**Anexa nr. 9 la Acordul de Implementare**

**Garanții pentru nivelele de protecție a persoanelor fizice cu privire la prelucrarea și transferul internațional de date cu caracter personal între Casa Națională de Asigurări Sociale**

**a Republicii Moldova și Agenția de Asigurări Sociale de Stat a Republicii Letonia**

**Articolul 1**

**Scopul transferului de date și restricții**

Instituțiile competente prelucrează datele cu caracter personal numai în scopul (scopurile) specific(e) al(e) transferului, în conformitate cu dispozițiile Acordului. Acestea pot prelucra datele cu caracter personal în alt scop, numai în cazul în care:

1. au obținut consimțământul prealabil al persoanei vizate;

2. este necesar pentru constatarea, exercitarea sau apărarea unor pretenții legale în contextul unor proceduri administrative, de reglementare sau judiciare specifice; sau

3. este necesar pentru a proteja interesele vitale ale persoanei vizate sau ale unei alte persoane fizice.

**Articolul 2**

**Domeniul de aplicare al datelor cu caracter personal**

Instituțiile competente prelucrează doar categoriile de date cu caracter personal prevăzute în anexele nr. 2 - 8 și 10 ale Acordului de implementare și în modul în care este prevăzut.

**Articolul 3**

**Limitarea stocării**

l. Instituțiile competente vor păstra datele cu caracter personal nu mai mult decât este necesar pentru scopul (scopurile) pentru care sunt prelucrate pentru perioada stabilită în legislația națională.

2. Instituțiile competente revizuiesc periodic necesitatea și proporționalitatea stocării continue a datelor. În cazul în care legislația națională prevede necesitatea unei stocări suplimentare, perioada de stocare poate fi prelungită.

3. După expirarea perioadei de stocare, datele cu caracter personal vor fi șterse.

**Articolul 4**

**Destinatarii datelor cu caracter personal**

l. Instituțiilor competente le este interzis să dezvăluie părților terțe datele cu caracter personal obținute la implementarea dispozițiilor Acordului de Implementare, cu excepția instituțiilor publice ale ambelor părți în cazurile prevăzute de legislația care reglementează activitatea acestora.

2. Instituțiile competente au obligația de a evalua fiecare solicitare a instituției publice prin care se solicită emiterea datelor cu caracter personal, prin verificarea scopului prelucrării datelor cu caracter personal, a temeiului legal și a conformității cantității necesare de date cu caracter personal cu scopul prelucrării. Instituția competentă refuză să furnizeze instituției publice datele cu caracter personal solicitate în totalitate sau în parte, dacă solicitarea nu este justificată sau cantitatea de date cu caracter personal solicitată este mai mare decât este necesar pentru realizarea scopului prelucrării.

**Articolul 5**

**Obligații și responsabilități**

1. Instituțiile competente se asigură că datele cu caracter personal sunt exacte și, dacă este necesar, actualizate. Instituțiile competente iau toate măsurile rezonabile pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopul (scopurile) prelucrării, sunt șterse sau rectificate fără întârziere.

2. În cazul în care una dintre instituțiile Competente constată că datele cu caracter personal pe care le-a transferat sau primit sunt inexacte sau au expirat, aceasta informează cealaltă Instituție competentă fără întârzieri nejustificate.

3. Instituțiile competente se asigură că datele cu caracter personal sunt adecvate, relevante și limitate la ceea ce este necesar în raport cu scopul (scopurile) prelucrării.

4. Fiecare instituție Competentă care prelucrează datele cu caracter personal ale persoanei vizate informează persoanele vizate despre aspectele prelucrării datelor cu caracter personal în conformitate cu procedurile și în măsura prevăzută la articolele 13 și 14 ale Regulamentului general privind protecția datelor.

5. Alineatul (4) nu se aplică în cazul în care persoana vizată deține deja informațiile, inclusiv atunci când aceste informații au fost deja furnizate de Instituțiile competente sau furnizarea informațiilor se dovedește imposibilă sau ar implica un efort disproporționat pentru instituțiile Competente. În acest din urmă caz, instituțiile Competente fac, în măsura posibilului, informațiile disponibile publicului.

6. În cazul în care transferul implică date cu caracter personal care dezvăluie date referitoare la sănătate (denumite în continuare - Date sensibile), instituțiile Competente aplică restricții specifice și/sau garanții suplimentare adaptate caracterului specific al datelor și riscurilor implicate. Acesta poate include restricționarea personalului autorizat să acceseze datele cu caracter personal, măsuri suplimentare de securitate.

