APPROVED BY
27 December 2021 Order No 1T-117 (1.12.E) of the Director of the State Data Protection Inspectorate

**(Standard contractual clauses for the data processing agreement)**

# STANDARD CONTRACTUAL CLAUSES FOR THE DATA PROCESSING AGREEMENT

_____ 20__ No _
(date)

_____
(place)

The Data Controller _____

_____,
(name, registration number, address of the registered office, telephone number and e-mail address of the data controller; if the data controller is a natural person, name and surname, individual activity certificate or business licence number, address of the place of residence, telephone number and e-mail address)

represented by _____,
(name and surname, position of the person representing the data controller, basis of representation)

and the Data Processor _____

_____,
(name, registration number, address of the registered office, telephone number and e-mail address of the data processor; if the data processor is a natural person, name and surname, individual activity certificate or business licence number, address of the place of residence, telephone number and e-mail address)

represented by _____,
(name and surname, position of the person representing the data processor, basis of representation)

(hereinafter individually referred to as a "Party" and collectively as the "Parties")

following 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) (hereinafter referred to as the "Regulation (EU) 2016/679"),

**have agreed** on these clauses on the Processing of Personal Data on the basis of Article 28 of Regulation (EU) 2016/679 (hereinafter referred to as the "Clauses") which shall consist of the annexes specified in the Clauses and concluded between the Parties during the term of the Clauses.

Where these Clauses use the terms defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

## CHAPTER I
## PURPOSE OF THE CLAUSES

1. For the purposes of implementation of Article 28(3) of Regulation (EU) 2016/679, the rights

and obligations of the Data Controller and the Data Processor in processing of personal data on behalf of the Data Controller shall be set out herein. The Clauses shall be aimed at protecting the rights of the data subjects, minimising the specific risks with respect to protection of personal data and ensure the clarity of the relationship between the Data Controller and the Data Processor and the respective rights and obligations of the Data Controller and the Data Processor.

2. For the purposes of provision of *[name of the service]* services *[where applicable, details of the agreement on provision of such services, e. g. date / number / title]*, the Data Processor shall process personal data on behalf of the Data Controller hereunder. The terms and conditions of processing of personal data shall be set forth in Annex 1 hereto.

## CHAPTER II
## OBLIGATIONS OF THE PARTIES

3. The Data Controller:

3.1. is responsible for ensuring that personal data is processed in accordance with Regulation (EU) 2016/679 (see Article 24 of hereof), other European Union or Member State law[1] governing protection and/or processing of personal data and these Clauses;

3.2. has the right and obligation to make decisions on the purposes and means of processing of personal data;

3.3. shall be responsible, among other, for ensuring that processing of personal data which is assigned to the Data Processor has legal grounds.

4. The Data Processor:

4.1. processes personal data only in accordance with the documented instructions issued by the Data Controller except for the cases where this is required by the European Union or Member State law applicable to the Data Processor (in such cases Data Processor shall inform the Data Controller of the legal requirement before processing, unless that law prohibits such information for reasons of substantial public interest). Such instructions shall be set out in Annex 1 and Annex 3 to the Clauses. The Data Controller shall also be entitled to issue further instructions during the entire period of the processing of personal data; however, such instructions related to the Clauses must always be in line with the respective rights and obligations of the Parties set out in the Clauses and documented;

4.2. shall immediately notify the Data Controller if, in the opinion of the Data Processor, the Data Controller's instructions are in conflict with Regulation (EU) 2016/679 or other European Union or Member State law governing protection of personal data;

4.3. shall maintain records related to the activities of processing of personal data carried out on behalf of the Data Controller. The afore-mentioned obligation shall apply to each Data Processor and, where applicable, the representative of the Data Processor in accordance with Article 30(2) of Regulation (EU) 2016/679.

5. *[NOTE. The Parties should foresee the consequences which may arise as a result of any possibly unlawful instructions given by the Data Controller and regulate this in the agreement concluded between the Parties].*

6. These Clauses shall not release the Parties from other obligations applicable to them under Regulation (EU) 2016/679 or other legal acts.

[1] For the purposes of the Clauses, a "Member State" shall be understood as a Member State of the European Economic Area.

