Defendocs

This Data Processing Agreement ("DPA", "Agreement") is an agreement between You (**Customer**) and DEFENDOCS LIMITED incorporated and registered in Ireland whose registered office is at Lee View House, 13 South Terrace, Cork, Cork, Ireland, T12 T0CT **(Provider)** to reflect the parties' agreement for the provision of the Data Processor Services by the Provider (as amended from time to time) and processing of Customer's Personal Data in accordance with the requirements of the Data Protection Legislation.

If you are accepting this Data Processing Agreement on behalf of Customer, you warrant that: (a) you have full legal authority to bind Customer to this Data Processing Agreement; (b) you have read and understand this Data Processing Agreement; and (c) you agree, on behalf of Customer, to this Data Processing Agreement. If you do not have the legal authority to bind Customer, please do not accept this Data Processing Agreement.

BY CLICKING THE "I ACCEPT" BUTTON BELOW, YOU (A) ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTAND THIS AGREEMENT; (B) REPRESENT AND WARRANT THAT YOU HAVE THE RIGHT, POWER, AND AUTHORITY TO ENTER INTO THIS AGREEMENT; AND (C) ACCEPT THIS AGREEMENT AND AGREE THAT YOU ARE LEGALLY BOUND BY ITS TERMS.

BACKGROUND

(A) Provider may process Personal Data on behalf of the Customer in order to provide tools for corporate GDPR compliance.

(B) This Personal Data Processing Agreement (**Agreement**) sets out the additional terms, requirements and conditions on which the Provider will process Personal Data on behalf of Customer. This Agreement contains the mandatory clauses required by Article 28(3) of the General Data Protection Regulation (*(EU) 2016/679*) for contracts between controllers and processors.

AGREED TERMS

1. Definitions and Interpretation

The following definitions and rules of interpretation apply in this Agreement.

1.1 Definitions:

Authorised Persons: the persons or categories of persons that the Customer authorises to give the Provider written personal data processing instructions [as identified in ANNEX A OR [AUTHORISED PERSON DESCRIPTION] and from whom the Provider agrees solely to accept such instructions.

Business Purposes: the services to be provided by the Provider to the Customer as described in the Master Agreement and any other purpose specifically identified ANNEX A.

Supervisory authority: the Data Protection Commission of Ireland.

Controller, Processor, Data Subject, Personal Data, Personal Data Breach and Processing: have the meanings given to them in the Data Protection Legislation.

Data Protection Legislation: all applicable data protection and privacy legislation in force from time to time in Ireland and Europe including without limitation the General Data Protection Regulation ((*EU) 2016/679*) (GDPR), Data Protection Act 2018 of Ireland and Irish ePrivacy Regulations (2011).

Data Subject: the identified or identifiable living individual to whom the Personal Data relates.

EEA: the European Economic Area.

Personal Data: means any information relating to an identified or identifiable living individual that is processed by the Provider on behalf of the Customer as a result of, or in connection with, the provision of the services under the Master Agreement; an identifiable living individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

Processing, processes, processed, process: any activity that involves the use of the Personal Data. It includes, but is not limited to, any operation or set of operations which is performed on the Personal Data or on sets of the Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring the Personal Data to third-parties.

Personal Data Breach: a breach of security leading to the accidental, unauthorised or unlawful destruction, loss, alteration, disclosure of, or access to, the Personal Data.

Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

Records: has the meaning given to it in Clause 12.

Registration email: email used to create the account at gdpr.defendocs.com

Term: this Agreement's term as defined in Clause 10.

1.2 The Annexes form part of this Agreement and will have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Annexes.

2. Personal data types and processing purposes

2.1 The Customer and the Provider agree and acknowledge that for the purpose of the Data Protection Legislation:

(a) the Customer is the Controller and the Provider is the Processor.

(b) the Customer retains control of the Personal Data and remains responsible for its compliance obligations under the Data Protection Legislation, including but not limited to, providing any required notices and obtaining any required consents, and for the written processing instructions it gives to the Provider.

(c) ANNEX A describes the subject matter, duration, nature and purpose of the processing and the Personal Data categories and Data Subject types in respect of which the Provider may process the Personal Data to fulfil the Business Purposes.

