PATVIRTINTA
Akcinės bendrovės „Klaipėdos nafta“
Teisės ir administravimo direktorius
Rytis Valūnas
2021-08-02

PERSONAL DATA PRIVACY POLICY

NO POL013

VERSION 2

ASMENS DUOMENŲ PRIVATUMO POLITIKA

CONTENTS

1. SCOPE

1.1. This Personal Data Privacy Policy ('the *Policy*') contains information about the processing of personal data carried out by Stock Company 'Klaipėdos nafta' ('the *Company*'). Information about how to exercise the rights of the data subject as well as contact details of the *Company* are provided at the end of this document.

2. DEFINITIONS AND ABBREVIATIONS

2.1. The following definitions and abbreviations are used in this *Policy*:

Person ('the ***Data Subject'***) means a person (natural person) whose data is processed.

Personal Data ('the ***Data'***) means any information on the identified or identifiable *Data Subject*.

General Data Protection Regulation ('the *GDPR*') means 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 or Regulation (EU) 2016/679).

Processor means a natural or legal person which processes *Data* on behalf of and as instructed by the *Controller*.

Controller means a natural or legal person, which determines the purposes and means of the processing of *Data* concerning the *Data Subject*. The Controller is Stock Company 'Klaipėdos nafta' with a seat at Burių g. 19, LT-92219 Klaipėda, tel.: 8 46 391772, e-mail: info@kn.lt.

Other Processor means a third party engaged by the *Processor* to follow the instructions of the *Processor* and to process *Data* on behalf of the *Controller*.

Supervisory Authority means State Data Protection Inspectorate, which has the powers of a supervisory authority established by the *GDPR*.

Applicable Data Protection Laws mean any national or international data protection laws or legal acts applicable to the *Controller* or the *Processor*, as the case may be. Applicable Data Protection Laws include the EU General Data Protection Regulation 2016/679.

Processing means any operation or set of operations, which is performed on *Data* or on sets of *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, restriction, erasure or destruction.

Records of Activities mean records of *Data* processing activities that contain a detailed description of the *Data* processing carried out and the handling whereof is delegated to the *Controllers* and *Processors* and, where applicable, their representatives according to Article 30 of the GDPR.

2.2. Any other definitions used in this *Policy* shall correspond to those used in the *Applicable Data Protection Laws*.

3. PRINCIPLES RELATING TO PROCESSING OF DATA

3.1. The *Company* processes *Data* in accordance with the following principles:

3.1.1. lawfulness, fairness and transparency – the *Data* is processed in a lawful, transparent and fair manner in respect of a person whose data is processed;

3.1.2. purpose limitation – the *Data* is processed for the specific purposes and these purposes are indicated by the *Company* to the persons whose *Data* is collected. The *Company* does not collect *Data* for any undefined purposes;

3.1.3. data minimisation – the *Company* collects and processes only the *Data* that is necessary in relation to the purposes for which it is processed;

3.1.4. accuracy – the *Company* ensures that *Data* is accurate, kept up to date in view of the purposes for which it is processed, and rectified, where necessary;

3.1.5. storage limitation – the *Company* ensures that *Data* is stored for no longer than is necessary for the purposes for which it is processed;

3.1.6. integrity and confidentiality – technical or organisational protection measures are applied in the *Company* through the use of appropriate technologies to ensure the security of *Data*, including the protection against unauthorised or unlawful processing of *Data* and against accidental loss, destruction of or damage to the *Data*;

3.1.7. accountability – the *Company* shall be responsible for the compliance with the principles specified in clauses 3.1.1-3.1.6 in the processing of *Data* and shall not use *Data* for any purposes incompatible with the primary purpose.

4. RIGHTS OF DATA SUBJECTS AND IMPLEMENTATION OF SUCH RIGHTS

4.1. In the *Company*, the *Data* is processed in compliance with and by ensuring the following individual rights of *Data Subjects* (save for the cases where the exception of the *Law on Data Protection* is applied):

4.1.1. a right to know and to obtain communication with regard to the processing of *Data* concerning the *Data Subject*;

4.1.2. a right of access to processed *Data*;

4.1.3. a right to request rectification of imprecise or to supplement incomplete *Data*;

4.1.4. a right to request erasure of *Data* concerning the *Data Subject*;

4.1.5. a right to request restriction of processing of *Data*;

4.1.6. a right to *Data* portability;

4.1.7. a right to object to the processing of *Data*;

4.1.8. a right not to be subject to automated evaluation and profiling;

4.1.9. a right to file a complaint with the State Data Protection Inspectorate.

