptographic protection.

Art. 9 (1) The personal data shall be stored on paper, technical and / or electronic media, only for the time necessary for fulfilling the obligations of NIS PETROL and / or for the period specified by a normative act.

(2) The collection, processing and storage of personal data in the registers of NIS PETROL shall be carried out in paper, technical and / or electronic form on premises, in accordance with the provided security measures and the assessment of the appropriate security level of the respective register.

Art. 10. When the hypotheses of Art. 6, para. 1, letter "b" - "f" of Regulation 2016/679, the natural persons whose personal data is processed by NIS PETROL sign an informed consent according to a template.

Art. 11. (1) Only NIS PETROL employees, designated for this purpose, as well as processors of personal data, to whom the controller has assigned the processing of data from the respective register under the conditions of Art. 28 of the General Data Protection Regulation.

(2) The designation of employees under Art. 11, para 1 shall be carried out on the basis of a job description or by an explicit order of the Manager of "NIS Petrol" EOOD or a person authorized by him/her.

(3) The employees are responsible for providing and guaranteeing regulated access to the office premises and keeping the registers containing personal data secure. Any deliberate breach of the rules and restrictions on access to personal data by employees may justify disciplinary action against the concerned employees.

(4) Officials shall not have the right to disseminate information about personal data that became known to them in the course of and in connection with the performance of their official duties.

Art. 12. (1) The documents and files the work on which has been completed shall be stored on paper and on an electronic medium - NIS PETROL server.

(2) The permanent storage of documents containing personal data shall be carried out in paper form at the premises of departments in NIS PETROL, with storage periods in accordance with the legislation in force.


(3) Documents in electronic form shall be stored on specialized servers, computer systems and / or external media. The backup of personal data on a technical medium is periodically carried out by the processor / operator of the personal data in order to keep the information for the respective persons up-to-date and in order to provide an opportunity for recovery in case of the loss of the primary medium / system.

(4) Only persons designated for this purpose shall have access to documents containing personal data in accordance with the powers assigned to them.

Art. 13. (1) In order to protect the paper, technical and information resources, all employees shall be obliged to comply with the fire safety rules.

(2) The employees shall undergo compulsory briefing to familiarize themselves with the fire safety rules at once a year. For a conducting briefing shall be prepared protocol to a template.

Art. 14. (1) Once a year, periodic audits shall be carried out on the status and integrity of the personal data contained in the registers processed by NIS PETROL. The audits shall be carried out by a committee designated by the Manager, who shall prepare a Report on the outcome of the audit.

 NIS БУДУЋНОСТ <small>GAZPROM NEFT</small> НА ДЕЛУ NIS PETROL EOOD	Version 2.0	
ECONOMIC SECURITY DEPARTMENT		
PERSONAL DATA PROTECTION POLICY	Regulation 2016/679	20.02.2020

(2) The report under para. 1 shall include an assessment of the need for processing of personal data or erasure. The reports shall be addressed to the Data Protection Officer and to the Manager.

Art. 15. (1) When registering unauthorized access to the information files for personal data or in another incident, which breaches the security of personal data, the employee, having found this breach / incident, shall immediately report it to his / her direct manager, who in his / her duty is obliged to inform the Data Protection Officer of the incident in a timely manner. The notification of an incident shall be made in writing, by electronic means or in any other way, which allows to establish its occurrence and to comply with the requirement to notify the Commission for Personal Data Protection within 72 hours after having become aware of such incident.

(2) The process of reporting and managing incidents must include the registration of the incident, the time of its identification, the person who reports it, the person to whom it was reported, its consequences and the measures for its elimination.

Art. 16. (1) In case of increase of the level of sensitivity of the information arising from a change in its type or in the risks in its processing, NIS PETROL may determine additional measures for protection of the information from the respective register of personal data.

(2) Reports on the status, risks and sensitivity of the information shall be prepared once every 2 years or when the nature of the processed personal data changes.

Art. 17. (1) After achieving the purpose of processing the personal data contained in the registers maintained by NIS, respectively, upon expiry of the specified period, personal data should be erased in accordance with the procedures laid down in the applicable regulatory acts and in this Personal Data Protection Policy.

