EAGLESTATUS DATA PROCESSING ADDENDUM
(*Revision August 2021*)

This Data Processing Addendum ("**DPA**") is part of the Terms of Service and Privacy Policy, both as updated from time to time, or other written or electronic agreement between EagleStatus and Customer for the purchase and/or use of online services (including associated EagleStatus mobile components) from EagleStatus (identified either as "Services" or otherwise in the applicable agreement, and hereinafter defined as "**Services**") (the "**Agreement**") to reflect the parties' agreement with regard to the Processing of Personal Data.

Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of Customer's Authorized Affiliates, if and to the extent EagleStatus processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Services to Customer pursuant to the Agreement, EagleStatus may Process Personal Data on behalf of Customer and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

DATA PROCESSING TERMS

1. DEFINITIONS

"Affiliate" means (a) any entity on whose behalf Customer obtained the EagleStatus Services, and/or (b) any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"**Authorized Affiliate**" means any of Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and EagleStatus, but has not signed its own Agreement with EagleStatus and is not a "Customer" as defined under the Agreement.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"Customer Data" means what is described in the EagleStatus Privacy Policy as "your data", "your info" or similar terms.

"Data Protection Laws and Regulations" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.

"Data Subject" means the identified or identifiable person to whom Personal Data relates.

"**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"Personal Data" means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Customer Data.

"Processing" (including its various forms) means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Processor" means the entity which Processes Personal Data on behalf of the Controller.

"Security, Privacy and Architecture Documentation" means EagleStatus's security overview and security whitepaper, as updated from time to time, and accessible via an email request to support@eaglestatus.io, EagleStatus's Privacy Policy, as updated from time to time, and accessible via https://about.eaglestatus.io/privacy-policy.html, or as otherwise made reasonably available by EagleStatus.

"EagleStatus" means the EagleStatus entity which is a party to this DPA, as specified in the section "HOW THIS DPA APPLIES" above, being EagleStatus, Inc, a C-corp Company.

"Standard Contractual Clauses" means the agreements entered into by and between Customer and EagleStatus and attached hereto as Schedules 3 and 4 for the international transfer of personal data to third countries which according to the European Commission, the Swiss Federal Council, and/or the UK Government do not ensure an adequate level of data protection.

"Sub-processor" means any Processor engaged by EagleStatus.

"**Supervisory Authority**" means an independent public authority which is established by an EEA State pursuant to the GDPR, the UK's Information Commissioner's Office and/or the Swiss Federal Data Protection and Information Commissioner.

2. PROCESSING OF PERSONAL DATA

2.1 **Roles of the Parties.** The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is always a Controller of Personal Data and EagleStatus is either a Controller or a Processor depending on the type of and purpose for which the Personal Data are Processed. In particular, the parties acknowledge and agree that EagleStatus Processes Personal Data as a:

2.1.1 **Processor**: in the course of the provision of project management and email services to Customer. Where EagleStatus is Processing Personal Data as a Processor clauses 2.2 and 3 through 12 of this DPA shall apply to the Processing of Personal Data by EagleStatus; and

2.1.2 **Controller**: for purposes of Customer account management and billing, direct marketing, Customer support services, data analytics, information security, product fulfilment, in connection with surveys, competitions and blogs. Where EagleStatus is Processing Personal Data as a Controller clauses 2.2, 11, and 12.3 of this DPA shall apply to the Processing of Personal Data by EagleStatus.

2.2 **Customer's Processing of Personal Data.** Customer shall, in its use of the Services:

2.2.1 Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data (where EagleStatus is Processing Personal Data as a Processor) shall comply with Data Protection Laws and Regulations;

2.2.2 have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data;

2.2.3 have provided adequate notices to, and obtained valid consents from, any data subjects, relating to the Processing (including the sharing) of Personal Data by Customer and as applicable, to the transfer of such Personal Data outside of the EEA/Switzerland/UK; and

2.2.4 shall not, by act or omission, cause EagleStatus to violate any Data Protection Laws and Regulations, notices provided to, or consents obtained from, data subjects as result of Processing the Personal Data.