Requests of the *Data Subject*

4.2. The rights of *Data Subjects* shall be ensured free of charge. Where requests from a *Data Subject* are manifestly unfounded or excessive, in particular because of their repetitive character, the *Company* shall have a right to charge a reasonable fee considering the administrative costs of providing the information or communication and/or taking the action requested or to refuse, giving the reasons, to act on the request of the *Data Subject*.

4.3. The *Data Subjects* may submit their requests to the *Controller* regarding the implementation of any right of the *Data Subject* in several ways – directly to the Company, by post or by means of electronic communications. By filing their requests, the *Data Subjects* must confirm their identity in the following manner: 1) if a request is delivered directly to the *Company's* employee, he/she shall present a proof of identity; 2) if a request is delivered by post, he/she shall also present a copy of a personal ID document certified in accordance with other procedure established by the laws; 3)

in case of use of means of electronic communications, he/she shall sign with a qualified electronic signature or tprepare it by using electronic means allowing to ensure the integrity and inalterability of text.

4.4. Having received a request of the *Data Subject*, the *Company* shall without any undue delay, but in any case no later than within 1 (one) month from the day of receipt of request and identification of person, inform the *Data Subject* on the actions that were taken according to the request submitted by the *Data Subject*. In view of the complexity and the number of requests, the *Company* shall have a right to extent a period of 1 month for another 2 months having informed the *Data Subject* hereof before the end of the first month and having specified the reasons for such extension.

4.5. If the request of the *Data Subject* is submitted by means of electronic communications, the *Company* shall also submit a reply by means of electronic communication, except for cases when it is impossible or when the *Data Subject* specifies a different method for submission.

4.6. In case of any circumstances provided for in the *Applicable Data Protection Laws* and any other legal acts, the *Company* may refuse, by giving the reasons, to act on the request of the *Data Subject* having informed the *Data Subject* hereof in writing.

4.7. If the *Data Subject* feels that the *Personal Data* concerning him/her is (was) processed unlawfully or his/her rights are/were breached in the *Company*, he/she shall have a right to file a complaint with a supervisory authority, i. e. the State Data Protection Inspectorate in the Republic of Lithuania (A. Juozapavičiaus g. 6, 09310 Vilnius; tel.: (8 5) 271 2804, 279 1445; e-mail: ada@ada.lt) regarding the *Company's* actions (inaction) within 3 months from the day of receipt of *Company's* reply or within 3 months from the final day of deadline for the submission of reply.

Information of *Data Subject* about the processing of *Data*

4.8. In any case, the *Company* shall present the *Data Subject* with the following information (save for the cases where the *Data Subject* has already been informed):

4.8.1. name, legal person's number and seat;

4.8.2. contact details of a data protection officer (if any) or an employee in charge of data protection;

4.8.3. the purposes of and legal grounds for processing of *Data* concerning the *Data Subject*;

4.8.4. recipients or categories of recipients of *Data*;

4.8.5. period for which the *Data* will be stored and criteria used to determine that period;

4.8.6. any additional information inasmuch it is necessary to ensure fair processing of *Data* without prejudice to the rights of *Data Subject*;

4.8.7. on the transfer of his/her *Data* to third persons no later than before the moment when *Data* is transferred for the first time and, if the *Data Subject* has not been aware of the fact that *Data* will be transferred to the other party.

4.9. Information about the processing of *Data* concerning the *Data Subject* in the *Company* specified in Articles 13 and 14 of the *GDPR* is made available on:

4.9.1. website www.kn.lt;

4.9.2. informational tables about the video surveillance of the *Company's* territory or premises;

4.9.3. at the time of communication with the *Data Subject* in the same manner as he/she applied to the *Company*.

