PrivacyEngine Terms and Conditions of Service.

Parties

(1) Sytorus Limited t/a PrivacyEngine with registered address at 77 Sir John Rogerson's Quay, Dublin 2, Ireland, D02 F540, (registration number 529183) (the "**Provider**"); and

(2) Registered end user (the "**Customer**")

Agreement

1. **DEFINITIONS**

1.1 Except to the extent expressly provided otherwise, in this Agreement:

"**Account**" means an account enabling a person to access and use the Hosted Services.

"**Agreement**" means this agreement including any Schedules, and any amendments to this Agreement from time to time.

"**Business Day**" means any weekday other than a bank or public holiday in Ireland

or the UK; "**Business Hours**" means the hours of 09:00 to 17:00 GMT/BST on a

Business Day; "**Charges**" means the following amounts:

(a) the amounts specified in letter of engagement/quote that you receive from us.

(b) such other amounts as may be agreed in writing by the parties from time to time.

(c) we reserve the right to increase price from time to time and notify you of any such increases in advance.

"**Customer Confidential Information**" means:

any confidential information disclosed by or on behalf of the Customer to the Provider during the Term / at any time before the termination of this Agreement (whether disclosed in writing, orally or otherwise) that at the time of disclosure:

(a) was marked as "confidential"; or

(b) should have been reasonably understood by the Provider to be confidential; and

(c) the Customer Data.

"**Customer Data**" means all data, works and materials: uploaded to or stored on the Platform by the Customer; transmitted by the Platform at the instigation of the Customer; supplied by the Customer to the Provider for uploading to, transmission by or storage on the Platform; or generated by the Platform as a result of the use of the Hosted Services by the Customer.

"**Data Processing Agreement**" or "**DPA**" means the data processing agreement between the Provider and the Customer which is hereby incorporated by reference into this Agreement in its entirety with the same force and effect as though fully set forth herein.

"**Documentation**" means the documentation in relation to the Hosted Services produced by the Provider and delivered or made available by the Provider to the Customer.

"**Force Majeure Event**" means an event, or a series of related events, that is outside the reasonable control of the party affected (including failures of the internet or any public telecommunications network, hacker attacks, denial of service attacks, virus or other malicious software attacks or infections, power failures, industrial disputes affecting any third party, changes to the law, disasters, explosions, fires, floods, riots, terrorist attacks and wars);

"**GDPR**" means the General Data Protection Regulation ((EU) 2016/679);

"**Hosted Services**" means the PrivacyEngine web portal, as specified on PrivacyEngine.io or other PrivacyEngine URLs, which will be made available by the Provider to the Customer as a service via the internet in accordance with this Agreement.

"**Hosted Services Specification**" means the specification for the Platform and Hosted Services set out in clause 3 of this document.

"**Intellectual Property Rights**" means all intellectual property rights wherever in the world, whether registrable or unregistrable, registered or unregistered, including any application or right of application for such rights (and these "intellectual property rights" include copyright and related rights, database rights, confidential information, trade secrets, know-how, business names, trade names, trademarks, service marks, passing off rights, unfair competition rights, patents, petty patents, utility models, semi-conductor topography rights and rights in designs);

"**Maintenance Services**" means the general maintenance of the Platform and Hosted Services, and the application of Updates and Upgrades.

"**Permitted Purpose**" means the use of PrivacyEngine as a support tool for data protection related queries, knowledge base, and online training.

"**Platform**" means the platform managed by the Provider and used by the Provider to provide the Hosted Services.

"**Services**" means any services that the Provider provides to the Customer, or has an obligation to provide to the Customer, under this Agreement.

"**Support Services**" means support in relation to the use of, and the identification and resolution of errors in, the Hosted Services, as more particularly set out in Schedule 2, but shall not include the provision of training services.

"**Term**" means the term of this Agreement, commencing in accordance with Clause 2.1 and ending in accordance with Clause 2.2.

"**Update**" means a hotfix, patch or minor version update to any Platform software; and

"**Upgrade**" means a major version upgrade of any Platform software.

2. TERM

2.1 This Agreement shall come into force upon signing of the Letter of Agreement or the Quote.

2.2 Term refers to 12 months period from the date of first using the platform.

2.3 This Agreement shall commence upon execution and continue in force unless terminated in accordance with Clause 18.

3. HOSTED SERVICES

3.1 The Provider shall ensure that the Platform will automatically generate an Account for the Customer and provide to the Customer login details for that Account.

3.2 The Provider hereby grants to the Customer a worldwide, non-exclusive license to use the Hosted Services for the internal business purposes of the Customer during the Term.

3.3 Except to the extent expressly permitted in this Agreement or required by law on a non-excludable basis, the license granted by the Provider to the Customer under Clause 3.2 is subject to the following prohibitions:

3.3.1 the Customer must not sub-license its right to access and use the Hosted Services.

3.3.2 the Customer must not permit any unauthorised person to access or use the Hosted Services.

3.3.3 the Customer must not use the Hosted Services to provide services to third parties.