(2) In cases where the erasure of a personal data medium is required, NIS PETROL shall apply the necessary actions for the deletion of personal data in a way that excludes data recovery and misuse, such as:

1. Personal data stored on electronic media shall be erased by permanent deletion, incl. copying of electronic means or physical destruction of media;
2. Paper documents containing data shall be destroyed by cutting.

(3) Erasure shall be carried out by employees authorized by an explicit written order of the Manager and after notification to the Data Protection Officer.


(4) For the performed erasure of personal data and data carriers, a Protocol shall be drawn up, signed by the employees under para. 3.

Art. 18. (1) Access to personal data shall be granted to persons only if they are entitled to such access according to the current legislation and / or for the purpose of fulfilling their official duties, after submitting an application for access to information and after legitimizing it.

(2) NIS PETROL shall announce its decision to grant or refuse access to personal data for the respective person within 1 month as from the submission of the application. If necessary, this period may be extended by two months, taking into account the complexity and number of applications from a specific person. NIS PETROL shall inform the data subject of any extension within one month of receipt of the application, indicating the reasons for the extension.

(3) The information may be provided in the form of:

1. oral information;
2. written information;
3. review of the data by the person;

 NIS БУДУЋНОСТ <small>GAZPROM NEFT</small> НА ДЕЛУ NIS PETROL EOOD	Version 2.0
ECONOMIC SECURITY DEPARTMENT	
PERSONAL DATA PROTECTION POLICY	Regulation 2016/679 20.02.2020

4. providing the requested information on a technical and / or electronic medium.

(4) Any legal subject that processes personal data by appointment of and on behalf of the controller is a personal data processor and should sign a data processing agreement in accordance with a template, including the clauses under Art. 28, para. 2-4 of the General Data Protection Regulation.

(5) Third parties shall have access to personal data processed in NIS PETROL, provided there is a legal ground for the processing of personal data (eg. NRA, NSSI, etc.).

Art. 19. Physical protection at NIS PETROL is provided through a set of applicable technical and organizational measures to prevent unauthorized access and for protection of the building and premises where personal data processing activities are carried out.

Art. 20. (1). The main *organizational measures for physical protection* in NIS PETROL include:

1. designation of the premises in which personal data will be processed;
2. designation the premises in which the elements of the communication-information systems for processing of personal data will be located,
3. designation of the organization of physical access;

(2) The premises in which personal data will be processed shall be defined as all premises where personal data are collected, processed and stored for the normal course of the work process. Access to them is physically restricted and controlled - only for employees with a view to fulfilling their official duties and if their place of work or job description allows access to the relevant premises and the relevant personal data register. Where such premises are accessible to outsiders, the premises shall set up a "non-public" part, where the processing of personal data is carried out, which is physically restricted and accessible only to employees who need to have access for the purposes of performance their duties and the "public part" - accessed by outsiders and in which no processing activities are performed, including no data stored, whatever their medium.

(3) *Communication and information systems used for the processing of personal data* shall be located in premises, the access to which is restricted only to those employees who, in order to fulfill their official duties, need such access to the data, as well as the persons charged with service commitments to maintain the proper functioning of these systems.


(4) *The organization of physical access to premises* where personal data processing activities are carried out is based on limited physical access, including access to be restricted for those in which the information systems are located. Access is only given to employees who need it for the performance of their duties.

(5) *Controlled access zones* are all premises on the territory of NIS PETROL in which personal data is collected, processed and stored.

(6) *The technical means used for the physical protection of personal data* in NIS PETROL shall be consistent with the legislation in force and the level of impact of such data. All physical areas with paper and electronic records are restricted only to employees who must have access through the "Need-to-know" principle in order to fulfill their work responsibilities.

(7) All paper records and documents containing personal data shall be stored in lockable cabinets. Access is restricted and is only available to employees who need it.

(8) Access to systems processing electronically personal data is restricted by unique user IDs and passwords, and electronic media, including servers, are adequately protected in areas with access control.

 NIS БУДУЋНОСТ <small>GAZPROM NEFT</small> НА ДЕЛУ	Version 2.0	
ECONOMIC SECURITY DEPARTMENT		
PERSONAL DATA PROTECTION POLICY	Regulation 2016/679	20.02.2020

Art. 21. (1). The main *technical measures for physical protection* in NIS PETROL include:

1. use of security-alarm equipment;
2. use of locks and locking mechanisms;
3. cabinets, metal cases;
4. equipping the premises with fire extinguishers.