4.10. The *Data Subject* shall have a right to receive *Company's* confirmation, if the *Company* processes *Data* concerning the *Data Subject* as well as the right of access to the *Data* concerning the *Data Subject* processed in the *Company* and information on the purposes of *Processing*, categories of *Data* being processed, categories of *Data* recipients, period of *Processing*, sources of receipt of *Data*, if such information was not submitted to the *Data Subject* or is insufficient for the *Data Subject*.

4.11. In cases where the *Company* processes *Data* on the basis of consent, the *Data Subject* shall have a right to withdraw his/her consent at any time and the processing of *Data* based on a consent shall be terminated, if there are no other legal grounds for processing. In order to withdraw his/her consent, the *Data Subject* must apply to the *Company* in writing by submitting a withdrawal of a specific consent at Burių g. 19, Klaipėda or, in case of signing with a qualified electronic signature, by e-mail ***info@kn.lt***.

5. DATA PROCESSING ACTIVITIES

Collection of *Data* and categories of *Data Subjects*

5.1. *Data* is collected directly from the *Data Subject*, is received from external *Data* sources, such as private and public registers, other database administrators, as well as *Data* recipients specified in the *Records of Activities*. The *Company* shall have a right to record phone conversations, to make video and/or audio recordings, store e-mail correspondence or otherwise document the relations and communication with clients, partners, *Data Recipients*, *Data Subjects*, etc.

5.2. The *Company* collects *Data* about natural persons who concluded agreements with the *Company* or when the processing of such *Data* is necessary for the performance of contracts with other legal persons (e. g. persons signing the documents or representatives of legal person, natural persons whose *Data* is processed during the assessment of legal person's credibility, representatives of legal person having access to the *Company's* informational resources, etc.), candidates to employees, shareholders and other stakeholders of legal persons, contact persons of a customer (legal person), members of management board, sole bodies or other collegial bodies, beneficiaries, visitors of *Company's* terminals, as well as other *Data Subjects* whose *Data* has to be collected in order to ensure the defending of *Company's* legal interests and performance of the requirements of legal acts.

Categories of *Data*

5.3. The *Company* collects and processes *Data* of the following categories:

5.3.1. personal identification and contact data – first name, last name, personal ID number, date of birth, data of personal identification document, actual and declared place of residence, telephone number, e-mail, nationality;

5.3.2. financial data – data about the accounts and property owned. This data is collected in case of assessment of *Data Subject's* credibility or in order to ensure the compliance with the laws as well as in case of application of any measures regarding the coordination of *Company's* and private interests;

5.3.3. *Data* obtained and/or created in order to comply with the requirements of legal acts – *Data* that is obtained according to the enquiries of law-enforcement authorities, courts and bailiffs, in performance of briefings stipulated by the occupational health and safety laws;

5.3.4. *Data* collected by using communication and other technical measures – *Data* collected when the *Data Subjects* arrive to the *Company's* terminals and other units by using computer network infrastructure, *Company's* assets and by visiting *Company's* website;

5.3.5. special categories of *Data* – *Data* related to the health and/or legal misconduct of the *Data Subject*. In certain cases, in order to provide healthcare services, to ensure prevention of accidents at work and investigation of accidents or otherwise ensure the compliance with the requirements of legal acts in the *Company*, the *Company* must process special categories of *Data*;

5.3.6. *Data* about closely related persons – Information about the family members of *Data Subject* and other related persons as specified by the Law on Prevention of Corruption of the Republic of Lithuania and any implementing regulations or to the extent it is necessary to notify about the cases of accidents at work;

5.3.7. *Data* related to the profession and qualification – *Data* concerning the education and occupational activities.

Storage period

5.4. *Data* shall be stored for the periods listed below according to the types of *Data*, whereas specific storage periods are stipulated in the *Records of Processing Activities*.

Item No	Purposes of *Processing*	Storage period
1.	Selection of candidates to employees	Up to 2 years after the end of candidate selection process.
2.	Ensuring of the security of *Company's* business and prevention of fraud	Up to 30 calendar days from the expiry of employment contract taking into account public and private interests. Until the end of selection process in case of evaluation of candidates to employees. Up to 1 year in case of assessment of credibility of legal persons. Up to 1 year after the final judgement is passed following the investigation of a possible corruptive activity.
3.	Performance of employment contracts, collective agreements and related activities	Up to 50 years after the termination of employment contract according to the Index of Periods for Storage of Documents of General Nature.
4.	Calculation of wages, premiums, bonuses, benefits, gifts and other pay-outs, transfers, data transfers to public authorities	Up to 50 years after the termination of employment contract and up to 10 years after the expiry of other contracts according to the Index of Periods for Storage of Documents of General Nature.
5.	Bookkeeping (other than related to labour relations)	Up to 10 years according to the Index of Periods for Storage of Documents of General Nature.

