



Republic of Moldova

**NATIONAL CENTER FOR PERSONAL DATA PROTECTION OF THE
REPUBLIC OF MOLDOVA**

ORDER No. 31 of 31 July 2026

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

Published: 7 August 2026 in the Official Gazette No. 363–366, Art. 644b

Pursuant to Article 28 paragraph (7) of Law No. 195/2024 on personal data protection
(Official Gazette of the Republic of Moldova, 2024, No. 367–396, Art. 574),

This Order transposes Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, published in the Official Journal of the European Union No. 199 of 7 June 2021, CELEX: 32021D0914.

I ORDER:

1. The Standard Contract for the transfer of personal data to states that do not ensure an adequate level of personal data protection (attached hereto) shall be approved.
2. The National Center for Personal Data Protection (NCPDP), following the exercise of the powers and duties established by Law No. 195/2024 on personal data protection, may order the suspension of data flows to a recipient in another state or to an international organisation, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data, where:
 - a) the national law of the controller or processor whose processing activity is carried out in a state that does not ensure an adequate level of personal data protection obliges it not to comply with the Standard Contract, and this is not motivated by reasons relating to national defence, national security, public order, the prevention, investigation and combating of criminal offences, important economic or financial interests of the State, activities carried

out in the exercise of official authority relating to the aforementioned areas, the protection of the data subject or the fundamental rights and freedoms of other persons;

b) a personal data supervisory authority competent for the processing has established that the controller or processor whose processing activity is carried out in a state that does not ensure an adequate level of personal data protection has failed to comply with the Standard Contract and the transfer of personal data presents a risk of prejudice to the rights of the data subject.

3. The resumption of the transfer of personal data by the parties involved may take place after the grounds that determined the application of the measures referred to in point 2 have ceased to exist, 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 be published in the Official Gazette of the Republic of Moldova and shall enter into force on 23 August 2026.

6. On the date of entry into force of this Order, Order No. 33/2022 of the Director of the National Center for Personal Data Protection 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 (Official Gazette of the Republic of Moldova, 2022, No. 151–157, Art. 584), registered with the Ministry of Justice under No. 1716 of 11 May 2022, shall be repealed.

Director

Victoria MUNTEAN

No. 31. Chişinău, 31 July 2026.

Approved by Order of the Director of the
National Center for Personal Data Protection
No. 31/2026

**STANDARD CONTRACT
for the 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 Law No. 195/2024 on personal data protection (hereinafter – *Law No. 195/2024*) in the case of the transfer of personal data to states that do not ensure an adequate level of personal data protection (hereinafter – *transfer of personal data*).

2. The Parties:

a) the natural or legal person(s) under public or private law, including public authority/ies, any other institution(s) or organisation(s) (hereinafter – *entity/entities*) transferring the personal data, as listed in Annex No. 1 – Information on the transfer of personal data (hereinafter – *Annex No. 1*), Section A (hereinafter – *data exporter*); and

b) the entity/entities 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, through another entity that is also a party to these clauses, as listed in Annex No. 1, Section A (hereinafter – *data importer*), have agreed to these standard contractual clauses (hereinafter – *clauses*).

3. These clauses shall apply 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 a clear distinction shall be made between the information applicable to each transfer or category of transfers and, for this purpose, the role(s) of the parties as data exporter(s) and/or data importer(s) shall be established.

5. It is not mandatory to complete and sign separate annexes for each transfer/category of transfers and/or contractual relationship *where the transparency obligation can be complied with by using a single document*. Separate annexes shall be used where 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 46 paragraphs (1) and (2) letter c) of Law No. 195/2024 and, with respect to transfers of data from controllers to processors and/or from processors to processors, standard contractual clauses pursuant to Article 28 paragraph (7) of Law No. 195/2024, provided that they are not modified, except for the selection of the appropriate module(s) or the addition or updating of information provided in the Annexes. This does not prevent the parties from including the standard contractual clauses laid down herein in a wider contract and/or from adding 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 shall be concluded by the parties in writing, either on paper or in the form of an electronic document signed with a qualified advanced electronic signature.