## CHAPTER III
## CONFIDENTIALITY

7. The Data Processor shall grant access to the personal data processed on behalf of the Data Controller only to the persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need-to-know basis. Parties ensure that:

7.1 In case of a need to change in the persons having access to personal data, their right of access to the Data Controller's personal data shall be revoked not later than on the last day on which their tasks require them to have access to the personal data of the Data Controller entrusted to Data Processor. In case of discontinuation of employment relationship with the employee of the Data Processor, the access rights to the Data controller's personal data shall be revoked not later than on the last day of work.

7.2. The list of persons granted access to personal data shall be reviewed on a periodical basis *[by the data processing agreement the Parties shall agree on the particular intervals of review, for example, at least every 6 months]*. Following the afore-mentioned review, such access to personal data shall be suspended if such access is no longer necessary; thus, personal data cannot be accessible to such persons.

8. Upon the Data Controller's request, the Data Processor shall demonstrate that the persons who are supervised by the Data Processor and to whom processing of personal data is assigned shall be subject to the obligation of confidentiality provided for in paragraph 7 hereof.

## CHAPTER IV
## SECURITY OF PROCESSING

9. Following Article 32 of Regulation (EU) 2016/679, the Data Controller and the Data Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

10. The Data Controller shall assess possible risk to the rights and freedoms of natural persons in processing of personal data and implement measures to minimise such risk. Depending on the appropriateness of the measures, they may be as follows:

10.1. the pseudonymisation and/or encryption of personal data;

10.2. the ability to ensure the continues confidentiality, integrity, availability and resilience of processing systems and services;

10.3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

10.4. a process for regular testing, inspecting and evaluating the technical and organisational measures for ensuring the security of the processing.

11. According to Article 32 of Regulation (EU) 2016/679, the Data Processor shall also – independently from the Data Controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing activity entrusted to it by the Data Controller, and implement the measures to mitigate those risk. To this end, the Data Controller shall provide the Data Processor with all information necessary for identification and assessment of such risk.

12. Furthermore, the Data Processor shall help the Data Controller in ensuring compliance with the Data Controller's obligation provided for in Article 32 of Regulation (EU) 2016/679 *inter alia* providing the Data Controller with information on technical and organisational measures which have already been implemented by the Data Processor under Article 32 of Regulation (EU) 2016/679 together with all other information necessary for the Data controller to comply with its obligation under Article 32 of Regulation (EU) 2016/679.

13. If, according to the assessment made by the Data Controller, the mitigation of the identified risks requires further measures to be implemented by the Data Processor, the Data Controller shall specify these additional measures in Annex 3 hereto and the Data Processor shall implement additional measures and the measures which have already been implemented under Article 32 of Regulation (EU) 2016/679. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with its obligations as provided in Chapter X of the Clauses.

## CHAPTER V
## ENGAGEMENT OF OTHER DATA PROCESSORS

14. The Data Processor shall comply with the requirements set forth in Articles 28(2) and 28(4) of Regulation (EU) 2016/679 in order to engage another data processor (hereinafter referred to as the "sub-processor").

15. The terms and conditions of the Data Controller in accordance with which the Data Processor may engage sub-processors and the list of the sub-processors authorised by the Data Controller shall be laid down in Annex 2 hereto.

16. The Data Processor shall not engage a sub-processor for performance of the processing carried out under these Clauses without a prior *[[OPTION 1] special written authorisation of the Data Controller] / [[OPTION 2] general written authorisation of the Data Controller]*:

16.1. *[[OPTION 1] special written authorisation of the Data Controller]*. The Data Processor shall engage sub-processors only with special prior authorisation of the Data Controller. The Data Processor shall submit a written request for special authorisation at least *[specify the period]* before the date of engagement of the respective sub-processor.

16.2. *[[OPTION 2] general written authorisation of the Data Controller]*. The Data Processor has the general written authorisation to engage sub-processors of the Data Controller. The Data Processor shall notify the Data Controller of any planned amendments related to engagement or replacement of sub-processors in writing no later than *[specify the period]* in advance, thus, enabling the Data Controller to object to such amendments before engagement of the respective sub-processor(s). Longer periods of prior notification of specific processing services may be set out in Annex 2 hereto.