Item No	Purposes of *Processing*	Storage period
6.	Video surveillance and video surveillance with sound in order to ensure the safety of persons and protection of property and technological processes.	Up to 60 calendar days from the moment of recording.
7.	Control of access to the territory and premises to ensure the protection of persons and property	Up to 1 year from the moment of capture and up to 10 years in case of data processed in other organisational documents according to the Index of Periods for Storage of Documents of General Nature.
8.	Management and administration of infrastructure and assets	Up to 3 years according to the Index of Periods for Storage of Documents of General Nature.
9.	Ensuring of cyber security and protection of confidential information	Up to 6 months in case of data recorded by cyber security controls and up to 10 years in case of data processed in other organisational documents according to the Index of Periods for Storage of Documents of General Nature.
10.	Recording of landline telephone and radio communication conversations to ensure the safety of activities at the terminals and investigation of incidents	Up to 30 calendar days from the moment of recording.
11.	Administration of services provided and activities performed by the *Company* and administration of *Company's* compliance with the requirements of laws and operational standards	Up to 10 years according to the Index of Periods for Storage of Documents of General Nature.
12.	Organisation and performance of public procurement procedures	Up to 10 years after the expiry of contracts according to the Index of Periods for Storage of Documents of General Nature.
13.	Administration of *Company's* operational documents	Up to 10 years according to the Index of Periods for Storage of Documents of General Nature.
14.	Implementation of civil, occupational, fire-safety and health requirements, investigation and prevention of incidents	Up to 75 years from the investigation of accident at work and up to 10 years in case of data processed in other organisational documents according to the Index of Periods for Storage of Documents of General Nature.
15.	Performance of internal and external communication, enhancement of work culture	Until the withdrawal of consent or up to 10 years after the expiry of contracts according to the Index of Periods for Storage of Documents of General Nature.

Item No	Purposes of *Processing*	Storage period
		Up to 26 months in case of data of website visitors.
16.	Sale of terminal services and customer services, maintaining of relations with customers, dispute settlement and filing as well as examination of claims.	Up to 10 years after the expiry of contracts according to the Index of Periods for Storage of Documents of General Nature.
17.	Purchase of goods and/or services (works) and sale of assets that are no longer necessary for the activities as well as the sale of services	Up to 10 years after the expiry of contracts according to the Index of Periods for Storage of Documents of General Nature.
18.	Legal proceedings, preparation of legal documents	Up to 10 years according to the Index of Periods for Storage of Documents of General Nature.
19.	Ensuring of safe and healthy environment for the employees in case of any outbreak of contagious diseases, when an extreme situation or quarantine is declared on the national scale.	21 calendar days in case of management of outbreaks of diseases. Data is not collected in case of implementation of preventive measures.
20.	Management and administration of information resources, infrastructure and other property for the accounting of shared vehicles	Up to 30 calendar days.

5.5. The *Controller* applies different *Data* storage periods subject to the purpose of processing of specific *Data* when indication of such period for storage and/or erasure is possible.

5.6. Exceptions to the periods for storage specified in this *Policy* are set in the *Records of Activities* provided that such deviations do not breach the rights of *Data Subjects*, comply with the legal requirements, and are appropriately documented in *Company's Records of Activities*.

5.7. *Data* can also be stored for a period longer than specified in order to file, enforce and defend legal claims or *Company's* legal interest, as well as in enforcement of the Applicable Data Protection Laws, provided, however, that this does not breach the rights of *Data Subjects*, complies with the legal requirements and the storage is appropriately documented.

Destruction of *Data*

5.8. Upon the expiry of *Data* storage period or disappearance of the legal ground for storage of *Data*, such *Data* shall be destroyed immediately.