(2) Documents containing personal data shall be stored in *lockable cabinets or filing cabinets*, the latter being located in restricted (controlled) areas. The key to the cabinets is only provided to the explicitly charged persons (by explicit order or by virtue of their official duties and job description).

(3) *The equipment of the premises* where personal data is collected, processed and stored includes: security-alarm equipment, locks (mechanical or electronic) for restricting access only to authorized persons; lockable cabinets and fire extinguishers.

(4) *Fire extinguishers* shall be disposed of in accordance with the requirements of the applicable legislation.

Art. 22. (1). The *main personal protection measures* for the personal data applicable in NIS PETROL are:


1. Obligation of employees to undergo training and to familiarize themselves with the regulations in the field of personal data protection and this Personal Data Protection Policy, with the completed training and instruction with the rules on personal data protection being certified by a signature on instructed to protect personal data;
2. Familiarity with and awareness of the dangers of personal data processed by NIS PETROL;
3. Prohibition on the sharing of critical information (identifiers, access passwords, etc.) between staff and any other unauthorized persons;
4. Declaring consent to a non-disclosure obligation.

(2) In addition to the measures personal data evaluated with higher risk, such as sensitive personal data, shall apply the measures under para. 1 and the following additional measures:

1. Conducting specialized trainings to work with and for protection of personal data, if the specificity of the duties requires such;
2. Training of personnel to respond to events that threaten data security in the event that the specificity of the duties requires such.

Art. 23. (1). The main *measures for documentary protection* of personal data are:

1. *Designation of the registers to be stored electronically with the departmental coordinators* - all personal data is stored electronically, which requires filling it in on certain blank documents and / or forms related to meeting the requirements of the current legislation or directly related to the performance of the normal activities of NIS PETROL, conclusion of contracts, performance of contracts, exercise of the rights stipulated by law and obligations established by law;
2. *Designation the conditions for the processing of personal data* - personal data is collected and processed only for a specific purpose, directly related to the fulfillment of the legal obligations and /

 NIS БУДУЋНОСТ <small>GAZPROM NEFT</small> НА ДЕЛУ NIS PETROL EOOD	Version 2.0	
ECONOMIC SECURITY DEPARTMENT		
PERSONAL DATA PROTECTION POLICY	Regulation 2016/679	20.02.2020

or the normal activity of NIS PETROL, and the manner of its storage is tailored to the specific processing needs and the physical storage medium;

3. *Regulating the access to personal data registers* - access to personal data registers is restricted and is only granted to authorized employees in accordance with the "Need-to-know" principle;
4. *Determination of storage periods* - personal data shall be retained for no longer than is necessary to achieve the purpose for which it was collected or until the expiry of the period specified in the legislation in force.
5. *Destruction Procedures*: Documents containing personal data, storage periods that have expired and are not necessary for the proper functioning of NIS PETROL or for the establishment, exercise or defense of legal claims shall be destroyed in an appropriate and secure manner (e.g. combustion, slicing, electronic deletion and other appropriate methods in accordance with the physical medium).

(2) For personal data evaluated with a higher degree of risk, in addition to the measures under para. 1, the following additional measures shall also apply:

1. *Control of access to the registers*, restricting access of personnel or, in limited cases, of other specially authorized persons, in accordance with the "Need-to-know" principle, in order to fulfill their duties;
2. *Reproduction and dissemination rules*, which allow the copying and distribution of personal data only in cases where this is necessary for legal purposes, arises at the requirement of a law and / or a request of a public authority, and only be made available to persons, which are required in connection with the performance of the assigned work to have it. Unauthorized copying and distribution is subject to disciplinary sanctions and other measures if it represents a violation of any kind other than violation of the discipline of labor.


Art. 24. (1) *Protection of information systems / databases and / or networks* in NIS PETROL shall include a set of applicable technical and organizational measures for preventing unauthorized access to the systems and / or networks in which personal data is created, processed and stored.

