



## EEA DATA PROCESSING AGREEMENT (Module 3 Processor to Processor)

This Data Processing Agreement is made the 25th day of November 2022 between:

- (1) **Exclaimer Europe B.V.** having its registered office at Bollenmarkt 8 E, 1681 PJ Zwaagdijk-Oost, The Netherlands (Chamber of Commerce registration number 37161598) (hereinafter referred to as “us”, “we” or “Exclaimer” and “Data Importer”); and
- (2) **SHL Group Limited** whose registered office/place of business is at The Pavilion, 1 Atwell Place, Thames Ditton, Surrey KT7 ONE (hereinafter referred to as “you”, “your” or “Partner” and “Data Exporter”).

Capitalized terms used but not defined in this Data Processing Agreement (including the Appendix) have the meanings given to them in the agreement into which these Clauses are incorporated (the "Master Agreement").

### STANDARD CONTRACTUAL CLAUSES SECTION I

#### **Clause 1**

##### **Purpose and scope**

1. The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation)<sup>1</sup> for the transfer of personal data to a third country.
2. The Parties:
  - a. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter ‘entity/ies’) transferring the personal data, as listed in Annex 1 (hereinafter each ‘data exporter’), and
  - b. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex 1 (hereinafter each ‘data importer’) have agreed to these standard contractual clauses (hereinafter: ‘Clauses’).
3. These Clauses apply with respect to the transfer of personal data as specified in Annex 1.
4. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

#### **Clause 2**

##### **Effect and invariability of the Clauses**

1. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
2. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

#### **Clause 3**

##### **Third-party beneficiaries**

1. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  - a. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - b. Clause 8 – Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

# exclaimer

- c. Clause 9 – Clause 9(a), (c), (d) and (e);
  - d. Clause 12 – Clause 12(a), (d) and (f);
  - e. Clause 13;
  - f. Clause 15.1(c), (d) and (e);
  - g. Clause 16(e);
  - h. Clause 18 – Clause 18(a) and (b);
2. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679. **Clause 4 Interpretation**
1. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
  2. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
  3. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

## **Clause 5**

### **Hierarchy**

In the event of a contradiction between these Clauses and the provisions of the Master Agreement between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

## **Clause 6**

### **Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex 1.

## **Clause 7 – Not used**

## **SECTION II – OBLIGATIONS OF THE PARTIES**

## **Clause 8**

### **Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

### **8.1 Instructions**

1. The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.
2. The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.
3. The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.
4. The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter<sup>5</sup>.

### **8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex 1, unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

### **8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On



request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

#### **8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

#### **8.5 Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex 1. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

#### **8.6 Security of processing**

1. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex 2. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
2. The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
3. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
4. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.



### **8.7 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex 1.

### **8.8 Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union<sup>6</sup> (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation. **8.9 Documentation and compliance**

1. The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.
2. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.
3. The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.
4. The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of noncompliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer. In normal circumstances the Data Exporter agrees that Data Importer's ISO27001 certification and information relating thereto shall satisfy Data Exporter's rights to information herein.
5. Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.
6. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice but always at the sole cost and expense of the Data Exporter, including paying for the reasonable costs of the Data Importer in assisting with the audit.
7. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

### **Clause 9**

#### **Use of sub-processors**

1. The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list in Annex 3. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).



2. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects<sup>9</sup>. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the subprocessor complies with the obligations to which the data importer is subject pursuant to these Clauses.
3. The data importer shall provide, at the data exporter's or controller's request, a copy of such a subprocessor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
4. The data importer shall remain fully responsible to the data exporter for the performance of the subprocessor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
5. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the subprocessor to erase or return the personal data.

#### **Clause 10**

##### **Data subject rights**

1. The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.
2. The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
3. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

##### **Clause 11 Redress**

1. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
2. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
3. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
  - a. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - b. refer the dispute to the competent courts within the meaning of Clause 18.
4. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
5. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
6. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.