5.9. *Data* stored in an electronic form shall be destroyed by erasure without a possibility of retrieval.

5.10. Paper documents that contain *Data* shall be shredded and the residues shall be utilised in a safe manner.

Profiling and automated decision-making

5.11. The Company does not perform profiling of personal data concerning the *Data subjects* based on which automated decisions could be made that could cause legal consequences to or have a considerable effect on the *Data Subjects*.

***Data* protection officer**

5.12. Pursuant to the *Applicable Data Protection Laws,* the *Company* is not obliged to appoint a data protection officer.

5.13. By the order of *Company's* chief executive officer, an employee in charge of data protection has been appointed.

***Data* protection impact assessment**

5.14. As specified by the *Applicable Data Protection Laws*, in cases where *Data* processing operations are likely to result in a high risk to the rights and freedoms of the *Data Subject*, the employees or units of the *Company* appointed to oversee these data protection operations specified in the *Records of Activities* carry out data protection impact assessment.

5.15. By initiating new activity processes or by changing the current ones due to a potentially great influence of the processes of such activity that involves (is likely to involve) the processing of *Data* on the rights and freedoms of *Data Subjects* the employees carry out prior consultations with a person in charge of *Data* protection in the *Company*.

5.16. The persons appointed to oversee *Data* protection and coordinating the data protection impact assessment to be carried out shall, where necessary, consult with the *Supervisory Authority* in accordance with the procedure set by the *Applicable Data Protection Laws*.

Records of *Processing* activities

5.17. According to the procedure set by the *Applicable Data Protection Laws,* the *Records of Activities* are maintained in the *Company*.

5.18. The *Records of Activities* specify the contact details of *Company's* representative related to the data protection and the following information:

5.18.1. purposes of *Processing*;

5.18.2. categories of *Data Subjects*;

5.18.3. description of *Data* categories;

5.18.4. categories of the recipients of disclosed *Data* or *Data* to be disclosed ;

5.18.5. information about the *Data* transfer to a third country or international organisation;

5.18.6. *Data* erasure time-limits or criteria for their determination;

5.18.7. description of technical and organisational measures for the protection of *Data*.

5.19. The *Records of Activities* are processed on an accrual basis to ensure the traceability of any changes made in such records.

5.20. Processing of *Data* for the purposes other than those specified in the *Records of Activities* shall be prohibited.

6. LEGAL GROUNDS FOR AND PURPOSES OF PROCESSING

Consent

6.1. In certain cases, the *Company* requests a consent of *Data Subjects* for the processing of their *Data*. Such request includes information about the *Processing* activities for which the consent is required. The *Company* processes *Data* concerning the *Data Subjects* at the time of candidacy to the position of employee, when making a decision on the allocation of support, organisation of excursions to the *Company's* terminals at the request of *Data Subject*, through external and internal communication, including publication of the image of *Data Subject*, or by selling services through

direct marketing, as well as by rendering services of preventive medicine at the *Company's* medical unit.

6.2. The *Data Subject* can withdraw his/her consent at any time and shall also be informed about the consequences of such withdrawal.

Performance of contract

6.3. The main purpose of *Processing* carried out by the *Company* is to conclude, perform and administer contracts with employees and other *Data Subjects*. Such *Processing* includes the *Processing* for the following purposes:

6.3.1. conclusion and performance of employment, collective and internship contracts, provision of work tools;

6.3.2. selection of a candidate in order to conclude an employment contract;

6.3.3. administration of the work of members of control and supervisory bodies;

6.3.4. calculation of wages, premiums, bonuses, benefits, gifts and other pay-outs, transfers, data transfers to public authorities as well as bookkeeping (other than related to employment relations);

6.3.5. internal and external communication with employees, customers and partners about the services rendered by the *Company* or events where the *Data Subjects* participate in such projects.

