# GDPR POLICY

This GDPR Policy Document (the **Document**) forms part of the agreement between **PHRONESIS TECHNOLOGIES LIMITED** (the **Supplier**) and you (the **Customer**), (the **Agreement**). Capitalised terms used in this Document shall have the same meaning as ascribed to them in the Agreement.

This GDPR Policy Document was last updated on 27th November 2018,

## 1 Definitions and interpretation

1.1 In this Document:

**Applicable Law** means as applicable and binding on the Customer, the Supplier and/or the Services:

(a) any law, statute, regulation, byelaw or subordinate legislation in force from time to time to which a party is subject and/or in any jurisdiction that the Services are provided to or in respect of;

(b) the common law and laws of equity as applicable to the parties from time to time;

(c) any binding court order, judgment or decree; or

(d) any applicable direction, policy, rule or order that is binding on a party and that is made or given by any regulatory body having jurisdiction over a party or any of that party's assets, resources or business;

**Appropriate Safeguards** means such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under Data Protection Laws from time to time;

**Data Controller** has the meaning given to that term (or to the term 'controller') in Data Protection Laws;

**Data Processor** has the meaning given to that term (or to the term 'processor') in Data Protection Laws;

**Data Protection Laws** means as applicable and binding on the Customer, the Supplier and/or the Services:

(a) in the United Kingdom:

(i) the Data Protection Act 2018 and any laws or regulations implementing Directive 95/46/EC (Data Protection Directive); and/or

(ii) the GDPR, and/or any corresponding or equivalent national laws or regulations;

(b) in member states of the European Union: the Data Protection Directive or the GDPR, once applicable, and all relevant member state laws or regulations giving effect to or corresponding with any of them; and

(c) any Applicable Laws replacing, amending, extending, re-enacting or consolidating any of the above Data Protection Laws from time to time;

**Data Protection Losses** means all liabilities, including all:

(a) costs (including legal costs), claims, demands, actions, settlements, interest, charges, procedures, expenses, losses and damages (including relating to material or non-material damage); and

(b) to the extent permitted by Applicable Law:

(i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority;

(ii) compensation which is ordered by a Supervisory Authority to be paid to a Data Subject; and

(iii) the reasonable costs of compliance with investigations by a Supervisory Authority;

| | |
|---|---|
| **Data Subject** | has the meaning given to that term in Data Protection Laws; |
| **Data Subject Request** | means a request made by a Data Subject to exercise any rights of Data Subjects under Data Protection Laws; |
| **GDPR** | means the General Data Protection Regulation (EU) 2016/679; |
| **International Organisation** | means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries; |
| **International Recipient** | has the meaning given to that term in clause 8.1; |
| **Personal Data** | has the meaning given to that term in Data Protection Laws; |
| **Personal Data Breach** | means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Protected Data; |
| **processing** | has the meanings given to that term in Data Protection Laws (and related terms such as **process** have corresponding meanings); |
| **Processing Instructions** | has the meaning given to that term in clause 3.1.1; |
| **Protected Data** | means Personal Data received from or on behalf of the Customer in connection with the performance of the Supplier's obligations under this Agreement; |
| **Sub-Processor** | means another Data Processor engaged by the Supplier for carrying out processing activities in respect of the Protected Data on behalf of the Customer; |
| **Supervisory Authority** | means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws; |
| **White List** | means a list of the Personal Data of End Users whose information is processed during the course of the provision of the Services, which also identifies the lawful basis (as defined under the GDPR) for all such processing of Personal Data (including the nature and circumstances of the consent given by End Users (if relevant)).; |

1.2 In this Document:

1.2.1 references to any Applicable Laws (including to the Data Protection Laws and each of them) and to terms defined in such Applicable Laws shall be replaced with or incorporate (as the case may be) references to any Applicable Laws replacing, amending, extending, re-enacting or consolidating such Applicable Law (including the GDPR and any new Data Protection Laws from time to time) and the equivalent terms defined in such Applicable Laws, once in force and applicable; and

1.2.2 a reference to a law includes all subordinate legislation made under that law.

1.3 Your use of the Site means that you must also comply with our Acceptable use policy, our Privacy policy, our Cookie policy and our Online terms and conditions for the supply of goods, where applicable.

**2 Data Processor and Data Controller**

2.1 The parties agree that, for the Protected Data, the Customer shall be the Data Controller and the Supplier shall be the Data Processor.