3.3.4 the Customer must not republish or redistribute any content or material from the Hosted Services other than to individuals within its own organisation; and

3.3.5 the Customer must not make any alteration to the Platform, except as permitted by the Documentation.

3.4 The Customer shall use reasonable endeavours, including regular monitoring of usage and reasonable security measures relating to Account access details, to ensure that no unauthorised person may gain access to the Hosted Services using an Account.

3.5 The Provider shall use reasonable endeavours to maintain the availability of the Hosted Services to the Customer at the gateway between the public internet and the network of the hosting services provider for the Hosted Services but does not guarantee 100% availability.

3.6 For the avoidance of doubt, downtime caused directly or indirectly by any of the following shall not be considered a breach of this Agreement:

3.6.1 a Force Majeure Event.

3.6.2 a fault or failure of the internet or any public telecommunications network.

3.6.3 a fault or failure of the Customer's computer systems or networks.

3.6.4 any breach by the Customer of this Agreement; or

3.6.5 scheduled maintenance carried out in accordance with this Agreement.

3.7 The Customer must comply with and ensure that all persons using the Hosted Services with the authority of the Customer or by means of an Account comply with the PrivacyEngine Acceptable Use Policy https://app.privacyengine.io/Upload/documentation/AcceptableUsePolicy.pdf

3.8 The Customer must not use the Hosted Services in any way that causes, or may cause, damage to the Hosted Services or Platform or impairment of the availability or accessibility of the Hosted Services.

3.9 The Customer must not use the Hosted Services:

3.9.1 in any way that is unlawful, illegal, fraudulent, or harmful; or

3.9.2 in connection with any unlawful, illegal, fraudulent or harmful purpose or activity.

3.10 For the avoidance of doubt, the Customer has no right to access the software code (including object code, intermediate code and source code) of the Platform, either during or after the Term.

3.11 The Provider may suspend the provision of the Hosted Services if any amount due to be paid by the Customer to the Provider under this Agreement is overdue, and the Provider has given to the Customer at least 30 days' written notice, following the amount becoming overdue, of its intention to suspend the Hosted Services on this basis and the amount due remains unpaid after the notice period has expired.

4. MAINTENANCE SERVICES

4.1 The Provider shall provide the Maintenance Services to the Customer during the Term.

4.2 The Provider shall where practicably give to the Customer at least 10 Business Days' prior written notice of scheduled Maintenance Services that are likely to affect the availability of the Hosted Services or are likely to have a material negative impact upon the Hosted Services, without prejudice to the Provider's other notice obligations under this main body of this Agreement.

5. SUPPORT SERVICES

5.1 The Provider shall provide the Support Services to the Customer during the Term, as outlined in Schedule 2 of this Agreement.

5.2 The Provider shall make available to the Customer contact details in accordance with the provisions of this main body of this Agreement.

6. CUSTOMER DATA

6.1 The Customer hereby grants to the Provider a non-exclusive license to process the Customer Data to the extent reasonably required for the performance of the Provider's obligations and the exercise of the Provider's rights under this Agreement, together with the right to sub-license these rights to its hosting, connectivity and telecommunications service providers to the extent reasonably required for the performance of the Provider's obligations and the exercise of the Provider's rights under the Agreement.

6.2 The Customer warrants to the Provider that the Customer Data / the use of the Customer Data by the Provider in accordance with this Agreement will not:

6.2.1 breach the provisions of any law, statute, or regulation.

6.2.2 infringe the Intellectual Property Rights or other legal rights of any person; or

6.2.3 give rise to any cause of action against the Provider,

in each case in any jurisdiction and under any applicable law.

6.3 The Provider shall create a back-up copy of the Customer Data at least daily, shall ensure that each such copy is sufficient to enable the Provider to restore the Hosted Services to the state they were in at the time the back-up was taken, and shall retain and securely store each such copy for a minimum period of 30 days.

7. NO ASSIGNMENT OF INTELLECTUAL PROPERTY RIGHTS

7.1 The Customer acknowledges and agrees that the Provider and/or its licensors own all intellectual property rights in the Services and the Documentation. Except as expressly stated herein, this agreement does not grant the Customer any rights to, under or in, any patents, copyright, database right, trade secrets, trade names, trademarks (whether registered or unregistered), or any other rights or licences in respect of the Services or the Documentation.

8. CHARGES

8.1 The Customer shall pay the Charges to the Provider in accordance with letter of engagement or the quote accompanying this Agreement.

8.2 All amounts stated in or in relation to this Agreement are, unless the context requires otherwise, stated exclusive of any applicable value added taxes, which will be added to those amounts and payable by the Customer to the Provider.

8.3 The Provider shall be entitled to increase the Charges at the start of each anniversary of this Agreement upon 60 days' prior notice to the Customer and the applicable terms of this Agreement shall be deemed to have been amended accordingly.

9. PAYMENTS

9.1 The Provider may issue invoices for the Charges to the Customer in advance of the period to which they relate from time to time during the Term.

