NATIONAL CENTER FOR PERSONAL DATA PROTECTION OF THE REPUBLIC OF MOLDOVA

MD-2004, mun. Chișinău, str. Serghei Lazo, 48, tel: (+373-22) 820801, 811801, fax: 820807, www.datepersonale.md

UNOFFICIAL TRANSLATION

ORDER NO 33

„22" Aprilie 2022

on the approval of the Standard Contract for the cross-border transfer of personal data to states that do not ensure an adequate level of personal data protection

REGISTERED:
Ministry of Justice
of the Republic of Moldova
no. 1716 of May 11, 2022
Minister _____ Sergiu LITVINENCO

Pursuant to Article 32 para. (5) let. i) of the Law No. 133/2011 on personal data protection (Official Gazette of the Republic of Moldova, 2011, No. 170-175, Art. 492), as amended,

I ORDER:

1. The Standard Contract for the cross-border transfer of personal data to states that do not ensure an adequate level of personal data protection (hereinafter - the Standard Contract) is hereby approved (is attached).

2. The National Centre for Personal Data Protection (NCPDP), following the control of the compliance of personal data processing, may order by decision, the suspension or cessation of the cross-border transfer of personal data by the parties involved, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data, if:

a) the national law of the controller or processor whose data processing activity is carried out in a State which does not ensure an adequate level of personal data protection obliges him or her not to comply with the Standard Contract and this is not motivated by reasons relating to national defense, national security, public order, the prevention, investigation and prosecution of criminal offences, important economic or financial interests of the State, activities carried out in the exercise of official authority

in the aforementioned areas, the protection of the personal data subject or of the fundamental rights and freedoms of others;

b) a competent personal data supervisory authority has established that the controller or processor whose data processing activity is carried out in a State which does not ensure an adequate level of personal data protection has not complied with the Standard Contract and the cross-border transfer of personal data presents a risk of prejudicing the rights of data subject.

3. The resumption of cross-border transfer of personal data by the parties involved may take place after the reasons for the measures referred to in paragraph 2 have ceased to apply, with prior notification to the NCPDP.

4. The provisions of this Order shall not affect the application of other legal provisions on personal data protection.

5. This Order shall enter into force on the date of its publication in the Official Gazette of the Republic of Moldova.

Victoria MUNTEAN
Director

UNOFFICIAL TRANSLATION

Approved by Order of the
National Center for Personal Data Protection
No. 33 of 22.04.2022

STANDARD CONTRACT

for the cross-border transfer of personal data to states that do not ensure an adequate level of personal data protection

(Standard contractual clauses)

SECTION I

CLAUSE 1 PURPOSE AND SCOPE

1. The purpose of these standard contractual clauses is to ensure compliance with the requirements of the Law No 133/2011 on personal data protection (hereinafter – Law No 133/2011) in the case of cross-border transfer of personal data.

2. The Parties:

a) the natural or legal person(s) under public or private law, public authority/ies, agency/ies, any other institution(s) or organization(s) [hereinafter "entity(ies)"] transferring the personal data, as listed in Annex 1 - Information on the cross-border transfer of personal data (hereinafter "Annex 1"), section A (hereinafter "data exporter"), and

b) the entity(ies) in a state that does not ensure an adequate level of personal data protection [hereinafter "other state"] receiving the personal data from the data exporter directly or indirectly via another entity also party to these clauses as listed in Annex No 1, Section A [hereinafter "data importer"]

have agreed to these standard contractual clauses.

3. These clauses apply with respect to the transfer of personal data as specified in Annex No 1, Section B.

4. The Annexes form an integral part of this contract, and it is necessary to make a clear distinction between the information applicable to each transfer or category of transfers and, to that end, to establish the role (s) of the parties as exporter (s); and / or data importer (s).

5. It is not necessary to complete and sign separate annexes for each transfer / category of transfers and / or contractual relationship, *where it is possible that the obligation of transparency will be respected if only one document is used*. Separate annexes shall be used if this is necessary to ensure sufficient clarity.