3. These clauses are without prejudice to the obligations incumbent upon the data exporter under Law No. 195/2024.

4. This contract shall be concluded in Romanian and/or English (as 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 and Clause 7;
- b) Clause 8 – Module 1: point 8.5, subpoint 5 and point 8.9, subpoint 2; Module 2: point 8.1, subpoint 2, point 8.9, subpoints 1, 3, 4 and 5; Module 3: point 8.1, subpoints 1, 3 and 4 and point 8.9, subpoints 1, 3, 4, 5, 6 and 7; Module 4: point 8.1, subpoint 2 and point 8.3, subpoint 2;
- c) Clause 9 – Module 2: subpoints 1, 3, 4 and 5; Module 3: subpoints 1, 3, 4 and 5;
- d) Clause 12 – Module 1: points 1 and 4; Modules 2 and 3: points 1, 4 and 6;
- e) Clause 13;
- f) Clause 15, point 15.1, subpoints 3, 4 and 5;
- g) Clause 16, point 5;
- h) Clause 18 – Modules 1, 2 and 3: points 1 and 2; Module 4.

2. Point 1 is without prejudice to the rights of data subjects under Law No. 195/2024.

CLAUSE 4. INTERPRETATION

1. Where these clauses use terms defined in Law No. 195/2024, 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 Law No. 195/2024.
3. These clauses shall not be interpreted in a way that conflicts with the rights and obligations provided for in Law No. 195/2024.

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 treaties on fundamental human rights to which the Republic of Moldova and the State of destination are parties, the international treaties shall prevail.

CLAUSE 6. DESCRIPTION OF THE TRANSFER(S)

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 No. 1, Section B.

CLAUSE 7. CLAUSE ON THE ACCESSION 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 as a data exporter or data importer by completing and signing Annex No. 1, Section A.
2. Upon completion and signing of Annex No. 1, Section A, the acceding entity shall become a party to these clauses and shall have the rights and obligations of a data exporter or data importer, in accordance with its designation in Annex No. 1, Section A.
3. The acceding entity shall have no rights or obligations arising under these clauses for the period preceding its accession as 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 fulfil its obligations under these clauses by implementing appropriate technical and organisational measures.

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 No. 1, Section B. It may process the personal data for another purpose only:

- a) where it has obtained the data subject's prior consent;
- b) where necessary for the establishment, exercise or defence of a legal claim in the context of specific administrative, regulatory or judicial proceedings; or
- c) where necessary 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 under Clause 10, 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), as well as of the purpose and legal ground for such onward transfer pursuant to point 8.7 of Clause 8.

2. Subpoint 1 shall not apply where the data subject already has the information, including where such information has already been provided by the data exporter, or where 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 Annex 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 personal

data, the parties may redact part of the text of the Annexes before providing a copy, but shall provide a meaningful summary where, without such summary, the data subject would not be able to understand its content or exercise his or her rights. Upon request, the parties shall inform the data subject of the reasons for the redaction, to the extent possible without disclosing the redacted information.

4. Subpoints 1–3 are without prejudice to the obligations incumbent upon the data exporter under Articles 13 and 14 of Law No. 195/2024.

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 all reasonable steps to ensure that personal data which is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

2. Where 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 implement appropriate technical or organisational measures to ensure compliance with this obligation, including the erasure or anonymisation, (in a manner ensuring that the natural person can no longer be identified by anyone and that the process is irreversible) 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 personal data breach leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data (hereinafter referred to as a *personal data breach*). When assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks to which data subjects are exposed as a result of the processing. In particular, the parties shall consider the use of

encryption or pseudonymisation, including during transmission, where such measures do not prevent the fulfilment of the purpose of processing.

2. The parties have agreed on the technical and organisational measures intended 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 guarantee an adequate level of security.

3. The data importer shall ensure that persons authorised to process 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 any adverse effects.

5. In case of a personal data breach likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority under Clause 13. Such notification shall contain:

a) a description of the nature of the personal data breach (including, where possible, categories and approximate number of data subjects and personal data records concerned);

b) the likely consequences of the personal data breach;

c) the measures taken or proposed to be taken to address the personal data breach; and

d) the details of a contact point from whom more information can be obtained. Where the data importer is unable to provide all the information at the same time, it may provide the information in stages, without undue further delay.