9.2 The Customer must pay the Charges to the Provider within the period of 30 days following the issue of an invoice in accordance with this Clause 9.3.

9.3 The Customer must pay the Charges by debit card, credit card, direct debit, bank transfer or cheque (using such payment details as are notified by the Provider to the Customer from time to time).

9.4 If the Customer does not pay any amount properly due to the Provider under this Agreement, the Provider may suspend access to the Services until such time as overdue amounts have been resolved.

10. PROVIDER'S CONFIDENTIALITY OBLIGATIONS

10.1 The Provider must:

10.1.1 keep the Customer Confidential Information strictly confidential.

10.1.2 not disclose the Customer Confidential Information to any person without the Customer's prior written consent,

10.1.3 use the same degree of care to protect the confidentiality of the Customer Confidential Information as the Provider uses to protect the Provider's own confidential information of a similar nature, being at least a reasonable degree of care.

10.1.4 act in good faith always in relation to the Customer Confidential Information; and

10.1.5 not use any of the Customer Confidential Information for any purpose other than the Permitted Purpose.

10.2 Notwithstanding Clause 10.1, the Provider may disclose the Customer Confidential Information to the Provider's officers, employees, professional advisers, insurers, agents, and subcontractors who have a need to access the Customer Confidential Information for the performance of their work with respect to the Permitted Purpose and who are bound by a written agreement or professional obligation to protect the confidentiality of the Customer Confidential Information.

10.3 This Clause 10 imposes no obligations upon the Provider with respect to Customer Confidential Information that:

10.3.1 is known to the Provider before disclosure under this Agreement and is not subject to any other obligation of confidentiality; or

10.3.2 is or becomes publicly known through no act or default of the Provider.

10.4 The restrictions in this Clause 10 do not apply to the extent that any Customer Confidential Information is required to be disclosed by any law or regulation, by any judicial or governmental order or request, or pursuant to disclosure requirements relating to the listing of the stock of the Provider on any recognised stock exchange.

11. DATA PROTECTION

The parties shall comply with the data protection requirements as set out in Schedule 1.

12. WARRANTIES

12.1 The Provider warrants to the Customer that it has and will maintain all necessary licences, consents, and permissions necessary for the performance of its obligations under this Agreement.

12.2 The Provider undertakes that the Hosted Services will be performed substantially in accordance with the Hosted Services Specification and with reasonable skill and care.

12.3 The Customer warrants to the Provider that it has the legal right and authority to enter into this Agreement and to perform its obligations under the Agreement and that it will not breach any laws, statutes, or regulations applicable to it under this Agreement.

12.4 The Customer warrants to the Provider that it shall provide the Provider with all necessary co-operation in relation to this Agreement and all necessary access to such information and systems as may be required by the Provider in order to provide the Hosted Services, including but not limited to security access information, configuration services, and the data processing environment necessary to enable the Provider to install, operate and maintain the Platform.

12.5 All of the parties' warranties and representations in respect of the subject matter of this Agreement are expressly set out in this Agreement. To the maximum extent permitted by applicable law, no other warranties or representations concerning the subject matter of this Agreement will be implied into the Agreement or any related contract.

13. ACKNOWLEDGEMENTS AND WARRANTY LIMITATIONS

13.1 The undertaking at clause 12.2 shall not apply to the extent of any non-conformance which is caused by use of the Platform and/or the Hosted Services contrary to the Documentation and/or the Provider's instructions, or modification or alteration of the Hosted Services by any party other than the Provider or the Provider's duly authorised contractors or agents. If the Hosted Services do not conform with the foregoing undertaking, Provider will, at its expense, use all reasonable commercial endeavours to correct any such non-conformance promptly, or provide the Customer with an alternative means of accomplishing the desired performance. Such correction or substitution constitutes the Customer's sole and exclusive remedy for any breach of the undertaking set out in Clause 12.2.

13.2 The Customer acknowledges that complex software is never wholly free from defects, errors, and bugs; and subject to the other provisions of this Agreement, the Provider gives no warranty or representation that the Hosted Services will be wholly free from defects, errors and bugs.

13.3 The Customer acknowledges that complex software is never entirely free from security vulnerabilities; and subject to the other provisions of this Agreement, the Provider gives no warranty or representation that the Hosted Services will be entirely secure.

13.4 The Customer acknowledges that the Hosted Services are designed to be compatible only with that software and those systems specified as compatible in the Hosted Services Specification; and the Provider does not warrant or represent that the Hosted Services will be compatible with any other software or systems.

13.5 The Customer acknowledges that the Provider will not provide any legal, financial, accountancy or taxation advice under this Agreement or in relation to the Hosted Services; and, except to the extent expressly provided otherwise in this Agreement, the Provider does not warrant or represent that the Hosted Services or the use of the Hosted Services by the Customer will not give rise to any legal liability on the part of the Customer or any other person.

13.6 The Provider does not warrant that the Customer’s use of the Services will be uninterrupted or error-free; or that the Services, Documentation and/or the information obtained by the Customer through the Services will meet the Customer’s requirements.