(2) The main measures for *the protection of information systems / databases and / or networks* processing personal data in NIS PETROL shall include:

1. *Identification and authentication* through the use of unique user accounts and passwords for each person accessing the NIS PETROL network and resources. The implementation of this measure is aimed at regulating levels of access and introducing access in accordance with the "Need-to-know" principle;
2. *Management of registers*, in order to restrict access to the relevant register only to persons who are directly entrusted and / or ex officio engaged in its maintenance, maintenance and processing;
3. *Management of external connections and / or connectivity*, which include:

- Defining the scope of internal networks: All *local area networks* and / or point-to-point telecommunication connections under the control and administration of NIS PETROL are considered as *internal networks*. *External networks* are considered all networks, incl. and wireless networks, the Internet, Internet connections, third-party network connections, third-party hosting systems that are not under the administrative control of NIS PETROL.

- Regulating access to the internal network: Only employees and / or persons specifically authorized by the Manager have access to the internal network. Access to the network and personal data processed shall be granted for the purpose of fulfilling their direct duties and shall comply with the "Need to know" principle. The minimum

 NIS БУДУЋНОСТ <small>GAZPROM NEFT</small> НА ДЕЛУ			
NIS PETROL EOOD		Version 2.0	
ECONOMIC SECURITY DEPARTMENT			
PERSONAL DATA PROTECTION POLICY		Regulation 2016/679	20.02.2020

required level of security for access to internal networks requires identification with a unique username and password.

- Administration of access to the internal network: Responsibilities related to the implementation of access administration are assigned to persons with the necessary qualifications. Responsibilities under the respective contracts also include activities related to approving the installation of all devices, technologies and software for network access, including switches, routers, wireless access points, network access points, Internet connections, connections to external networks and other devices, technologies, and software that may allow access to the Administrator's internal networks.

- Control of access to the internal network: Responsibilities related to the implementation of access control are assigned to persons with the necessary qualifications. They are required to take adequate measures to minimize the risk of unauthorized (physical and / or remote) access to NIS PETROL networks, incl. and by using firewalls and other adequate measures and tools.

1. *Malware protection* includes:

- the use of standard configurations for each computer and / or network platform, with the system and if possible, the application software being controlled, installed and maintained by persons designated by the Manager. Installation of software products without the explicit approval of NIS Petrol's IT department is prohibited.

- use of the built-in functionality of the operating system and / or hardware, which can only be configured by persons authorized by the Manager. Any modification and / or deactivation of protection systems against unauthorized persons is prohibited.

- enabling automatic protection and scanning for malware and updating antivirus definitions. Users are prohibited from denying automatic software processes that update virus definitions.

- ban on transmission of data from infected computers. In case of suspected or detectable contamination of a computer system, the employee shall be obliged to notify the persons authorized by the Manager and to suspend any actions for the operation and / or sending information from the infected computer (through external media, e-mail and / or other electronic means exchange of information). Until the removal of malware, the infected computer should be immediately isolated from the internal networks.

2. *A backup creation and maintenance policy which governs:*

- The main purpose of backing up is to prevent the loss of information related to personal data, which would impede the normal functioning of NIS PETROL.

- Backup method: The information should be backed up appropriately and on a medium other than the specific physical computer and allow full recovery of the data in the event of their primary medium being lost.


- Responsible for backing up is the person who processes the personal data.

- The back up period should comply with the applicable legislation.

- Keeping the back up in a separate room. All back ups containing confidential and / or official information must be stored with physical access control.

3. The main *electronic storage media* are: internal hard drives (part of a computer and / or storage system), single and / or rewritable external media (external hard drives, rewritable cards, memory tapes and other storage media, non-rewritable mediums, etc.)

4. *The personal data protection* is a part of the overall security of NIS PETROL.

 NIS БУДУЋНОСТ <small>GAZPROM NEFT</small> НА ДЕЛУ			
NIS PETROL EOOD		Version 2.0	
ECONOMIC SECURITY DEPARTMENT			
PERSONAL DATA PROTECTION POLICY		Regulation 2016/679	20.02.2020

5. *The personal data in electronic form shall be stored* in accordance with the statutory periods and in accordance with the specifics and needs of NIS PETROL.
6. Data that is no longer needed for NIS PETROL purposes and whose storage period has expired *shall be destroyed by an applicable method* (for example by cutting, combustion or permanent deletion by electronic means).