7. Instituțiile competente se asigură că orice persoană care acționează sub autoritatea sa, inclusiv un operator, prelucrează datele numai în baza instrucțiunilor sale.

8. Instituțiile competente trebuie să poată demonstra conformitatea cu obligațiile care îi revin în temeiul prezentului Acord de implementare. În special, instituțiile Competente păstrează documentația corespunzătoare a activităților de prelucrare desfășurate sub responsabilitatea sa. Instituțiile competente pun această documentație la dispoziția autorității de supraveghere competente, la cerere.

9. Instituțiile competente pun în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura securitatea datelor cu caracter personal, inclusiv protecția împotriva unei violări a securității care duce la distrugere accidentală sau ilegală, pierdere, modificare, dezvăluire sau acces neautorizat (denumită în continuare - Încălcarea datelor cu caracter personal) . La evaluarea nivelului adecvat de securitate, aceștia țin seama în mod corespunzător de stadiul tehnicii, costurile de implementare, natura, domeniul de aplicare, contextul și scopul (scopurile) prelucrării și riscurile pe care le implică pentru persoana vizată. Instituțiile competente iau în considerare în special recurgerea la criptare sau pseudonimizare, inclusiv în timpul transmiterii, atunci când scopul prelucrării poate fi îndeplinit în acest mod.

10. Instituțiile competente efectuează controale regulate pentru a se asigura că măsurile tehnice și organizatorice implementate continuă să ofere un nivel adecvat de securitate.

11. Instituțiile competente se asigură că persoanele autorizate să prelucreze datele cu caracter personal sau angajat să respecte confidențialitatea sau au o obligație legală corespunzătoare de confidențialitate.

12. În cazul unei încălcări a datelor cu caracter personal privind datele cu caracter personal prelucrate de Instituțiile competente în temeiul Acordului de Implementare, instituțiile Competente iau măsurile adecvate pentru a aborda problema încălcării datelor cu caracter personal, inclusiv măsuri pentru atenuarea posibilelor efecte adverse ale acesteia.

13. În cazul unei încălcări a datelor cu caracter personal care ar putea duce la un risc pentru drepturile și libertățile persoanelor fizice, instituția Competentă în cauză notifică fără întârziere nejustificată atât cealaltă instituție Competentă, cât și autoritatea de supraveghere competentă. O astfel de notificare trebuie să conțină: o descriere a naturii încălcării (inclusiv, acolo unde este posibil, categoriile și numărul aproximativ de persoane vizate și înregistrările de date cu caracter personal în cauză); consecințele sale probabile; măsurile luate sau propuse pentru a remedia încălcarea; și detaliile unui punct de contact de la care se pot obține mai multe informații. În cazul în care nu este posibil ca instituția Competentă să furnizeze toate informațiile în același timp, aceasta poate face acest lucru în etape, fără întârzieri suplimentare nejustificate.

14. În cazul unei încălcări a datelor cu caracter personal care ar putea duce la un risc ridicat pentru drepturile și libertățile persoanelor fizice, instituția Competentă va notifica, de asemenea, fără întârzieri nejustificate, persoanele vizate cu privire la încălcarea datelor cu caracter personal și natura acesteia, dacă este necesar în cooperarea cu cealaltă instituție Competentă, împreună cu informațiile menționate în prezentul Articol, cu excepția cazului în care instituția Competentă a implementat măsuri pentru a reduce în mod semnificativ riscul pentru drepturile sau libertățile persoanelor fizice, sau notificarea ar implica eforturi disproporționate. În acest din urmă caz, instituția Competentă va emite în schimb o comunicare publică sau va întreprinde o măsură similară pentru a informa publicul cu privire la Încălcarea datelor cu caracter personal.

15. Instituția competentă va documenta toate faptele relevante legate de încălcarea datelor cu caracter personal, inclusiv efectele acesteia și orice acțiune de remediere întreprinsă și păstrează o evidență a acestora.

Instituțiile competente vor fi răspunzătoare față de persoana vizată, pentru orice daune materiale sau morale pe care le cauzează persoanei vizate prin încălcarea acestor cerințe.

**Articolul 6**

**Măsurile tehnice și organizatorice**

l. Au fost elaborate proceduri interne legate de protecția datelor cu caracter personal și securitatea tehnologiei informaționale.

