EU GDPR DATA PROCESSING ADDENDUM (DPA) INSTRUCTIONS FOR SCALEFLEX CUSTOMERS

Data Processing Addendum: v1.6
Updated: 21.10.2020

Who is this addendum relevant for?

If you have determined that you qualify as a data controller under the GDPR, and need a data processing addendum (DPA) in place with Scaleflex that processes personal data on your behalf, we want to help make things easy for you. This GDPR compliant DPA is attached and ready for your signature in accordance with the instructions below.

How to execute this DPA?

1. This DPA consists of two parts: the main body of the DPA, and Annexes 1, 2, and 3 (including Appendices 1 and 2).
2. This DPA has been pre-signed on behalf of Scaleflex. The Standard Contractual Clauses in Annex 2 (including Appendix 1 thereto) and the Security Measures in Annex 3 have been pre-signed by Scaleflex as the data importer.
3. To complete this DPA, you (Customer) must complete the information in the signature boxes and sign on Pages 10, 18, 20 and 24.
4. Send the completed and signed DPA to Scaleflex by email, indicating the Customer's Legal Name, to privacy@scaleflex.com

Upon receipt of the validly completed DPA by Scaleflex at this email address, this DPA will become legally binding.

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**"), forms part of the Scaleflex Terms & Conditions (available at https://privacy.scaleflex.com/), or other written or electronic agreement, by and between Scaleflex SAS ("**Scaleflex**", "**Cloudimage**", "**Filerobot**") and the undersigned customer of Scaleflex (**"Customer")** for certain image processing, optimization, and/or other website services (collectively, the "**Service**") provided by Scaleflex. Together, the DPA, the Scaleflex Terms & Conditions, the Scaleflex Privacy Policy and the Scaleflex Cookie Policy form the "**Principal Agreement**". All capitalized terms not defined herein shall have the meanings set forth in the Terms of Use. Each of Customer and Scaleflex may be referred to herein as a "**party**" and together as the "**parties**".

In connection with the Service, the parties anticipate that Scaleflex may process outside of the European Economic Area ("**EEA**") and United Kingdom, certain Personal Data in respect of which the Customer or any member of the Customer Group may be a data controller or data processor, as applicable, under applicable EU Data Protection Laws. The parties have agreed to enter into this DPA in order to ensure that adequate safeguards are put in place with respect to the protection of such Personal Data as required by EU Data Protection Laws.

How to execute this DPA?

1. This DPA consists of two parts: the main body of the DPA, and Annexes 1, 2, and 3 (including Appendices 1 to 2).
2. This DPA has been pre-signed on behalf of Scaleflex. The Standard Contractual Clauses in Annex 2 (including Appendix 1 thereto) and the Security Measures in Annex 3 have been pre-signed by Scaleflex as the data importer.
3. To complete this DPA, you (Customer) must complete the information in the signature boxes and sign on Pages 10, 18, 20 and 24.
4. Send the completed and signed DPA to Scaleflex by email, indicating the Customer's Legal Name, to privacy@scaleflex.com

Upon receipt of the validly completed DPA by Scaleflex at this email address, this DPA will become legally binding.

How this DPA applies?

This DPA is an addendum to and forms part of the Principal Agreement. The Customer entity signing this DPA must be the same as the Customer entity party to the Principal Agreement. If the Customer entity signing this DPA is not a party to the Principal Agreement directly with Scaleflex, but is instead a customer indirectly via an authorized reseller of Scaleflex services, this DPA is not valid and is not legally binding. Such entity should contact the authorized reseller to discuss whether any amendment to its agreement with that reseller may be required.

Data Processing Terms

In the course of providing the Service to Customer pursuant to the Principal Agreement, Scaleflex may Process Personal Data on behalf of Customer. Scaleflex agrees to comply with the following provisions with respect to any Personal Data submitted by or for Customer to Scaleflex or collected and processed by or for Customer using Scaleflex's services. The parties agree that the obligations under this DPA.

