Data Processing Addendum (DPA)

www.multitouch-appstore.com | Version 1.0 | Date: 30.09.2020

This eyefactive Data Processing Addendum (the "**DPA**"), including its annexes and appendices, governs the Processing of Personal Data by eyefactive GmbH having a business address at Haferweg 40, 22769 Hamburg, Germany, and the company registration number HRB 158902 ("**eyefactive**") providing touchscreen software applications and the related services (the "**Software**"). This DPA forms the part of the Contract and governs the Processing of Personal Data submitted by an individual user or entity (the "**Customer**") within the scope of the Software. eyefactive and the Customer are hereby collectively referred to as the "**Parties**" and each individually a "**Party**". The DPA explains rights and obligations of the Parties regarding the Processing of Personal Data, where eyefactive acts in the capacity of the Data Processor and the Customer acts in a capacity of the Data Controller. The DPA is drafted in accordance with EU Standard Contractual Clauses attached as Annex I of the DPA.

By signing the DPA, the Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Law, in the name and on behalf of its authorised affiliates, if and to the extent eyefactive Processes the Personal Data for which such authorised affiliates qualify as the Data Controller. The conclusion of this DPA constitutes the acceptance of the EU Standard Contractual Clauses incorporated herein.

HOW TO EXECUTE THIS DPA:

1. This DPA consists of the main body and Annex I.
2. This DPA and its Annex have been pre-signed by eyefactive.
3. To complete the DPA, the Customer must:
   i. Complete the information in the signature box on page 4;
   ii. Sign the DPA; and
   iii. Send the DPA to support (at) eyefactive.com indicating, if applicable, the Customer number.

Upon receipt of the validly completed DPA by eyefactive to the email address indicated above, this DPA will become legally binding.

1. Definitions

In this DPA, the following definitions shall apply:

"**Contract**" shall mean a service agreement concluded between the Parties governing the provision of the Services.

"**Data Controller**" shall have the meaning of "controller" as defined in Art. 4(7) of the GDPR.

"**Processor**", "**Data Processor**", "**Processing**" shall have the meaning of "processor" and "processing" as defined in Art. 4(2) and 4(8) of the GDPR.

"**Data Protection Law**" shall mean the statutory data privacy and protection regulations applicable to the Customer protecting the fundamental rights and freedoms of persons with regard to data privacy and the Processing of Customer's Data by eyefactive.

"**Data Subject**" shall have the meaning of "data subject" as defined in Art. 4(1) of the GDPR.

"**EEA**" shall mean the European Economic Area.

"**EU**" shall mean European Union.

"**GDPR**" shall mean the Regulation (EU) 2016/679 (General Data Protection Regulation).

"**Instruction**" shall mean an instruction issued by the Customer to eyefactive and directing eyefactive to perform a specific action with regard to the Processing of Customer's Data in order to achieve compliance with the Data Protection Law.

"**Customer's Data**" shall mean the Personal Data of which the Customer is the Data Controller.

"**Personal Data**" shall have the meaning as defined in Art. 4(1) of the GDPR related to the Services.

"**Sub-processor**" shall mean an entity that Processes Personal Data as a subcontractor of the Data Processor.

2. Subject matter of Processing

2.1 The Customer engages eyefactive to provide a license to use the Software to the Customer by means of the Contract and agrees that eyefactive shall carry the Processing of Customer's Data, the categories of which are described in Section 4 of this DPA, pursuant to the terms stated herein.

2.2 This DPA stipulates the rights and obligations of the Parties with regard to the Processing of Customer's Data in connection with the Software. It shall apply to all activities within the scope of the Software and the Contract in the context of which eyefactive or the Sub-processors may come into contact with Customer's Data.

2.3 To ensure the transparency of the Processing, the Parties shall keep records of all Processing activities regarding Personal Data as required by Art. 30 of the GDPR.

3. Scope, nature, and purpose of Processing

3.1. eyefactive shall Process Customer's Data on behalf of the Customer as Customer's Processor. The scope, extent, and nature of the Processing are the sole purpose of facilitation of the provision of the Software by eyefactive to the Customer.