6. In case of a personal data breach likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify, without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in point 5, letters b)–d), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

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

8.6. Special categories of personal 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 – *special categories of personal data*), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. These may include restricting access to the personal data to authorised personnel, additional security measures (such as pseudonymization) and/or additional restrictions on 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 referred to as an “*onward transfer*”, unless the third party has obligations or agrees to assume obligations under these clauses, under the appropriate module. Otherwise, an onward transfer by the data importer may take place only if:

- a) it is made to a state included in the list of states ensuring an adequate level of data protection, approved by decision of the National Center for Personal Data Protection;
- b) the third party otherwise ensures adequate safeguards pursuant to Article 46 or 47 of Law No. 195/2024 with regard to the processing in question;
- c) the third party enters into a legally binding instrument with the data importer ensuring the same level of data protection as that provided under these clauses, and the data importer provides the data exporter with a copy of such safeguards;
- d) it is necessary for the establishment, exercise or defence of a legal claim in the context of specific administrative, regulatory or judicial proceedings;
- e) it is necessary to protect the vital interests of the data subject or of another natural person;
or
- f) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject to an onward transfer in a specific situation, after having

informed the data subject of its purpose(s), the identity of the recipient and the possible risks of such transfer to the data subject due to the absence of adequate data protection safeguards. In such case, the data importer shall inform the data exporter and, upon request, provide it with a copy of the information provided to the data subject.

Any onward transfer shall be subject to compliance by the data importer with all the other safeguards provided for in these clauses, in particular purpose limitation.

8.8. Processing under the authority of the data importer

The data importer shall ensure that no 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 concerning the processing activities carried out under its responsibility.
2. The data importer shall make such documentation available to the competent personal data supervisory authority (hereinafter – *competent supervisory Authority*) upon 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 issue 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, Section B, unless it receives further instructions from the data exporter.

8.3. Transparency

Upon request, the data exporter shall make a copy of these clauses, including the Annex 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 provided for in Annex No. 2 and personal data, the data exporter may redact part

of the text of the Annexes before providing a copy, but shall provide a meaningful summary where, without such summary, the data subject would not be able to understand its content or exercise his or her rights. On request, the parties shall inform the data subject of the reasons for the redaction, to the extent possible without disclosing the redacted information. This clause is without prejudice to the obligations incumbent upon the data exporter under Articles 13 and 14 of Law No. 195/2024.

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 such 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 take place only 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. Where national law applicable to the data importer prohibits the return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these clauses and shall process the data only to the extent and for as long as required by that national law. This is without prejudice to Clause 14, in particular the obligation incumbent upon the data importer under Clause 14, 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 that are not in compliance with Clause 14, point 1.

8.6. Security of processing

1. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organizational measures to ensure the security of personal data, including protection against a personal data breach leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to personal data (hereinafter – *personal data breach*). When assessing the appropriate level of security, the parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing, and the risks to which data subjects are exposed as a result of the processing. In particular, the parties shall consider the use of encryption or pseudonymization, including during transmission, where this does not prevent the

fulfilment of the purpose of processing. In the case of pseudonymization, the additional information enabling the attribution of the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with the obligations under this point, the data importer shall implement at least the technical and organizational measures specified in Annex No. 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 members of its personnel access to personal data only to the extent strictly necessary for the implementation, management and monitoring of the contract. The data exporter shall ensure that persons authorized to process personal data have committed themselves to confidentiality or are under an appropriate legal obligation of confidentiality.

3. In the case of a personal data breach concerning personal data processed by the data importer under these clauses, the data importer shall take appropriate measures to remedy the personal data breach, including measures to mitigate its adverse effects. After becoming aware of such personal data breach, the data importer shall notify the data exporter without undue delay the controller. The notification shall contain the contact details of a contact point from which further information may be obtained, a description of the nature of the personal data breach (including, where possible, the categories of data subjects concerned, as well as the approximate number of data subjects and personal data records concerned), the likely consequences of the personal data breach, and the measures taken or proposed to be taken to remedy the personal data breach, including, where appropriate, measures to mitigate any adverse effects. Where and to the extent that it is not possible to provide all information at the same time, the initial notification shall contain the information available at that time, with further information to be provided subsequently, without undue delay, as it becomes available.

4. The data importer shall cooperate with and assist the data exporter in complying with its obligations under Law No. 195/2024, in particular to inform the competent supervisory authority and the affected data subjects, taking into account the nature of the processing and the information available to the data importer.

8.7. Special categories of personal 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 – *special categories of personal data*), the data importer shall

apply the specific restrictions and/or additional safeguards described in Annex No. 1, Section B.