14. INDEMNITY

14.1 The Customer shall defend, indemnify, and hold harmless the Provider against claims, actions, proceedings, losses, damages, expenses, and costs (including without limitation court costs and reasonable legal fees) arising out of or in connection with the Customer's use of the Hosted Services, the Platform and/or the Documentation, provided that:

(a) the Customer is given prompt notice of any such claim.

(b) the Provider provides reasonable co-operation to the Customer in the defence and settlement of such claim, at the Customer's expense; and

(c) the Customer is given sole authority to defend or settle the claim.

14.2 The Provider shall defend the Customer, its officers, directors, and employees against any claim that the Hosted Services infringe any patent, copyright, trademark, database right or right of confidentiality during the Term, and shall indemnify the Customer for any amounts awarded against the Customer in judgment or settlement of such claims, provided that:

14.2.1 on the Customer becoming aware of any such claim, the Provider is given prompt notice of any such claim.

14.2.2 the Customer provides reasonable co-operation to the Provider in the defence and settlement of such claim, at the Provider’s expense; and

14.2.3 the Provider is given sole authority to defend or settle the claim.

14.3 In the defence or settlement of any claim referred to in Clause 14.2, the Provider may procure the right for the Customer to continue using the Hosted Services, replace or modify the Hosted Services so that they become non-infringing or, if such remedies are not reasonably available, terminate this Agreement on two (2) Business Days' notice to the Customer without any additional liability or obligation to pay liquidated damages or other additional costs to the Customer.

14.4 In no event shall the Provider, its employees, agents, and sub-contractors be liable to the Customer to the extent that the alleged infringement is based on:

14.4.1 a modification of the Hosted Services or Platform or Documentation by anyone other than the Provider.

14.4.2 the Customer's use of the Hosted Services or Platform or Documentation in a manner contrary to the instructions given to the Customer by the Provider; or

14.4.3 the Customer's use of the Hosted Services or Platform or Documentation after notice of the alleged or actual infringement from the Provider or any appropriate authority.

15. LIMITATION OF LIABILITY

15.1 This Clause 15 sets out the entire financial liability of the Provider (including any liability for the acts or omissions of its employees, agents, and sub-contractors) to the Customer:

15.1.1 arising under or in connection with this Agreement.

15.1.2 in respect of any use made by the Customer of the Hosted Services or any part of them; and

15.1.3 in respect of any representation, statement or tortious act or omission (including negligence) arising under or in connection with this Agreement.

15.2 Except as expressly and specifically provided in this Agreement:

15.2.1 the Customer assumes sole responsibility for results obtained from the use of the Hosted Services by the Customer, and for conclusions drawn from such use. The Provider shall have no liability for any damage caused by errors or omissions in any information, instructions or scripts provided to the Provider by the Customer in connection with the Hosted Services, or any actions taken by the Provider at the Customer's direction.

15.3 Nothing in this Agreement excludes the liability of the Provider:

15.3.1 for death or personal injury caused by the Provider's negligence; or

15.3.2 for fraud or fraudulent misrepresentation.

15.4 Subject to Clause 15.2 and Clause 15.3:

15.4.1 the Provider shall not be liable whether in tort (including for negligence or breach of statutory duty), contract, misrepresentation, restitution or otherwise for any loss of profits, loss of business, depletion of goodwill and/or similar losses or loss or corruption of data or information, or pure economic loss, or for any special, indirect, or consequential loss, costs, damages, charges, or expenses however arising under this Agreement.

15.4.2 the Provider's total aggregate liability in contract, tort (including negligence or breach of statutory duty), misrepresentation, restitution or otherwise, arising in connection with the performance or contemplated performance of this Agreement shall be limited to the total amount paid and payable by the Customer to the Provider under the Agreement in the 12-month period preceding the commencement of the event or events.

16. FORCE MAJEURE EVENT

16.1 If a Force Majeure Event gives rise to a failure or delay in either party performing any obligation under this Agreement (other than any obligation to make a payment), that obligation will be suspended for the duration of the Force Majeure Event.

16.2 A party that becomes aware of a Force Majeure Event which gives rise to, or which is likely to give rise to, any failure or delay in that party performing any obligation under this Agreement, must:

16.2.1 promptly notify the other; and

16.2.2 inform the other of the period for which it is estimated that such failure or delay will continue.

16.3 A party whose performance of its obligations under this Agreement is affected by a Force Majeure Event must take reasonable steps to mitigate the effects of the Force Majeure Event.

17. TERM AND TERMINATION

17.1 This Agreement shall, unless otherwise terminated as provided, commence on the Effective Date and shall continue for a period of 12 months and thereafter the agreement shall be automatically renewed for successive periods of 12 months.

17.2 Either party may terminate this Agreement on any anniversary of this Agreement by giving to the other party at least 30 days’ written notice of termination on the first anniversary, and, thereafter on 60 days’ notice of termination on any subsequent anniversary or as otherwise may be agreed between the parties in writing.

17.3 Either party may terminate this Agreement immediately by giving written notice of termination to the other party if the other party commits a material breach of this Agreement.