3. EAGLESTATUS'S PROCESSING OF PERSONAL DATA

3.1 EagleStatus shall treat Personal Data as confidential information and shall only Process Personal Data on behalf of and in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement; (ii) Processing initiated by Customers and/or Invited Users in their use of the Services; and
(iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

3.2 **Details of the Processing.** The subject-matter of Processing of Personal Data by EagleStatus is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 2 (Details of the Processing) to this DPA.

4. DATA SUBJECT REQUESTS

EagleStatus shall, to the extent legally permitted, promptly notify Customer if EagleStatus receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("Data Subject Request"). Taking into account the nature of the Processing, EagleStatus shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, EagleStatus shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent EagleStatus is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from EagleStatus's provision of such assistance.

5. EAGLESTATUS PERSONNEL

5.1 **Confidentiality.** EagleStatus shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. EagleStatus shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

5.2 **Reliability.** EagleStatus shall take commercially reasonable steps to ensure the reliability of any EagleStatus personnel engaged in the Processing of Personal Data.

5.3 **Limitation of Access.** EagleStatus shall ensure that EagleStatus's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

5.4 **Data Protection Officer.** Based on EagleStatus's processing activities, EagleStatus is not required to appoint a Data Protection Officer. EagleStatus reserves the right to voluntarily appoint a Data Protection Officer in the future. For questions about this DPA, GDPR compliance, data privacy, Privacy Shield, or any other privacy issues please send an email to support@eaglestatus.io .

6. SUB-PROCESSORS

6.1 **Appointment of Sub-processors.** Customer acknowledges and agrees that (a) EagleStatus's Affiliates may be retained as Sub-processors; and (b) EagleStatus and

EagleStatus's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. EagleStatus or a EagleStatus Affiliate has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA with respect to the protection of Customer Data to the extent applicable to the nature of the Services provided by such Sub-processor.

6.2 **List of Current Sub-processors and Notification of New Sub-processors.** EagleStatus shall make available to Customer the current list of Sub-processors for the EagleStatus Services. Such Sub-processor lists shall include the identities of those Sub-processors and their country of location ("**Sub-processor Documentation**"). Customer may find on EagleStatus's webpage at https://about.eaglestatus.io/privacy-policy.html the Sub-processor Documentation. EagleStatus, through notification to the Customer shall provide notification of a new Sub-processor(s) before authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Services.

6.3 **Objection Right for New Sub-processors.** Customer may object to EagleStatus's use of a new Sub-processor by notifying EagleStatus promptly in writing within ten (10) business days after receipt of EagleStatus's notice in accordance with the mechanism set out in Section 6.2. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, EagleStatus will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected- to new Sub-processor without unreasonably burdening the Customer. If EagleStatus is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the applicable Agreement with respect only to those Services which cannot be provided by EagleStatus without the use of the objected-to new Sub-processor by providing written notice to EagleStatus. EagleStatus will refund Customer any prepaid fees covering the remainder of the term of such Agreement following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.

6.4 **Liability.** EagleStatus shall be liable for the acts and omissions of its Sub-processors to the same extent EagleStatus would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

7. SECURITY

7.1 **Controls for the Protection of Customer Data.** EagleStatus shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data, as set forth in the Security, Privacy and Architecture Documentation. EagleStatus regularly monitors compliance with these measures. EagleStatus will not materially decrease the overall security of the Services during a subscription term.

7.2 **Third-Party Certifications and Audits.** EagleStatus has obtained the third-party certifications and audits set forth in the Security, Privacy and Architecture Documentation. Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, EagleStatus shall make available to Customer that is not a competitor of EagleStatus (or Customer's independent, third- party auditor that is not a competitor of EagleStatus) a copy of EagleStatus's then most recent third- party audits or certifications, as applicable.

8. CUSTOMER DATA INCIDENT MANAGEMENT AND NOTIFICATION

EagleStatus maintains security incident management policies and procedures specified in the Security, Privacy and Architecture Documentation and the Agreement. EagleStatus shall, notify Customer without undue delay, and in compliance with applicable laws, after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, including Personal Data, transmitted, stored or otherwise Processed by EagleStatus or its Sub-processors of which EagleStatus becomes aware (a "**Customer Data Incident**"). EagleStatus shall make reasonable efforts to identify the cause of such Customer Data Incident and take those steps as EagleStatus deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident to the extent the remediation is within EagleStatus's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's Invited Users.