Compliance with a legal obligation

6.4. In order to ensure the compliance with legal obligations applied to the *Company*, the *Company* must process *Data* according to the requirements of the applicable laws. Such *Processing* includes the following objectives:

6.4.1. to observe the requirements of laws and other legal acts related to bookkeeping, provision of information to national authorities;

6.4.2. to ensure the performance of requirements of safe and healthy working environment, occupational healthcare and control of emergency situations at the terminals;

6.4.3. to control, in a proper manner, the safety of property located at the terminals operated by the *Company* and persons working at or visiting them;

6.4.4. to realise the requirements of the legal acts to allow the *Data Subject* to exercise the special rights in the fields of occupational and social security law;

6.4.5. to adequately perform the requirements of the applicable public procurement laws;

6.4.6. to ensure and implement the requirements of the laws related to cyber security and information protection;

6.4.7. to perform the requirements of any other laws that are applicable to the activities performed as well as the court letters and bailiff arrangements.

Protection of the vital interests of *Data Subject* or any other natural person

6.5. Where an extreme situation or a quarantine is declared on the national scale, to ensure a safe and healthy working environment for the employees at the time of the outbreak of contagious diseases, the *Company* can process personal data on the basis of protection of vital interests of *Data Subject* and any other natural person by implementing the measures for the prevention of such outbreaks.

6.6. On this basis, personal data may be processed in the *Company* when first aid is provided in the medical unit, when the *Data Subject* is unable to give his/her consent due to physical or legal reasons.

Legitimate interest

6.7. The *Company* processes *Data* concerning the *Data Subjects* seeking for a legitimate interest. Such *Processing* is necessary when the *Company's* legitimate interest, in the view of the *Company*, overrides the interest of the *Data Subject* that is related to his/her right to privacy. Such *Processing* includes the following purposes:

6.7.1. to defend the legitimate interests of *Company's* customers, the *Company* itself and/or *Company's* employees, by implementing the necessary security measures, carrying out the assessments of credibility and good repute;

6.7.2. to carry out prevention of corruption, fraud and abuse of position;

6.7.3. to maintain relations with customers;

6.7.4. to ensure adequate management and administration of *Company's* infrastructure, property and information resources;

6.7.5. to sell the services provided by terminals controlled by the *Company* and ensure customer service, to maintain relations with customers, to settle disputes and to examine any claims filed;

6.7.6. to purchase goods and/or services (works) and to sell property that is no longer necessary for the performance of activities including the sale of services;

6.7.7. to prevent disturbances of *Company's* activities or to investigate the unlawful use of *Company's* resources;

6.7.8. to carry out the assessment of credibility of candidates to employees, assessment of legal person's credibility (where *Data* of legal person's representatives, natural persons is provided);

6.7.9. to ensure high-quality provision of *Company's* services, protection of information related to the provision of services to the customer, as well as to improve, develop and maintain software, technical and IT systems;

6.7.10. to adequately administer operational documents (designing and technical documentation, correspondence, internal audit reports, etc.);

6.7.11. to ensure customer service in performance of logistics, loading and regasification operations and product quality assessments;

6.7.12. to file, enforce and defend legal claims, to reply to and to examine any claims filed or to participate in the settlement of disputes;

6.7.13. to adequately carry out investigations of incidents at the terminals or to submit material to the law-enforcement and other national authorities in charge of investigation of such incidents;

6.7.14. to represent the *Company* in public.

7. COOKIES

7.1. While the *Data Subject* browses the *Company's* website, the *Company* uses cookies. The list of all cookies used is provided in the *Company's* Website Privacy Policy available at https://www.kn.lt/en/privacy-policy/2527.

8. SELECTION OF CANDIDATES TO EMPLOYEES

8.1. When *Data Subject* participates in the selection to vacant positions organised by the *Company*, the *Company* processes *Data* according to the Personal Data Privacy Policy for Candidate's to Employees available at https://www.kn.lt/uploads/files/dir96/dir4/8_0.php (only in Lithuanian).

9. VIDEO SURVEILLANCE

9.1. Video surveillance performed in the *Company's* territory is one of the measures to ensure the safety of property, persons and technological processes.

9.2. The following objects of the *Company* are under video surveillance:

9.2.1. territory of Klaipėdaoil terminal;

9.2.2. territory of Subačius oil terminal;

9.2.3. *Company's* administration premises in Klaipėda, Vilnius and Subačius;

9.2.4. territory of gas metering station;

9.2.5. LNG terminal jetty;

9.2.6. territory of valves stations.