17.4 The Provider may terminate this agreement if the Customer fails to pay any amount due under this agreement on the due date for payment and remains in default not less than thirty days after being notified in writing to make such payment.

17.4.1 Either party may terminate this Agreement immediately by giving written notice of termination to the other party if the other party:

(a) is dissolved.

(b) ceases to conduct all (or substantially all) of its business.

(c) is or becomes unable to pay its debts as they fall due.

(d) is or becomes insolvent or is declared insolvent; or

(e) convenes a meeting or makes or proposes to make any arrangement or composition with its creditors.

(f) an administrator, administrative receiver, liquidator, receiver, trustee, manager or similar is appointed over any of the assets of the other party.

(g) an order is made for the winding up of the other party, or the other party passes a resolution for its winding up (other than for the purpose of a solvent company reorganization where the resulting entity will assume all the obligations of the other party under the Agreement);

18. **EFFECTS OF TERMINATION**

18.1 Upon termination of this Agreement for any reason:

18.1.1 All licenses granted under this agreement shall immediately terminate and the Customer shall immediately cease all use of the Services and/or the Documentation

18.1.2 the Provider may destroy or otherwise dispose of any of the Customer Data in its possession unless the Provider receives, no later than ten days after the effective date of the termination of this agreement, a written request for the delivery to the Customer of the then most recent back-up of the Customer Data. The Provider shall use reasonable commercial endeavors to deliver the back-up to the Customer within 30 days of its receipt of such a written request, provided that the Customer has, at that time, paid all fees and charges outstanding at and resulting from termination (whether or not due at the date of termination). The Customer shall pay all reasonable expenses incurred by the Provider in returning or disposing of Customer Data

18.1.3 all of the provisions of this Agreement shall cease to have effect, save that the following provisions of this Agreement shall survive and continue to have effect (in accordance with their express terms or otherwise indefinitely): Clauses 1, 3.11, 7, 9.2, 9.4, 9, 14, 15, 18, 21 and 22.

18.2 The termination of this Agreement shall not affect the accrued rights of either party.

18.3 Within 30 days following the termination of this Agreement for any reason the Customer must pay to the Provider any Charges in respect of Services provided to the Customer before the termination of the Agreement and without prejudice to the parties' other legal rights.

19. **NOTICES**

19.1 Any notice from one party to the other party under this Agreement must be given by one of the following methods using the relevant contact details set out in Clause 19.2

19.1.1 delivered personally or sent by courier, in which case the notice shall be deemed to be received upon delivery.

19.1.2 sent by recorded signed-for post, in which case the notice shall be deemed to be received 2 Business Days following posting: or

19.1.3 by email via an authorised person on behalf of the Customer/The Provider to a designated contact.

providing that if the stated time of deemed receipt is not within Business Hours, then the time of deemed receipt shall be when Business Hours next begin after the stated time.

19.2 The Provider's contact details for notices under this Clause 20 are as follows: info@privacyengine.io or Sales Department, PrivacyEngine, 77 Sir John Rogerson's Quay I Dublin 2 I Ireland I D02 F540.

19.3 The addressee and contact details set out in Clause 19.2 may be updated from time to time by a party giving written notice of the update to the other party in accordance with this Clause 19.

20. SUBCONTRACTING

20.1 The Provider must not subcontract any of its obligations under this Agreement without the prior written consent of the Customer, provided that the Customer must not unreasonably withhold or delay the giving of such consent.

20.2 The Provider shall remain responsible to the Customer for the performance of any subcontracted obligations.

20.3 Notwithstanding any other provision of this Agreement, the Customer acknowledges and agrees that the Provider may subcontract to any reputable third-party hosting business the hosting of the Platform and the provision of services in relation to the support and maintenance of elements of the Platform.

21. GENERAL

21.1 No breach of any provision of this Agreement shall be waived except with the express written consent of the party not in breach.

21.2 If any provision of this Agreement is determined by any court or other competent authority to be unlawful and/or unenforceable, the other provisions of the Agreement will continue in effect. If any unlawful and/or unenforceable provision would be lawful or enforceable if part of it were deleted, that part will be deemed to be deleted, and the rest of the provision will continue in effect (unless that would contradict the clear intention of the parties, in which case the entirety of the relevant provision will be deemed to be deleted).

21.3 This Agreement may not be varied except by a written document signed by or on behalf of each of the parties.

21.4 Neither party may without the prior written consent of the other party assign, transfer, charge, license or otherwise deal in or dispose of any contractual rights or obligations under this Agreement.

21.5 This Agreement is made for the benefit of the parties and is not intended to benefit any third party or be enforceable by any third party. The rights of the parties to terminate, rescind, or agree any amendment, waiver, variation, or settlement under or relating to this Agreement are not subject to the consent of any third party.

21.6 Subject to Clause 12 (above), this Agreement shall constitute the entire agreement between the parties in relation to the subject matter of this Agreement, and shall supersede all previous agreements, arrangements, and understandings between the parties in respect of that subject matter.