1. Definitions

1.1 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "**Adequate Country**" means a country or territory that is recognized under EU Data Protection Laws as providing adequate protection for Personal Data;

1.1.2 "**Applicable Laws**" means (a) European Union or Member State laws with respect to any Customer Personal Data in respect of which any Customer Group Member is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Customer Personal Data in respect of which any Customer Group Member is subject to any other Data Protection Laws;

1.1.3 "**Customer Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Customer, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.4 "**Customer Group Member**" means Customer or any Customer Affiliate;

1.1.5 "**Customer Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of a Customer Group Member pursuant to or in connection with the Principal Agreement;

1.1.6 "**Contracted Processor**" means Scaleflex or a Sub-processor;

1.1.7 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.8 "**EEA**" means the European Economic Area;

1.1.9 "**EU Data Protection Laws**" "EU Data Protection Laws" means all laws and regulations of the European Union, the European Economic Area, their member states, and the United Kingdom, applicable to the processing of

Personal Data under the Agreement, including (where applicable) the General Data Protection Regulation ("GDPR");

1.1.10 "**GDPR**" "GDPR" means the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data);

1.1.11 "**Personal Data**" means all data which is defined as 'personal data' under EU Data Protection Laws and to which EU Data Protection Laws apply and which is provided by the Customer to Scaleflex, and accessed, stored or otherwise processed by Scaleflex as a data processor as part of its provision of the Service to Customer;

1.1.12 "**Restricted Transfer**" means:

1.1.12.1 a transfer of Customer Personal Data from any Customer Group Member to a Contracted Processor; or

1.1.12.2 an onward transfer of Customer Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established under section [6.4.3 or] 12 below;

1.1.13 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Scaleflex for Customer Group Members pursuant to the Principal Agreement;

1.1.14 "**Standard Contractual Clauses**" means the contractual clauses set out in Annex 2, amended as indicated (in square brackets and italics) in that Annex and under section 13.4;

1.1.15 "**Sub-processor**" means any person (including any third party and any Scaleflex Affiliate, but excluding an employee of Scaleflex or any of its sub-contractors) appointed by or on behalf of Scaleflex or any Scaleflex Affiliate to Process Personal Data on behalf of any Customer Group Member in connection with the Principal Agreement; and

1.1.16 "**Scaleflex Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Scaleflex, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

1.3 The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Status of the parties

2.1 The type of Personal Data processed pursuant to this DPA and the subject matter, duration, nature and purpose of the processing, and the categories of data subjects, are as described in Annex 1.

2.2 Each party warrants in relation to Personal Data that it will comply (and will procure that any of its personnel comply and use commercially reasonable efforts to procure that its sub-processors comply), with EU Data Protection Laws. As between the parties, the Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which the Customer acquired Personal Data.

2.3 In respect of the parties' rights and obligations under this DPA regarding the Personal Data, the parties hereby acknowledge and agree that the Customer is the data controller or processor, and Scaleflex is the data processor or sub-processor, as applicable, and accordingly Scaleflex agrees that it shall process all Personal Data in accordance with its obligations pursuant to this DPA.

2.4 If Customer is a data processor, Customer warrants to Scaleflex that Customer’s instructions and actions with respect to the Personal Data, including its appointment of Scaleflex as another processor and concluding the standard contractual clauses (Annex 2), have been authorised by the relevant controller.

2.5 Where and to the extent that Scaleflex processes data which is defined as *‘personal data’* under EU Data Protection Laws as a data controller as set out in Scaleflex Privacy Policy available at https://privacy.scaleflex.com/, Scaleflex will comply with applicable EU Data Protection Laws in respect of that processing

2.6 Each party shall appoint an individual within its organization authorized to respond from time to time to enquiries regarding the Personal Data and each party shall deal with such enquiries promptly.

3. Scaleflex and Scaleflex Affiliate Personnel

Scaleflex and each Scaleflex Affiliate shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Customer Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Customer Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Scaleflex and each Scaleflex Affiliate shall in relation to the Customer Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, Scaleflex and each Scaleflex Affiliate shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Sub-processing

5.1 Each Customer Group Member authorises Scaleflex and each Scaleflex Affiliate to appoint (and permit each Sub-processor appointed in accordance with this section 5 to appoint) Sub-processors in accordance with this section 5 and any restrictions in the Principal Agreement.

5.2 Scaleflex and each Scaleflex Affiliate may continue to use those Sub-processors already engaged by Scaleflex or any Scaleflex Affiliate as at the date of this Addendum, subject to Scaleflex and each Scaleflex Affiliate in each case as soon as practicable meeting the obligations set out in section 5.4.