CLAUSE 2 EFFECT AND INVARIABLE CHARACTER OF THE CLAUSES

1. These clauses set out adequate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 32 (5) let. (i) of Law No 133/2011 and, with respect to data

transfers from controllers to controllers, from controllers to processors and/or from processors to controllers, provided they are not modified, except to select the appropriate module(s) or to add or update information in the Appendix. This does not prevent the parties from including the standard contractual clauses laid down in these clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these clauses or prejudice the fundamental rights or freedoms of data subjects.

2. These clauses are concluded by the parties in written form, presented on paper or in the form of an electronic document, signed with a qualified advanced electronic signature.

3. These clauses are without prejudice to obligations to which the data exporter is subject by virtue of the Law No 133/2011.

4. This contract will be concluded in the language (s) _____ (to be indicated by the parties).

CLAUSE 3 THIRD-PARTY BENEFICIARIES

1. Data subjects may invoke and enforce these clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

a) clause 1, clause 2, clause 3, clause 6, clause 7;

b) clause 8 - module 1: point 8.5, sbp. 5 and point 8.9, sbp. 2; module 2: pt. 8.1, sbp. 2, point 8.9, sbp. 1, 3, 4 and 5; module 3: point 8.1, sbp. 2 and point 8.3, sbp. 2;

c) clause 11 - module 1: points 1 and 4; module 2: points 1, 4 and 6;

d) clause 12;

e) clause 14, point 14.1, sbp. 3, 4, 5;

f) clause 15, point 5;

g) clause 17 - modules 1 and 2: points 1 and 2; module 3.

2. Point 1 is without prejudice to the rights of data subjects under Law No. 133/2011.

CLAUSE 4 INTERPRETATION

1. Where these clauses use terms that area defined in Law No 133/2011, those terms shall have the same meaning as in that law.

2. These clauses shall be read and interpreted in the light of the provisions of the Law No 133/2011.

3. These clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in the Law No 133/2011.

CLAUSE 5 HIERARCHY

1. In the event of a contradiction between these clauses and the provisions of related agreements between the parties, existing at the time these clauses are agreed or entered into thereafter, these clauses shall prevail.

2. If there are inconsistencies between these contractual clauses and the treaties on fundamental human rights to which the Republic of Moldova and the State of destination are a party, international regulations have priority.

CLAUSE 6 DESCRIPTION OF CROSS-BORDER TRANSFER (TRANSFERS)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex 1 Section B.

CLAUSE 7 - CLAUSE ON THE ADHERENCE OF NEW PARTIES [optional clause]

1. An entity that is not a party to these clauses may, with the agreement of the parties, accede to these clauses at any time, either as a data exporter or as a data importer, by completing the appendix and signing Annex 1 Section A.

2. Once it has completed the Appendix and signed Annex 1 Section A, the acceding entity shall become a party to these clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex 1 Section A.

3. The acceding entity shall have no rights or obligations arising under these clauses from the period prior to becoming a party.

SECTION II – OBLIGATIONS OF THE PARTIES

CLAUSE 8 DATA PROTECTION SAFEGUARDS

The data exporter warrants that it has used reasonable efforts to ensure that the data importer is able to meet its obligations under these clauses by implementing the necessary technical and organizational measures to protect personal data against destruction, alteration, blocking, copying, dissemination and other unlawful acts, which are designed to ensure an adequate level of security in relation to the risks presented by the processing and the nature of the data processed.

Module 1: Transfer controller to controller

8.1. Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex 1 Section B. It may only process the personal data for another purpose:

a) where it has obtained the data subject's prior consent;
b) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
c) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2. Transparency

1. In order to enable data subjects to effectively exercise their rights pursuant to clause 9, the data importer shall inform them, either directly or through the data exporter:

a) of its identity and contact details;

b) of the categories of personal data processed;

c) of the right to obtain a copy of these clauses;

d) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to point 8.7 of the clause 8.

2. Subpoint 1 shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

3. On request, the parties shall make a copy of these clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

4. Subpoints 1- 3 are without prejudice to the obligations of the data exporter under Article 12 of the Law No. 133/2011.

8.3. Accuracy and data minimisation

1. Each party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

2. If one of the parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other party without undue delay.

3. The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4. Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

8.5. Security of processing

1. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access, measures to ensure an adequate level of security with regard to the risks presented by the processing and the nature of the data processed.