3.2. eyefactive shall ensure that any of its officers, directors, employees, consultants, representatives and other natural persons that participate in the Processing of Customer's Data agree to the same restrictions and conditions as those listed in this DPA.

3.3. The Customer as the Data Controller shall be responsible for complying with the applicable Data Protection Law, including, but not limited to, the lawfulness of the Processing and the lawfulness of the transmission (if any) of Customer's Data to eyefactive.

3.4. eyefactive shall Process Customer's Data only to the extent required and with the purpose of fulfilling eyefactive's obligations under the Contract, to the extent necessary for the provision of the Software, and in accordance with Customer's Instructions.

3.5. Should eyefactive wish to use Customer's Data for the purposes that are not specified in this Section 3, eyefactive shall request the Customer to provide prior consent in writing.

4. Categories of Personal Data

4.1. eyefactive shall Process all Customer's Data submitted by the Customer within the scope of the Software. To the extent Customer's Data contains Personal Data, it may consist of Data Subjects' identifying information, such as:

1. First name;
2. Last name;
3. Address;
4. Email address;
5. Company name;
6. VAT number;
7. Position;
8. Payment details;
9. Website address;
10. IP address; and
11. Other personal data submitted by the Customer.

4.2. No special categories of Personal Data as defined in Art. 9(1) of the GDPR are processed according to this DPA, unless the Customer decides, at its sole discretion, to submit such Personal Data for Processing.

5. Categories of Data Subjects

5.1. The affected Data Subjects shall include natural persons whose personal data is supplied by the Customer to eyefactive through the Sofware.

5.2. eyefactive does not interact with the Data Subjects directly in any manner.

6. Duration of Processing

6.1. Except where this DPA expressly stipulates any surviving obligation, this DPA shall follow the term of the Contract.

6.2. eyefactive shall Process Customer's Data for as long as Customer's Data is necessary for the purpose described in Section 3 of this DPA.

6.3. eyefactive shall return to the Customer or securely erase Customer's Data from its storage systems as soon as Customer's Data is no longer necessary for the purpose described in Section 3 of this DPA or the Customer requests eyefactive to do so. Upon request of the Customer, eyefactive shall provide the Customer with a proof of erasure of Customer's Data.

7. Security of Processing

7.1. eyefactive shall exercise a reasonable degree of care to protect Customer's Data from any misuse, unauthorised access, disclosure, and transfer to any third parties unauthorised by the Customer. Such measures shall include, without limitation:

a) Maintaining adequate access control mechanisms (e.g., two-factor authentication, password protection, and limited access) covering any systems, servers, or files in which Customer's Data is stored;

b) DDOS mitigation;

c) Using SSL encryption for any transmission of Customer's Data electronically; and

d) Limiting access to Customer's Data by eyefactive officers, directors, employees, consultants, and representatives only to the purpose stated in Section 3 of this DPA.

7.2. eyefactive hereby declares that it has taken appropriate technical and organisational measures according to Art. 32 GDPR to keep Customer's Data secure and protected against unauthorised or unlawful processing and accidental loss, destruction or damage, and undertakes to continue doing so during the term of this DPA.

7.3. If, under applicable laws, eyefactive is compelled to disclose Customer's Data, eyefactive shall inform the Customer before any such mandatory disclosure within 24 hours after such a disclosure is requested.

7.4. Any significant changes to the security measures listed in Section 7.1 of the DPA shall be documented by eyefactive and reported to the Customer.

7.5. eyefactive shall appropriately document the technical and organisational measures actually implemented (including each update) for the Processing of Customer's Data and will hand out the then current version of such documentation to the Customer, upon Customer's request (e.g., for audit purposes).

7.6. For the purpose of documentation, eyefactive shall be entitled to provide evidence for the implementation of the security measures by providing up-to-date attestations, reports or extracts from independent bodies that scrutinise and confirm the Processing of Customer's Data is in accordance with the agreed to measures herein.