2.2 The Supplier shall process Protected Data in compliance with:

2.2.1 the obligations of Data Processors under Data Protection Laws in respect of the performance of its obligations under this Agreement; and

2.2.2 the terms of this Agreement.

2.3 The Customer shall comply with:

2.3.1 all Data Protection Laws in connection with the processing of Protected Data, the Services, the Relevant Services and the exercise and performance of its respective rights and obligations under this Agreement, including maintaining all relevant regulatory registrations and notifications as required under Data Protection Laws; and

2.3.2 the terms of this Agreement.

2.4 The Customer warrants, represents and undertakes, that:

2.4.1 all data sourced by the Customer for use in connection with the Services and the Relevant Services shall comply in all respects, including in terms of its collection, storage and processing (which shall include the Customer providing all of the required fair processing information to, and obtaining all necessary consents from, Data Subjects), with Data Protection Laws;

2.4.2 all instructions given by it to the Supplier in respect of Protected Data shall at all times be in accordance with Data Protection Laws; and

2.4.3 it is satisfied that:

(a) the Supplier's processing operations are suitable for the purposes for which the Customer proposes to use the Services and engage the Supplier to process the Protected Data; and

(b) the Supplier has sufficient expertise, reliability and resources to implement technical and organisational measures that meet the requirements of Data Protection Laws.

2.5 The Customer shall not withhold, delay or condition its agreement to any Change requested by the Supplier in order to ensure the Services and the Supplier (and each Sub-Processor) can comply with Data Protection Laws.

**3 Instructions and details of processing**

3.1 Insofar as the Supplier processes Protected Data on behalf of the Customer, the Supplier:

3.1.1 unless required to do otherwise by Applicable Law, shall (and shall take steps to ensure each person acting under its authority shall) process the Protected Data only on and in accordance with the Customer's documented instructions as set out in this Document as updated from time to time in accordance with the Change Control Procedure (**Processing Instructions**);

3.1.2 if Applicable Law requires it to process Protected Data other than in accordance with the Processing Instructions, shall notify the Customer of any such requirement before processing the Protected Data (unless Applicable Law prohibits such information on important grounds of public interest); and

3.1.3 shall as soon as reasonably practicable inform the Customer if the Supplier becomes aware of a Processing Instruction that, in the Supplier's opinion, infringes Data Protection Laws, provided that:

(a) this shall be without prejudice to clauses 2.3 and 2.4;

(b) to the maximum extent permitted by mandatory law, the Supplier shall have no liability howsoever arising (whether in contract, tort (including negligence) or

otherwise) for any losses, costs, expenses or liabilities (including any Data Protection Losses) arising from or in connection with any processing in accordance with the Customer's Processing Instructions following the Customer's receipt of that information.

3.2 The processing of Protected Data to be carried out by the Supplier under this Agreement shall comprise the processing set out in any relevant Order, as may be updated from time to time in accordance with the Change Control Procedure.

**4 Technical and organisational measures**

4.1 The Supplier shall implement and maintain, at its cost and expense, the technical and organisational measures:

4.1.1 in relation to the processing of Protected Data by the Supplier, as set out in clause 13 below (Technical and organisational measures); and

4.1.2 taking into account the nature of the processing, to assist the Customer insofar as is possible in the fulfilment of the Customer's obligations to respond to Data Subject Requests relating to Protected Data.

4.2 Any additional technical and organisational measures shall be at the Customer's cost and expense.

**5 Customer obligations**

5.1 The Customer shall ensure that, at all times, it: (i) has in place and maintains, using transparent mechanisms, any and all valid, lawful, appropriate, accurate, freely given, specific, informed and unambiguous consent that complies with Data Protection Laws from End Users with respect to and during any period in which that End User's Personal Data is used in connection with the Services and/or the Relevant Services; or (ii) is otherwise lawfully entitled to process any personal data under Data Protection Laws in respect of (a) the provision of any Relevant Services; (b) the use of any Services under this Agreement; and (c) the use of any information, including but not limited to Personal Data of such End Users, in connection with the Services and/or the Relevant Services.

5.2 The Customer shall ensure that:

5.2.1 where applicable, it maintains a White List for each Relevant Service, provide any White List to the Supplier within no more than five Business Days of the Supplier's request and as soon as reasonably practicable (and in any event within one Business Day of an End User ceasing to consent) instruct the Supplier to remove the relevant Personal Data from the White List in the event an End User revokes their consent and/or the method used by the Customer to obtain such consent is updated or changed in any way; and

5.2.2 in respect of End Users that are considered to be minors or otherwise people unable to give their own consent for the purposes of Data Protection Laws, that consent is obtained from a parent, guardian or other responsible person.