2. Se organizează periodic cursuri de formare pentru personalul instituțiilor Competente privind protecția datelor cu caracter personal și securitatea tehnologiei informației. Treningurile includ, de asemenea, aspecte privind acțiunile care trebuie întreprinse în cazul unei încălcări a protecției datelor cu caracter personal și în cazul detectării unui incident de securitate în tehnologia informației.

3. A fost instituită o procedură de informare a personalului cu privire la obligația de a nu dezvălui datele cu caracter personal (inclusiv după încetarea muncii, a serviciului sau a unui alt raport juridic).

4. Perioadele de stocare a datelor cu caracter personal sunt stabilite prin reguli interne.

5. Există proceduri de ștergere sau distrugere a datelor cu caracter personal.

6. A fost instituită o procedură de gestionare a încălcării protecției datelor cu caracter personal, pentru a permite instituției Competente să investigheze, să evalueze și să informeze autoritatea de supraveghere și persoanele vizate cu privire la incidentele care au avut loc conform procedurilor și în măsura stabilit- prin Acordul de implementare.

7. Au fost desemnate persoane responsabile pentru resursele informaționale, resursele tehnice și protecția datelor cu caracter personal.

8. În funcție de riscul potențial, instituțiile Competente asigură o protecție suficientă împotriva amenințărilor fizice (inclusiv condiții climatice necorespunzătoare, incendii, inundații, întreruperi de alimentare cu energie electrică, deteriorare intenționată) a spațiului în care datele personale sunt stocate în format de hârtie, a serverelor și a sediilor serverului, dacă este necesar prin instalarea alarmei de incendiu, a sistemului automat de stingere a incendiilor, prin instalarea de echipamente alternative de alimentare cu energie electrică și echipamente de răcire cu aer.

9. Instituțiile competente asigură o protecție fizică suficientă prin prelucrarea datelor cu caracter personal în așa fel încât acestea să nu poată fi accesate, conectate la sau deteriorate, fără autorizație sau neobservate, de către persoane care nu sunt asociate cu instituțiile Competente, precum și să nu poată fi accesate, conectate sau deteriorate fără autorizație, sau deteriorate accidental din neglijență de către personalul instituțiilor Competente sau clienți.

10. Sunt implementate următoarele proceduri privind prelucrarea electronică a datelor:

- reguli de utilizare a resurselor sistemului informatic;

- reguli pentru menținerea securității fizice a resurselor sistemului informațional;

- reguli de gestionare a incidentelor de securitate a rețelei de transport;

- reguli de gestionare a drepturilor de utilizare a resurselor sistemului informațional;

- reguli de gestionare a evenimentelor și încălcărilor privind protecția datelor cu caracter personal.

**Articolul 7**

**Drepturile persoanelor vizate**

1. Instituția competentă, dacă este cazul, cu asistența celeilalte instituții Competente, se ocupă de orice întrebări și solicitări pe care le primește de la o persoană vizată cu privire la prelucrarea datelor sale cu caracter personal și la exercitarea drepturilor sale în temeiul prezentului Acord de implementare fără întârzieri nejustificate și cel târziu în termen de o lună de la primirea anchetei sau cererii. (i) Instituțiile competente vor lua măsurile corespunzătoare pentru a facilita astfel de anchete, solicitări și exercitarea drepturilor persoanelor vizate. Orice informație furnizată persoanei vizate trebuie să fie într-o formă inteligibilă și ușor accesibilă, folosind un limbaj clar și simplu.

2. În special, la cererea persoanei vizate, instituțiile Competente, în mod gratuit, trebuie:

2.1. să furnizeze confirmarea persoanei vizate cu privire la faptul că datele cu caracter personal care o privesc sunt în curs de prelucrare și, dacă este cazul, o copie a datelor care o privesc și a informațiilor de mai sus; dacă datele cu caracter personal au fost sau vor fi transferate ulterior, va furniza informații despre destinatarii sau categoriile de destinatari (după caz, în vederea furnizării de informații semnificative) a cărora datele cu caracter personal au fost sau vor fi transferate ulterior, scopul acestor transferuri ulterioare și motivul lor în conformitate cu articolul 4; și să furnizeze informații cu privire la dreptul de a depune o plângere la o autoritate de supraveghere în conformitate cu articolul 9;

2.2. să rectifice datele inexacte sau incomplete referitoare la persoana vizată;

2.3. să șteargă datele cu caracter personal referitoare la persoana vizată dacă aceste date sunt sau au fost prelucrate cu încălcarea oricăror prevederi ale Acordului de Implementare.