2. The parties have agreed on the technical and organisational measures to ensure the security of personal data set out in Annex No 2 (hereinafter - Annex No 2). The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

3. The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4. In the event of a personal data breach concerning personal data processed by the data importer under these clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

5. The data importer shall keep documentation of all relevant elements relating to personal data breach, including documentation of the effects of personal data breach and any remedial action taken, and keep a record thereof.

8.6. Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, social affiliation, data concerning health or a person's sex life or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7. Onward transfers

The data importer shall not disclose personal data to a third party located in the same state as the data importer or in another state, hereinafter "onward transfer", unless the third party has obligations or agrees to be bound by these clauses, under the appropriate module. Otherwise, an onward transfer by the data importer may only take place if:

a) is performed to a state which is on the list of states ensuring an adequate level of personal data protection, approved by decision of the National Centre for Personal Data Protection;

b) is performed to other companies or organisations in the same group as the data controller, subject to compliance with mandatory corporate rules;

c) the transfer is necessary for the establishment, exercise or defence of a right in court, whether in the context of judicial proceedings or in the context of administrative or extra-judicial proceedings, including proceedings before regulatory authorities;

d) is necessary to protect the life, physical integrity or health of the data subject; or

e) with the consent of the data subject, with information on the possible risks that such transfers may involve for the data subject due to the lack of a decision on the adequate level of protection and adequate safeguards.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

1. Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

2. The data importer shall make such documentation available to the competent supervisory authority (hereinafter –hereinafter the Competent Supervisory Authority) request.

Module 2: Transfer controller to processor

8.1 Instructions

1. The data importer shall process the personal data only on documented instructions (contract or other legal act) from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

2. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex no.1.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex no.2 and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 12 of the Law no 133/2011.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex no.1, section B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of national laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that national law. This is without prejudice to Clause 13, in particular the requirement for the data importer under Clause 13, point 5 to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 13, point 1.

8.6 Security of processing

1. The data importer and also, during the transmission, the data exporter shall implement appropriate technical and organizational measures to ensure the security of personal data, for the protection of

personal data against destruction, alteration, blocking, copying, dissemination and other unlawful actions, which are designed to ensure an adequate level of security in relation to the risks presented by the processing and the nature of the data processed. In complying with its obligations under this paragraph, the data importer shall implement at least the technical and organizational measures specified in Annex 2. The data importer shall carry out regular checks to ensure that these measures continue to guarantee an adequate level of security.

2. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3. In the event of a personal data security breach in respect of personal data processed by the data importer under these clauses, the data importer shall take appropriate measures to remedy the data security breach, including measures to mitigate its adverse effects.

4. The data importer shall cooperate with and assist the data exporter in complying with its obligations under Law No 133/2011.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex 1 section B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions (contract or other legal act) from the data exporter. In addition, the data may only be disclosed to a third party (located in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

a) it is done to a State which is on the list of States ensuring an adequate level of data protection, approved by decision of the National Centre for Personal Data Protection of the Republic of Moldova;

b) to other companies or organizations from the same group as the data controller, provided that the mandatory corporate rules are complied with;

c) the transfer is necessary for establishing, exercising or defending a right in court, whether in the context of judicial proceedings or in the context of administrative or extra-judicial proceedings, including proceedings before regulatory authorities;

(d) it is necessary to protect the life, physical integrity or health of the subject of the personal data..;

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9. Documentation and compliance

1. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

2. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

3. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

4.The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

5.The Parties shall make the information referred to in sbp (2) and (3), including the results of any audits, available to the competent supervisory authority on request.

Module 3: Transfer processor to processor

8.1 Instructions

1. The data exporter processes personal data only on the basis of documented instructions (contract or other legal act) from the data importer acting as controller.

2. The data exporter shall immediately inform the data importer if it is unable to follow these instructions, including if these instructions violate Law No 133/2011 or other provisions of national data protection law.

3. The data importer shall not take any action that would prevent the data exporter from fulfilling its obligations under Law No 133/2011, including cooperation with the competent supervisory authorities.

4. After the end of the provision of processing services, the data exporter shall, at the choice of the data importer, either delete all personal data processed on behalf of the data importer and provide the data importer with proof that it has done so or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

1. The parties shall implement appropriate technical and organizational measures to ensure the security of personal data, including the protection of personal data against destruction, alteration, blocking, copying, dissemination and other unlawful actions, which are designed to ensure an adequate level of security in relation to the risks presented by the processing and the nature of the data processed.