17. Where the Data Processor engages a sub-processor for carrying out the particular processing on behalf of the Data Controller, the same data protection obligations as set out between the Data Controller and the Data Processor shall be imposed on the sub-processor by way of a contract or another legal act under European Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures so that processing meets the requirements of Regulation (EU) 2016/679. Prior to processing, the data processor shall inform the sub-processor of the identity and contact details of the Data Controller for which the sub-processor processes personal data

18. Upon request of the Data Controller, a copy of the contract with a sub-processor and subsequent

amendments thereto, shall be provided to the Data Controller, thus, enabling the Data Controller to ensure that the sub-processor was subject to the same data protection obligations as laid down by the Clauses. The Data Processor shall notify the Data Controller of any failure by the sub-processor to fulfil its obligations under that contract or other legal act binding on sub-processor. The Data Processor is not obliged to provide the provisions of the data processing agreement on the business-related issues which do not have an impact on the terms and conditions of the legal protection of personal data of the contract concluded with the sub-processor.

19. The Data Processor shall agree on a third-party beneficiary clause with a sub-processor (if any) providing that in case of bankruptcy of the primary Data Processor, the Data Controller shall be entitled to enforce the data processing agreement directly against the sub-processor engaged by the primary Data Processor and/or issue direct instructions on processing, for example, instruct the sub-processor to delete or return personal data.

20. The data processor shall be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR. If the sub-processor fails to fulfil the personal data protection obligations, the primary Data Processor with which/whom data processing agreement is concluded shall remain fully liable towards the Data Controller for fulfilment of the sub-processor's obligations. This shall not affect the data subjects' rights provided for in Regulation (EU) 2016/679, in particular, the rights provided for in Articles 79 and 82 of Regulation (EU) 2016/679 in respect of the Data Controller and the Data Processor including the rights in respect of the sub-processors.

## CHAPTER VI
## TRANSFER OF DATA TO THIRD COUNTRIES[2] OR INTERNATIONAL ORGANISATIONS

21. The Data Processor shall be entitled to transfer personal data to third countries or international organisations only after receipt of the documented instructions of the Data Controller and in accordance with the requirements of Chapter V of Regulation (EU) 2016/679.

22. If personal data must be transferred to third countries or international organisations in accordance with European Union or Member State law which must be complied with by the Data Processor although the Data Controller has not given instructions to do this to the Data Processor, the Data Processor shall notify the Data Controller of the afore-mentioned legal requirement prior to transfer of data unless such legal act prohibits communication of such information.

23. The Data Processor shall not be entitled to carry out the following actions without the documented instructions of the Data Controller or the particular request under European Union or Member States law in accordance with these Clauses:

23.1. to transfer personal data to a Data Controller or a Data Processor in a third country or in an international organisation;

23.2. to transfer processing of personal data to a sub-processor in a third country;

23.3. to allow the Data Processor to process personal data in a third country.

24. The Data Controller's instructions or approval regarding transfers of personal data to a third country including, if applicable, the transfer tool under Chapter V of Regulation (EU) 2016/679 on which the Data Controller's instructions are based, shall be set out in Annex 3 of these Clauses.

[2] NOTE. 'Third countries' refers to countries outside the European Economic Area.

25. These Clauses shall not be standard data protection clauses defined in Articles 46(2)(c) and 46(2)(d) of Regulation (EU) 2016/679 and the Parties shall not be entitled to rely on the Clauses as the basis of transfer of personal data to third countries or international organisations in accordance with Chapter V of Regulation (EU) 2016/679.

## CHAPTER VII
## ASSISTANCE TO THE DATA CONTROLLER

26. Taking into account the nature of processing, the Data Processor shall assist the Data Controller to fulfil the Data Controller's obligation to respond to the requests for exercise of the data subject's rights provided for in Chapter III of Regulation (EU) 2016/679 by appropriate technical and organisational measures, insofar as this is possible. This implies that the Data Processor shall, insofar as this is possible, assist the Data Controller in its obligation to give effect to the following data subject rights:

26.1. the right to be informed when personal data has been obtained from the data subject;

26.2. the right to be informed when personal data has been obtained not from the data subject;

26.3. the data subject's right to access data;

26.4. the right to rectification;

26.5. the right to erasure ("right to be forgotten");

26.6. the right to restriction of processing;

26.7. the notification obligation regarding rectification or erasure of personal data or restriction of processing;

26.8. the right to data portability;

26.9. the right to object to processing;

26.10. the right not to be subject to decisions based solely on automated processing, including profiling.