8. Correction and deletion of Personal Data

8.1. eyefactive may be required to correct, erase and/or block Customer's Data if and to the extent the functionality of the Software does not allow the Customer to do so. However, eyefactive shall not correct, erase or block Customer's Data, unless instructed by the Customer.

8.2. Unless mandatory Data Protection Law provides otherwise, there shall not be any direct communication between the Data Subjects and eyefactive. In the event that a Data Subject does apply directly to eyefactive in writing, e.g., to request the correction or deletion of his/her Personal Data, eyefactive shall forward this request to the Customer without undue delay and shall not respond directly to the Data Subject.

9. eyefactive obligations

9.1. eyefactive shall:

a) Process Customer's Data only on documented instructions from the Customer;

b) Ensure that persons authorised to Process Customer's Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. eyefactive shall regularly train those persons to whom it grants access to Customer's Data on IT security and privacy law compliance. The undertaking to data secrecy shall continue after the termination of this DPA;

c) Implement appropriate technical and organisational security measures to ensure a level of security appropriate to Customer's Data;

d) Ensure that any natural person acting under the authority of eyefactive who has access to the Personal Data does not process them except on instructions from the Customer;

e) Assist the Customer in compliance with Customer's obligations under Art. 32 to 36 of the GDPR;

f) Make available to the Customer all information necessary to demonstrate compliance with eyefactive obligations under the DPA, the Data Protection Law, and allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer;

g) Appoint a data protection officer if it is legally obliged to do so or, if it is not obliged to do so, a contact person for data protection issues;

h) Provide the Customer, upon request in writing, with the name and contact details of its data protection officer or the contact person for data protection issues;

i) Monitor the Processing by way of regular reviews concerning the performance of and compliance with this DPA, the Contract, and the applicable Data Protection Law;

j) At Customer's written request, reasonably support the Customer in dealing with requests from individual Data Subjects and/or a supervisory authority with respect to the Processing of Personal Data hereunder;

k) Assist the Customer with the implementation of appropriate technical and organisational measures in order to respond to applications by the Data Subjects for the exercise of their rights (in particular, Art. 13 to 23 of the GDPR);

l) Provide at minimum the information set out in Art. 33(3) of the GDPR in the case of a Personal Data breach;

9.2. eyefactive commits to observe any and all other duties that are imposed to eyefactive pursuant to Art. 28 of the GDPR.

9.3. eyefactive shall collaborate with Customer's data protection officer to generate the records of processing activities, pursuant to Art. 30 of the GDPR, and provide all the necessary details to the Customer.

10. Sub-processors

10.1. The Customer hereby authorises eyefactive to engage Sub-processors as further specified in this Section 10, provided that eyefactive remains responsible for any acts or omissions of its Sub-processors in the same manner as for its own acts and omissions hereunder.

10.2. eyefactive may remove or appoint suitable and reliable other Sub-processor(s) at its own discretion in accordance with the following conditions:

a) eyefactive shall inform the Customer 30 days in advance of any envisaged changes to the list of Sub-processors;

b) If the Customer has a legitimate data protection related reason to object to eyefactive use of Sub-processor(s), the Customer shall notify eyefactive within fourteen (14) days after receipt of the eyefactive notice;

c) If the Customer does not object during this time period, the new Sub-processor(s) shall be deemed accepted;

d) If the Customer objects to the use of the Sub-processor(s) concerned, eyefactive shall have the right to cure the objection through one of the following options (to be selected at eyefactive sole discretion):

i. eyefactive will abort its plans to use the Sub-processor(s) with regard to Customer's Data; or

ii. eyefactive will take corrective steps and proceed to use the Sub-processor(s) with regard to Customer's Data.

e) If eyefactive decides not to implement option 10.2.d.i or 10.2.d.ii above, eyefactive shall notify the Customer without undue delay. In this case, the Customer shall be entitled within further fourteen (14) days to notify in writing eyefactive about its termination of the DPA and any such termination would become effective upon the expiry of the second (2nd) calendar month after eyefactive receipt of the termination notice.

10.3. eyefactive shall pass on to its subcontractors acting as the Sub-processors eyefactive obligations under this DPA.