2. The data exporter shall assist the data importer to ensure adequate data security in accordance with the provisions laid down in sbp 1.

3. The data exporter shall ensure that persons authorized to process personal data have undertaken to respect confidentiality or have an appropriate legal obligation of confidentiality.

8.3 Documentation and compliance

1. The parties must be able to demonstrate compliance with their obligations under these clauses.

2. The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these clauses and shall allow and contribute to audits.

CLAUSE 9 *DATA SUBJECTS' RIGHTS*

Module 1: transfer controller- controller

1. The data importer, where appropriate with the assistance of the data exporter, shall respond to all requests for information and other requests from a data subject which relate to the processing of his personal data and the exercise of his rights under these clauses, without undue delay, no later than one month after receipt. The data importer shall take appropriate measures to facilitate the making of such requests for information and other requests by data subjects and the exercise of data subjects' rights. Any information provided to the data subject shall be presented in an intelligible and easily accessible form, using clear and plain language.

2. In particular, at the request of the data subject and free of charge, the data importer:

(a) confirm to the data subject whether personal data relating to him or her are being processed and, if so, provide him or her with a copy of the data relating to him or her and inform him or her of the information provided for in Annex No.1 if the data subject's personal data have been or will be further transferred, it shall provide the data subject with information on the recipients or categories of recipients (to the extent appropriate for the purposes of providing relevant information) to whom the personal data have been or will be further transferred, the purpose of and the reasons for such further transfers pursuant to Clause 8, Module 1, point 8.7 of Module 1 of this Clause; and provide the data subject with information on the right to lodge a complaint to a supervisory authority under Clause 10, Modules 1 and 2, point 3(a);

(b) rectify inaccurate or incomplete data relating to the data subject;

c) delete personal data relating to the data subject if such data are or have been processed in breach of any of these clauses guaranteeing the rights of third party beneficiaries or if the data subject withdraws the consent on which the processing is based.

3. Where the data importer processes personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to such processing.

4. The data importer shall not take a decision based solely on automated processing of the personal data transferred (hereinafter referred to as "automated decision") which would produce legal effects concerning the data subject or would similarly affect him to a significant extent, unless it does so with the explicit consent of the data subject or is authorised to do so under the law of the country of destination, provided that that law provides for adequate measures to protect the rights and legitimate interests of the data subject. In this case, if necessary in cooperation with the data exporter, the data importer:

(a) informs the data subject of the intended automated decision and its intended consequences and of the logic involved; and

(b) implements appropriate safeguards allowing at least the data subject to challenge the decision, to express his or her point of view and to have the decision reviewed by a natural person.

5. Where requests from a data subject are excessive, in particular because of their repetitive nature, the data importer may either charge a reasonable fee, taking into account the administrative costs of dealing with the request, or refuse to process the request.

6. The data importer may refuse a data subject's request if the refusal is permitted under the law of the country of destination and it is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 15 of Law No 133/2011.

7. If the data importer intends to refuse a request from a data subject, he must inform the data subject of the reasons for the refusal and of the possibility to lodge a complaint with the supervisory authority and/or to challenge the refusal in court.

Module 2: Transfer controller to processor

1. The data importer shall promptly notify the data exporter of any request received from a data subject. He shall not respond to such a request until he has been authorised to do so by the data exporter.

2. The data importer shall assist the data exporter in fulfilling its obligations to respond to requests from data subjects regarding the exercise of their rights under Law No 133/2011. To this end, the parties shall set out in Annex No 2 the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance is to be provided, as well as the scope and extent of the assistance required.

3. In fulfilling of the obligations under point 1 and 2, the data importer shall comply with the instructions of the data exporter.

Module 3: Transfer processor - controller

The parties shall assist each other in responding to requests for information and other requests from data subjects under the national law applicable to the data importer or, in the case of data processing by the data exporter in the Republic of Moldova, under Law No 133/2011.

CLAUSE 10 *APPEALS*

1. The data importer shall inform data subjects in a transparent and easily accessible way, either by individual notification or on its website, of the contact point authorised to deal with complaints. It shall promptly resolve any complaints received from a data subject.