3. În cazul în care cererile din partea unei persoane vizate sunt excesive, în special din cauza caracterului lor repetitiv, instituțiile Competente pot fie să perceapă o taxă rezonabilă, ținând cont de costurile administrative de acordare a cererii, fie să refuze să dea curs cererii.

4. Instituțiile competente pot refuza cererea persoanei vizate dacă acest refuz este permis de legile țării de destinație și este necesar și proporțional într-o societate democratică pentru a proteja unul dintre obiectivele enumerate la Articolul 23 litera (l) din Regulamentul (UE) 2016/679.

5. În cazul în care instituțiile Competente intenționează să refuze cererea unei persoane vizate, aceasta o informează cu privire la motivele refuzului și posibilitatea de a depune o plângere la autoritatea de supraveghere competentă și/sau de a solicita o cale de atac judiciar.

**Articolul 8**

**Despăgubiri**

1. Instituția competentă ia în considerare numai plângerile persoanelor vizate care locuiesc pe teritoriul UE, SEE și Republicii Moldova, ale căror date cu caracter personal au fost prelucrate de către aceasta, cu excepția cazului în care natura plângerii este legată de acțiunile cu privire la datele cu caracter personal efectuate de către cealaltă instituție Competentă. În acest din urmă caz, instituția Competentă, primind reclamația, o trimite în partea respectivă prin e-mail persoanei de contact a celeilalte instituții Competente pentru a evalua legalitatea acțiunii sale și a oferi un răspuns, oferind suportul necesar.

2. Instituțiile competente informează persoanele vizate într-un mod transparent și ușor accesibil, prin notificare individuală sau pe site-ul său web, cu privire la un punct de contact autorizat să gestioneze reclamațiile. Acestea vor trata cu promptitudine orice plângeri pe care le primesc de la persoanele vizate.

3. În cazul unui litigiu între o persoană vizată și una dintre instituțiile Competente cu privire la respectarea dispozițiilor prezentului Acord de Implementare, instituția Competentă respectivă va depune toate eforturile pentru a rezolva problema pe cale amiabilă în timp util. Instituțiile competente se informează reciproc cu privire la astfel de dispute și, după caz, cooperează pentru soluționarea acestora.

**Articolul 9**

**Cooperarea cu Autoritățile de Supraveghere**

1. Autoritate de supraveghere competentă:

Pentru Republica Moldova - Centrul Naţional pentru Protecţia Datelor cu Caracter Personal al Republicii Moldova;

Pentru Republica Letonia - Inspectoratul de Stat al Datelor din Letonia.

2. Instituțiile competente sunt de acord să coopereze cu autoritatea de supraveghere competentă în orice proceduri menite să asigure respectarea dispozițiilor Acordului de implementare. În special, Instituțiile competente sunt de acord să răspundă la întrebări, să se supună auditurilor și să se conformeze măsurilor adoptate de autoritatea de supraveghere, inclusiv măsuri de remediere și compensare. Instituțiile competente furnizează autorității de supraveghere competente o confirmare scrisă că au fost întreprinse măsurile necesare.

**DISPOZIȚII FINALE**

**Articolul 10**

**Neconformitate și reziliere**

1. Instituțiile competente se informează reciproc cu promptitudine în cazul în care nu pot îndeplini aceste cerințe, indiferent de motiv.

2. În cazul în care Instituția competentă încalcă aceste cerințe sau nu le poate respecta, cealaltă instituție Competentă suspendă transferul datelor cu caracter personal până când conformitatea este din nou asigurată sau Acordul este suspendat.

3. În cazul în care legile naționale aplicabile instituției Competente nu prevăd returnarea sau ștergerea datelor cu caracter personal transferate, instituția Competentă în cauză garantează că va continua să asigure respectarea acestor cerințe și va prelucra datele numai în măsura și atât timp cât este cerut de legea națională respectivă.

**Articolul 11**

**Alegerea forului și a jurisdicției**

O persoană vizată în conformitate cu Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, și de abrogare a Directivei 95/46/EC (Regulamentul general privind protecția datelor) în Republica Letonia și Legea privind protecția datelor cu caracter personal în Republica Moldova poate înainta o acțiune în justiție împotriva Instituțiilor competente în fața instanțelor de judecată ale Părții acordului în care a avut loc încălcarea.