3. Provider's obligations

3.1 The Provider will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Customer's written instructions. The Provider will not process the Personal Data for any other purpose or in a way that does not comply with this Agreement or the Data Protection Legislation. The Provider must promptly notify the Customer if, in its opinion, the Customer's instructions do not comply with the Data Protection Legislation.

3.2 The Provider must comply promptly with any Customer written instructions requiring the Provider to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.

3.3 The Provider will maintain the confidentiality of the Personal Data and will not disclose the Personal Data to third-parties unless the Customer or this Agreement specifically authorises the disclosure, or as required by domestic or EU law, court or regulator (including the Data Protection Commission of Ireland). If a domestic or EU law, court or regulator (including the Data Protection Commission of Ireland) requires the Provider to process or disclose the Personal Data to a third-party, the Provider must first inform the Customer of such legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement, unless the domestic or EU law prohibits the giving of such notice.

3.4 The Provider will reasonably assist the Customer, at no additional cost to the Customer, with meeting the Customer's compliance obligations under the Data Protection Legislation, taking into account the nature of the Provider's processing and the information available to the Provider, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with the Supervisory authority or other relevant regulator under the Data Protection Legislation.

3.5 The Provider must notify the Customer promptly of any changes to the Data Protection Legislation that may reasonably be interpreted as adversely affecting this Agreement.

4. Provider's employees

4.1 The Provider will ensure that all of its employees:

(a) are informed of the confidential nature of the Personal Data and are bound by written confidentiality obligations and use restrictions in respect of the Personal Data;

(b) are aware both of the Provider's duties and their personal duties and obligations under the Data Protection Legislation and this Agreement.

4.2 The Provider will take reasonable steps to ensure the reliability, integrity and trustworthiness of all of the Provider's employees with access to the Personal Data.

5. Security

5.1 The Provider must at all times implement appropriate technical and organisational measures against accidental, unauthorised or unlawful processing, access, copying, modification, reproduction, display or distribution of the Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including, but not limited to, the security measures set out in ANNEX B.

5.2 The Provider must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

(a) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(b) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

(c) a process for regularly testing, assessing and evaluating the effectiveness of the security measures.

6. Personal data breach

6.1 The Provider will immediately and in any event without undue delay notify the Customer in writing to the registration email address if it becomes aware of:

(a) the loss, unintended destruction or damage, corruption, or unusability of part or all of the Personal Data. The Provider will restore such Personal Data at its own expense as soon as possible.

(b) any accidental, unauthorised or unlawful processing of the Personal Data; or

(c) any Personal Data Breach.

6.2 Where the Provider becomes aware of (a), (b) and/or (c) above, it will, without undue delay, also provide the Customer with the following written information:

(a) description of the nature of (a), (b) and/or (c), including the categories of in-scope Personal Data and approximate number of both Data Subjects and the Personal Data records concerned;

(b) the likely consequences; and

(c) a description of the measures taken or proposed to be taken to address (a), (b) and/or (c), including measures to mitigate its possible adverse effects.

6.3 Immediately following any accidental, unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. Further, the Provider will reasonably co-operate with the Customer at no additional cost to the Customer, in the Customer's handling of the matter, including but not limited to:

(a) assisting with any investigation;

(b) providing the Customer with physical access to any facilities and operations affected;

(c) facilitating interviews with the Provider's employees, former employees and others involved in the matter including, but not limited to, its officers and directors;

(d) making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Customer; and

(e) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or accidental, unauthorised or unlawful Personal Data processing.

6.4 The Provider will not inform any third-party of any accidental, unauthorised or unlawful processing of all or part of the Personal Data and/or a Personal Data Breach without first obtaining the Customer's written consent, except when required to do so by domestic or EU law.

6.5 The Provider agrees that the Customer has the sole right to determine:

(a) whether to provide notice of the accidental, unauthorised or unlawful processing and/or the Personal Data Breach to any Data Subjects, the Supervisory authority, other in-scope regulators, law enforcement agencies or others, as required by law or regulation or in the Customer's discretion, including the contents and delivery method of the notice; and

(b) whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

6.6 The Provider will cover all reasonable expenses associated with the performance of the obligations under clause 6.1 to clause 6.3 unless the matter arose from the Customer's specific written instructions, negligence, wilful default or breach of this Agreement, in which case the Customer will cover all reasonable expenses.