[OPTION: The data importer agrees that data subjects may also file a complaint with an independent dispute resolution body at no cost. It shall inform data subjects, in the manner set out in point 1, on this mechanism of appeal and inform them that they are not obliged to resort to it or to pursue the appeal in a particular order].

Module 1: Transfer controller - controller

Module 2: Transfer controller - processor

2. In the case of a dispute between the data subject and one of the parties regarding compliance with these clauses, the party concerned shall use its best efforts to resolve the dispute amicably in a timely manner. The parties shall inform each other of such disputes and, where appropriate, cooperate in resolving them.

3. If the personal data subject invokes a third-party beneficiary right under Clause 3, the data importer shall accept the data subject's decision:

(a) to lodge a complaint with the supervisory authority of the Republic of Moldova or with the competent supervisory authority under clause 12;

(b) to bring an action before the competent courts for the purposes of Clause 17.

4. The parties accept that the data subject may be represented by a non-profit body, organisation or association whose statutory objectives are in the public interest and which is active in the field of the protection of the rights and freedoms of personal data subjects with regard to the protection of personal data.

5. The data importer shall comply with the decision issued by the institutions referred to in point 3, which is binding under the applicable national law.

6. The data importer agrees that the choice made by the personal data subject will be without prejudice to his or her substantive and procedural rights to bring actions for damages under applicable law.

CLAUSE 11 *LIABILITY*

Module 1: Transfer controller to controller

Module 3: Transfer processor to controller

1. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

2. Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under art.33 of the Law no.133/2011.

3. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

4. The Parties agree that if one Party is held liable under point (3), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

5. The data importer may not invoke the conduct of a processor to avoid its own liability.

Module 2: Transfer controller to processor

1. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

2. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or moral damages the data importer or causes the data subject by breaching the third-party beneficiary rights under these Clauses.

3. Notwithstanding point (2), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer causes the data subject by breaching the third-party beneficiary rights under these Clauses.

4. The Parties agree that if the data exporter is held liable under point (3) for damages caused by the data importer, it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

5. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

6. The Parties agree that if one Party is held liable under point (5), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

7. The data importer may not invoke the conduct of a processor to avoid its own liability.

CLAUSE 12 SUPERVISION

Module 1: Transfer controller to controller

Module 2: Transfer controller to processor

1.The supervisory authority in which the data subject of this personal data are transferred under these clauses in connection with the provision of goods or services or the behavior is monitored, as provided in Annex no. 1, Section C, shall act as the competent supervisory authority.

2. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LAWS AND OBLIGATIONS APPLICABLE IN CASE OF ACCESS BY PUBLIC AUTHORITIES

CLAUSE 13 NATIONAL LEGISLATION AND PRACTICES AFFECTING COMPLIANCE WITH CLAUSES

Module 1: Transfer controller to controller

Module 2: Transfer controller to processor

Module 3: Transfer processor to controller

(*Where the RM processor combines the personal data received from the third country-controller with personal data collected by the processor in the RM*)

1. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 15 of Law no. 133/2011, are not in contradiction with these Clauses.

2. The Parties declare that in providing the warranty in point 1, they have taken due account in particular of the following elements:

a) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

b) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

c) any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination..

3. The data importer warrants that, in carrying out the assessment under point 2, it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

4. The Parties agree to document the assessment under point 2 and make it available to the competent supervisory authority on request.

5. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under point 1, including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in point 1.

6. Following a notification pursuant to point 5, or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 15 point (4) and (5) shall apply.

CLAUSE 14 OBLIGATIONS OF THE DATA IMPORTER IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Module 1: Transfer controller to controller

Module 2: Transfer controller to processor

Module 3: Transfer processor to controller

(where the RM processor combines the personal data received from the third country-controller with personal data collected by the processor in the RM)

14.1 Notification

1. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

a) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
b) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer; or

c) become aware of any accidental or unauthorized access, which has led to a breach of the security of personal data.

2. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

3. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

4. The data importer agrees to preserve the information pursuant to sbp. 3-5 for the duration of the contract and make it available to the competent supervisory authority on request.