5.3 Scaleflex shall give Customer prior written notice of the appointment of any new Sub-processor, including full details of the Processing to be undertaken by the Sub-processor. If, within ten (10) days of receipt of that notice, Customer notifies Scaleflex in writing of any objections (on reasonable grounds) to the proposed appointment:

5.3.1 Scaleflex shall work with Customer in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Sub-processor; and

5.3.2 where such a change cannot be made within twenty (20) days from Scaleflex's receipt of Customer's notice, notwithstanding anything in the Principal Agreement, Customer may by written notice to Scaleflex with immediate effect terminate the Principal Agreement to the extent that it relates to the Services which require the use of the proposed Sub-processor.

5.4 With respect to each Sub-processor, Scaleflex or the relevant Scaleflex Affiliate shall:

5.4.1 before the Sub-processor first processes Customer Personal Data (or, where relevant, in accordance with section 5.2), carry out adequate due diligence to ensure that the Sub-processor is capable of providing the level of protection for Company Personal Data required by the Principal Agreement;

5.4.2 ensure that the arrangement between on the one hand (a) Scaleflex, or (b) the relevant Scaleflex Affiliate, or (c) the relevant intermediate Sub-processor; and on the other hand the Sub-processor, is governed by a written contract including terms which offer at least the same level of protection for Customer Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR;

5.4.3 if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand (a) Scaleflex, or (b) the relevant Scaleflex Affiliate, or (c) the relevant intermediate Sub-processor; and on the other hand the Sub-processor, or before the Sub-processor first processes Customer Personal Data procure that it enters into an agreement incorporating the Standard Contractual Clauses with the relevant Customer Group Member(s) (and Customer shall procure that each Customer Affiliate party to any such Standard Contractual Clauses co-operates with their population and execution);

5.5 Scaleflex and each Scaleflex Affiliate shall ensure that each Sub-processor performs the obligations under sections 3, 4, 6.1, 7.2, 8 and 10.1, as they apply to Processing of Company Personal Data carried out by that Sub-processor, as if it were party to this Addendum in place of Vendor.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Scaleflex and each Scaleflex Affiliate shall assist each Customer Group Member by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company Group Members' obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Scaleflex shall:

6.2.1 promptly notify Customer if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Customer Personal Data; and

6.2.2 ensure that the Contracted Processor does not respond to that request except on the documented instructions of Customer or the relevant Customer Affiliate or as required by Applicable Laws to which the Contracted Processor is subject, in which case Scaleflex shall to the extent permitted by Applicable Laws inform Customer of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1 Scaleflex shall notify Customer without undue delay upon Customer or any Sub-processor becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information to allow each Customer Group Member to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Scaleflex shall co-operate with Customer and each Customer Group Member and take such reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Deletion or return of Customer Personal Data

8.1 Subject to sections 8.2 and 8.3 Scaleflex and each Scaleflex Affiliate shall promptly and in any event within ninety (90) days of the date of cessation of any Services involving the Processing of Customer Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of those Company Personal Data.

8.2 Subject to section 8.3, Customer may in its absolute discretion by written notice to Vendor within thirty (30) of the Cessation Date require Scaleflex and each Scaleflex Affiliate to (a) return a complete copy of all Customer Personal Data to Customer by secure file transfer in such format as is reasonably notified by Customer to Scaleflex; and (b) delete and procure the deletion of all other copies of Customer Personal Data Processed by any Contracted Processor.

8.3 Each Contracted Processor may retain Customer Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that Scaleflex and each Scaleflex Affiliate shall ensure the confidentiality of all such Customer Personal Data and shall ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

9. Audit and records

9.1 Scaleflex shall, in accordance with EU Data Protection Laws, make available to the Customer such information in Scaleflex's possession or control as the Customer may reasonably request with a view to demonstrating Scaleflex's compliance with the obligations of data processors under EU Data Protection Law in relation to its processing of Personal Data.

9.2 The Customer may exercise its right of audit under EU Data Protection Laws in relation to Personal Data, through Scaleflex providing:

(a) an audit report not older than eighteen (18) months, prepared by an independent external auditor demonstrating that Scaleflex's technical and organizational measures are sufficient and in accordance with an accepted industry audit standard; and

b) additional information in Scaleflex's possession or control to an EU supervisory authority when it requests or requires additional information in relation to the processing of Personal Data carried out by Scaleflex under this DPA.

10. Data transfers

10.1 To the extent any processing of Personal Data by Scaleflex takes place in any country outside the EEA (except if in an Adequate Country), the parties agree that the standard contractual clauses approved by the EU authorities under EU Data Protection Laws and set out in Annex 2 will apply in respect of that processing, and Scaleflex will comply with the obligations of the 'data importer' in the standard contractual clauses and the Customer will comply with the obligations of the 'data exporter'.