9. RETURN AND DELETION OF CUSTOMER DATA

EagleStatus shall return Customer Data to Customer and, to the extent allowed by applicable law, delete Customer Data in accordance with the procedures and timeframes specified in the Security, Privacy and Architecture Documentation.

10. AUTHORIZED AFFILIATES

10.1 **Contractual Relationship.** The parties acknowledge and agree that, by entering into the DPA, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between EagleStatus and each such Authorized Affiliates subject to the provisions of the Agreement and this Section 10. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, by Customer entering into this DPA, an Authorized Affiliate is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the Services and Content by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

10.2 **Communication.** The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with EagleStatus under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliate.

10.3 **Rights of Authorized Affiliates.** Where an Authorized Affiliate becomes a party to the DPA with EagleStatus, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

   10.3.1 Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against EagleStatus directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for all of its Authorized Affiliates together (as set forth, for example, in Section 10.3.2, below).

   10.3.2 The parties agree that the Customer that is the contracting party to the Agreement shall, when carrying out an on-site audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on EagleStatus and its Sub-processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of different Authorized Affiliates in one single audit.

11. LIMITATION OF LIABILITY

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and EagleStatus, whether in contract, tort or under any other theory of liability, is subject to the limitations of liability set forth in the Agreement, and such limitations apply to the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAstogether.

For the avoidance of doubt, EagleStatus's and its Affiliates' total liability for all claims from the Customer and all of its Authorized Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Customer and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA.

Also for the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Schedules and Appendices.

12. EUROPEAN SPECIFIC PROVISIONS

12.1 **GDPR.** EagleStatus will Process Personal Data in accordance with Data Protection Laws and Regulations including the GDPR requirements directly applicable to EagleStatus's provision of its Services.

12.2 **Data Protection Impact Assessment.** Upon Customer's request, EagleStatus shall provide Customer with reasonable cooperation and assistance needed to fulfill Customer's obligation under the GDPR, or other Data Protection Laws and Regulations, to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to EagleStatus. EagleStatus shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to Section 12.2 of this DPA, to the extent required under the GDPR or other Data Protection Laws and Regulations.

12.3 **Transfer mechanisms for data transfers.** Subject to the additional terms in Schedule 1, EagleStatus makes available the transfer mechanisms listed below which shall apply, to any transfers of Personal Data under this DPA from the European Economic Area and/or their member states, Switzerland and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations of the foregoing territories, to the extent such transfers are subject to such Data Protection Laws and Regulations:

12.3.1 The Standard Contractual Clauses set forth in Schedule 3 to this DPA apply to transfers of personal data made in connection with the Processing described in clause 2.1.1 of this DPA subject to the additional terms in Schedule 1;

12.3.2 The Standard Contractual Clauses set forth in Schedule 4 to this DPA apply to transfers of personal data made in connection with the Processing described in clause 2.1.2 of this DPA (other than as described in clause 12.3.3 below) subject to the additional terms in Schedule 1; and

12.3.3 Article 49(1)(b) of the GDPR (the transfer is necessary for the performance of a contract), and the equivalent provisions in the Data Protection Laws and Regulations, applies to transfers of personal data made in connection with product fulfilment, in connection with surveys, newsletters and blogs, in connection with providing Customer support to prospective Customers, and in connection with recruiting for prospective new hires.

List of Schedules

Schedule 1: Transfer Mechanisms for European Data Transfers
Schedule 2: Details of the Processing
Schedule 4: Standard Contractual Clauses (controller to processor)
Schedule 5: Standard Contractual Clauses (controller to controller)

The parties' authorized signatories have duly executed this Agreement:

CUSTOMER

Signature:_____

Customer Legal Name:_____

Print Name: _____

Title:
_____

 Date: _
_____

EAGLESTATUS

Signature:_____

Print Name:__S A M

G A T H E R C O L E____.

Title:__CEO_____.