**Annex No 9 to the Implementing Agreement**

**Guarantees for Protection Levels of Natural Persons with Regard to the Processing and International Transfer of Personal Data between the State Social Insurance Agency of the Republic of Latvia and National Office of Social Insurance of the Republic of Moldova**

**Article 1**

**Purpose of the data transfer and limitations**

The Competent institutions shall process the personal data only for the specific purpose(s) of the transfer, as set in the Agreement. It may only process the personal data for another purpose:

1. where it has obtained the data subject’s prior consent;

2. where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

3. where necessary in order to protect the vital interests of the data subject or of another natural person.

**Article 2**

**Scope of personal data**

Competent institutions shall only process the categories of personal data as specified in the Annex No 2 – 8, 10 of the Implementing Agreement and to the extent specified there.

**Article 3**

**Storage limitation**

1.The Competent institutions shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed for the period set in the national legislation.

2.The Competent institutions periodically review the need and proportionality of continued data storage. If the need for further storage is prescribed in the national legislation, the storage period may be extended.

3.After the expiry of storage period, personal data shall be erased.

**Article 4**

**Recipients of personal data**

1.Competent institutions are prohibited from disclosing personal data obtained within the framework of the Implementing Agreement to third parties, except for public institutions of both Parties in cases specified in the legislation governing their activity.

2.Competent institutions have an obligation to assess each request of the public institution concerned to issue personal data, by checking the purpose of processing of personal data, the legal basis and the compliance of the required amount of personal data with the purpose of processing. The Competent institution refuses to provide the requested personal data to the public institution in whole amount or in part, if the request is not justified or the requested personal data amount is larger than necessary to achieve the purpose of the processing.

**Article 5**

**Obligations and Liability**

1. Competent institutions shall ensure that the personal data is accurate and, where necessary, kept up to date. The Competent institutions 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 Competent institutions becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Competent institution without undue delay.
3. The Competent institutions shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.
4. Each Competent institution that processes the data subject's personal data informs the data subjects about the aspects of personal data processing in accordance with the procedures and to the extent specified in Articles 13 and 14 of the General Data Protection Regulation.
5. Paragraph 4 shall not apply where the data subject already has the information, including when such information has already been provided by the Competent institutions, or providing the information proves impossible or would involve a disproportionate effort for the Competent institutions. In the latter case, the Competent institutions shall, to the extent possible, make the information publicly available.
6. Where the transfer involves personal data revealing data concerning health, the Competent institutions 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.
7. The Competent institutions shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.
8. The Competent institutions shall be able to demonstrate compliance with its obligations under these Implementing Agreement. In particular, the Competent institutions shall keep appropriate documentation of the processing activities carried out under its responsibility. The Competent institutions shall make such documentation available to the competent supervisory authority on request.
9. The Competent institutions shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter - personal data breach). In 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 involved in the processing for the data subject. The Competent institutions shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
10. The Competent institutions shall carry out regular checks to ensure that implemented technical and organisational measures continue to provide an appropriate level of security.
11. The Competent institutions shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
12. In the event of a personal data breach concerning personal data processed by the Competent institutions under Implementation Agreement, the Competent institutions shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.
13. In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the Competent institution concerned shall without undue delay notify both the other Competent institution and the Competent supervisory authority. Such notification shall contain: a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned); its likely consequences; the measures taken or proposed to address the breach; and the details of a contact point from whom more information can be obtained. To the extent it is not possible for the Competent Institution to provide all the information at the same time, it may do so in phases without undue further delay.
14. In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the Competent institution shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the other Competent institution, together with the information referred to in this Article unless the Competent institution 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 Competent institution shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.
15. The Competent institution shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

The Competent institutions shall be liable to the data subject, for any material or non-material damages that it causes the data subject by breaching these requirements.

**Article 6**

**The technical and organisational measures**

1. Internal procedures related to personal data protection and information technology security have been developed.

2. Regular trainings shall be organized for the staff of the Competent institutions regarding personal data protection and information technology security. Trainings also include issues on actions to be taken in the event of personal data breach and in case of detection of an information technology security incident.