21.7 This Agreement shall be governed by and construed in accordance with Irish law.

21.8 The courts of Ireland shall have exclusive jurisdiction to adjudicate any dispute arising under or in connection with this Agreement.

22. INTERPRETATION

22.1 In this Agreement, a reference to a statute or statutory provision includes a reference to:

22.1.1 that statute or statutory provision as modified, consolidated and/or re-enacted from time to time; and

22.1.2 any subordinate legislation made under that statute or statutory provision.

22.2 The Clause headings do not affect the interpretation of this Agreement.

22.3 In this Agreement, general words shall not be given a restrictive interpretation by reason of being preceded or followed by words indicating a particular class of acts, matters or things.

Execution

By signing the LoE or the quote or by using the Platform both parties accept this Agreement.

Schedule 1- (Data Processing Terms)

DEFINITIONS

Controller, Processor, Data Subject, Personal Data, Personal Data Breach, processing and appropriate technical and organisational measures: as defined in the Data Protection Legislation.

Data Protection Legislation: all applicable data protection and privacy legislation in force from time to time in Ireland including the Data Protection Act 2018, Data Protection Acts 1988 and 2003, the General Data Protection Regulation ((EU) 2016/679); the Law Enforcement Directive 2016/680; the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (SI 336/2011).

1. DATA PROTECTION

1.1 Both parties will comply with all applicable requirements of the Data Protection Legislation. This clause is in addition to, and does not relieve, remove, or replace, a party's obligations or rights under the Data Protection Legislation. In this clause 1, **Applicable Laws** means (for so long as and to the extent that they apply to the Provider) the law of the European Union and the law of any member state of the European Union.

1.2 The parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller, and the Provider is the Processor. Annex A sets out the scope, nature and purpose of processing by the Provider, the duration of the processing and the types of Personal Data and categories of Data Subject.

1.3 Without prejudice to the generality of clause 1.1, the Customer will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the Personal Data to the Provider and/or lawful collection of the Personal Data by the Provider on behalf of the Customer for the duration and purposes of this agreement.

1.4 Without prejudice to the generality of clause 1.1, the Provider shall, in relation to any Personal Data processed in connection with the performance by the Provider of its obligations under this agreement:

(a) process that Personal Data only on the documented written instructions of the Customer unless the Provider is required by Applicable Laws to otherwise process that Personal Data. Where the Provider is relying on Applicable Laws as the basis for processing Personal Data, the Provider shall promptly notify the Customer of this before performing the processing required by the Applicable Laws unless those Applicable Laws prohibit the Provider from so notifying the Customer.

(b) ensure that it has in place appropriate technical and organisational measures, reviewed and approved by the Customer, to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it);

(c) ensure that all personnel who have access to and/or process Personal Data are obliged to keep the Personal Data confidential; and

(d) not transfer any Personal Data outside of the European Economic Area unless the prior written consent of the Customer has been obtained and the following conditions are fulfilled:

(i) the Customer or the Provider has provided appropriate safeguards in relation to the transfer;

(ii) the data subject has enforceable rights and effective legal remedies.

(iii) the Provider complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and

(iv) the Provider complies with reasonable instructions notified to it in advance by the Customer with respect to the processing of the Personal Data.

(e) taking into account the nature of the processing, assist the Customer by appropriate technical and organisational measures, in responding to any request from a Data Subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators.

(f) notify the Customer without undue delay on:

(i) becoming aware of a Personal Data Breach.

(ii) receiving any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation; or

(iii) receiving a request from a Data Subject for access to their Personal Data or to exercise any of their related rights under the Data Protection Legislation.

(g) at the written direction of the Customer, delete or return Personal Data and copies thereof to the Customer on termination of the agreement unless required by Applicable Law to store the Personal Data; and

(h) maintain complete and accurate records and information to demonstrate its compliance with this clause and at the Customer’s expense allow for audits by the Customer or the Customer's designated auditor and immediately inform the Customer if, in the opinion of the Provider, an instruction infringes the Data Protection Legislation.

1.5 The Customer generally authorises the Provider to appoint subcontractors as third-party processor of Personal Data under this agreement provided:

(a) the Provider informs the Customer of any intended changes concerning the addition or replacement of other processers thereby giving the Customer the opportunity to object to such changes within a reasonable timeframe after the Provider supplies the Customer with full details regarding such subcontractor.

(b) the Provider enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this Agreement, in particular, in relation to requiring appropriate technical and organisational data security measures, and, upon the Customer's written request, provides the Customer with copies of such contracts.

(c) the Provider maintains control over all Personal Data it entrusts to the subcontractor; and

(d) the subcontractor's contract terminates automatically on termination of this Agreement for any reason.

1.6 Those subcontractors approved as at the commencement of this Agreement are as set out in Part 4 of Annex A. The Provider must list all approved subcontractors in Annex A and include any subcontractor's name and location and contact information for the person responsible for privacy and data protection compliance.

1.7 Either party may, at any time on not less than 30 days’ notice, revise this Schedule by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when replaced by attachment to this agreement).

