RULES
OF PERSONAL DATA PROCESSING OF UAB "TUTUTIS"

I. CONCEPTS

1. The main concepts used in the Rules of Personal Data Processing (hereinafter – Rules) shall be the following:

1.1. **LLPPD** means Law on Legal Protection of Personal Data of the Republic of Lithuania.

1.2. **Personal data** means any information relating to an identified or identifiable natural person;

1.3. **Data recipient** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not;

1.4. **Data subject** means a natural person 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;

1.5. **Data processing** 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;

1.6. **Data processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

1.7. **Data controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

1.8. **Profiling** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

1.9. **Regulation** means Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016.

1.10. **Sub-processor** means other external data processor assigned by the data processor for processing of personal data in the name of data controller, while implementing the assigned functions of service provision;

1.11. **Data concerning health** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

1.12. **Direct marketing** means an activity intended for offering goods or services to individuals by post, telephone or any other direct means and/or for obtaining their opinion about the offered goods or services;

1.13. **Video surveillance** means processing of image data concerning natural person (hereinafter - "video data") by using automated video surveillance means (video and photo cameras, etc.) irrespective of whether these data are recorded in a file or not.

1.14. **SDPI** means State Data Protection Inspectorate;

1.15. **Other concepts** are defined in the Regulation, LLPPD, and other legal acts regulating processing and security of personal data.

II. GENERAL PROVISIONS

2. UAB "Tututis" (hereinafter – Company) Rules set objectives, grounds of personal data processing, categories of data subjects, personal data categories, conditions of transmission of personal data to third parties, storage terms of personal data, destruction conditions, restrictions and procedure of personal data, rights of data subjects, organizational and technical security measures of personal data, regulate employment procedure of personal data processors, the Company's relationship with the data

processors, content and preparation procedure of records on data processing, as well as responsibility of employees, who process personal data.

3. The purpose of the Rules is to ensure proper processing and security of personal data, to safeguard inviolability of private life of natural persons, to protect fundamental rights and freedoms of natural persons related to their personal data processing.

4. The Rules shall be applicable when personal data is processed by automatic and non-automatic means.

5. The requirements of the Rules are mandatory for all the Company's employees, who process personal data or learn such data while carrying out job functions.

III. PRINCIPLES AND OBJECTIVES OF PERSONAL DATA PROCESSING

6. When processing personal data, the Company shall follow the principles related to personal data protection established in the Regulation:

6.1. principle of lawfulness and fairness – personal data have to be processed lawfully and fairly in relation to the data subject;

6.2. principle of transparency – information and notices related to personal data protection must be easy to access, comprehensive and resented in clear and simple language;

6.3. principle of purpose limitation – personal data have to be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

6.4. principle of data minimisation – personal data have to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

6.5. principle of accuracy – personal data have to be accurate and, where necessary, kept up to date;

6.6. principle of storage limitation – personal data have to be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

6.7. principle of integrity and confidentiality – personal data have to be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;

6.8. principle of accountability – the Company shall be responsible for safeguarding of appropriate security of personal data, lawful processing of personal data, and rights of data subjects.

IV. COMPANY'S FUNCTIONS, RIGHTS AND DUTIES

7. The Company shall perform the following functions:

7.1. shall safeguard appropriate processing and protection of personal data of clients (natural persons), when selling goods and services;

7.2. shall provide information to the data subjects about their personal data processing from the moment when personal data are received in brief, transparent, comprehensive and easy-to-access form, in clear and simple language;

7.3. shall analyse technological, methodological and organizational data processing problems and take decisions necessary to ensure appropriate security of personal data;

7.4. shall provide methodological assistance regarding personal data processing to employees;

7.5. shall organize training of employees regarding personal data processing and protection;

7.6. shall safeguard appropriate implementation of the data subjects' rights;

7.7. shall implant technical or organisational measures for protection of personal data that would be in compliance with character of the personal data that need to be protected, their scope and risk of data processing;

7.8. shall perform other functions necessary to carry out rights and obligations of the Company in the area of personal data processing and security.

8. The Company has the following rights:

8.1. to prepare and adopt internal legal acts regulating personal data processing and security;

8.2. to assign the data processors to process personal data provided in the agreement on personal data processing;

8.3. other rights established in the Regulation and in other legal acts of the Republic of Lithuania.

9. The Company has the following duties:

9.1. to ensure compliance with these Rules, Regulation, LLPPD and other legal acts regulating personal data processing and security;

9.2. to implement properly the rights of the data subject in compliance with the Regulation's requirements;

9.3. to safeguard security of personal data using appropriate technical or organisational measures;

9.4. to administer records of data processing activities;

9.5. to notify the State Data Protection Inspectorate about infringement of personal data security not later than within 72 hours after having learnt thereof, unless infringement of personal data security does not cause any hazard to rights and freedom of natural persons;

9.6. to notify the data subject about infringement of personal data security without unreasonable delay, when such infringement may cause high risk to rights and freedoms of data subject;

9.7. to ensure storage of personal data for the term specified herein, but not longer than needed to achieve the goals established in the Rules;

9.8. to use services only of such data processors for personal data processing, who would guarantee appropriate technical or organisational measures used to protect personal data;

9.9. to protect, not to disclose and not to transmit processed personal data, and not to create conditions to access them by any means for any person who is not authorized to process such personal data and who has not been granted access to such data neither in the Company nor beyond it;

9.10. other duties established in the Regulation, LLPPD and in other legal acts of the Republic of Lithuania.