27. In addition to the Data Processor's obligation to assist the Data Controller in accordance with paragraph 12 hereof, the Data Processor, taking into account the nature of processing and information available to the Data Processor, shall also assist the Data Controller in ensuring compliance with:

27.1. the Data Controller's obligation to without undue delay and, where feasible, not later than within 72 hours after having become aware of it, notify the competent supervisory authority *[specify the competent supervisory authority]* of the personal data breach unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

27.2. the Data Controller's obligation to notify without undue delay the data subject if personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

27.3. the Data Controller's obligation to carry out a data protection impact assessment of the envisaged personal data processing operations where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

27.4. the Data Controller's obligation to consult the competent supervisory authority *[specify the competent supervisory authority]* prior to processing if the data protection impact assessment indicates that processing of data would result in high risk if the Data Controller fails to take measures to mitigate the risk.

28. The Parties shall establish in Annex 3 hereto the appropriate technical and organisational measures, which should be taken by the Data Processor to assist the Data Controller with the data subject rights and with the obligations under Articles 33 to 36 of Regulation (EU) 2016/679, as set

out in paragraphs 27 hereof.

## CHAPTER VIII
## NOTIFICATION OF PERSONAL DATA BREACH

29. The Data Processor shall notify the Data Controller without undue delay after becoming aware of a personal data breach. The Data Processor shall notify the Data Controller within *[number of hours]* from the moment on which the Data Processor becomes aware of the personal data breach so that the Data Controller could fulfil the Data Controller's obligations to report the personal data breach to the competent supervisory authority in accordance with Article 33 of Regulation (EU) 2016/679.

30. The obligation to assist the Data Controller to notify the competent supervisory authority of a personal data breach provided for in paragraph 27.1 hereof shall imply that the Data Processor must assist the Data Controller to obtain the information specified below which, according to Article 33(3) of Regulation (EU) 2016/679, must be indicated in the Data Controller's notification to the competent supervisory authority:

30.1. the nature of the personal data including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data concerned;

30.2. the likely consequences of the personal data breach;

30.3. the measures taken or proposed to be taken by the Data Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects;

30.4. any other relevant information which is or may be necessary for the Data Controller when preparing the notification or responding to additional requests of the competent supervisory authority related to the personal data breach.

31. Annex 3 to the Clauses shall set out all elements which must be provided by the Data Processor to assist the Data Controller to notify the competent supervisory authority of a personal data breach. If the Data Processor fails to provide all information on the personal data breach to the Data Controller or later additional information becomes evident, the Data Processor shall be obliged to without undue further delay but not later than within [*number of hours.*] from the moment of becoming aware of new information give an additional notification to the Data Controller specifying all missing information.

32. Upon request of the Data Controller, in addition to the information provided for in paragraph 31 hereof, the Data Processor shall provide copies of the documents, for example, the documents justifying the carried out actions, applied measures or carried out internal inspections and conclusions of the inspections.

## CHAPTER IX
## ERASURE AND RETURN OF DATA

33. Upon termination of the provision of personal data processing services, the Data Processor shall be obliged, at the choice of the controller *[OPTION 1]* to delete all personal data processed on behalf of the Data Controller and demonstrate to the Data Controller that he/it did this and/or *[OPTION 2]* return all personal data to the Data Controller and in any event delete the existing copies unless the personal data must be stored in accordance with the laws of the European Union or its Member State.

The Data Controller is entitled to modify the choice made at the time of the signature of the Clauses throughout the life cycle of the Clauses and upon its termination.

34. *[OPTIONALLY]* Upon termination of provision of personal data processing services, personal data must be stored according to the following European Union or Member Sate law applicable to the Data Processor:

34.1. [*List the laws*]

35. *[IF APPLICABLE]* Upon termination of provision of personal data processing services, the Data Processor shall undertake to process personal data only for the purposes and within the time limits provided for in the law set out in paragraph 34 hereof and strictly in accordance with the terms and conditions set forth therein.