5.3 The Customer shall comply with all Data Protection Laws when providing any Relevant Services.

5.4 The Customer shall implement and maintain, at all times, a transparent and easily accessible privacy notice in accordance with Data Protection Laws, which shall contain sufficient information to ensure that any End User whose Personal Data is processed in connection with the Services and/or the Relevant Services is aware of the purpose and the extent to which both the Supplier and (where relevant) its partners and suppliers will process their Personal Data in connection with the Services and/or the Relevant Services (**Privacy Notice**). The Privacy Notice shall be brought to all End Users' attention by the Customer prior to the use of their Personal Data in connection with the Services and/or the Relevant Services. The Customer agrees to promptly provide a copy of the Privacy Notice on the Supplier's request. The Customer shall update the Privacy Notice with the Supplier's reasonable suggestions where required to ensure compliance with Data Protection Laws.

**6 Using staff and other processors**

6.1 The Supplier shall not engage any Sub-Processor for carrying out any processing activities in respect of the Protected Data without the Customer's written authorisation of that specific Sub-Processor (such

authorisation not to be unreasonably withheld, conditioned or delayed) provided that the Customer authorises the appointment of any of the Sub-Processors listed in any relevant Order.

6.2 The Supplier shall:

6.2.1 prior to the relevant Sub-Processor carrying out any processing activities in respect of the Protected Data, appoint each Sub-Processor under a written contract containing materially the same obligations as under clauses 2 to 14 (inclusive) that is enforceable by the Supplier;

6.2.2 ensure each such Sub-Processor complies with all such obligations; and

6.2.3 remain fully liable for all the acts and omissions of each Sub-Processor as if they were its own.

6.3 The Supplier shall ensure that all persons authorised by it (or by any Sub-Processor) to process Protected Data are subject to a binding written contractual obligation to keep the Protected Data confidential (except where disclosure is required in accordance with Applicable Law, in which case the Supplier shall, where practicable and not prohibited by Applicable Law, notify the Customer of any such requirement before such disclosure).

**7 Assistance with the Customer's compliance and Data Subject rights**

7.1 The Supplier shall refer all Data Subject Requests it receives to the Customer within five Business Days of receipt of the request, provided that if the number of Data Subject Requests exceeds 2 per calendar month, the Customer shall pay the Supplier's Charges calculated on a time and materials basis at the Supplier's rates set out in the Agreement and/or the Platform and/or the relevant Order for recording and referring the Data Subject Requests in accordance with this clause 7.1.

7.2 The Supplier shall provide such reasonable assistance as the Customer reasonably requires (taking into account the nature of processing and the information available to the Supplier) to the Customer in ensuring compliance with the Customer's obligations under Data Protection Laws with respect to:

7.2.1 security of processing;

7.2.2 data protection impact assessments (as such term is defined in Data Protection Laws);

7.2.3 prior consultation with a Supervisory Authority regarding high risk processing; and

7.2.4 notifications to the Supervisory Authority and/or communications to Data Subjects by the Customer in response to any Personal Data Breach,

provided the Customer shall pay the Supplier's Charges for providing the assistance in this clause 7.2, such Charges to be calculated on a time and materials basis at the Supplier's rates set out in the Agreement and/or the Platform and/or the relevant Order.

**8 International data transfers**

8.1 The Customer agrees that the Supplier may transfer Protected Data to countries outside the European Economic Area (EEA) or to any International Organisation(s) (an **International Recipient**), provided all transfers by the Supplier of Protected Data to an International Recipient shall (to the extent required under Data Protection Laws) be effected by way of Appropriate Safeguards and in accordance with Data Protection Laws. The provisions of this Agreement shall constitute the Customer's instructions with respect to transfers in accordance with clause 3.1.

8.2 The Customer shall not (and shall ensure that any End Users shall not) transfer any Protected Data outside the EEA or to any International Recipient without the Supplier's prior written consent.

**9 Records, information and audit**

9.1 The Supplier shall maintain, in accordance with Data Protection Laws binding on the Supplier, written records of all categories of processing activities carried out on behalf of the Customer.