V. RECRUITMENT, SELECTION AND EMPLOYMENT OF CANDIDATES TO JOB VACANCIES

10. The Company shall process the following personal data of the candidates for the purpose of their recruitment, selection and employment:

10.1. name;

10.2. surname;

10.3. phone number;

10.4. e-mail address;

10.5. personal data present in CV (curriculum vitae):

10.5.1. education;

10.5.2. work experience;

10.5.3. qualification;

10.5.4. other information about candidate to the job vacancy.

11. The personal data of candidates to job vacancies are processed in order to take steps at the request of such candidate prior to entering into a contract (sub-paragraph b of paragraph 1 of article 6 of the Regulation), i.e. to check suitability of the candidate for employment contract.

12. Each candidate to a job vacancy in the Company is notified that in assessment of compliance of his/her qualification, work experience and other skills for the job vacancy, as well as when the candidate is invited to an interview or is selected otherwise, his/her personal data are processed.

13. The personal data of candidate to job vacancies may be transmitted to other companies or institutions only upon receipt of written consent of the candidate.

14. The company may transmit personal data of candidates to job vacancies to data processors on the ground of agreements on personal data processing.

15. The personal data of candidates to job vacancies shall be processed by employees authorized by the Company's director. Only the employees assigned to process appropriate data shall have access to the personal data of candidates to job vacancies.

16. The personal data of candidates to job vacancies shall be processed until the employment contract is signed or until the candidacy is rejected. The personal data of candidates to job vacancies have to be deleted from computers, internal database of the Company in 10 (ten) business days after the rejection of the candidacy, whereas the copies of CV (curriculum vitae) and other documents containing personal data of candidates to job vacancies have to be destroyed.

VI. INTERNAL ADMINISTRATION

17. The Company shall process the following personal data of employees for the purpose of internal administration:

17.1. name;
17.2. surname;
17.3. permanent residence;
17.4. phone number;
17.5. date of birth;
17.6. personal number;
17.7. data of personal identity card/passport;
17.8. bank account number;
17.9. e-mail address;
17.10. personal data available in CV and description of activities;
17.11. social insurance number;
17.12. data of health check-up bool and other data related to employee's health;
17.13. information about:
17.13.1. standing;
17.13.2. education;
17.13.3. qualification;
17.13.4. work experience;
17.13.5. work skills.
17.14. position;
17.15. signature;
17.16. amount of wages;
17.17. redundancy pays, compensations;
17.18. allowances;
17.19. information about work hours;
17.20. information about incentives and disciplinary offences of employee;
17.21. information about evaluation of employee's performance;
17.22. information about employee's holidays;
17.23. information about marital status;
17.24. information about level of working capacity;
17.25. information about disability;
17.26. vehicle's number plate.

18. The Company shall process the following personal data of shareholders and their representatives for the purpose of internal administration:

18.1. name;
18.2. surname;
18.3. phone number;
18.4. e-mail address;
18.5. signature.

19. The Company may process personal data about its employees' marital status, level of working capacity, disability, other data concerning health only when it wants to safeguard guarantees granted to employees by the laws and legal acts of the Republic of Lithuania regulating employment and social relations. The purpose set by the Company for processing of personal data of employees of special categories satisfies the condition defined in sub-paragraph b of paragraph 2 of article 9 of the Regulation that allows processing of personal data of special category when it is necessary for the purposes of

carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law; and condition defined in sub-paragraph h of paragraph 2 of article 9 of the Regulation that allows processing of personal data of special category when it is processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee.

20. The Company's internal administration consists of management of the Company's structure, documents, personnel, capital, held material and financial resources, record keeping, financial accountability of the Company, convening of general meetings of shareholders, their registration and implementation of adopted decisions.

21. Personal data of employees are processed for implementation of conditions of employment contracts made with the employees (sub-paragraph b of paragraph 1 of article 6 of the Regulation), as well as for implementation of legal obligations of the Company arising from laws and legal acts of the Republic of Lithuania in the field of employment and social relations (sub-paragraph c of paragraph 1 of article 6 of the Regulation).

22. Personal data of shareholders and their representatives are processed for implementation of legal obligations of the Company arising from the Company's memorandum of association and Law on Companies of the Republic of Lithuania (sub-paragraph c of paragraph 1 of article 6 of the Regulation).

23. The Company shall transmit personal data of its employees to the State Tax Inspectorate under the Ministry of Finance, Board of National Social Insurance Fund under the Ministry of Social Security and Labour, State Labour Inspectorate under the Ministry of Social Security and Labour, SE Centre of Registers, Lithuanian Labour Exchange under the Ministry of Social Security and Labour, Agency of Determination of Disability and Working Capacity under the Ministry of Social Security and Labour, and other governmental and municipal authorities, in order to implement legal obligations established in the laws and legal acts of the Republic of Lithuania. Only the personal data of employees processed by the Company and required by governmental and municipal authorities and companies may be transmitted. Personal data of employees may be transmitted to other authorities and companies, to whom no legal obligation to transmit the data exists, and transmission of personal data to whom is not necessary to safeguard continuance of activities, only upon written consent of such employees.