10.4. The exhaustive list of the Sub-processors used by eyefactive shall be provided upon Customer's request and includes without limitation the following subcontractors:

· Hosting and cloud storage service providers Netcup (https://www.netcup.eu) located in Germany and AWS (https://aws.amazon.com) located in the United States;

· Newsletter service provider CleverReach (https://www.cleverreach.com/en) located in Germany;

· Marketing and advertising service providers Google (https://www.google.com), Facebook (https://www.facebook.com), and Twitter (https://twitter.com) located in the United States; and

· eyefactive independent contractors and consultants.

11. Personal Data breaches

11.1. Within 24 hours after eyefactive becomes aware of any unauthorised use or disclosure of Customer's Data, eyefactive shall promptly report the unauthorised use or disclosure of the Customer's Data to the Customer.

11.2. eyefactive shall cooperate with any remediation that the Customer, in its discretion, determines is necessary to (i) address any applicable reporting requirements and (ii) mitigate any effects of unauthorised use or disclosure of the Customer's Data.

11.3. In consultation with the Customer, eyefactive must take appropriate measures to secure Customer's Data and limit any possible detrimental effect on the Data Subjects. Where obligations are placed on the Customer under the Data Protection Law, eyefactive shall provide commercially reasonable assistance in meeting them.

12. Notifications

12.1. If eyefactive receives a request, subpoena or court order (including through an obligation due to legal provisions or official injunctions from state authorities) requesting to provide any Customer's Data to an authority, eyefactive shall attempt to redirect the relevant authority to request that data directly from the Data Controller, and notify the Customer without undue delay.

12.2. Where Customer's Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while in eyefactive control, eyefactive shall notify the Customer of such action without undue delay.

13. Instructions

13.1. The Instructions to eyefactive are initially laid out in this DPA. However, the Customer shall be entitled to issuing modifications to Instructions and to issue new Instructions, subject to feasibility.

13.2. The Customer shall designate a person competent to issue the

Instructions. Modifications or new Instructions shall be issued in writing and shall need to be agreed between the Parties as a contract modification/change request under this DPA.

13.3. eyefactive shall notify the Customer if eyefactive considers any Instruction to be in violation of the applicable Data Protection Law. eyefactive shall not be obligated to perform a comprehensive legal examination and shall in no event render any legal services to the Customer.

13.4. eyefactive shall not be responsible for any consequences of the Instructions issued by the Customer and the Customer shall indemnify and hold eyefactive harmless against any damages and third-party claims resulting from the Instruction.

13.5. Unless otherwise agreed, eyefactive shall be entitled to charge any efforts incurred in connection with the Instructions on time and material basis.

14. Miscellaneous

14.1. No modification of this DPA shall be valid and binding unless made in writing and then only if such modification expressly states that such modification applies to the regulations of this DPA. The foregoing shall also apply to any waiver or modification of this mandatory written form.

14.2. This DPA shall take precedence over any conflicting provisions of the Contract.

14.3. This DPA will commence on the date when both Parties sign the DPA and continue until terminated earlier by either Party.

14.4. eyefactive may terminate this DPA for any reason upon thirty (30) calendar days' notice to the Customer. Upon Customer's termination of the Contract, this DPA shall terminate automatically.

14.5. Each Party may terminate this DPA with immediate effect by delivering a notice of the termination to the other Party if:

a) The other Party fails to perform, has made or makes any inaccuracy in, or otherwise materially breaches, any of its obligations, covenants, or representations; and

b) The failure, inaccuracy, or breach continues for a period of thirty (30) calendar days' after the injured Party delivers notice to the breaching Party reasonably detailing the breach.

14.6. If either Party becomes insolvent, bankrupt, or enters receivership, dissolution, or liquidation, the other Party may terminate this DPA with immediate effect.

14.7. Upon expiration or termination of this DPA or on Customer's request, eyefactive shall:

a) Promptly securely delete or return any Customer's Data available to eyefactive and any other information and documents, provided by the Customer; and

b) Deliver to the Customer a certificate confirming eyefactive compliance with the destruction obligation under this Section 14.7.