## CHAPTER X
## AUDIT AND INSPECTION OF THE DATA PROCESSOR

36. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations set out in Article 28 of Regulation (EU) 2016/679 and the Clauses and enable and assist the Data Controller or another auditor mandated by the Data Controller to carry out an audit including on-the-spot inspections.

37. An audit (including inspections) of the Data Processor and sub-processors carried out by the Data Controller shall be subject to the procedures provided for in paragraphs 7 and 8 of Annex 3 hereto.

38. The Data Processor shall grant the supervisory authorities which, according to the law in force, have access to the equipment of the Data Controller and the Data Processor, or the representatives acting on behalf of such supervisory authorities access to data processor's physical facilities or fulfil other instructions of the supervisory authorities to carry out an audit or another inspection. The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority on request.

## CHAPTER XI
## FINAL PROVISIONS

39. The terms and conditions of the Clauses shall come into force from the date of signature of the Clauses.

40. During the period of provision of personal data processing services, the Clauses cannot be terminated if the Parties have not agreed on other terms and conditions of the Clauses regulating provision of personal data processing services.

41. If provision of personal data processing services is terminated and personal data is deleted or returned to the Data Controller in accordance with paragraph 33 of the Clauses and paragraph 4 of Annex 3 to the Clauses, the Clauses may be terminated by a written notice given by either Party.

42. Without prejudice to any provisions of Regulation (EU) 2016/679, if the Data Processor breaches his/its obligations hereunder, the Data Controller shall be entitled to order the Data Processor to suspend personal data processing on a temporary basis till the latter complies with the Clauses or the Clauses are terminated. The Data Processor shall immediately notify the Data Controller if he/it cannot perform its tasks as agreed in the Clauses for any reason.

43. The Data Controller shall be entitled to terminate the Clauses if:

43.1. the Data Processor substantial or persistent breaches the Clauses or his/its obligations under Regulation (EU) 2016/679;
43.2. the Data Processor fails to comply with the binding decision of the court or supervisory authority in relation to his/its obligations provided for in the Clauses or Regulation (EU) 2016/679;
43.3. the processing of personal data by the Data Processor has been suspended by the Data Controller pursuant to paragraph 43.1 and (or) 43.2 of the Clauses and compliance with these Clauses is not restored within a [*certain amount of time. Note: please choose reasonable time which in any event should be no longer than one month from the moment of suspension*] following suspension.
44. The Clauses shall take precedence over any similar provisions related to processing of personal data set out in other agreements between the Parties.
45. Each Party shall appoint a person responsible for executing the Clauses.

## CHAPTER XII
## DETAILS AND SIGNATURES OF THE PARTIES

| For and on behalf of the Data Controller: | For and on behalf of the Data Processor: |
|---|---|
| *position* | *position* |
| *name, surname* | *name, surname* |
| *date* | *date* |
| *L.S.* | *L.S.* |

Annex 1 to
The standard contractual clauses for the data processing agreement

**INFORMATION ON PROCESSING OF PERSONAL DATA**

**1.Information on processing of personal data:**

*[NOTE. If several data processing activities are carried out, the following parts must be separately filled in for each processing activity].*

**1.1. The purpose of processing of personal data by the Data Processor shall be:**

*[Describe the purpose of processing of personal data by wording it clearly and specifically, i.e. with sufficient details to determine what kind of processing it covers and assess if the particular purpose is not in conflict with the requirements of the legislation].*

*[EXAMPLES. "Preparation of the Data Controller's documents for their storage in accordance with the requirements of the Law on documents and archives and requirements of Chief archivist of Lithuania, or for their deletion, if the retention period has come to an end", "Storing the personal data of the Data Controller"].*

**1.2. Processing of personal data by the Data Processor shall be mainly related to (nature of processing):**

*[Describe the nature of processing].*

*[EXAMPLE. "Preparation of the Data Controller's documents for their storage in accordance with the requirements of the Law on documents and archives and requirements of Chief archivist of Lithuania, or for their deletion, if the retention period has come to an end, i. e.:*
*1. Preparation of document of long-term retention for their storage for the archiving purposes;*
*2. Preparation of document of short-term retention for their storage for the archiving purposes;*
*3. Selection of documents that shall be destroyed and / or deleted and preparation of destruction certificate"].*