10.2 The Customer acknowledges and accepts that the provision of the Service under the Principal Agreement may require the processing of Personal Data by sub-processors in countries outside the EEA.

10.3 If, in the performance of this DPA, Scaleflex transfers any Personal Data to a sub-processor located outside of the EEA (without prejudice to clause 5), Scaleflex shall in advance of any such transfer ensure that a legal mechanism to achieve adequacy in respect of that processing is in place, such as:

(a) the requirement for Scaleflex to execute or procure that the sub-processor execute to the benefit of the Customer standard contractual clauses approved by the EU authorities under EU Data Protection Laws and set out in Annex 2; or

(b) the existence of any other specifically approved safeguard for data transfers (as recognised under EU Data Protection Laws) and/or a European Commission finding of adequacy.

11. General

11.1 This DPA is without prejudice to the rights and obligations of the parties under the Principal Agreement which shall continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of the Principal Agreement, the terms of this DPA shall prevail so far as the subject matter concerns the processing of Personal Data.

11.2 Scaleflex's liability under or in connection with this DPA (including under the standard contractual clauses set out in Annex 3) is subject to the limitations on liability contained in the Principal Agreement.

11.3 This DPA does not confer any third-party beneficiary rights, it is intended for the benefit of the parties hereto and their respective permitted successors and assigns only, and is not for the benefit of, nor may any provision hereof be enforced by, any other person.

11.4 This DPA and any action related thereto shall be governed by and construed in accordance with the laws of France, without giving effect to any conflicts of laws principles.

11.5 This DPA is the final, complete and exclusive agreement of the parties with respect to the subject matter hereof and supersedes and merges all prior discussions and agreements between the parties with respect to such subject matter. Other than in respect of statements made fraudulently, no other representations or terms shall apply or form part of this DPA. No modification of, amendment to, or waiver of any rights under the DPA will be effective unless in writing and signed by an authorized signatory of each party. This DPA may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement. Each person signing below represents and warrants that he or she is duly authorized and has legal capacity to execute and deliver this DPA. Each party represents and warrants to the other that the execution and delivery of this DPA, and the performance of such party's obligations hereunder, have been duly authorized and that this DPA is a valid and legally binding agreement on each such party, enforceable in accordance with its terms.

[Customer]

Signature ______________________________

Name _________________________________

Title __________________________________

Date Signed ____________________________

[Scaleflex]

Signature: ENovakov.

Name: Emil Novakov

Title: CEO

Date Signed: 21.10.2020

Annex 1

Details of the Personal Data and processing activities

(a) The personal data comprises: in relation to visitors of the Customer's online properties identification data, connection data, or IP addresses. Customer, its online visitors and/or other partners may also upload content to Customer's online properties which may include personal data and special categories of data, the extent of which is determined and controlled by the Customer in its sole discretion. Such special categories of data include, but may not be limited to, information revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning an individual's health or sex life.

(b) The duration of the processing will be: until the earliest of (i) expiry/termination of the Principal Agreement, or (ii) the date upon which processing is no longer necessary for the purposes of either party performing its obligations under the Principal Agreement (to the extent applicable). In the case of visitors IP addresses, this duration is set to seven (7) days.

(c) The processing will comprise: Processing necessary to provide the Service to Customer, pursuant to the Principal Agreement;

(d) The purposes of the processing are: necessary for the provision of the Service;

(e) Personal data may concern the following data subjects:

- Prospective customers, customers, resellers, referrers, business partners, and vendors of the Customer (who are natural persons);
- Employees or contact persons of the Customer's prospective customers, customers, resellers, referrers, sub-processors, business partners, and vendors (who are natural persons);
- Employees, agents, advisors, and freelancers of the Customer (who are natural persons); and/or
- Natural persons authorized by the Customer to use the Service.

Annex 2

2010 EU Model clauses extracted from 2010/87/EU Annex EU Standard Contractual Clauses for the transfer of personal data to data processors established in third countries which do not ensure an adequate level of data protection

INTRODUCTION

Both parties have agreed on the following Contractual Clauses (the "**Clauses**") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

AGREED TERMS

1. Definitions

For the purposes of the Clauses:

a) "**personal data**", "**special categories of data**", "**process/processing**", "**controller**", "**processor**", "**data subject**" and "**supervisory authority**" shall have the same meaning as in EU Data Protection Laws 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

b) the "**data exporter**" means the entity who transfers the personal data;

c) the "**data importer**" means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of EU Data Protection Laws 95/46/EC;

d) the "**sub-processor**" means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

e) the "**applicable data protection law**" means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established; and

f) "**technical and organisational security measures**" means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

3. Third-party beneficiary clause

3.1 The data subject can enforce against the data exporter this Clause, Clause 4.1(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

3.2 The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.3 The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub- processor shall be limited to its own processing operations under the Clauses.