Annex A. Processing, Personal Data and Data Subjects

1. Processing by the Provider

1.1 Scope

i. The subject Matter of the Customers Personal Data are set out in the Terms of this engagement

1.2 Nature

i. The nature of processing the Customers Personal Data is set out in the Terms of this engagement

1.3 Purpose of processing

i. The purpose of processing the Customers Personal Data is set out in the Terms of this engagement

1.4 Duration of the processing

i. The duration of the Processing of the Customers Personal Data is set out in the Terms of this engagement

2. Types of Personal Data

The processing conducted via the PrivacyEngine platform on behalf of the Controller is with regard to the below type(s) of Personal Data of Data Subjects:

i. Name and contact details of staff of the Data Controller, their [customers/patients/students/Data Subjects]

2.1 Personal data relating to Data Subjects which is processed by the Controller.

3. Categories of Data Subject

i. Categories of Personal Data will include name, contact details, title and role within the organisation, correspondence between staff members, results from assessments as well as between staff and [customers/patients/students/Data Subjects].

ii. Personal data relating to Data Subjects which is processed by the Controller.

4. Subcontractors

4.1

SUB-PROCESSOR NAME	PURPOSE OF PROCESSING	TYPE OF DATA SHARED	LOCATION
Mailgun	Send emails regarding PrivacyEngine updates to users	Name, email, IP address and personal data included in message content	US based organisation but all EU data held within EU data centre
Beamer	Push notifications to inform users of new features	Only sending anonymised data (user id's)	The USA based, but we only send anonymised data
Custify	Customer Management Software	Customer data: email, name, company name and PrivacyEngine data	Data centre based in the EU
Microsoft	Cloud Platform provider	Customer data: email, name, company name and PrivacyEngine data,	Data centres based in the EU-Amsterdam and Dublin
Carbonite	Cloud based Data Backup services	PrivacyEngine Data	Data centre in the EU

Schedule 2- (Service Level Agreement)

1. INTRODUCTION

The purpose of the Service Level Agreement (SLA) is to provide clarifications on the appropriate integrity, availability, and responsiveness of the PrivacyEngine system within the following KPIs. Any failures to address KPIs over a three-month time period may be flagged to the Sytorus Account Manager, assigned, for escalation with senior management in Sytorus, for immediate resolution. Save for security issues which will be dealt with on an immediate basis and in line with Data Breach Notification policies of the Data Controller (the Client):

2. DESCRIPTION

2.1 First-line technical support to users of the Supported Software is available through the Support Function Tab on the Platform specifically to assist the Customer with general enquiries in connection with the Supported Software.

2.2 Where required, telephone and/or remote diagnosis and, where possible, correction of faults using the software management software, more specifically to correct all errors, bugs and failures of the Software to comply with any warranty or term of the agreement (as if such warranty or term continued beyond its expiry date).

2.3 Support available during Business Hours on Business Days only

2.4 Full details of the support query including context must be provided.

3. SERVICE LEVELS

Performance indicators	Area of Performance	Measure	Performance target
3.1 Response Time	System Efficiency	PrivacyEngine will provide, a target response time from PrivacyEngine. This will be a reasonable value, determined from the capabilities which are under Sytorus' direct control, such as application performance, hardware capability, and database efficiency.	An average server response time of 250ms.
3.2 Uptime	System Availability	PrivacyEngine will ensure availability of the system based on Microsoft's Azure availability commitment and will put in place actions to resolve any uptime issues. We will provide support Mon-Friday from 9AM to 17.30PM GMT. Issues can be logged on our Online Support Ticket in PrivacyEngine.	Sytorus will provide a 99% availability of the system.
		Any issues relating to System Availability will be treated as *Critical*, as defined above and will be resolved within 1 hour of the issue being logged.	
		PrivacyEngine maintenance windows will be between 6PM and 11PM during work weeks. Some loss of access may occur, but a public announcement will be made up to 5 days prior to a scheduled release, and no less than 6 hours for any emergency	
3.3 Patching	System Availability	PrivacyEngine will apply system and application patches to the PrivacyEngine infrastructure once a month on the first Saturday at 9AM. We may require rebooting of the production environment during this time period. All patches will be deployed and tested on our staging environment first to identify compatibility with the live environment before commencement of deployment.	No more than three manual reboots of the production environment for the deployment of system patches, all on the first Saturday in each month, per quarter.
3.4 Infrastructure Support	Quality Assurance	Infrastructure issues will be resolved based on a process of identification, validation and then resolution. Based on the nature of the issue reported Sytorus will:	Sytorus will provide the following response and resolution targets for issue fixing:
		Validate the existence of the issue through internal testing;	**Response Targets:**
		Agree within internal governance processes, as to the severity of the issue;	· *Critical*- 1 hour;