(3) For personal data evaluated with a higher degree of risk, in addition to the measures under para. 2 additional measures shall apply, related to:

1. *Organization of telecommunication links and remote access* to NIS PETROL's internal networks:

- Remote access to NIS PETROL's internal networks is not provided. By way of exception, and subject to the express permission of the management of NIS PETROL, such access may be granted to explicitly designated persons, using adequate and applicable modern methods of protecting the connection and the data exchanged.

- NIS PETROL personnel may be provided with Internet access (remote access) to fulfill their job responsibilities to the electronic registers with personal data. The range of access and the type of resources available (including sites, files, services, etc.) is determined by the discretion of the NIS PETROL Manager. Remote Internet access to certain resources, incl. and internal ones, may be terminated at any time at the discretion of the NIS PETROL Manager, as well as in the event of a threat to data security.

- Publication of official information on the Internet, no matter in what form or platform, is made only with the written permission of the Manager.

2. The measures related to the current *maintenance and operation* of NIS PETROL's information systems and resources shall include:


- Security assessment, including periodic tests and assessments of the vulnerability of NIS PETROL's networks and systems against external and internal attacks (Vulnerability test), including impact assessment, adequacy of the measures and methods of protection used, and recommendations for its technical and organizational improvement. The evaluation shall also cover the aspects mentioned, as well as the security of the personal data collected, processed and stored.

- Prohibition on the possession and use of hardware or software tools by NIS PETROL personnel that could be used to compromise the security of information systems. This group also includes tools that promote copyright infringement, the disclosure of secret passwords, the identification of security vulnerabilities, or the decryption of encrypted files. It is also forbidden to use any hardware or software that remotely monitors network or operating computer traffic.

3. Measures related to the creation of a *physical environment (surrounding)* include physical access control (security-alert equipment, locks, metal grilles and other applicable methods), creation of a suitable working environment, incl. by maintaining a proper temperature as well as a suitable fire-extinguishing system. They aim to provide an environment for normal operation, to protect IT equipment from unauthorized access and to control the risk of damage and destruction.

Art. 25. (1) Measures related to *cryptographic data protection* through standard cryptographic capabilities of operating systems, database management systems and communication equipment shall also be applied to personal data.

VII. BASIC RULES AND MEASURES FOR PROVIDING THE PROTECTION OF PERSONAL DATA IN COMPUTER PROCESSING

 NIS БУДУЋНОСТ <small>GAZPROM NEFT</small> НА ДЕЛУ			
NIS PETROL EOOD		Version 2.0	
ECONOMIC SECURITY DEPARTMENT			
PERSONAL DATA PROTECTION POLICY		Regulation 2016/679	20.02.2020

Art. 26. (1) Computer access through the local network to files containing personal data shall be exercised only by officials with regulated rights, only from their physical workplace, by a specially designated computer for this purpose and after identification by a name and password to the system. At closing hours, employees shut down or lock their local computer.

(2) NIS PETROL applies adequate technical and administrative control measures (IP restriction, MAC address, physical location, unique username and password, setting of all workstations in “the automatic screen lock” mode in the absence of activity, such as this ensures that only authorized personnel have access to the data for the performance of their assigned functions.

(3) The identification of the authorized persons for the use of personal data must also include identification through a unique user account, which contains the user name and password, access rights to the system and use of its resources.

(4) The user account shall be locked after three unsuccessful attempts to register in the system, and its unlocking can be done only by the system administrator.

(5) In order to improve the security of access to information, employees must change their passwords used for a period determined by NIS PETROL, not exceeding 3 months. In the event that the grounds for access to personal data are terminated, the rights of the respective persons shall be terminated (including by deleting the account).

(6) Systems processing and / or storing personal data include a control system that records the following actions in an audit report (log): attempts to log in and effectively log in, log out, user actions in each work session, change passwords. When an atypical activity is detected (for example entering an atypical time, shutting down / unlocking a workstation after work hours, etc.), the system administrator shall immediately notify the economic security Management and the Data Protection Officer of a verification check of the case.

Art. 27. (1) The hardware used for storage and processing of personal data meets the modern requirements and allows to guarantee a reasonable degree of fault tolerance, possibilities for backing up and restoration of the data and the working condition of the environment.

(2) In case of need for repair of the computer equipment, its provision to the service organization shall be carried out without the devices on which personal data is stored.