9.2.7. When the *Company* performs video surveillance, the processed *Data* includes the image and video recording of the *Data Subject* when the *Data Subject* is present in the territories listed in Item 8.2, including the inside of the premises.

9.3. The *Company* can perform video surveillance with sound in the premises where the industrial processes are controlled. Processing of personal data for this purpose is performed on the basis of the legitimate interest of the *Company* which is based on the seek to defend the interest of *Company's* employees in performance of investigations of any incidents at the terminals in case of extreme situation.

9.4. Video recorders installed in the vehicles of *Company's* security and fire-safety units are used for making video recordings with sound based on the legitimate interest of the *Company* to ensure adequate investigation of incidents (car accidents or extreme situations at the terminals) in order to defend the employees driving *Company's* vehicles and to ensure a proper submission of evidence to the law-enforcement authorities.

9.5. Video surveillance performed by the *Company* is based on the legal obligation to ensure the security of property, persons and technical processes of the *Company* being of strategic importance to the national security of the Republic of Lithuania.

9.6. Information of video and/or audio recordings may be submitted to the law-enforcement or other controlling authorities in any cases when it becomes necessary for the investigation of criminal activities, events, or breaches, and it is also accessible to the employees in charge of technical maintenance of video surveillance equipment and to the organisation that is in charge of security functions and processes *Data* on behalf of the *Company*.

10. DATA RECIPIENTS AND OTHER PROCESSORS

10.1. The *Company* engages *Other Processors* for the processing of *Data* and takes all the necessary measures for *Other Processors* to process *Data* according to the instructions laid down in the *Company's* documents, by observing the necessary and sufficient security measures and requirements of the *Applicable Data Protection Laws*.

10.2. *Processing* performed by *Other Processors* is regulated by signing a data processing agreement.

10.3. Data processing agreements are prepared before the planned start of *Processing* operations.

10.4. The *Company* can transfer the *Data* being processed to state authorities that investigate criminal activities and incidents (the Police, State Labour Inspectorate, etc.), other state authorities in cases

stipulated by the laws (State Tax Inspectorate, SODRA, etc.), as well as institutions and companies in charge of C*ompany's* external audits.

11. ENSURING OF DATA SECURITY AND CONFIDENTIALITY

11.1. When storing *Data*, the *Company* undertakes to implement and ensure adequate organisational and technical measures that are necessary to protect *Data* against accidental or unlawful destruction, alteration and disclosure as well as against any other unlawful processing, i.e.:

11.1.1. information that constitutes *Data* is included in the *List of Confidential Information*;

11.1.2. users of information systems are identified on the basis of a unique identifier not bound with data;

11.1.3. *Data* is stored in encrypted electronic databases and encrypted computerised information mediums;

11.1.4. protection and control software is used in computerised places of works, service stations and mobile devices;

11.1.5. remote connection to *Company's* data networks and information systems is encrypted by using reliable VPN protocols;

11.1.6. unified computer network protection system is used for the safety of internal data network against any threats arising in public data networks;

11.1.7. automated cyber security controls are used to monitor security events and traffic on internal network, automated and timely software updates and vulnerability management;

11.1.8. electronic information and data (data contained servers, workstations and notebooks) is constantly backed up and archived;

11.1.9. Information and Cyber Security Incidents Management Procedure is used in the *Company* to identify, evaluate, stop, and rectify data breaches. Data incidents management is carried out by Computer Incident Response Team (CIRT). A proper control of breaches of data protection and a timely response to these breaches is the responsibility of an employee assigned to be in charge of data protection;

11.1.10. *Data*, information and cyber security is regulated by the *Company's* Information and Cyber Security Policy and its guidelines as well as any other internal legislation related to this policy;

11.1.11. *Company's* employees and third parties are regularly educated on the matters of information, data protection and cyber security awareness.

11.2. The *Company* shall ensure the security of premises wherein the *Data* is stored, a proper layout and maintenance of hardware, observance of the fire safety regulations, proper administration of data network infrastructure, maintenance of information systems and implementation of any other technical controls that are necessary to ensure the protection of *Data*.

11.3. The rights and obligations of *Company's* employees in receiving, using, providing, and storing information that constitutes *Data* and ensuring that this information is not disclosed to any persons not authorised to know it are regulated by the *Information Classification and Control Guidelines*.