Performance indicators	Area of Performance	Measure	Performance target
			· *High*- 2-3 hours;
		Put in place a work-around if possible;	· *Medium*- 1 Working Day;
			· *Low*- 3 Working Days;
		Based on the severity we will agree to resolve the issue within an agreed timeframe;	**Resolution Targets:**
		The definition of support request priorities is as follows:	· *Critical*- 1 Working Day;
			· *High*- 2 Working Days;
		Critical- System down and non-responsive;	· *Medium*- 5 Working Days;
			· *Low*- 15 Working Days;
		High- System non-functional. No work around possible;	
		Medium- An issue is preventing complete access to the service. A workaround is possible;	
		Low- An issue that is not preventing the availability of the service and a workaround is possible;	
3.5 Monitoring	System Efficiency	PrivacyEngine will monitor the performance of the PrivacyEngine infrastructure in real time, 24/7/365. We will monitor CPU usage, RAM Usage, HDD capacity & performance and system response times.	We will maintain an average CPU usage below 90% on a monthly measurement cycle.
		We will action with Microsoft Azure as appropriate if CPU usage goes over 90% for more than three hours, RAM usage goes over 95% for more than two hours and HDD capacity is over 70%. Long term patterns will be managed in consultation with Microsoft for the deployment of added resources.	We will maintain an average memory usage of below 95% on a monthly measurement cycle.
		We will action system response times as discussed in *Response Time*, above.	We will maintain an average HDD capacity below 70% on a monthly measurement cycle.

Performance indicators	Area of Performance	Measure	Performance target
3.6 Backups & Redundancy		PrivacyEngine will perform regular backups of both the database and all necessary application folders across the PrivacyEngine Infrastructure system as well as appropriate periodic testing. Backups will be encrypted utilizing 256bit encryption to a remote secure environment in a separate datacentre.	Transaction Log backups every hour.
		Interim database backups (Incremental &/or Transaction log) will be automatically executed every hour.	Full database backup each night.
		Full database backups will be automatically executed nightly.	Secure and encrypted transfer to a remote location.
		Full application backups will be manually executed after the successful deployment of a new version or release.	Full backups of the application folders and unstructured data folders each night.
		Full redundancy is built into the infrastructure and is covered by Uptime, above.	
3.7 Recovery	System Availability	Full redundancy is built into the System layer and there will be minimum loss of service. If the System fails a replacement will be put in situ within 3 working hours, depending on the nature of the fault. Full consultation with clients will take place during this time.	Target availability is 99.5% Full restore within 3 hours.
		All data and applications will be restored utilizing the backup services in place with Microsoft Azure and within the timelines specified above with regards to a system failure.	
3.8 Infrastructure/Application /Database Security	Security	PrivacyEngine will put in place all required best practice to ensure the infrastructure, application and database is secure. We will provide an agreed suite of automated tests to verify on at least a quarterly basis and will hire a third party to conduct pen tests once a year.	Maintain a 24/7/365 Azure Security Centre to audit and alert on any threats to the infrastructure, application, or database.
		We will audit & monitor:	

Performance indicators	Area of Performance	Measure	Performance target
		· Buffer overflow, cross-site scripting, SQL injection.	
		· Network eavesdropping, Brute force attack, dictionary attacks, cookie replay, credential theft.	
		· Elevation of privilege, disclosure of confidential data, data tampering, luring attacks,	
		· Unauthorized access, over-privileged service and process accounts.	
		· Session hi-jacking, session replay.	
		· Poor key generation, weak or custom encryption.	
		· Query string manipulation, form field manipulation, cookie manipulation.	
		· Denial & Distributed Denial of Service.	
		· Multi-factor Authentication over VPN services integrity.	
		· Third Party Security & Certification Obligations.	
		· Continuous vulnerability scanning & reporting.	
		· Server, Database and Application Log scanning and reporting with centralized storage.	
		· Incident Detection, Response and Notification capability.	
3.9 Office & Remote Working Security	Security	PrivacyEngine will put in place required security practices for its internal staff and office facilities as well as IT assets, to ensure no compromising of PrivacyEngine information is allowed.	Ensure continuous oversight and reporting on performance and improvement.
		Controls will include:	
		· CCTV	
		· Visitors' policy	
		· Mobile devices (to include full security encryption and entry/password controls on laptops etc.)	
		· Controlled paper environment	
		· Shredding facilities	
		· Storage	
		· Security signs & notices	

Performance indicators	Area of Performance	Measure	Performance target
		PrivacyEngine will also put in place best practice controls for office & remote working staff, incl contractors.	
		Controls will include:	
		· Microsoft Endpoint Manager for policy enforcement.	
		· IT Asset Register.	
		· Device Encryption.	
		· Daily Anti-Malware definition updates.	
		· Monthly OS scheduled updates.	
		· Multi-factor authentication to company applications.	
		· Multi-factor authentication over VPN to servers.	
		· Movers-Leavers policy to change or revoke access rights to applications & servers.	
		· Centralised real time reporting to the Security Operations Centre for any incident or alerts relating to employees & contractors.	
		· Information Classification enforcement on all documentation with business rules.	
		· Anti-phishing and attachment malware detection for all mailboxes.	
		· Continuous staff and contractor security training & assessment.	