24. The Company shall transmit personal data of its shareholders and their representatives to the State Tax Inspectorate under the Ministry of Finance, SE Centre of Registers, and other governmental and municipal authorities, in order to implement legal obligations established in the laws and legal acts of the Republic of Lithuania. Personal data of the Company's shareholders and their representatives may be transmitted to other authorities and companies, to whom the Company has no legal obligation to transmit the data, only upon written consent of such shareholders and their representatives.

25. The Company may transmit personal data of its employees, shareholders and their representatives to data processors on the ground of agreements on personal data processing.

26. Personal data of the Company's employees, shareholders and their representatives shall be processed by employees authorized by the Company's director. Only the employees assigned to process appropriate data shall have access to the personal data of particular employees, shareholders and their representatives.

27. Personal data of employee shall be processed (save for storage) until the end of employment relations. When employment relations are over, the employee's personal data shall be stored for the term specified in the Index of General Storage Terms of Documents and for the term set by the Company.

28. Personal data of shareholders and their representatives shall be processed (save for storage) until the shareholders and their representatives take part in general meetings of shareholders and implement other shareholders' rights and obligations specified in the memorandum of association and in the Law on Companies of the Republic of Lithuania with regard to the Company. When the shareholder's representative ceases to represent the shareholder in relations with the Company, his/her personal data shall be stored for the term specified in the Index of General Storage Terms of Documents and for the term set by the Company.

29. Personal data of employees, shareholders and their representatives shall be deleted from all the computers, external media, internal and external databases, and the contracts, registration journals, statements of work time registration, minutes, decisions and other documents containing personal data of employees, shareholders and their representatives shall be destroyed when the storage terms set for

personal data of employees, shareholders and their representatives in the Index of General Storage Terms of Documents and in the Company expire.

VII. STOCK AND OTHER GOODS DELIVERED TO THE COMPANY BY SUPPLIERS

30. The Company shall process the following personal data of representatives of its suppliers for the purpose of delivery of stock and other goods to the Company:

30.1. name;

30.2. surname;

30.3. signature;

30.4. phone number;

30.5. e-mail address.

31. Personal data of suppliers' representatives are processed for performance of sale and purchase agreements (sub-paragraph b of paragraph 1 of article 6 of the Regulation), i.e. when the Company enters into sale and purchase agreements in the procedure established in the Civil Code of the Republic of Lithuania and other legal acts of the Republic of Lithuania that set requirements for entering into sale and purchase agreements, and when it implements its rights and obligations provided in such sale and purchase agreements.

32. Personal data of suppliers' representatives may be transmitted to the State Tax Inspectorate under the Ministry of Finance, SE Centre of Registers, and other governmental and municipal authorities without consent of the suppliers' representatives only in order for the Company to implement its legal obligations to disclose personal data of respective representative. In other cases, personal data of the suppliers' representatives may be transmitted only upon their written consent.

33. The Company may transmit personal data of its suppliers' representatives to data processors on the ground of agreements on personal data processing.

34. Personal data of the Company's suppliers' representatives shall be processed by employees authorized by the Company's director. Only the employees assigned to process appropriate data shall have access to the personal data of particular suppliers' representatives.

35. Personal data of suppliers' representatives shall be processed (save for storage) until the sale and purchase agreement expires and all the mutual obligations of the supplier and the Company are implemented.

36. When the sale and purchase agreements entered into with the suppliers expire, personal data of suppliers' representatives shall be stored for the term specified in the Index of General Storage Terms of Documents and for the term set by the Company and shall be deleted from all the computers, external media, internal and external databases, and the contracts, invoices and other documents containing personal data of suppliers' representatives shall be destroyed when these terms expire.

VIII. DIRECT MARKETING

37. The Company shall process the following personal data of data subjects for the purpose of direct marketing:

37.1. name;

37.2. surname;

37.3. phone number;

37.4. e-mail address.

38. The Company carries out direct marketing by sending newsletters to subscribers, by providing other information to data subjects on offered services, promotional events, news, events, and by conducting surveys about quality of provided services.

39. In order to achieve the objectives set in this chapter, personal data of data subjects are processed on the ground of data subject's consent (sub-paragraph a of paragraph 1 of article 6 of the Regulation).

40. Personal data of the data subject processed for the purpose of direct marketing may be transmitted without consent of the data subject only when the Company is implementing its legal obligation

to disclose personal data of certain data subject to governmental and municipal authorities in accordance with laws. In other cases, personal data of the data subject may be transmitted only upon his/her written consent.

41. The Company may transmit personal data of the data subject processed for the purpose of direct marketing to data processors on the ground of agreements on personal data processing without advance consent of the data subjects.

42. Personal data of the data subject processed for the purpose of direct marketing shall be processed by employees authorized by the Company's director. Only the employees assigned to process appropriate data shall have access to the personal data of data subjects.

43. Personal data of the data subject processed for the purpose of direct marketing shall be processed until the data subject withdraws his/her consent; however, the processing duration cannot be longer than 10 (ten) years after acquisition of personal data. When the data subject withdraws the consent, his/her personal data shall be deleted from all the computers, servers, external databases and media.

IX. VIDEO SURVEILLANCE AND VIDEO DATA PROCESSING

44. Video surveillance and video data processing shall be performed for legal interests of the Company and third parties, in order to safeguard safety of employees and third parties, protection of the Company's assets, work organization procedure, control of entrance to the Company's territory and premises. Other measures, for example, additional mechanical locks are not sufficient to implement the aforementioned purposes.