14.8. Neither Party may assign this DPA or any of their rights or obligations under this DPA without the other Party's prior consent.

14.9. The Parties shall attempt to resolve any dispute arising out of or relating to this DPA in a good faith through negotiations between senior executives of the Parties, who have authority to settle the same. If the matter is not resolved by negotiation within thirty (30) days of receipt of a written invitation to negotiate, the dispute shall be resolved by using binding arbitration services.

14.10. The headings used in this DPA and its division into sections, schedules, exhibits, appendices, and other subdivisions do not affect its interpretation.

14.11. If there is any inconsistency between the terms of this DPA and those in any document entered into under this DPA, the terms of this DPA shall prevail. The Parties shall take all necessary steps to conform the inconsistent terms to the terms of this DPA.

Attached Annex I: Commission Decision C(2010)593 Standard Contractual Clauses (processors)

The Parties have executed this DPA on the date indicated below:

EYEFACTIVE

Name (Print)

Title

Location, Date

Signature

THE CUSTOMER

Name (Print)

Title

Location, Date

Signature

ANNEX I

EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE

Directorate C: Fundamental rights and Union citizenship
Unit C.3: Data protection

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting Organization: *the name of the the Customer using the Software*

Address: *the address of the Customer using the Software*

Tel.: *the phone number of the Customer using the Software*

E-mail: *the email address of the Customer using the Software*

(the data **exporter**)

And

Name of the data importing Organization: *eyefactive GmbH*

Address: *Haferweg 40, 22769 Hamburg, Germany*

Tel.: *+49 9999 695* – 0

E-mail: *support (at) eyefactive.com*

Other information needed to identify the Organization: *company registration number HRB 158902*

(the data **importer**)

each a "party"; together "the 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.

Clause 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 Directive 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[1];

(b) '*the data exporter'* means the controller 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 Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

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;

(f) *'technical and Organizational 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.

Clause 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.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(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.
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. The data subject can enforce against the subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.
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.

Clause 4

Obligations of the data exporter

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 Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor 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 subprocessing 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 subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor 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).

Clause 5

Obligations of the data importer[2]

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 Organizational 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 subprocessing, 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

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

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 subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

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 subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

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 subprocessor 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 of 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 subprocessor of its obligations in order to avoid its own liabilities.

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 subprocessor 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 subprocessor agrees that the data subject may issue a claim against the data subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

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.

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.

Clause 8

Cooperation with supervisory authorities

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.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, 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.

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

Clause 9

Governing Law

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

Clause 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.

Clause 11

Subprocessing

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 subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[3]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing 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.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor 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.
2. The data importer and the subprocessor 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.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

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 (please specify briefly your activities relevant to the transfer): *a business entity using the touchscreen software provided by the data importer.*

Data importer

The data importer is (please specify briefly activities relevant to the transfer): *the provider of touchscreen software (more information: https://www.eyefactive.com).*

[3] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify): *the affected data subjects include natural persons whose personal data is submitted by the data exporter to the data importer within the scope of the services provided by the data importer to the data exporter.*

Categories of data

The personal data transferred concern the following categories of data (please specify): *first name, last name, address, email address, company name, VAT number, position, payment details, website address, IP address, and other personal data submitted by the data importer.*

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify): *no special categories of data as defined in Art. 9(1) of the GDPR should be submitted by the data exporter.*

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify): *collection, recording, organisation, structuring, storage, retrieval, consultation, use, disclosure by transmission, dissemination and otherwise making available personal data within the scope of the services provided by the data importer to data exporter.*

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):

1. *Secured networks;*
2. *SSL encryption;*
3. *Strong passwords;*
4. *Limited access to personal data by data importer's staff; and*
5. *Anonymisation of personal data (when possible).*

INDEMNIFICATION CLAUSE

Liability

The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon:

(a) the data exporter promptly notifying the data importer of a claim; and

(b) the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim[4].

[4] Paragraph on liabilities is optional.