8.8. Onward transfers

The data importer shall disclose personal data to a third party only on the basis of documented instructions (contract or other legal act) from the data exporter. In addition, personal data may be disclosed to a third party (located in the same country as the data importer or in another third country, hereinafter referred to as an *onward transfer*), only if the third party is subject to or agrees to assume obligations under these clauses, under the appropriate module, or if:

- a) the onward transfer is made to a state included in the list of states ensuring an adequate level of data protection, approved by decision of the National Center for Personal Data Protection of the Republic of Moldova;
- b) the third party otherwise ensures adequate safeguards pursuant to Article 46 or 47 of Law No. 195/2024;
- c) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- d) the onward transfer is necessary to protect the vital interests of the data subject or of another natural person.

Any onward transfer shall be subject to compliance by the data importer with all the other safeguards provided for in these clauses, in particular purpose limitation.

8.9. Documentation and compliance

1. The data importer shall promptly and adequately respond to requests for information from the data exporter relating to the processing carried out under these clauses.
2. The parties shall be able to demonstrate compliance with their obligations under these clauses. In particular, the data importer shall keep appropriate documentation concerning 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 provided for in these clauses and, at the request of the data exporter, shall allow audits of the processing activities covered by these clauses to be carried out and shall contribute to such audits, at reasonable intervals or where there are indications of non-compliance. In deciding whether to carry out a review or an

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 itself or mandate an independent auditor for this purpose. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out following reasonable notice.

5. Upon request, the parties shall make available to the competent supervisory authority the information referred to in subpoints 2 and 3, including the results of any audit.

Module 3: Transfer processor to processor

8.1. Instructions

1. The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

2. The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

3. The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller

4. The data exporter shall ensure that it has imposed on the data importer the same data protection obligations as those provided for in the contract or other legal act under Law No. 195/2024 or other provision of national data protection legislation, concluded between the controller and the data exporter.

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, Section B, unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3. Transparency

On request, the data exporter shall provide the data subject, free of charge, with a copy of these clauses, as completed by the parties. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the annexes 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.

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 rectify or erase the data.

8.5. Duration of processing and erasure or return of data

The processing by the data importer shall take place only 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 controller 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 deletion or return of the data, the data importer shall continue to ensure compliance with these clauses. Where the national law applicable to the data importer prohibits the return or deletion of personal data, the data importer shall guarantee that it will continue to ensure compliance with these clauses and shall process the data only to the extent and for as long as the processing is permitted by that law. This provision shall be without prejudice to Clause 14, in particular to the obligation of the data importer under Clause 14, 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 that are not in compliance with the provisions of Clause 14, point 1.

8.6. Security of processing

1. The data importer and, also during transmission, the data exporter shall implement appropriate technical and organisational measures necessary for the protection of personal data against destruction, modification, blocking, copying, dissemination, as well as against other unlawful actions, measures aimed at ensuring an adequate level of security in relation to the risks presented by the processing and the nature of the data processed. When assessing the appropriate level of security, the parties shall take due account of the state of

the art, the costs of implementation, the nature, scope, context and purpose(s) of processing, and the risks to which data subjects are exposed as a result of the processing. In particular, the parties shall consider the use of encryption or pseudonymization, including during transmission, where this does not prevent the fulfilment of the purpose of processing. In the case of pseudonymization, the additional information enabling the attribution of the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with the obligations under this point, the data importer shall implement at least the technical and organizational measures specified in Annex No. 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 members of its personnel access to the data only to the extent strictly necessary for the implementation, management and monitoring of the contract. The data exporter shall ensure that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate legal obligation of confidentiality.

3. 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 remedy the personal data breach, including measures to mitigate its adverse effects. After becoming aware of the personal data breach, the data importer shall notify the data exporter without undue delay and, where appropriate and feasible, the controller. The notification shall contain the contact details of a contact point from which further information may be obtained, a description of the nature of the personal data breach (including, where possible, the categories of data subjects concerned and the approximate number of data subjects and personal data records concerned), the likely consequences of the personal data breach and the measures taken or proposed to remedy the breach, including, where appropriate, measures to mitigate any adverse effects. Where and to the extent that it is not possible to provide all information at the same time, the initial notification shall contain the information available at that time, with further information to be provided subsequently, without undue delay, as it becomes available.