45. Each visitor and employee know about video surveillance as s/he is notified about video surveillance in the Company's territory and premises by informative references. The informative references must contain the following information:

45.1. general information about the Company and contact data of its representative;

45.2. objectives of the video surveillance;

45.3. lawful interest, on the ground of which the Company is carrying out video surveillance of its territory;

45.4. categories of certain personal data;

45.5. storage period of video data defined by particular term or other criteria;

45.6. rights of filmed persons;

45.7. right to appeal to the State Data Protection Inspectorate;

45.8. source of collected video data – video cameras used in the Company's territory.

46. Video surveillance is carried out in the following territory of the Company:

46.1. in the parking lot, yard at 127, Raudondvario rd., Kaunas;

46.2. in the smoking lounge (ground floor), in metal production premises (ground floor), in the warehouse of ready-made production (ground floor), access to the lift (ground floor), sewing workshop (first floor), cutting workshop (second floor), embroidery workshop (second floor), mechanical (assembly) workshop (third floor), and in the administrative premises (ground floor) at 127, Raudondvario rd., Kaunas.

47. Video data may be transmitted to law enforcement authorities, prosecutor or court as evidence in civil, administrative or criminal proceedings, as well as to other authorities or institutions according to laws, without written consent of the data subjects.

48. The Company's data processors may process video data on the ground of agreements on personal data processing.

49. Video data shall be processed by employees authorized by the Company's director. Only the employees assigned to process appropriate data shall have access to the Video data. The employees authorized by the Company's director shall be responsible for technical maintenance of video surveillance system and video data processing.

50. Video data shall be stored in the recording devices for 14 calendar days. After this period, the video data shall be deleted automatically.

51. The video recording device allows searching for video records according to the date and time.

52. If video data are recorded to external media, they shall be stored in the locked capacities. External media containing recorded video data needed as evidence shall be kept in sealed envelopes.

53. The transmitted copies of video records shall be registered in the covering letter.

54. Video data in external media shall be stored for 14 calendar days, unless longer storage of personal data is necessary to protect the interests of the Company, its employees, clients or other natural persons in the civil, administrative or criminal proceedings.

X. ONLINE SALE OF GOODS

55. The Company shall process the following personal data of purchasers for the purpose of online sale of goods:

55.1. name;
55.2. surname;
55.3. address;
55.4. phone number;
55.5. city;
55.6. date of birth;
55.7. e-mail address;
55.8. bank account number;
55.9. data of credit card;
55.10. particulars of credit institution;
55.11. information of Paysera account;
55.12. information of Paypal account.

56. Personal data of purchasers are processed for performance of sale and purchase agreements (sub-paragraph b of paragraph 1 of article 6 of the Regulation), i.e. when the Company enters into sale and purchase agreements in the procedure established in the Civil Code of the Republic of Lithuania and other legal acts of the Republic of Lithuania that set requirements for entering into sale and purchase agreements, and when it implements its rights and obligations provided in such sale and purchase agreements.

57. Personal data of purchasers may be transmitted to the State Tax Inspectorate under the Ministry of Finance, SE Centre of Registers, and other governmental and municipal authorities without consent of the purchasers only in order for the Company to implement its legal obligations to disclose personal data of purchasers. In other cases, personal data of the purchasers may be transmitted only upon their written consent.

58. The Company may transmit personal data of its purchasers to data processors on the ground of agreements on personal data processing.

59. Personal data of the Company's purchasers shall be processed by employees authorized by the Company's director. Only the employees assigned to process appropriate data shall have access to the personal data of purchasers.

60. Personal data of purchasers shall be processed (save for storage) until the sale and purchase agreement expires and all the mutual obligations of the purchasers and the Company are implemented.

61. When the sale and purchase agreements entered into with the purchasers expire, personal data of purchasers shall be stored for the term specified in the Index of General Storage Terms of Documents and for the term set by the Company and shall be deleted from all the computers, external media, internal and external databases, and the contracts, invoices and other documents containing personal data of purchasers shall be destroyed when these terms expire.

XI. MANAGEMENT OF ACCOUNTS

62. When persons create personal accounts on the website www.tutis.lt, the Company shall process the following personal data:

62.1. name;
62.2. surname;
62.3. date of birth;
62.4. e-mail address.

63. Personal data are processed in order to make shopping on the Company's website easier and to provide possibility to persons to acquire goods and services under favourable conditions, to apply discounts and promotional events, to keep present purchasers and to attract new purchasers, to maintain long-term relations with them, and to improve quality of the services provided by the Company.

64. Personal data are processed on the ground of consent (sub-paragraph a of paragraph 1 of article 6 of the Regulation), i.e. when a person completes an application for creation of personal account and gives consent for personal data processing.

65. When the Company asks to indicate the date of birth in the application for creation of personal account, it ensures that the account will not be created by persons under 14 (fourteen), unless consent pf parents of such persons is submitted.

66. Personal data may be transmitted to the State Tax Inspectorate under the Ministry of Finance, SE Centre of Registers, and other governmental and municipal authorities without consent of the persons only in order for the Company to implement its legal obligations to disclose personal data of respective person. In other case, personal data of the purchasers may be transmitted only upon their written consent.