Date: December 2, 2021_____

SCHEDULE 1
TRANSFER MECHANISMS FOR EUROPEAN DATA TRANSFERS

1. ADDITIONAL TERMS FOR SCC SERVICES

1.1 Customers covered by the Standard Contractual Clauses. The Standard Contractual Clauses and the additional terms specified in this Section 1 of this Schedule 1 apply to (i) the legal entity that has entered into the Standard Contractual Clauses as a data exporter and its Invited Users and (ii) all Affiliates, including, but not limited to, Invited Users of Customer established within the European Economic Area, Switzerland and the United Kingdom, which have entered into Agreements for the SCC Services. For the purpose of the Standard Contractual Clauses and this Schedule 1, the aforementioned entities shall be deemed "data exporters".

1.2 Instructions. This DPA and the Agreement are Customer's complete and final documented instructions to EagleStatus for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of Schedule 3, the following is deemed an instruction by the Customer to process Personal Data: (a) Processing in accordance with the Agreement; (b) Processing initiated by Users in their use of the Services and (c) Processing to comply with other reasonable documented instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

1.3 Appointment of new Sub-processors and List of current Sub-processors. Pursuant to Clause 5(h) of Schedule 3 and Annex A of Schedule 4, Customer acknowledges and expressly agrees that (a) EagleStatus's Affiliates may be retained as Sub-processors; and
(b) EagleStatus and EagleStatus's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. For purposes of Clause 5(h) of Schedule 3, EagleStatus shall make available to Customer the current list of Sub-processors in accordance with Section 6.2 of this DPA

2.4 Notification of New Sub-processors and Objection Right for new Sub-processors. Pursuant to Clause 5(h) of Schedule 3, Customer acknowledges and expressly agrees that EagleStatus may engage new Sub-processors as described in Sections 6.2 and 6.3 of the DPA.

25. Copies of Sub-processor Agreements. The parties agree that the copies of the Sub-processor agreements that must be provided by EagleStatus to Customer pursuant to Clause 5(j) of Schedule 3 may have all commercial information, or clauses unrelated to the Standard Contractual Clauses in Schedule 3 or their equivalent, removed by EagleStatus beforehand; and, that such copies will be provided by EagleStatus, in a manner to be determined in its discretion, only upon request by Customer.

26. **Audits and Certifications.** The parties agree that the audits described in Clause 5(f) and Clause 12(2) of Schedule 3 and Clause II(g) of Schedule 4 shall be carried out in accordance with Clause 7.2 of the DPA.

27. **Certification of Deletion.** The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of Schedule 3 shall be provided by EagleStatus to Customer only upon Customer's request.

28. **Conflict.** In the event of any conflict or inconsistency between the body of this DPA and any of its Schedules (not including the Standard Contractual Clauses) and the Standard Contractual Clauses in Schedule 5, the Standard Contractual Clauses shall prevail.

SCHEDULE 2
DETAILS OF THE
PROCESSING

Nature and Purpose of Processing
EagleStatus will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the DPA, and as further instructed by Customer in its use of the Services.

Duration of Processing
Subject to Section 8 of the DPA, EagleStatus will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Categories of Data Subjects
Customer may submit Personal Data to the Services, the categories, extent and detail of which is determined and controlled by Customer in its sole discretion.

Type of Personal Data
Customer may submit Personal Data to the Services, the type, extent and detail of which is determined and controlled by Customer in its sole discretion.

SCHEDULE 3
STANDARD CONTRACTUAL CLAUSES
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.

The entity identified as "Customer" in the DPA (the data **exporter)**

and

EagleStatus, Francisco Martinez 2, Valencia 46020, Spain (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;

(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 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, unauthorized 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 organizational 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, unauthorized 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

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 thecontract;

(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 enforcementinvestigation,

(ii) any accidental or unauthorized access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized 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 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 casethe 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. 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.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature:_____

(stamp of organization)

On behalf of the data importer:

Name (written out in full): Sam
Payá Gathercole
 Position: CEO
Address: Francisco Martinez 2, Valencia 46020, Valencia Spain
Other information necessary in order for the contract to be binding (if any): Not applicable.