**1.3. The processing shall cover the following the type of personal data:**

*[Describe the type of processed personal data].*

*[EXAMPLE. Name, surname, e-mail address, telephone number, address of the place of residence, national identification number (personal identification number), detailed information on payment, membership number, type of membership].*

*[NOTE. The description should be as detailed as possible, not limited to such statements as "personal data as defined in Article 4(1) of Regulation (EU) 2016/679" or only specification of the categories of personal data (i.e. Articles 6, 9 and/or 10 of Regulation (EU) 2016/679)].*

**1.4. The processing shall cover the following categories of data subjects:**

*[Describe the category of the data subject]*.

*[EXAMPLES. "Persons who are members of the loyalty programme of the Data Controller", "Natural persons who have subscribed e-mails", "Children to whom information society services are offered", "Customers from third countries"]*.

**1.5. The Data Processor shall be entitled to process personal data on behalf of the Data Controller after entry into force of the Clauses. Duration of processing:**

*[Describe the duration of processing]*.

_____

Annex 2 to
The standard contractual clauses for the data processing agreement

**INFORMATION ON SUB-PROCESSORS**

**1. Authorised sub-processors:**

Upon entry into force of the Clauses, the Data Controller shall allow to engage the following sub-processors:

| Corporate name, name, surname | Registration number/ individual activity certificate number or business licence number | Address of the registered office/address of the place of residence | Description of processing of personal data |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

Upon entry into force of the Clauses, the Data Controller shall allow the other Party to engage the sub-processors listed in this Annex hereto for the purposes provided for in paragraph 1.1 of Annex 1 to the Clauses in accordance with the requirements of Chapter VI hereof. In order to engage the afore-mentioned sub-processors for processing of personal data for the purposes other than the purposes provided for in paragraph 1.1 of Annex 1 hereto, a written authorisation of the Data Controller shall be required.

**2. Prior notification of granting authorisation to the new sub-processors**

*[Please specify the periods of a prior notification of granting authorisation to the new sub-processors and other related terms and conditions, for example, how information must be provided to the Data Controller, how the Data Controller must notify the Data Processor of his/its decision to grant authorisation (not to grant authorisation) to engage the particular new sub-processor etc. This Annex may also state if a separate auhotirsation of the Data Controller is necessary when renewal of the data processing agreement with the sub-processor is sought].*

_____

Annex 3 to
The standard contractual clauses for the data processing agreement

# INSTRUCTIONS ON PROCESSING OF PERSONAL DATA

## 1. Instruction to Process Data

The Data Processor shall carry out the following actions in the course of processing of personal data on behalf of the Data Controller:

*[Describe the processing entrusted to the Data Processor]*.

## 2. Security of Processing

The level of security shall be established taking into account:

*[Describe in detail taking into account the nature, scope, context and purposes of processing operations as well as the risk to the rights and freedoms of natural persons. Describe the elements which are relevant to the level of security.]*

*[EXAMPLE. In the light of the fact that processing of data is related to a large amount of personal data to which Article 9 of Regulation (EU) 2016/679 concerning special categories of personal data applies, "high" level of security should be established].*

The Data Processor shall be entitled and obliged to take decisions on use of technical and organisational security measures to ensure necessary (and agreed) level of security of the data.

However, in any case the Data Processor shall implement the following measures agreed with the Data Controller [*NOTE. The degree of detail of this list must be such as enable the Data Controller to assess the appropriateness of the measures to comply with its obligation of accountability*. *Parties should consider to include a description of the measures for the protection of software applications used to process personal data*]:

*[Describe the technical and/or organisational measures which must be applied by the Data Processor including conformity with the particular standards, recommendations or other good practices when processing personal data under the Clauses]*.

*[If applicable, describe the requirements for pseudonymisation and encryption of personal data]*.

*[Describe the requirements ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services]*.

*[Describe the requirements related to the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident]*.

*[Describe the requirements for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing]*.

*[Describe the requirements for access (including remote access) to personal data]*.