67. The Company may transmit personal data to data processors on the ground of agreements on personal data processing.

68. Personal data shall be processed by employees authorized by the Company's director. Only the employees assigned to process appropriate data shall have access to the personal data.

69. Personal data shall be processed until the data subject withdraws his/her consent; however, the processing duration cannot be longer than 10 (ten) years after acquisition of personal data.

XII. IMPLEMENTATION OF LOYALTY PROGRAMME

70. In implementation of loyalty programme, the Company shall process the following personal data of such programme's participants:

70.1. name;
70.2. surname;
70.3. date of birth;
70.4. phone number;
70.5. e-mail address;
70.6. city.

71. Personal data of participants of the loyalty programme are processed on the ground of consent (sub-paragraph a of paragraph 1 of article 6 of the Regulation), i.e. when a person completes a Company's questionnaire regarding loyalty programme and gives consent for personal data processing.

72. Personal data are processed in order to provide possibility to participants of the loyalty programme to acquire goods and services under favourable conditions, to apply discounts and promotional events, to keep present purchasers and to attract new purchasers, to maintain long-term relations with them, and to improve quality and assortment of goods and services provided by the Company, taking the needs of participants of the loyalty programme into account. The loyalty programme implemented by the Company consists of invitations issued to the programme's participants to exclusive events, organization of competitions, personalized offers and services, promotional events and discounts for the programme's participants. Direct marketing is also an integral part of the loyalty programme as it helps to implement the content of loyalty programme. The requirements for personal data processing set for direct marketing of the Company are established in chapter XI of the Rules.

73. The nominal loyalty cards are issued to the participants of the loyalty programme. They confirm their participation in the loyalty programme and right to receive services offered by the Company's loyalty programme.

74. Person becomes participant of the Company's loyalty programme upon completion of the Company's questionnaire regarding loyalty programme in writing or electronically.

75. When the Company asks to indicate the date of birth in the questionnaire regarding loyalty programme, it ensures that persons under 14 (fourteen) will not participate in the loyalty programme, unless consent pf parents of such persons is submitted.

76. The Company may transmit personal data of the participants of the loyalty programme to data processors on the ground of agreements on personal data processing.

77. Personal data of the participants of the loyalty programme shall be processed by employees authorized by the Company's director. Only the employees assigned to process appropriate data shall have access to the personal data of particular participants of the loyalty programme.

78. Personal data of participants of the loyalty programme shall be processed until the programme's participant cancels his/her participation in the loyalty programme and returns the nominal loyalty card issued by the Company (if applicable); however, the processing duration cannot be longer than 10 (ten) years after acquisition of personal data. When the participants of the loyalty programme cancel their participation in the loyalty programme and return the nominal loyalty card issued by the Company (if applicable), their personal data shall be deleted manually from the Company's computers, where the data used to be stored and processed. The nominal cards shall be also destroyed.

XIII. RIGHTS AND DUTIES OF DATA SUBJECT

79. The data subjects have the following rights:

79.1. right to access processed personal data;

79.2. right to request rectification or revision of incorrect or inaccurate personal data;

79.3. right to request erasure of processed personal data;

79.4. right to request restriction of personal data processing;

79.5. right to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller;

79.6. right to object to processing of personal data;

79.7. right to withdraw the granted consent for personal data processing at any time.

80. The rights of data subjects, their restrictions and implementation procedure shall be established by the Description of Implementation Procedure of the Rights of Data Subjects approved by the Company's director.

81. The data subjects have the following duties:

81.1. to submit exhaustive and correct personal data to the Company;

81.2. when personal data of the data subject change or the data subject submits incorrect personal data, to notify the Company thereof immediately and to submit new or revised personal data;

81.3. to use the granted rights fairly and not to abuse them.

XIV. ORGANISATIONAL AND TECHNICAL MEASURES USED TO PROTECT PERSONAL DATA

82. Security of personal data in the Company is safeguarded by the appropriate organisational and technical measures:

82.1. management and control of access to personal data are ensured;

82.2. integrity of processed personal data is ensured;

82.3. access to personal data is granted only to the employees authorized to process personal data. The employees working with personal data must sign pledges to process personal data properly and to preserve their confidentiality;

82.4. when the data subject requests to rectify or specify his/her personal data, the application is registered and examined in accordance with Description of Implementation Procedure of the Rights of Data Subjects and, if the request is satisfied, personal data of the data subject in internal data base are updated and unnecessary personal data are erased;

82.5. the files on the Company's personnel, finances, accounting and accountability, other archival files and appropriate electronic files shall be transferred to the employees newly appointed by the

Company's director by conveyance-acceptance deed, when the employees responsible for management of these files are replaced;

82.6. when the data, the storage terms of which have expired and which contain personal data of data subjects, are destroyed, the data and their copies have to be destroyed in such a way that they could not be restored or so that their content could not be recognized;

82.7. requirements set for logging to the Company's computers, local area network, where personal data are stored, and passwords of software and e-mail accounts:

82.7.1. new password has to be unique, consisting of at least 8 symbols, where one symbol has to be a number and one symbol has to be a capital letter;

82.7.2. when the combination of password's symbols is created, it is forbidden to use information of personal character.