4. The data importer shall cooperate with and assist the data exporter in complying with its obligations under Law No. 195/2024, in particular the obligation to notify its controller, so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of the processing and the information available to the data importer.

8.7. Special categories of personal 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 – *special categories of personal data*), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex No. 1, Section B.

8.8. Onward transfers

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

- a) the onward transfer is made to a state included in the list of states ensuring an adequate level of data protection, approved by decision of the National Center for Personal Data Protection of the Republic of Moldova;
- b) the third party otherwise ensures adequate safeguards pursuant to Article 46 or 47 of Law No. 195/2024;
- c) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- d) the onward transfer is necessary to protect the vital interests of the data subject or of another natural person.

Any onward transfer shall be subject to compliance by the data importer with all the other safeguards provided for in these clauses, in particular purpose limitation.

8.9. Documentation and compliance

1. The data importer shall promptly and adequately respond to requests for information from the data exporter or the controller relating to the processing carried out under these clauses.
2. The parties shall be able to demonstrate compliance with their obligations under these clauses. In particular, the data importer shall keep appropriate documentation concerning the processing activities carried out on behalf of the controller.

3. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations provided for in these clauses, and the data exporter shall provide such information to the controller.
4. The data importer shall allow the data exporter to carry out audits of the processing activities covered by these clauses and shall contribute to such audits, at reasonable intervals or where there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.
5. Where the audit is carried out at the controller's instruction, the data exporter shall make the results available to the controller.
6. The data exporter may choose to conduct the audit itself or mandate an independent auditor for this purpose. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
7. Upon request, the parties shall make available to the competent supervisory authority the information referred to in points 2 and 3, including the results of any audit.

Module 4: Transfer processor to controller

8.1. Instructions

1. The data exporter shall process 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 such instructions, including where such instructions infringe Law No. 195/2024 or other provisions of national data protection legislation.
3. The data importer shall not take any action that would prevent the data exporter from fulfilling its obligations under Law No. 195/2024, including with regard to cooperation with the competent supervisory authorities.
4. After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer 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 organisational measures to ensure the security of personal data, including during transmission, and protection against a personal data breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of personal data or unauthorised access to it. When assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data (7), the nature, scope, context and purpose(s) of the processing and the risks posed by the processing to data subjects and, in particular, shall consider the use of encryption or pseudonymisation, including during transmission, where this does not prevent the fulfilment of the purpose of the processing.

2. The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with the provisions set out in subpoint 1. In case of a personal data breach concerning personal data processed by the data exporter under these clauses, the data exporter shall notify the data importer of such breach without undue delay after becoming aware of it and shall assist the data importer in remedying the breach.

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

8.3. Documentation and compliance

1. The parties shall 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 for and contribute to audits.

CLAUSE 9. USE OF SUB-PROCESSORS

Module 2: Transfer controller to processor

1. OPTION 1: SPECIFIC PRIOR AUTHORISATION. The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [*specify period*] prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-

processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION. The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*specify period*] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

2. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by means of a written contract which provides, in substance, for the same data protection obligations as those imposed on the data importer under these clauses, including with regard to third-party beneficiary rights for data subjects. The parties agree that, by complying with this clause, the data importer fulfils its obligations under Clause 8, point 8.8. The data importer shall ensure that the sub-processor complies with the obligations imposed on the data importer under these clauses.

3. The data importer shall provide the data exporter, at its request, with a copy of such a subcontracting contract and any subsequent amendments thereto. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the contract before providing a copy.

4. The data importer shall remain fully responsible towards the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

5. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Module 3: Transfer processor to processor

1. OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not subcontract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the prior specific written authorisation of the controller. The data importer shall submit the request for specific authorisation at least

[*specify period*] prior to the engagement of the sub-processor, together with the information necessary to enable the controller to decide on the authorisation. It shall inform the data exporter of such engagement. The list of sub-processors already authorised by the controller can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*specify period*] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

2. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by means of a written contract which provides, in substance, for the same data protection obligations as those imposed on the data importer under these clauses, including with regard to third-party beneficiary rights for data subjects. The parties agree that, by complying with this clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations imposed on the data importer under these clauses.