Art. 28. (1) Only software with regulated copyright is used in NIS PETROL. The installation and / or use of any other type of copyrighted software is prohibited.

(2) Only the software installed by the system administrator is used on the office computers. It is forbidden to unintentionally install any other type of software.

(3) When introducing a new software product for processing of personal data, the capabilities of the product shall be tested and verified in order to comply with the requirements of Regulation 2016/679, the Law on Protection of Personal Data and to ensure the maximum protection of data from unauthorized access, loss, corruption or destruction.

Art. 29. Employees assigned to sign correspondence with a Qualified Electronic Signature (QES) shall not be entitled to provide this QES to third parties, respectively to share their PIN with third parties.

VIII. SUPPORTED REGISTERS WITH PERSONAL DATA AND THEIR MANAGEMENT

 NIS БУДУЋНОСТ <small>GAZPROM NEFT</small> НА ДЕЛУ NIS PETROL FOOD	Version 2.0	
ECONOMIC SECURITY DEPARTMENT		
PERSONAL DATA PROTECTION POLICY	Regulation 2016/679	20.02.2020

Art. 30. (1) Each department working with personal data shall maintain the register of personal data. The Data Protection Officer maintains a common register, which lists all the local registers.

(2) Registers maintained by NIS Petrol:

1. *"Economic Security" Register;*
2. *"Legal" Register;*
3. *"Development and Construction" Register;*
4. *"Wholesale Trade" Register;*
5. *"Logistics" Register;*
6. *"Retail Trade" Register;*
7. *"Finance" Register;*
8. *"Personnel" Register;*
9. *"Orders" Register;*
10. *"Information Technology" Register;*
11. *"Labor and Environmental Safety" Register;*

(3) The data in the registers under para. (1) shall be maintained in accordance with the legal basis for processing.


Art. 31. For processing the data from the registers of Art. 30, NIS PETROL keeps a register of processing activities.

IX. RIGHTS AND OBLIGATIONS OF PROCESSORS

Art. 32. (1) The Data Protection Officer shall be appointed by the company Manager.

(2) The Data Protection Officer shall have the following powers and duties:

1. Ensures compliance with the specific measures for protection and control of access according to the specifics of the kept registers with personal data;
2. Exercise control over compliance with the requirements for the protection of the registers in accordance with the current legislation and this Personal Data Protection Policy;
3. Liaises with the Commission for Personal Data Protection on the measures taken and the means of protection of the registers and the applications for providing personal data;
4. Conducts periodic monitoring of compliance with data protection requirements and, in case of detected irregularities, takes measures for their elimination;
5. Keeps a register of personal data processing activities at NIS PETROL.

 NIS БУДУЩНОСТ <small>GAZPROM NEFT</small> НА ДЕЛУ NIS PETROL EOOD	Version 2.0	
ECONOMIC SECURITY DEPARTMENT		
PERSONAL DATA PROTECTION POLICY	Regulation 2016/679	20.02.2020

Art. 33. The employees of NIS PETROL are obliged to:

1. All employees of NIS PETROL are obliged to familiarize themselves with this Personal Data Protection Policy and to observe it on a daily basis in the performance of their duties related to the respective position and their assigned work.
2. To process personal data lawfully and in good faith;
3. To use the personal data they have access to for the purposes for which it is collected and not further process it in a manner incompatible with those purposes;
4. To update the registers of personal data as necessary;
5. Erasing or rectifying personal data when found to be inaccurate or disproportionate to the purposes for which it is processed;
6. Keep personal data in a form that allows identification of the individuals concerned for a period no longer than is necessary for the purposes for which the data are processed, respectively. no longer than legally defined.

Art. 34. (1) Employees shall bear disciplinary responsibility for non-compliance with the provisions of this Personal Data Protection Policy.

(2) If, as a result of the actions of a relevant personal data processing officer, damages have occurred to NIS PETROL or to a third party, the latter may be liable under the general civil legislation.

X. ADDITIONAL PROVISIONS

Art. 35. (1) For all issues not covered by this Personal Data Protection Policy, the provisions of the General Data Protection Regulation (EU) 2016/679, the applicable European Union law and the legislation of the Republic of Bulgaria on personal data protection shall apply.

(2) The template documents prepared during and in relation with the processing of personal data are listed in the package of procedures for protection of personal data of NIS PETROL.