9.2 The Supplier shall, in accordance with Data Protection Laws, make available to the Customer such information as is reasonably necessary to demonstrate the Supplier's compliance with its obligations under Article 28 of the GDPR (and under any Data Protection Laws equivalent to that Article 28), and

allow for and contribute to audits, including inspections, by the Customer (or another auditor mandated by the Customer) for this purpose, subject to the Customer:

9.2.1 giving the Supplier reasonable prior notice of such information request, audit and/or inspection being required by the Customer;

9.2.2 ensuring that all information obtained or generated by the Customer or its auditor(s) in connection with such information requests, inspections and audits is kept strictly confidential (save for disclosure to the Supervisory Authority or as otherwise required by Applicable Law);

9.2.3 ensuring that such audit or inspection is undertaken during normal business hours, with minimal disruption to the Supplier's business, the Sub-Processors' business and the business of other customers of the Supplier; and

9.2.4 paying the Supplier's reasonable costs for assisting with the provision of information and allowing for and contributing to inspections and audits.

**10 Breach notification**

10.1 In respect of any Personal Data Breach involving Protected Data, the Supplier shall, without undue delay:

10.1.1 notify the Customer of the Personal Data Breach; and

10.1.2 provide the Customer with details of the Personal Data Breach.

**11 Deletion or return of Protected Data and copies**

11.1 The Supplier shall, at the Customer's written request, either delete or return all the Protected Data to the Customer in such form as the Customer reasonably requests within a reasonable time after the earlier of:

11.1.1 the end of the provision of the relevant Services related to processing; or

11.1.2 once processing by the Supplier of any Protected Data is no longer required for the purpose of the Supplier's performance of its relevant obligations under this Agreement,

and delete existing copies (unless storage of any data is required by Applicable Law and, if so, the Supplier shall inform the Customer of any such requirement).

**12 Liability, indemnities and compensation claims**

12.1 The Customer shall indemnify and keep indemnified the Supplier in respect of all Data Protection Losses suffered or incurred by, awarded against or agreed to be paid by, the Supplier and any Sub-Processor arising from or in connection with any:

12.1.1 non-compliance by the Customer with the Data Protection Laws;

12.1.2 processing carried out by the Supplier or any Sub-Processor pursuant to any Processing Instruction that infringes any Data Protection Law; or

12.1.3 breach by the Customer of any of its obligations under clauses 2 to 14 (inclusive) of this Document.

12.2 If a party receives a compensation claim from a person relating to processing of Protected Data, it shall promptly provide the other party with notice and full details of such claim. The party with conduct of the action shall:

12.2.1 make no admission of liability nor agree to any settlement or compromise of the relevant claim without the prior written consent of the other party (which shall not be unreasonably withheld or delayed); and

12.2.2 consult fully with the other party in relation to any such action.

12.3 The parties agree that the Customer shall not be entitled to claim back from the Supplier any part of any compensation paid by the Customer in respect of such damage to the extent that the Customer is liable to indemnify the Supplier in accordance with clause 12.1.

12.4 This clause 12 is intended to apply to the allocation of liability for Data Protection Losses as between the parties, including with respect to compensation to Data Subjects, notwithstanding any provisions under Data Protection Laws to the contrary, except:

12.4.1 to the extent not permitted by Applicable Law (including Data Protection Laws); and

12.4.2 that it does not affect the liability of either party to any Data Subject.

**13 Technical and organisational security measures**

13.1 The Supplier shall implement and maintain the following technical and organisational security measures to protect the Protected Data:

13.1.1 in accordance with the Data Protection Laws, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of the Protected Data to be carried out under or in connection with this Agreement, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons and the risks that are presented by the processing, especially from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Protected Data transmitted, stored or otherwise processed, the Supplier shall implement appropriate technical and organisational security measures appropriate to the risk, including as appropriate those matters mentioned in Articles 32(a) to 32(d) (inclusive) of the GDPR.

**14 Survival of data protection provisions**

14.1 Clauses 2 to 14 (inclusive) of this Document shall survive termination (for any reason) or expiry of this Agreement and continue:

14.1.1 indefinitely in the case of clauses 11 to 14 (inclusive); and

14.1.2 until 12 months following the earlier of the termination or expiry of this Agreement in the case clauses 2 to 10 (inclusive),

provided always that any termination or expiry of clauses 2 to 10 (inclusive) shall be without prejudice to any accrued rights or remedies of either party under any such clauses at the time of such termination or expiry.