82.8. User names and passwords of computers and local area network are personal. When the work is finished, it is important to log out from any used computer or local area network and to make sure that other persons will not make use of the user name and password used in the computer or local area network;

82.9. The passwords of accounts of the Company's computers, local area network and software, where personal data are processed, have to be changed at least once in 2 months. The standard passwords granted by the manufacturer to users of video cameras gave to be changed once in a year. In case of infringement of personal data in local area network, all the passwords of local area network's users have to be changed without delay. If it is possible that the password of certain computer of the Company, local area network, equipment or e-mail address has been disclosed to third parties or made public, such password has to be changed without delay;

82.10. It is forbidden to send e-mails of malicious, illegal or other inappropriate content through the Company's e-mail accounts. If an-email of suspicious content or attachments is received, it is forbidden to open or save such e-mail and its attachments, whereas the sender's e-mail address has to be blocked. It is also forbidden to open or use any executable file received by e-mail (.exe, .cmd, .bat, .scr, .com, etc.). The content of the e-mailed letter has to be checked always before replying or forwarding the letter to third party. It is forbidden to configure work e-mail in personal computer, phone, tablet or another device;

82.11. The possibilities for public online search systems and robots of search engines to copy the website's information and to find the copies of previously posted but already removed information from the website have to be restricted maximally;

82.12. It is forbidden to use improperly the Company's work computers and to cause damage to them. When the work with the computer is finished, its screen always has to be closed. Only the accounts related to the Company's activities and work shall be used in the Company's computers, where personal data are processed;

82.13. It is forbidden to use external media that may have malicious programmes or viruses in the Company's computers (USB, CD-ROM, DVD discs, external HDD, SSD, etc.);

82.14. The operating system and software used by the Company are supported and licenced. The operating system and software are used by the Company are updated automatically in the procedure applied by the licencing company-manufacturer. The Company's programmes are licenced only for their usage in the Company and nowhere else;

82.15. The accounts of software and e-mail of employees or other persons, who do not process personal data assigned by the Company any more, in computers and local area network shall be deleted within 12 months.

82.16. The latest licenced antivirus software is installed in all the computers of the Company;

82.17. The Company's local area network and computers have firewalls;

82.18. The security of premises, where personal data are stored, is ensured. The access of third parties and persons not authorized to work with appropriate personal data to the premises, where personal data are stored, is restricted;

82.19. The Company's documents, their copies, files of finances, accounting and accountability, archival and other files containing personal data of the Company's data subjects shall be stored in locked cabinets, safes or premises;

82.20. Personal files of employees conveyed for archival storage shall be stored in locked storage of the Company's documents before transfer to the archive;

82.21. The Company's employees responsible for video data processing cannot allow unaccompanied strangers to enter the premises, where video recording devices are present. When the disorders in the work of video system are noticed, the Company's director and persons in charge of technical maintenance of video surveillance have to be notified thereof without delay;

82.22. The security control and erasure of personal data held in the external data media have to be safeguarded;

82.23. It has to be safeguarded that testing of information systems in the Company would not be carried out sing the real personal data, unless appropriate organisational and technical measures are used to safeguard security of real personal data;

82.24. Personal data can be transmitted to external networks from the Company's local area network only after having encoded them at first;

82.25. The video surveillance system used by the Company is technically maintained. The system's disorders have to be removed rapidly using all the available technical resources.

XV. USAGE OF SERVICES OF PERSONAL DATA PROCESSOR

83. The Company is entitled to use services of data processor, who will process personal data assigned by the Company.

84. When the Company decides to use services of data processor to process personal data, the written agreement on personal data processing shall be entered into by the Company and the data processor. This agreement is prepared on the ground of the main contract between the Company and the data processor, for appropriate implementation of which the data processor has to process personal data assigned by the Company.

85. The Company has the following duties to the data processor:

85.1. to ensure that the technical and organisational measures applied by the data processor guarantee appropriate protection of rights and legal interests of data subjects and personal data assigned to data processor;

85.2. to inform the data processor about infringement of data security if such infringement is hazardous for personal data processing carried out by the data processor;

85.3. to appoint persons responsible for additional written orders or instructions to the data processor, implementation of other rights and duties of the Company, and for coordination of actions of the data processor and the Company;

85.4. to notify the data processor in writing within reasonable term about satisfied request of the data subject to rectify and erase certain personal data or restrict personal data processing and to order the data processor in writing to rectify, erase personal data or restrict their processing. The Company is obliged to inform the data processor in writing about rectification, erasure of personal data or restriction of data processing, and to give written directions to the data processor only if the data subject and his/her personal data rectified, erased or restricted by the Company are included into the categories of data subjects and personal data processed by data processors indicated in the agreement on personal data processing. The written order of the Company must contain the data subject's name, surname, category, list of personal data rectified, erased or restricted by the Company, actions that the data processor has to carry out, term of performance of actions, with regard to amount and processing scope of personal data instructed to rectify, erase or restrict. When the data processor is instructed to rectify certain personal data of data subject, the Company must also indicate, how rectification should be done;

85.5. to perform other duties provided in the Regulation, LLPPD, and other legal acts that set requirements for personal data processing and protection as much as implementation of these duties is related to proper implementation of personal data processing.