Signature:_____

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the 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):

Data exporter is (i) the Customer which as a legal entity or as an individual has entered into the Standard Contractual Clauses as a data exporter and, (ii) all Affiliates (as defined in the Agreement) of Customer established within the European Economic Area (EEA) and Switzerland that have purchased Services on the basis of one or more subscription(s).

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

EagleStatus is a cloud-based software-as-a-service provider of collaboration and communication software which processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

As defined in Schedule 2 of the DPA

Categories of data

The personal data transferred concern the following categories of data (please specify):

As defined in Schedule 2 of the DPA

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

Data exporter may submit special categories of data to EagleStatus, the type, category, extent and detail of which is determined and controlled by the data exporter in its sole discretion.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

The objective of Processing of Personal Data by data importer is the performance of EagleStatus's Services pursuant to the Agreement.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses.

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

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services, as described in the Security, Privacy and Architecture Documentation applicable to the specific Services purchased by data exporter. Data Importer will not materially decrease the overall security of the Services during a subscription term.

SCHEDULE 4
STANDARD CONTRACTUAL CLAUSES
Standard Contractual Clauses (controllers)

Data transfer agreement

between

The entity identified as "**Customer**" in the DPA (the data **exporter)**

and

EagleStatus, Fracisco Martinez 2, Valencia 46020, Spain (hereinafter the "**data importer**")

each a "party"; together "the parties".

Definitions

For the purposes of the clauses:

a) "personal data", "special categories of data/sensitive data", "process/processing", "controller", "processor", "data subject" and "supervisory authority/authority" shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby "the authority" shall mean the competent data protection authority in the territory in which the data exporter is established);

b) "the data exporter" shall mean the controller who transfers the personal data;

c) "the data importer" shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country's system ensuring adequate protection;

d) "clauses" shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

I. Obligations of the data exporter

The data exporter warrants and undertakes that:

a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.

d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.

e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority whererequired.

II. Obligations of the data importer

The data importer warrants and undertakes that:

a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

b) It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.

c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any suchlaws.

d) It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.

e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).

f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).

g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.

h) It will process the personal data, at its option, in accordance with:

 i. the data protection laws of the country in which the data exporter is established, or

 ii. the relevant provisions [1] of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data[2], or

 iii. the data processing principles set forth in Annex A.

  Data importer to indicate which option it selects: Option (iii)

  Initials of data importer....JF..;

i) It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

 i. the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

 ii. the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

---

[1] "Relevant provisions" means those provisions of any authorisation or decision except for the enforcement provisions of any authorisation or decision (which shall be governed by these clauses).

[2] However, the provisions of Annex A.5 concerning rights of access, rectification, deletion and objection must be applied when this option is chosen and take precedence over any comparable provisions of the Commission Decision selected.

iii. data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards,or

iv. with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer

III. Liability and third party rights

a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

IV. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

V. Resolution of disputes with data subjects or the authority

a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

c) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

VI. Termination

a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

b) In the event that:

    i. the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

    ii. compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

    iii. the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

    iv. a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or

    v. a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VII. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VIII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

ANNEX A

DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.

2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.

4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.

7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to "opt-out" from having his data used for such purposes.

8. Automated decisions: For purposes hereof "automated decision" shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

    a)   i.   such decisions are made by the data importer in entering into or performing a contract with the data subject, and

          ii.   the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

   or

  c) where otherwise provided by the law of the data exporter.

ANNEX B

DESCRIPTION OF THE TRANSFER

Data subjects

The personal data transferred concern the following categories of data subjects:

As defined in Schedule 2 of the DPA

Purposes of the transfer(s)
The transfer is made for the following purposes:

As defined in Clause 12.3.2 of the DPA

Categories of data
The personal data transferred concern the following categories of data:

As defined in Schedule 2 of the DPA

Recipients
The personal data transferred may be disclosed only to the following recipients or categories of recipients on a need-to-know basis:

As defined in the Security, Privacy and Architecture Documentation

Sensitive data
The personal data transferred concern the following categories of sensitive data:

Data exporter may submit special categories of data to EagleStatus, the type, category, extent and detail of which is determined and controlled by the data exporter in its sole discretion.

Data protection registration information of data exporter
Not applicable

Additional useful information
Not applicable

Contact points for data protection enquiries
As set out in DPA