5. Sbp. 1-3 are without prejudice to the obligation of the data importer pursuant to Clause 13 point 5 and Clause 15 to inform the data exporter promptly where it is unable to comply with these Clauses.

14.2 Review of legality and data minimisation

1. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 13 point 5.

2. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

3. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

CLAUSE 15 NON-COMPLIANCE WITH THE CLAUSES AND TERMINATION

1. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

2. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 13 point 6.

3. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

a) the data exporter has suspended the transfer of personal data to the data importer pursuant to point 2 and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

b) the data importer is in substantial or persistent breach of these Clauses; or

c) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

4. [For Modules One, and Two: Personal data that has been transferred prior to the termination of the contract pursuant to point 3 of this clause, shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Three: Personal data collected by the data exporter in the Republic of Moldova that has been transferred prior to the termination of the contract pursuant to point 3 shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that national law.

5. Either Party may revoke its agreement to be bound by these Clauses where National Centre of Personal Data Protection adopts a decision pursuant to Art. 32 para. (3) of Law no. 133/2011, that covers the transfer of personal data to which these Clauses apply. This is without prejudice to other obligations applying to the processing in question under Law no. 133/2011.

CLAUSE 16 GOVERNING LAW

Module 1: Transfer controller to controller

Module 2: Transfer controller to processor

Module 3: Transfer processor to controller

These contractual clauses are regulated by the legislation of the Republic of Moldova.

CLAUSE 17 CHOICE OF FORUM AND JURISDICTION

Module 1: Transfer controller to controller

Module 2: Transfer controller to processor

Module 3: Transfer processor to processor

1. Any dispute arising from these Clauses shall be resolved by the courts of Republic of Moldova.

2. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Republic of Moldova.

3. The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

INFORMAŢII PRIVIND TRANSMITEREA TRANSFRONTALIERĂ A DATELOR CU CARACTER PERSONAL

Section A. LIST OF PARTIES

Module 1: Transfer controller to controller

Module 2: Transfer controller to processor

Module 3: Transfer processor to controller

Data exporter(s): *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the Republic of Moldova]*

1.Name:
_____

Address:
_____

Contact person's name, position and contact details: _____

Activities relevant to the data transferred under these Clauses:: _____

Signature and date:
_____

Role (controller/processor): _____

2._____
___

(to be completed if there are several exporters)

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1.Name:
_____

Address:
_____

Contact person's name, position and contact details:: _____

Activities relevant to the data transferred under these Clauses: _____

Signature and date:
_____

Role (controller/processor): _____

2._____
___

(to be completed if there are several importers)

Section B. DESCRIPTION OF TRANSFER

Module 1: Transfer controller to controller

Module 2: Transfer controller to processor

Module 3: Transfer processor to controller

Categories of data subjects whose personal data is transferred

_____
__

Categories of personal data transferred

_____
__

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

_____
_

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

_____
__

Nature of the processing

_____
__

Purpose(s) of the data transfer and further processing

_____
__

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

_____
__

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Section C. COMPETENT SUPERVISORY AUTHORITY

Module 1: Transfer controller to controller

Module 2: Transfer controller to processor

Identify the competent supervisory authority (ies) in accordance with clause 12 of the Standard Contract for the cross-border transmission of personal data to States that do not provide an adequate level of protection of personal data.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Module 1: Transfer controller to controller

Module 2: Transfer controller to processor

Description of the technical and organizational measures implemented by the data importer (s) (including all relevant certifications) to ensure an adequate level of security of personal data.[1]

[Examples of possible measures:

- *Measures of pseudonymisation and encryption of personal data;*
- *Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
- *Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
- *Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing;*
- *Measures for user identification and authorisation;*
- *Measures for the protection of data during transmission;*
- *Measures for the protection of data during storage;*
- *Measures for ensuring physical security of locations at which personal data are processed; measures for ensuring events logging;*
- *Measures for ensuring system configuration, including default configuration;*
- *Measures for internal IT and IT security governance and management; measures for certification/assurance of processes and products;*
- *Measures for ensuring data minimisation;*
- *Measures for ensuring data quality;*
- *Measures for ensuring limited data retention; measures for ensuring accountability.*

[1] Technical and organizational measures must be described in a concrete (not generic) way.