3. A procedure has been put in place for informing the staff on the obligation not to disclose personal data (including after termination of labour, service or other legal relationship).

4. Personal data storage periods are set in internal rules.

5. Procedures for erasure or destruction of personal data are in place.

6. Personal data breach management procedure has been put in place, to enable the Competent institution to investigate, assess and inform the Competent supervisory authority and data subjects of the incidents that have occurred according to the procedures and to the extent determined by the Implementing Agreement.

7. Responsible persons for information resources, technical resources and personal data protection have been appointed.

8. Depending on the potential risk, the Competent institutions ensure sufficient protection against physical threats (including unsuitable climatic conditions, fire, floods, power supply interruptions, intentional damage) of the space where personal data is stored in paper format, servers and server premises, if necessary by installing fire alarm, automatic fire extinguishing system, by installing alternative power supply equipment and air-cooling equipment.

9. The Competent institutions ensure sufficient physical protection by processing personal data in such a way that they cannot be accessed, connected to or damaged, without authorization or unnoticed, by persons not associated with the Competent institutions, as well as that they cannot be accessed, connected to or damaged without authorization, or accidentally damaged by negligence by the staff of the Competent institutions or clients.

10. Following procedures are implemented concerning electronic data processing:

- rules for use of information system resources;

- rules for maintaining the physical security of Information System resources are in place;

- transmission network security incident management rules ae in place;

- rules for management of rights to use Information System resources are in place;

- rules for management of personal data protection events and violations are in place.

**Article 7**

**Data subject rights**

1. The Competent institution, where relevant with the assistance of the other Competent institution, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Implementing Agreement without undue delay and at the latest within one month of the receipt of the enquiry or request. ([[1]](#endnote-1)) The Competent institutions shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

2. In particular, upon request by the data subject the Competent institutions shall, free of charge:

2.1. 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 above; 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 Article 4; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Article 9;

2.2. rectify inaccurate or incomplete data concerning the data subject;

2.3. erase personal data concerning the data subject if such data is being or has been processed in violation of any provisions of the Implementing Agreement.

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

4. The Competent institutions 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(1) of Regulation (EU) 2016/679.

5. If the Competent institutions intends to refuse a data subject’s request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the Competent supervisory authority and/or seeking judicial redress.

**Article 8**

**Redress**

1. The Competent institution only considers complaints from data subjects living in the territory of the EU, EEA and Republic of Moldova, whose personal data it has processed, unless the nature of the complaint is related to actions with personal data by the other Competent institution. In the latter case, the Competent institution, receiving the complaint, sends it in the respective part via e-mail to the contact person of the other Competent institution for evaluating the legality of its action and providing a response, and provides the necessary support.

2.The Competent institutions 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.

3.In case of a dispute between a data subject and one of the Competent institutions as regards compliance with these Implementing Agreement, that Competent institution concerned shall use its best efforts to resolve the issue amicably in a timely fashion. The Competent institutions shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

**Article 9**

**Cooperation with Supervision Authorities**

1. Competent supervisory authority:

For the Republic of Latvia – Data State Inspectorate of Latvia;

For the Republic of Moldova – National Centre for Personal Data Protection of Moldova

2. The Competent institutions agrees to cooperate with the Competent supervisory authority in any procedures aimed at ensuring compliance with the Implementing Agreement. In particular, the Competent institutions agree to respond to enquiries, submit to audits and comply with the measures adopted by the Competent supervisory authority, including remedial and compensatory measures. Competent institutions shall provide the Competent supervisory authority with written confirmation that the necessary actions have been taken.

**FINAL PROVISIONS**

**Article 10**

**Non-compliance and termination**

1. The Competent institutions shall promptly inform each other in case of not being able to comply with these requirements, for whatever reason.

2. In the event that the Competent institution is in breach of these requirements or unable to comply with these requirements, the other Competent institution shall suspend the transfer of personal data until compliance is again ensured or the Agreement is suspended.

3. In case of local laws applicable to the Competent institution do not provide for the return or deletion of the transferred personal data, the Competent institution concerned warrants that it will continue to ensure compliance with these requirements and will only process the data to the extent and for as long as required under that local law.

**Article 11**

**Choice of forum and jurisdiction**

A data subject in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) in Latvia and Law on Personal Data Protection in Moldova may bring legal proceedings against the Competent institutions before the courts of the Party of the Agreement in which infringement has occurred.

1. [↑](#endnote-ref-1)