*[Describe the requirements for protection of personal data at the moment of communication of the data].*

*[Describe the requirements for protection of personal data during the period of storage of such data].*

*[Describe the requirements for physical security in the places in which personal data is stored].*

*[Describe the requirements for work at home/remote work].*

**3. Assistance to the Data Controller**

The Data Processor shall, insofar as this is possible and taking into account the area and scope of assistance specified below, assist the Data Controller to implement the following technical and organisational measures in accordance with paragraphs 26–28 of the Clauses:

*[Describe the scope and scale of the assistance provided by the Data Processor].*

*[Describe the particular technical and organisational measures which must be assumed by the Data Processor in order to assist the Data Controller].*

*[NOTE. This part should help the Data Processor to take certain action by certain means if one of the following issues arises, e. g. description of the steps to be taken or procedure to be followed in providing assistance to the Data Controller with regard to data breach notification, carrying out data protection impact assessments, data subject rights, assistance related to audit and etc., that has not been described in the Clauses.*

*[EXAMPLES: "Request of data subjects shall be without undue delay, but in any case, no later than [time limit specified] of receipt of the request, forward it to the Data Controller [means specified]", "Replies to data subjects shall be made in line with instructions of Data Controller", "In case of personal data breach, the Data Processor shall provide [information specified] to the Data Controller", "On the request of the Data Controller, the Data Processor provides extract of sub-processor's log book of the personal data breach [means and / duration for provision of this extract specified]", etc.]*

**4. Data Retention Period/Data Erasure Procedures**

*[Specify the data retention period/data erasure procedures intended for the Data Processor (if applicable, for example, how and within what time limits the Data Processor must demonstrate the fact of erasure of personal data].*

*[EXAMPLE 1. Personal data shall be stored [specify the period or event]; later, the Data Processor shall automatically delete personal data.*

*Having terminated provision of personal data processing services, the Data Processor shall [choose: delete or return] personal data in accordance with the requirements of paragraph 33 of the Clauses unless the Data Controller changes the initial choice of the Data Controller after signature of the Clauses. According to the Clauses, such amendments shall be documented].*

*[EXAMPLE 2. Personal data shall be stored [specify the period or event]; later, the Data Processor shall automatically delete personal data.*

*Having terminated provision of personal data processing services, the original documents transferred by the Data Controller to the Data Processor shall be returned to the Data Controller and copies of the documents shall be deleted and this shall be confirmed in writing except for the cases where storage of personal data is mandatory according to the legislation. The Data Processor shall also be obliged to notify the Data Controller about what personal data or copies thereof are not deleted and what law regulate this].*

**5. Data Processing Location**

According to the Clauses, personal data cannot be processed in other places, except for the locations specified below, without a prior written consent of the Data Controller:

*[Specify the locations in which data is processed] [Specify the address used by the Data Processor or sub-processor].*

**6. Instructions on Transfer of Personal Data to a Third Country or International Organisations**

*[Describe the instruction on transfer of personal data to a third country or international organisation].*

*[Specify the legal grounds for transfer of data according to Chapter V of Regulation (EU) 2016/679].*

If the Data Controller fails to indicate in the Clauses or later fails to provide the documented instructions on transfer of personal data to a third country or international organisations, the Data Processor shall not be entitled to carry out such transfer hereunder.

**7. Procedures for the Data Processor's Personal Data Processing Audits, Including on-the-spot Inspections, Carried Out by the Data Controller**

*[Describe the procedures for the Data Processor's personal data processing audits, including on-the-spot inspections, carried out by the Data Controller].*

*[EXAMPLE 1. "The Data Processor shall [specify how often] receive [choose: an audit report; an inspection report] on compliance with the requirements of Regulation (EU) 2016/679, valid personal data protection provisions of the European Union or its Member State and the Clauses from the independent third party designated by the Data Controller at the expense of the [Data Processor/Data Controller].*

*The Parties have agreed that, according to the Clauses, the following types of documents [choose: audit report/inspection report] may be used:*

*[Insert the approved audit reports/inspection reports].*

*The [choose: audit report/inspection report] shall be immediately provided to the Data Controller for information. The Data Controller shall be entitled to object to the scope and/or methods of the report and, in such cases, may request to carry out a new [choose: audit/inspection] according to the changed scope of application and/or other methods.*