86. The Company has the following rights with regard to the data processor:

86.1. to check and evaluate whether the data processor is implementing factually technical and organisation measures described by the data processor in the agreement on personal data processing;

86.2. to demand for additional technical and organisational measures from the data processor or correction of processing activities of personal data assigned by the Company, if the Company has a reason to believe that without additional technical and organisational measures or correction of personal data processing activities, the risk would rise for security of personal data and rights and legal interests of the data subjects, whose personal data are processed by the data processor. The data processor may refuse implementing the Company's order to apply additional technical and organisational measures or to correct the processing activities of personal data assigned by the Company if the implantation of additional

technical and organisational measures or correction of processing activities would result in unreasonably big expenses to the data processor and the Company refuses to reimburse them.

86.3. to receive a copy of audit report or certificate, if the data processor has carried out audit or has received a certificate of the approved certification company about compliance of applied technical and organisational measures with the requirements of the Regulation, LLPPD and other legal acts of the Republic of Lithuania;

86.4. to control, how the data processor and other persons authorized by the data processor to process the personal data assigned by the Company observe the confidentiality duty established in the agreement on personal data processing;

86.5. to allow the data processor to use services of other data processors (hereinafter – sub-processors) to process personal data assigned by the Company;

86.6. to use services of other data processor regarding processing of the same personal data for the same or different purposes;

86.7. to get familiar with the documents of the data processor used to document the personal data processing process in the Company, and to receive copies of these documents and other information from the data processor related to personal data processing assigned by the Company;

86.8. to restrict processing of personal data assigned by the Company or part of them when the Company has a ground to believe that the personal data processed by the data processing are inaccurate or incorrect, that the data processor or authorized persons process personal data for other purposes than specified in the agreement on personal data processing, that processing is not in compliance with the described character of personal data processing, that the data processor and the authorized employees do not observe the duty of confidentiality, that the technical ad organizational measures applied by the data processor do not safeguard proper protection of personal data processed by the data processor and rights and legal interests of data subjects, that the data processor is not implementing factually technical and organizational measures, or that the data processor violates the conditions of agreement on personal data processing and requirements of the Regulation, LLPPD and other legal acts of the Republic of Lithuania concerning personal data processing and protection. The implementation of the main contract is suspended for restriction period of personal data processing, unless such restriction does not prevent implementation of the main contract;

86.9. to terminate the main contract with the data processor on the same grounds that are applied for processing restriction, unless the Company has a reason to believe that the personal data of the Company processed by the data processor are inaccurate or incorrect;

86.10. to give additional written orders or instructions to the data processor regarding personal data processing and security in order to implement properly the requirements set for personal data processing and security;

86.11. other rights provided in the Regulation, LLPPD, and other legal acts of the Republic of Lithuania regarding the data processor.

87. The data processor has the following duties to the Company:

87.1. to process personal data only in accordance with additional orders and instructions given by the Company on the ground of these Rules and agreement on personal data processing, including transmission of personal data to third parties. The processor has to process personal data without the Company's order when the legal duty of data processing is established by the law of the European Union or the Member State. In such a case, before the data processor starts processing personal data and, in any case, not later than 2 days beforehand, it has to notify the Company about the legal obligation, unless such notification is prohibited because of important reasons of public interest specified in the law of the European Union or the Member State. If the data processor has not received any additional written orders or instructions from the Company, how to process personal data in particular situation, or if the additional written orders or instructions from the Company contradict to the Regulation, LLPPD and other legal acts of the Republic of Lithuania regulating personal data protection and processing, the data processor shall notify the Company thereof immediately and not later than in 2 days;

87.2. upon receipt of the notice from SDPI, to execute the orders or recommendations and to cooperate with SDPI otherwise in implementation of its direct functions. The data processor has to inform the Company about orders and recommendations given in the SDPI notice not later than in 2 days;

87.3. to help the Company to implement the rights of data subjects provided in chapter 3 of the Regulation, if the data processor has been appointed to process personal data of certain category of data subjects;

87.4. upon receipt of the request of the data subject to provide information about his/her personal data assigned for processing of the data processor or to implement another right provided in

chapter 3 of the Regulation, to transmit this request to the Company not later than in 2 days after receipt of respective request;

87.5. upon the Company's request, to provide all the information about personal data processing performed in its name;

87.6. to ensure factual implementation of appropriate technical and organisational measures, on implement additional technical and organisational measures on the Company's request, unless the data processor suffers unreasonably big expenses because of implantation of additional technical and organisational measures and the Company refuses to compensate them;

87.7. upon the Company's request, to furnish a copy of audit report or certificate if the data processor has carried out audit or has received a certificate of the approved certification company about compliance of applied technical and organisational measures with the requirements of the Regulation, LLPPD and other legal acts of the Republic of Lithuania;

87.8. not later than in 5 days after conclusion of the agreement on personal data processing, to make and approve the list of the data processor's employees authorized to process personal data assigned by the Company, and to submit tis list to the Company. If the data processor modifies, supplements, updates or re-approves the list of the data processor's employees authorized to process personal data assigned by the Company, the data processor has to submit the modified, supplemented or updated list to the Company in 5 days after the list's approval;

87.9. after conclusion of the agreement on personal data processing, to make pledges with the employees regarding appropriate processing of personal data that would meet the condition of confidentiality of the data processor and the authorized employees. It is prohibited for the data processor to allow the employees to get familiar with the Company's personal data, to start their processing and to grant access to such personal data until the respective pledges are not made;

87.10. to ensure that the authorized employees would process the Company's personal data for the purposes established in the agreement on personal data protection, would comply with the personal data processing character, duty of confidentiality, implementation procedure of technical and organisational measures and other requirements;