### **Clause 12**

#### **Liability**

1. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
2. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
3. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the thirdparty beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
4. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
5. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
6. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
7. The data importer may not invoke the conduct of a sub-processor to avoid its own liability. **Clause 13**

#### **Supervision**

1. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex 1, shall act as competent supervisory authority. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex 1, shall act as competent supervisory authority.
2. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

### **SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES Clause 14**

#### **Local laws and practices affecting compliance with the Clauses**

1. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
2. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
  - a. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers;





- the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
- b. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards<sup>12</sup>;
  - c. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
3. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
  4. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
  5. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The data exporter shall forward the notification to the controller.
  6. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply. **Clause 15**

**Obligations of the data importer in case of access by public authorities 15.1 Notification**

1. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
  - a. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - b. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer. The data exporter shall forward the notification to the controller.
2. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
3. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.



4. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
5. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

#### **15.2 Review of legality and data minimisation**

1. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
2. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. The data exporter shall make the assessment available to the controller.
3. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

#### **SECTION IV – FINAL PROVISIONS**

##### **Clause 16**

##### **Non-compliance with the Clauses and termination**

1. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
2. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
3. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
  - a. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
  - b. the data importer is in substantial or persistent breach of these Clauses; or
  - c. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority and the controller of such noncompliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

4. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
5. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of





personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679. **Clause 17**

#### **Governing law**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands.

#### **Clause 18**

##### **Choice of forum and jurisdiction**

1. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
2. The Parties agree that those shall be the courts of Ireland.
3. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
4. The Parties agree to submit themselves to the jurisdiction of such courts.

(1) Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing

---

Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(2) Not applicable (3) Not applicable

(4) Not applicable

(5) See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

(6) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

(7) Not applicable

(8) Not applicable

(9) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(10) Not applicable

(11) Not applicable

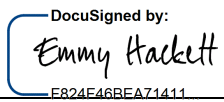
(12) As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

**SIGNED**



**EXCLAIMER EUROPE B.V.**

**SHL GROUP LIMITED**

Signature	Signature  F824E46BEA71411
Print Name	Print Name Emmy Hackett
Title	Title General Counsel
Date	Date 01 December 2022



## Annex 1 Processing Services

SCOPE AND PURPOSE OF PROCESSING	<p>We will process Personal Data provided by you or collected by us in order to manage your or your customer's account with us and to fulfil our contractual obligations to you and them. We may also process Personal Data to analyse trends and to track usages of and interactions with our Services to the extent necessary for our legitimate interest in developing and improving our Services and providing customers with more relevant content and service offerings.</p> <p>We will process the Personal Data for the duration of the period in which we provide Services to you and your customer.</p>
CATEGORIES OF DATA SUBJECTS AND PERSONAL DATA PROCESSED	<p>Personal Data provided by you to us or collected by us in order to manage your account. This includes the following:</p> <ul style="list-style-type: none"> <li>• Partner name.</li> <li>• Partner email address.</li> <li>• Partner business address.</li> <li>• Partner telephone number.</li> <li>• Partner credit card or direct debit information.</li> <li>• Debit/Credit card name.</li> <li>• Debit/Credit card type.</li> <li>• Debit/Credit card expiry date.</li> <li>• Debit/Credit card number.</li> </ul> <p>Where you or a customer logs a technical support case, we will process the name and contact details of the user logging the case and the other users involved in the case. If we are provided access to email content by you (with your express permission having been granted), we will have access to any Personal Data set out in that email.</p> <p>Personal Data provided to us or collected by us in order to provide the Services. This includes data aggregated from your Active Directory or Google Directory or from Lists and Content such as:</p> <ul style="list-style-type: none"> <li>• Sender's/Recipient's First, Last and Full name.</li> <li>• Sender's/Recipient's business address.</li> <li>• Sender's/Recipient's company name.</li> <li>• Sender's/Recipient's telephone number.</li> <li>• Sender's/Recipient's email address.</li> <li>• Sender's email subject line and content information for the inclusion of the signature block.</li> <li>• Any other information that you expose to us via Custom Attributes within the signature block.</li> </ul> <p>No sensitive data is processed by us unless included in the Content of emails.</p>
NATURE OF PROCESSING	<p>Personal Data provided to us or collected by us in order to manage your or your customer's account is stored for the duration of your/their relationship with us.</p> <p>Where you log a technical support case, the data relating to the case is stored within our CRM. Personal Data provided by you to us or collected by us in order to provide the Service(s) is aggregated from your Active Directory or Google Directory and stored. This stored copy of the data is then used during the processing of the signature block prior to inclusion within the signature. This data is held separately from the main signature block, with the signature block being deleted once it has been included within the email. The aggregated data is stored for the duration of your relationship with us, after which time it is deleted in its entirety.</p>