3. The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

4. The data importer shall remain fully responsible towards the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

5. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

CLAUSE 10. DATA SUBJECTS' RIGHTS

Module 1: Transfer controller to controller

UNOFFICIAL TRANSLATION

1. The data importer shall, where applicable with the assistance of the data exporter, respond to all requests for information and other requests from a data subject relating to the processing of their personal data and the exercise of their rights under these clauses, without undue delay and within a maximum of one month of receipt thereof. The data importer shall take appropriate measures to facilitate the submission of such requests for information and other requests by data subjects, as well as the exercise of the rights of data subjects. 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 shall:

a) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex No. 1; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8, Module 1, point 8.7; and inform the data subject of the right to lodge a complaint with a supervisory authority in accordance with Clause 11, Modules 1 and 2, point 3(a);

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

c) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, 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 such processing where the data subject objects to the processing.

4. The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter – *automated decision-making*) which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

a) inform the data subject about the envisaged automated-making, the envisaged consequences and the logic involved; and

b) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a by natural person.

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

6. The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23 paragraph (1) of Law No. 195/2024.

7. If the data importer intends to refuse a request from a data subject, it shall inform the data subject of the reasons for the refusal and of the possibility of lodging a complaint with the Supervisory Authority and/or bringing an action before a court.

Module 2: Transfer controller to processor

1. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it 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 concerning the exercise of their rights under Law No. 195/2024. In this regard, 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 shall be provided, as well as the scope and the extent of the assistance required.

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

Module 3: Transfer processor to processor

1. The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

2. The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Law No. 195/2024 or other normative acts, as applicable. In this regard, the parties shall specify in Annex No. 2 the appropriate technical and

organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

3. In fulfilling its obligations under points 1 and 2, the data importer shall comply with the instructions of the controller as communicated by the data exporter.

Module 4: Transfer processor to controller

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the national legislation applicable to the data importer or, where the data are processed by the data exporter in the Republic of Moldova, under Law No. 195/2024.

CLAUSE 11. REDRESS

1. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in point 1, of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

Module 1: Transfer controller to controller

Module 2: Transfer controller to processor

Module 3: Transfer processor to processor

2. In case of a dispute between the data subject and one of the parties concerning 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. Where the data subject invokes a third-party beneficiary right under Clause 3 the data importer shall accept the decision of the data subject to:

- a) lodge a complaint with the supervisory authority in the Republic of Moldova or with the competent supervisory authority under Clause 13;
- b) refer the dispute to the competent courts within the meaning of Clause 18.

4. The parties accept that the data subject may be represented by a body, organisation or non-profit association under the conditions laid down in Article 75 of Law No. 195/2024.

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

6. The data importer agrees that the choice made by the data subject shall not affect the data subject's substantive and procedural rights to bring actions for damages in accordance with the applicable legislation.

CLAUSE 12. LIABILITY

Module 1: Transfer controller to controller

Module 4: Transfer processor to controller

1. Each party shall be liable to the other party/parties for any damage it causes to the other party/parties 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 damage which the party causes to the data subject by breaching the third-party beneficiary rights under these clauses. This provision shall be without prejudice to the liability of the data exporter under Article 33 of Law No. 195/2024.

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 shall have the right to bring an action in court against any of those parties.

4. The parties agree that where the liability of one of the parties is established under point 3, that party shall be entitled to seek, amicably or, in the event of a dispute, through the courts, recovery from the other party/parties of that part of the compensation corresponding to its/their share of liability for the damage caused.

5. The data importer may not rely on the conduct of a processor in order to avoid liability.

Module 2: Transfer controller to processor

Module 3: Transfer processor to processor

1. Each party shall be liable to the other party or parties for any damages which it causes to the other party or parties 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 non-material damage which the data importer

or its sub-processor causes to the data subject by breaching the third-party beneficiary rights under these clauses.

3. Without prejudice to the provisions of 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 damage which the data exporter or the data importer (or its sub-processor) causes to 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 damage caused by the data importer (or its sub-processor), 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 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 shall be entitled to seek redress for the damage caused amicably and, in the event of disputes, to bring legal proceedings against any of those 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 rely on the conduct of a processor or a sub-processor in order to avoid liability.

CLAUSE 13. SUPERVISION

Module 1: Transfer controller to controller

Module 2: Transfer controller to processor

Module 3: Transfer processor to processor

1. The supervisory authority of the state in which the data subject whose personal data are transferred under these clauses is located, in connection with the offering of goods or services or the monitoring of his or her behaviour, as specified in Annex No. 1, Section C, shall act as the competent supervisory authority.