87.11. to process personal data only within the scope established in the agreement on personal data protection and necessary for implementation of the functions arising from this agreement;

87.12. upon request of the Company, to furnish the copies of the documents used to document personal data processing process;

87.13. to inform the Company about infringement of personal data security in accordance with the Description of Control of Infringements of Personal Data Security and Reaction thereto, and to undertake other actions in order to remove the infringement;

87.14. to reimburse the losses incurred by the Company because the data processor has violated the requirements of the Rules, agreement on personal data processing, the Regulation, LLPPD and other legal acts that regulate data processing and protection;

87.15. when the agreement on personal data processing expires, to return to the company the data assigned for processing and to erase the copies of personal data or t delete the Company's personal data without return;

87.16. to carry out other obligations provided in the Regulation, LLPPD, other legal acts that regulate personal data processing and protection, in the scope related to proper implementation of the agreement on personal data processing.

88. The data processor has the following rights with regard to the Company:

88.1. to modify, supplement, update the list of the data processor's employees authorized to process personal data;

88.2. to consult with the Company and ask for additional orders and instructions regarding personal data processing and protection in the cases not specified herein or in the agreement on personal data processing, in order to implement properly the requirements set for processing and protection of personal data carried out by the data processor;

88.3. upon the Company's consent, to use services of other data processors (hereinafter – sub-processors) to process personal data assigned by the Company;

88.4. to implant additional technical and organisational measures to protect the Company's personal data, after having coordinated this with the Company;

88.5. other rights with regard to the Company provided in the Regulation, LLPPD and other legal acts of the Republic of Lithuania.

89. Terms and conditions for usage of services of other data processor (sub-processor):

89.1. The data processor may use services of sub-processors only upon receipt of advance written consent of the Company;

89.2. The data processor has to notify the Company beforehand about the planned changes related to sub-processors or their replacement, and to receive the company's written consent;

89.3. The contract or other agreement between the data processor and the sub-processor must contain the same obligations and requirements as set for the data processor;

89.4. The data processor has a duty to make sure whether the sub-processor is implementing factually the technical and organisational measures provided in the contract or other agreement between the data processor and the sub-processor, and to control, how the sub-processor and its authorized employees are processing the Company's personal data;

89.5. The data processor shall be fully responsible to the Company for inappropriate personal data processing carried out by the sub-processor, as well as for other violations of the requirements and conditions.

90. Terms and conditions of erasure and return of personal data to the Company:

90.1. When the agreement on personal data processing expires, the data processor has to return all the personal data processed on the ground of such agreement to the Company, to delete or destroy hard and digital copies of these personal data, unless the Company orders the data processor to delete all the processed personal data without returning them, or if the return of processed personal data is impossible due to delivery mode, amount or other reasons or if return would demand for disproportionate efforts of the data processor. If the data processor does not return personal data to the Company because it is impossible or demands for disproportionate efforts of the data processor, the data processor has to delete or destroy such personal data;

90.2. The data processor shall not return the personal data processed on the ground of the agreement on personal data processing to the Company, shall not delete them or their copies when the data processor has a legal obligation to store certain personal data in accordance with the legal acts of the Republic of Lithuania.

91. Responsibility of the Company and the data processor:

91.1. The Company and/or the data processor shall be liable for violations of the Regulation, LLPPD and other legal acts of the Republic of Lithuania regulating personal data processing and protection as indicated in the Regulation and the laws;

91.2. The Company and/or the data processor has to compensate any tangible or intangible damage caused to any person by violation of the Regulation, LLPPD and other legal acts of the Republic of Lithuania regulating personal data processing and protection as indicated in the laws.

92. The Company shall select such data processor, who would guarantee appropriate technical and organisational measures and who would ensure observation of such measures.

XVI. RECORDS OF PERSONAL DATA PROCESSING ACTIVITIES

93. The Company shall maintain a record of processing activities under its responsibility. The records of processing activities in the Company shall be made for the purpose of internal administration, direct marketing and video surveillance. The records of processing activities may be made in the Company for other purposes, as well. The record of processing activities shall contain all of the following information:

93.1. the purposes of the processing;

93.2. general information about the Company;

93.3. contact details of the Company's representative;

93.4. character of processing activities related to the purpose of processing;

93.5. categories of data subjects and categories of personal data;

93.6. categories of recipients to whom the personal data have been or will be disclosed;

93.7. he envisaged time limits for erasure of personal data;

93.8. general description of the technical and organisational security measures;

93.9. rights granted to the data subjects.

94. The records of personal data processing activities shall be in writing, including in electronic form.

95. The Company shall make the record available to the State Data Protection Inspectorate on request.

96. The Company has an established form of records of processing activities.

XVII. FINAL PROVISIONS

97. All the Company's employees processing personal data and the data processors have to act in compliance with these Rules and main requirements for personal data processing, confidentiality and security established in the Regulation.

98. The employees processing personal data shall be introduced to the Rules under signature.

99. Non-compliance with these Rules by the employees processing personal data or having access to the personal data managed by the Company shall be regarded as violation of work duties.

100. The employees processing personal data, who violate requirements of the Regulation, LLPPD and other legal acts of the Republic of Lithuania regulating personal data processing and security shall be liable in accordance with laws.

_____