3.4 The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4. Obligations of the data exporter

4.1 The data exporter agrees and warrants:

a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

e) that it will ensure compliance with the security measures;

f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of EU Data Protection Laws 95/46/EC;

g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub- processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

j) that it will ensure compliance with Clause 4(a) to (i).

5. Obligations of the data importer

5.1 The data importer agrees and warrants:

a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

d) that it will promptly notify the data exporter about:

> (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
>
> (ii) any accidental or unauthorised access; and
>
> (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

6. Liability

6.1 The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

6.2 If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

6.3 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

7. Mediation and jurisdiction

7.1 The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

b) to refer the dispute to the courts in the Member State in which the data exporter is established.

7.2 The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8. Co-operation with supervisory authorities

8.1 The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

8.2 The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

8.3 The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

9. Governing law

The Clauses shall be governed by the laws of the Member State in which the data exporter is established.

10. Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

11. Sub-processing

11.1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

11.2 The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

11.3 The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

11.4 The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5.1(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12. Obligation after the termination of personal data-processing services

12.1 The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

12.2 The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.
This agreement has been entered into on the date shown at the beginning of the first page of this agreement.

On behalf of the data exporter:
[*Populated with details of, and deemed signed on behalf of, the data exporter:*]
Company:
Name (written out in full):
Position:
Address:
Date:

Signature……………………………………….

On behalf of the data importer:
Company: Scaleflex SAS
Name (written out in full): Emil Novakov
Position: CEO
Address: 53 Chemin Beauregard, 38330 Saint-Nazaire-Les-Eymes, France
Date: 21.10.2020

Signature........ ENovakov. ....

Appendix 1

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is:
The (i) legal entity that has created an account with Scaleflex SAS ("**Scaleflex**") for provision of the Service, and executed the Clauses as a data exporter and, (ii) all affiliates of such entity established within the EEA, which have purchased services from Scaleflex or its Affiliates.

Data importer
The data importer is:
Scaleflex, which provides Acceleration-as-a-Service services to improve the Customer's application loading times. The services store, process and deliver images, videos, static content and any content uploaded by the data exporter into the Scaleflex administration interface.

Data subjects
The personal data transferred concern the following categories of data subjects:
The data exporter may submit Personal Data to Scaleflex and its Affiliates, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospective customers, customers, resellers, referrers, business partners, and vendors of the data exporter (who are natural persons);

- Employees or contact persons of the data exporter's prospective customers, customers, resellers, referrers, subcontractors, business partners, and vendors (who are natural persons);

- Employees, agents, advisors, and freelancers of the data exporter (who are natural persons); and/or

- Natural persons authorized by the data exporter to use the services provided by Scaleflex SAS to the data exporter.

Categories of data
The personal data transferred concern the following categories of data:
The data exporter may submit Personal Data to Scalefle SAS and its Affiliates, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to, the following categories of Personal Data:

- Names, titles, position, employer, contact information (email, phone, fax, physical address etc.), identification data, connection data, or localization data (including IP addresses).

Processing operations

The personal data transferred will be subject to the following basic processing activities:
The objective of the processing of Personal Data by Scaleflex is to provide the Service, pursuant to the Principal Agreement.

On behalf of the data exporter:
[*Populated with details of, and deemed signed on behalf of, the data exporter:*]
Company:
Name (written out in full):
Position:
Address:
Date:

Signature………………………………………

On behalf of the data importer:
Company: Scaleflex SAS
Name (written out in full): Emil Novakov
Position: CEO
Address: 53 Chemin Beauregard, 38330 Saint-Nazaire-Les-Eymes, France
Date: 21.10.2020

Signature………………………………………

Appendix 2

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

See Annex 3 to the DPA.