*On the basis of the results of such [choose: audit/inspection], the Data Controller shall be entitled to request to adopt additional measures to ensure compliance with Regulation (EU) 2016/679, valid personal data protection provisions of the European Union or its Member State and the Clauses.*

*Furthermore, the Data Controller or the representative of the Data Controller shall be entitled to inspect the places, including their physical examination, in which the Data processor processes personal data including physical measures and systems used and related to data processing. Such inspection shall be carried out when the Data Controller believes that this is necessary]".*

*[EXAMPLE 2. "The Data Controller or the representative of the Data Controller shall [specify how often] physically examine the places in which the Data Processor processes personal data including physical measures and systems used and related to processing to make sure if the Data Processor complies with Regulation (EU) 2016/679, valid personal data protection provisions of the European Union or its Member State and the Clauses.*

*In addition to the scheduled inspection, the Data Controller shall also be entitled to carry out an inspection of the Data Processor when the Data Controller believes that this is necessary"].*

## 8. [If applicable] Procedures for Sub-Processors' Personal Data Processing Audits, Including on-the-spot Inspections

*[Describe the procedures for the sub-processors' personal data processing audits, including on-the-spot inspections, carried out by the Data Controller].*

*[EXAMPLE 1. The Data Processor shall [specify how often] receive [choose: an audit report; an inspection report] on compliance with the requirements of Regulation (EU) 2016/679, valid personal data protection provisions of the European Union or its Member State and the Clauses, from the independent third party designated by the Data Controller at the expense of the [Data Processor/Data Controller].*

*The Parties have agreed that, according to the Clauses, the following types of documents [choose: audit report/inspection report] may be used:*

*[Insert the approved audit reports/inspection reports].*

*The [choose: audit report/inspection report] shall be immediately provided to the Data Controller for information. The Data Controller shall be entitled to object to the scope and/or methods of the report and, in such cases, may request to carry out a new [choose: audit/inspection] according to the changed scope of application and/or other methods.*

*On the basis of the results of such [choose: audit/inspection], the Data Controller shall be entitled to request to adopt additional measures to ensure compliance with Regulation (EU) 2016/679, valid personal data protection provisions of the European Union or its Member State and the Clauses.*

*Furthermore, the Data Controller or the representative of the Data Controller shall be entitled to inspect the places, including their physical examination, in which the Data processor processes personal data including physical measures and systems used and related to data processing. Such inspection shall be carried out when the Data Controller believes that this is necessary.*

*The documents of such inspections shall be immediately provided to the Data Controller for information. The Data Controller shall be entitled to object to the scope and/or methods of the report and, in such cases, may request to carry out a new [choose: audit/inspection] according to the changed scope of application and/or other methods.]*

*[EXAMPLE 2. "The Data Controller or the representative of the Data Controller shall [specify how often] physically examine the places in which the sub-processor processes personal data including physical measures and systems used and related to processing to make sure if the sub-processor complies with Regulation (EU) 2016/679, valid personal data protection provisions of the European Union or its Member State and the Clauses.*

*In addition to the scheduled inspection, the Data Controller shall also be entitled to carry out an inspection of the sub-processor when the Data Controller believes that this is necessary.*

*The documents of such inspections shall be immediately provided to the Data Controller for information. The Data Controller shall be entitled to object to the scope and/or methods of the report and, in such cases, may request to carry out a new [choose: audit/inspection] according to the changed scope of application and/or other methods.]*

*On the basis of the results of such [choose: audit/inspection], the Data Controller shall be entitled to request to adopt additional measures to ensure compliance with Regulation (EU) 2016/679, valid personal data protection provisions of the European Union or its Member State and the Clauses.]*

*[If applicable, further to Example 2, specify the following: if necessary, the Data Controller shall be entitled to decide to initiate and take part in the physical inspection of the sub-processor. This may be applicable if the Data Controller believes that the Data Processor supervising the sub-processor has failed to provide sufficient documents to the Data Controller to determine if the sub-processor carries out processing under the Clauses.*

*Participation of the Data Controller's in the inspection of the sub-processor shall not change the fact that the Data Processor in questions is further fully liable for compliance of the sub-processor with Regulation (EU) 2016/679, valid personal data protection provisions of the European Union or its Member State and the Clauses.]*

_____