2. The data importer agrees to submit to the jurisdiction of the competent supervisory authority and to cooperate with it in any procedures aimed at ensuring compliance with these clauses. In particular, the data importer agrees to respond to requests for information, to be subject to audits, and to comply with 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 – APPLICABLE LEGISLATION AND OBLIGATIONS
IN THE CASE OF ACCESS BY PUBLIC AUTHORITIES
CLAUSE 14. NATIONAL LEGISLATION AND PRACTICES AFFECTING
COMPLIANCE WITH THE CLAUSES**

Module 1: Transfer controller to controller

Module 2: Transfer controller to processor

Module 3: Transfer processor to processor

Module 4: Transfer processor-to-controller (where the processor in the Republic of Moldova combines the personal data received from the controller in another state with personal data collected in the Republic of Moldova by the processor)

1. The parties warrant that they have no reason to believe that the laws and practices in another state applicable to the processing of personal data by the data importer, including any requirements to disclose personal data or measures authorising 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 go beyond what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Law No. 195/2024 are not in contradiction with these clauses.

2. The parties declare that, in providing the guarantee referred to 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; the intended onward transfers; the type of recipient; the purpose of the processing; the categories and format of the personal data transferred; the economic sector in which the transfer takes place; the location where the transferred data are stored;

b) the laws and practices of the destination state – including those requiring the disclosure of data to public authorities or authorising access by such authorities – which are relevant in light of the specific circumstances of the transfer, as well as the applicable limitations and safeguards;

c) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards provided for in these clauses, including measures applied during the transmission and processing of personal data in the destination state.

3. The data importer warrants that, in carrying out the assessment referred to in point 2, it has made all efforts to provide the data exporter with the relevant information and agrees to continue cooperating with the data exporter to ensure compliance with these clauses.

4. The parties agree to document the assessment referred to in point 2 and to make it available to the competent supervisory authority, upon request.

5. The data importer agrees to promptly notify the data exporter if, after agreeing to these clauses and throughout the duration of the contract, it has reason to believe that it is or has become subject to legislation or practices that are not in compliance with the provisions set out in point 1, including following an amendment to the legislation of its state or a measure (such as a disclosure request) indicating that such legislation is being applied in practice in a manner that is not in compliance with the provisions set out in point 1. [For Module 3: The data exporter shall transmit the notification to the controller.]

6. Following a notification under point 5 or where the data exporter has other reasons to believe that the data importer can no longer fulfil its obligations under these clauses, the data exporter shall promptly identify the appropriate measures (for example, technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or the data importer to remedy the situation. The data exporter shall suspend the transfer of data where it considers that adequate safeguards cannot be ensured for such transfer or where it receives instructions to that effect from the competent supervisory authority. In such case, the data exporter shall be entitled to terminate the contract insofar as it concerns the processing of personal data under these clauses. Where the contract involves more than two parties, the data exporter may exercise its right to terminate the contract only with regard to the party concerned, unless the parties have agreed otherwise. Where the contract is terminated under this clause, Clause 16, points 4 and 5 shall apply.

CLAUSE 15. 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 processor

Module 4: Transfer processor to controller (where the processor in the Republic of Moldova combines the personal data received from the controller in another state with personal data collected in the Republic of Moldova by the processor)

15.1. 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) becomes aware of any accidental or unauthorised access that has resulted in a personal data breach.

[For Module 3: The data exporter shall transmit the notification to the controller.]

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.). [For Module 3: The data exporter shall transmit the notification to the controller.]

4. The data importer agrees to retain the information referred to in subpoints 1–3 for the duration of the contract and to make it available to the competent supervisory authority upon request.

5. Subpoints 1–3 are without prejudice to the obligation incumbent upon the data importer under Clause 14, point 5, and Clause 16 to promptly inform the data exporter if it is unable to comply with these clauses.

15.2. 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 14, 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. [For Module 3: The data exporter shall make the assessment available to the controller.]

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

SECTION IV – FINAL PROVISIONS

CLAUSE 16. 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 14, point 6.

3. The data exporter shall have the right 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 under point 2 and compliance with these clauses is not restored within a reasonable period and, in any event, within one month of the suspension;
- b) the data importer has substantially or repeatedly breached these clauses; or
- c) the data importer fails to comply with a binding decision of a competent court or competent supervisory authority concerning its obligations under these clauses.