SUBPROCESSORS	The data centre that runs the Exclaimer Email Signature Service is owned and operated by a sub-processor named in Annex 3. We also use CRM and other systems of third parties to assist us in providing the Services to you as stated in Annex 3
DURATION AND FREQUENCY OF PROCESSING	Only for the duration of the subscription to the Service and frequency is determined by the number of emails/surveys sent by you/customer through our data centre.
CONTACT/LAW	<a href="mailto:dpo@exclaimer.com">dpo@exclaimer.com</a> or write to us at FAO: The DPO, Exclaimer Europe B.V., Bollenmarkt 8 E, 1681 PJ Zwaagdijk-Oost, The Netherlands. The authorities in the Netherlands shall have jurisdiction.

## ANNEX 2

### Technical and Organisational measures to ensure the security of your Personal Data implemented by Exclaimer:

Security Requirement	How Data Importer implements security measures
Physical access control measures to prevent unauthorized persons from gaining access to Processing systems or premises where Personal Data are Processed or used.	<i>Card access control system with documentation of key holders. Security patrolled business park. Physical security service inside building. Monitored alarm system. CCTV. Locked server room with authorized personnel access only.</i>
Access control measures to prevent Processing systems from being used without authorization. Including Importer's representatives access permissions segregation to Processing systems and Personal Data such as read, copy, modify, delete.	<i>Individual user log-in to corporate network. All development, staging, production systems are located within secure Data Centres. Access to production level infrastructure per tenancy is limited to secure certificate endpoint. Processors Password policy procedures are regulated by Password Policy. Automatic password-protected blocking of computer after a certain period of time without user activity.</i>
Transmission control measures taken in by Importer and Exporter to ensure that Personal Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of Personal Information by means of data transmission facilities is envisaged.	<i>Encrypted access via TLS Hard drive encryption of all processor employee machines used to facilitate business performance protected by Bitlocker. Locked server room at Processor's premises with authorized personnel access only.</i>
Describe the measures of input control to ensure that it is possible to check and establish whether and by whom Personal Data have been entered into Processing systems, modified or removed.	<i>Access rights. Functional responsibilities.</i>
Assignment control measures Importer takes to ensure that, in the case of commissioned Processing, the Personal Information are Processed strictly in accordance with the instructions of the principal.	<i>Training of all Processor's representatives involved in Personal Data Processing for technical and organizational security measures. Follow-up training at regular intervals. Specific clauses in Contractor/Employment agreements with all Processor's representatives, such as: The Right for Work Results, Confidentiality, Policies and work processes, Non-compete, Non Disclosure. Appointment of contact person in charge of data protection (<a href="mailto:dpo@exclaimer.com">dpo@exclaimer.com</a>).</i>
Availability control measures Importer applies to ensure that Personal Data are protected from accidental destruction or loss.	<i>Replication/Back-up processes. Active/Active and regional Data Centres. Centralized virus protection and firewall at Processor's infrastructure Air conditioning for work and server/network environment. Fire alarm system. Monitored alarm system. CCTV. Contingency plans.</i>
Measures of pseudonymisation and encryption of personal data	<i>All data at rest is encrypted. Data in transit encrypted via TLS between user end-points and core services. Pseudonymisation techniques assigned to all data sat within queues or at rest.</i>



Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	<i>Data Protection Officer, CTO and Director of Technical Services meet regularly to review current processes and risk register. Regular Penetration tests carried out on infrastructure and application (service and code level). 3<sup>rd</sup> party IDS and Cloud Native security products built into solution.</i>
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	<i>Multiple data centres operate in an active/active configuration. All personal data is aggregated across all per-geo data centres.</i>
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	<i>3<sup>rd</sup> party assessments of our security process and policies as part of our various ISO accreditations. Regular management reviews of process and risk register. Tooling to ensure adherence to process and policies, including but not limited to IDS, automated compliance tools, Managed Detection and Response systems and Zero Trust Access systems.</i>
Measures for user identification and authorisation	<i>MFA coupled with Zero trust.</i>
Measures for the protection of data during transmission	<i>TLS Encryption at all points of transmission, including between internal services.</i>
Measures for the protection of data during storage	<i>Data storage can only be accessed by internal services, all of which are protected by secured MFA access. Secure and encrypted transmission of data prior to storage. Storage technologies that incorporate encryption as standard. Partners only have access to their own data based on secure authentication and authorisation.</i>
Measures for ensuring physical security of locations at which personal data are processed	<i>Access controls at all Data Centres and Exclaimer offices. Secure door access, which is recorded and regularly reviewed. Camera surveillance and 24/7 security guard patrols in place.</i>
Measures for ensuring events logging	<i>3<sup>rd</sup> party tooling to ensure all external events are logged. In product logging of all key events.</i>
Measures for ensuring system configuration, including default configuration	<i>New tenancies are created using standard image which is regularly checked against a baseline. All delivery pipelines update default configurations where necessary, ensuring built-in security and compliance to standard images.</i>
Measures for internal IT and IT security governance and management	<i>Accredited to ISO27001 &amp; 27018. Robust process, policies and tooling to ensure compliance.</i>
Measures for certification/assurance of processes and products	<i>Regular external 3<sup>rd</sup> party penetration testing of product and infrastructure (on material infrastructure change, product change or annually). 3<sup>rd</sup> party quarterly assessment of compliance to process and certifications. Real-time tooling notifications on compliance to process and certifications.</i>
Measures for ensuring data minimisation	<i>Independent audit and product peer review of all data collected.</i>
Measures for ensuring data quality	<i>Independent teams assess multiple streams of data, with a focus on quality. Any quality issues are fed back into the process and resolved promptly.</i>
Measures for ensuring limited data retention	<i>All data storage retention timeframes are regularly reviewed and assessed. Audits of data storage are conducted by independent teams to ensure adherence to policies.</i>
Measures for ensuring accountability	<i>All core processes and procedures are owned by senior members of Exclaimer. All employees, contractual sub processors or other service providers are contractually bound to respect the confidential nature of all sensitive information.</i>
Measures for allowing data portability and ensuring erasure	<i>All data stored can be easily recreated from Partners own store. Export and import routines exist across core data points. Data erasure policies exist as part of our wider information security policies.</i>

### ANNEX 3

#### List of sub-processors



	Name of Sub-Processor	Company number	Address	Service Provided
1.	Microsoft Operations Limited (Where Signatures for O365 is used)	256796	70 Sir John Rogerson's Quay Dublin 2 D02R296 IRELAND	Cloud Provider for Email Signature solutions
2.	GPUK LLP	OC337146	51 De Montfort Street Leicester LE1 7BB UNITED KINGDOM	Credit Card Processing Services (only utilised if paying by Credit Card)
3	GoCardless	07495895	Sutton Yard 65 Goswell Road London EC1V 7EN UNITED KINGDOM	Direct debit payment handling facility.
4.	Google Cloud EMEA Limited (and each member of the group of companies to which it belongs) (Where Signature for G-Suite is used)	03977902	70 Sir John Rogerson's Quay, Dublin 2, Ireland	Cloud Provider for Email Signature Solutions (only utilised if using Google Workspace email service).
5.	Salesforce UK Limited	05094083	Floor 26, Salesforce Tower, 110 Bishopsgate, London EC2N 4AY	CRM Provider
6.	Mimecast Services Limited	4901524	1 Finsbury Avenue, London, United Kingdom, EC2M 2PF	Backup provider for Exclaimer internal systems (including email archive).
7.	Socketlabs	n/a	SocketLabs Acquisition, LLC 700 Turner Industrial Way, Suite 100 Aston, PA 19014 USA	Email delivery services (for Feedback product only)
8.	Cloudflare	n/a	101 Townsend Street San Francisco, CA 94107 USA	Content delivery network and DDoS mitigation services (for Feedback product only)