11.4. The right to process *Data* is granted only to those Company's employees who need such information to perform their functions or to hold positions and only to a specific extent and when it is necessary for the achievement of specific objectives, under one of the grounds of legitimate processing.

11.5. The rights of access to *Data* and mandate to process *Data* are given, withdrawn and modified pursuant to the *Procedure for Control of Access to Information Resources*.

11.6. Mandate to process *Data* is set in the employee's job description or granted with other documents regulating the *Company's* activity.

11.7. Without being any need, the files with *Data* shall not be digitally multiplied, i.e., no copies of files shall be created on local computer disks, portable mediums, remote file storage containers, etc.

11.8. The *Company* ensures the use of secure protocols and/or passwords when transmitting *Data* via external data transmission networks.

11.9. The security control of *Data* contained in external data storage mediums and e-mail and erasure thereof after use is ensured by transferring it to the databases.

11.10. The employees organise their work by restricting, as far as practicable, the possibility for other persons to get access to the *Data* being processed. This provision is implemented as follows:

11.10.1. by making sure not to leave any documents with *Data* being processed or a computer that can be used to open files with *Data* unattended so that the information contained therein could be not read by employees not authorised to work with specific *Data*, trainees or other persons;

11.10.2. by keeping documents in such a way as to prevent them (or their fragments) to be read by occasional persons;

11.10.3. if the documents containing *Data* are transferred to other employees, units, institutions through persons that are not authorised to process *Data* or by post or courier service, they shall be transferred in a sealed non-transparent envelope. This item does not apply if the aforementioned notices are delivered personally and confidentially.

11.11. The employees shall transfer documents that contain *Data* only to those employees who are authorised to work with *Data* on the basis of the positions they hold or under any individual delegations.

11.12. A confidentiality agreement shall be signed with all employees and trainees.

11.13. A non-disclosure agreement shall be signed with other legal or natural persons.

12. GEOGRAPHICAL SCOPE OF PROCESSING

12.1. The *Company* processes *Data* within the EU/EEA.

12.2. *Data* may be transferred and processed outside the EU/EEA when a legal ground for such data transfer exists and if adequate protection measures are used:

12.2.1. an agreement is concluded and covers all the standard terms and conditions approved by the European Commission or the transfer is performed according to any other terms and conditions applicable, such as codes of conduct, certificates, etc., which are approved by the *Applicable Data Protection Laws*;

12.2.2. the country that is not part of the EU/EEA and where the Data Recipient is based shall ensure a sufficient level of data protection by the decision of the European Commission;

12.2.3. when applied appropriate safeguards listed in Article 46 of the GDPR;

12.2.4. when appropriate derogations are used from the specific cases referred to listed in Article 49 of GDPR.

13. CONTACT DETAILS

13.1. The *Data Subject* shall apply to the *Company* in writing in order to exercise his/her rights by sending the application to Burių g. 19, Klaipėda or, if signed by a qualified electronic signature, by e-mail: ***info@kn.lt***.

13.2. In case of questions, problems, with recommendations, requests related to ensuring the protection of personal data, please contact the Data Protection Officer appointed by the *KN*:

13.2.1. e-mail: ***dap@juridicon.lt***,

13.2.2. tel.: ***+370 616 02 000***

13.2.3. by sending a letter to the address: ***UAB "Juridicon", Totoriu st. 5-7, 01121 Vilnius.***

14. AMENDMENTS AND THE VERSION OF POLICY CURRENTLY IN FORCE

14.1. This *Policy* shall be reviewed at least once a year or in each case of breach of *Data* protection or any changes made in the *Applicable Data Protection Laws*, and shall be supplemented and updated, where necessary.

14.2. *Data protection Officer* shall, at least once a year, initiate an internal inspection in order to find out if the provisions of this Policy are adequately implemented in practice and shall prepare and submit to the *Company's* chief executive officer any suggestions regarding the need to amend this *Policy*.

14.3. The assessment of *Data* protection risks shall be carried out at least once a year by preparing the assessment report and, where necessary, by stipulating the measures for the elimination or reductions of the risk. Risk assessment can be carried out together with the overall Information and Cyber Security Risk Assessment.