In such cases, the data exporter shall inform the competent supervisory authority of the non-compliance. Where the contract involves more than two parties, the data exporter may exercise its right to terminate only with regard to the party concerned, unless the parties have agreed otherwise.

4. [For Modules 1, 2 and 3: Personal data that were transferred prior to termination of the contract under point 3 of this clause shall be immediately returned to the data exporter or completely erased, at the choice of the data exporter. The same shall apply to any copies of the data.] [For Module 4: Personal data collected by the data exporter in the Republic of Moldova that were transferred prior to termination of the contract under point 3 shall be immediately and completely erased, including any copies thereof.] The data importer shall provide the data exporter with proof of the erasure of the data. Until the data are erased or returned, the data importer shall continue to ensure compliance with these clauses. Where national law applicable to the data importer prohibits the return or erasure of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these clauses and shall process the data only to the extent and for as long as required under that national law.

5. Either party may revoke its agreement to assume obligations under these clauses where the National Center for Personal Data Protection adopts a decision pursuant to Article 45 paragraph (3) of Law No. 195/2024 concerning the transfer of personal data to which these clauses apply. This provision shall be without prejudice to any other obligations applicable to the processing in question under Law No. 195/2024.

CLAUSE 17. GOVERNING LAW

Module 1: Transfer controller to controller

Module 2: Transfer controller to processor

Module 3: Transfer processor to processor

Module 4: Transfer processor to controller

These contractual clauses shall be governed by the legislation of the Republic of Moldova.

CLAUSE 18. CHOICE OF FORUM AND JURISDICTION

Module 1: Transfer controller to controller

Module 2: Transfer controller to processor

Module 3: Transfer processor to processor

Module 4: Transfer processor to controller

1. Any dispute arising from these clauses shall be resolved by the courts of the Republic of Moldova.
2. A data subject may bring legal proceedings against the data exporter and/or data importer in the Republic of Moldova.
3. The parties agree to submit themselves to the jurisdiction of such courts.

ANNEX No. 1

INFORMATION RELATING TO THE TRANSFER OF PERSONAL DATA

SECTION A. LIST OF PARTIES

Module One: Transfer controller to controller

Module Two: Transfer controller to processor

Module Three: Transfer processor to processor

Module Four: 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 where there are multiple data exporters)

Data importer(s): *[Identity and contact details of the data importer(s), including any contact person responsible 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 where there are multiple data importers)

SECTION B. DESCRIPTION OF THE TRANSFER

Module One: Transfer controller to controller

Module Two: Transfer controller to processor

Module Three: Transfer processor to processor

Module Four: Transfer processor to controller

Categories of data subjects whose personal data is transferred

Categories of personal data transferred

Special categories of personal 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, where that is not possible, the criteria used to determine that period

For transfers to processors, also specify the subject matter, nature and duration of the processing.

SECTION C. COMPETENT SUPERVISORY AUTHORITY

Module One: Transfer controller to controller

Module Two: Transfer controller to processor

Module Three: Transfer processor to processor

Identify the competent supervisory authority or authorities in accordance with Clause 13 of the Standard Contract for the transfer of personal data to States that do not ensure an adequate level of personal data protection.

ANNEX No.2

TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF PERSONAL DATA

Module One: Transfer controller to controller

Module Two: Transfer controller to processor

Module Three: Transfer processor to processor

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks to the rights and freedoms of natural persons.

[Examples of possible measures:

- measures of pseudonymisation and encryption of personal data;*

UNOFFICIAL TRANSLATION

- *measures for ensuring the confidentiality, integrity, availability and resilience of processing systems and services on an ongoing basis;*
- *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 ensuring the protection of personal data during transmission;*
- *measures for ensuring the protection of personal data during storage;*
- *measures for ensuring the physical security of locations where personal data are processed;*
- *measures for ensuring event 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;*
- *measures enabling data portability and ensuring data erasure]*

In the case of transfers to processors (sub-processors), also describe the specific technical and organisational measures that the processor (sub-processor) must take to be able to assist the controller and, in the case of transfers from a processor to a sub-processor, to be able to assist the data exporter.

ANNEX No. 3

LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

1.Name: _____

Address: _____

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

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): _____