Annex 3

Security Measures

A. Data importer/sub-processor has implemented and shall maintain a security program in accordance with industry standards.
B. More specifically, data importer/sub-processor's security program shall include:

Access Control of Processing Areas

Data importer/sub-processor implements suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment (namely telephones, database and application servers and related hardware) where the personal data are processed or used, including:

- establishing security areas;
- protection and restriction of access paths;
- establishing access authorizations for employees and third parties, including the respective documentation;
- all access to the data center where personal data are hosted is logged, monitored, and tracked; and
- the data center where personal data are hosted is secured by a security alarm system, and other appropriate security measures.

Access Control to Data Processing Systems

Data importer/sub-processor implements suitable measures to prevent their data processing systems from being used by unauthorized persons, including:

- use of adequate encryption technologies;
- identification of the terminal and/or the terminal user to the data importer/sub-processor and processing systems;
- automatic temporary lock-out of user terminal if left idle, identification and password required to reopen;
- automatic temporary lock-out of the user ID when several erroneous passwords are entered, log file of events, monitoring of break-in-attempts (alerts); and
- all access to data content is logged, monitored, and tracked.

Access Control to Use Specific Areas of Data Processing Systems

Data importer/sub-processor commits that the persons entitled to use their data processing system are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that personal data cannot be read, copied or modified or removed without authorization. This shall be accomplished by various measures including:

- employee policies and training in respect of each employee’s access rights to the personal data;
- allocation of individual terminals and /or terminal user, and identification characteristics exclusive to specific functions;
- monitoring capability in respect of individuals who delete, add or modify the personal data;
- release of data only to authorized persons, including allocation of differentiated access rights and roles;
- use of adequate encryption technologies; and
- control of files, controlled and documented destruction of data.

Availability Control

Data importer/sub-processor implements suitable measures to ensure that personal data are protected from accidental destruction or loss, including:

- infrastructure redundancy; and
- backup is stored at an alternative site and available for restore in case of failure of the primary system.

Transmission Control

Data importer/sub-processor implements suitable measures to prevent the personal data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by various measures including:

- use of adequate firewall, VPN and encryption technologies to protect the gateways and pipelines through which the data travels;
- certain highly confidential employee data (e.g., personally identifiable information such as National ID numbers, credit or debit card numbers) is also encrypted within the system; and
- providing user alert upon incomplete transfer of data (end to end check); and
- as far as possible, all data transmissions are logged, monitored and tracked.

Input Control

Data importer/sub-processor implements suitable input control measures, including:

- an authorization policy for the input, reading, alteration and deletion of data;
- authentication of the authorized personnel;
- protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;
- utilization of unique authentication credentials or codes (passwords);
- providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are kept locked;
- automatic log-off of user ID's that have not been used for a substantial period of time; and
- proof established within data importer/sub-processor’s organization of the input authorization; and

- electronic recording of entries.

Separation of Processing for different Purposes

Data importer/sub-processor implements suitable measures to ensure that data collected for different purposes can be processed separately, including:

- access to data is separated through application security for the appropriate users;
- modules within the data importer/sub-processor's database separate which data is used for which purpose, i.e. by functionality and function;
- at the database level, data is stored in different normalized tables, separated per module, per Controller Customer or function they support; and
- interfaces, batch processes and reports are designed for only specific purposes and functions, so data collected for specific purposes is processed separately.

Documentation

Data importer/sub-processor will keep documentation of technical and organizational measures in case of audits and for the conservation of evidence. Data importer/sub-processor shall take reasonable steps to ensure that persons employed by it, and other persons at the place of work concerned, are aware of and comply with the technical and organizational measures set forth in this Appendix 2.

Monitoring

Data importer/sub-processor shall implement suitable measures to monitor access restrictions to data importer/sub-processor's system administrators and to ensure that they act in accordance with instructions received. This is accomplished by various measures including:

- individual appointment of system administrators;
- adoption of suitable measures to register system administrators' access logs to the infrastructure and keep them secure, accurate and unmodified for at least six months;
- yearly audits of system administrators' activity to assess compliance with assigned tasks, the instructions received by the data importer/sub-processor and applicable laws;
- keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and tasks assigned and providing it promptly to the data exporter upon request.

On behalf of the data exporter:
[*Populated with details of, and deemed signed on behalf of, the data exporter:*]
Company:
Name (written out in full):
Position:
Address:
Date:

Signature……………………………………….

On behalf of the data importer:
Company: Scaleflex SAS
Name (written out in full): Emil Novakov
Position: COO
Address: 53 Chemin Beauregard, 38330 Saint-Nazaire-Les-Eymes,France
Date: 21.10.2020

Signature…………ENovakov.……………………….