6.7 The Provider will also reimburse the Customer for actual reasonable expenses that the Customer incurs when responding to an incident of accidental, unauthorised or unlawful processing and/or a Personal Data Breach to the extent that the Provider caused such, including all costs of notice and any remedy as set out in Clause 6.5.

7. Cross-border transfers of personal data

7.1 Customer agrees that Provider may process personal data in Russian Federation subject to appropriate safeguards under article 46 (2) (c) - GDPR Standard data protection clauses adopted by the Commission (SCC).

8. Subcontractors

8.1 Customer agrees that Provider will engage subcontractors to process the Personal Data.

8.2 Provider will only engage subcontractors to process the Personal Data if Customer is provided with an opportunity to object to the appointment of each subcontractor within 10 working days after the Provider supplies the Customer with full details in writing via registration email address regarding such subcontractor;

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

9. Complaints, data subject requests and third-party rights

9.1 The Provider must, at no additional cost to the Customer, take such technical and organisational measures as may be appropriate, and promptly provide such information to the Customer as the Customer may reasonably require, to enable the Customer to comply with:

(a) the rights of Data Subjects under the Data Protection Legislation, including, but not limited to, subject access rights, the rights to rectify, port and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and

(b) information or assessment notices served on the Customer by the Supervisory authority under the Data Protection Legislation.

9.2 The Provider must notify the Customer immediately in writing via registration email address if it receives 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.

9.3 The Provider must notify the Customer within 3 days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their other rights under the Data Protection Legislation.

9.4 The Provider will give the Customer, at no additional cost to the Customer, its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

9.5 The Provider must not disclose the Personal Data to any Data Subject or to a third-party other than in accordance with the Customer's written instructions, or as required by domestic or EU law.

10. Term and termination

10.1 This Agreement will remain in full force and effect so long as:

The business relationship between Customer and provider persists

11. Data return and destruction

11.1 At the Customer's request, the Provider will give the Customer, or a third-party nominated in writing by the Customer, a copy of or access to all or part of the Personal Data in its possession or control in the format and on the media reasonably specified by the Customer.

11.2 On termination of the Master Agreement for any reason or expiry of its term, the Provider will securely delete or destroy or, if directed in writing by the Customer, return and not retain, all or any of the Personal Data related to this Agreement in its possession or control.

11.3 If any law, regulation, or government or regulatory body requires the Provider to retain any documents, materials or Personal Data that the Provider would otherwise be required to return or destroy, it will notify the Customer in writing of that retention requirement, giving details of the documents, materials or Personal Data that it must retain, the legal basis for such retention, and establishing a specific timeline for deletion or destruction once the retention requirement ends.

11.4 Upon request, the Provider will certify in writing to the Customer that it has deleted or destroyed the Personal Data.

12. Audit

12.1 The Provider will permit the Customer and its third-party representatives to audit the Provider's compliance with its Agreement obligations, on at least 30 days' notice, during the Term. The Provider will give the Customer and its third-party representatives all necessary assistance to conduct such audits at no additional cost to the Customer. The assistance may include, but is not limited to:

(a) physical access to, remote electronic access to, and copies of the Records and any other information held at the Provider's premises or on systems storing the Personal Data;

(b) access to and meetings with any of the Provider's personnel reasonably necessary to provide all explanations and perform the audit effectively; and

12.2 If a Personal Data Breach occurs or is occurring, or the Provider becomes aware of a breach of any of its obligations under this Agreement or any of the Data Protection Legislation, the Provider will:

(a) promptly conduct its own audit to determine the cause;

(b) produce a written report that includes detailed plans to remedy any deficiencies identified by the audit;

(c) provide the Customer with a copy of the written audit report; and

(d) remedy any deficiencies identified by the audit within 30 days.

12.3 The Provider will promptly address any exceptions noted in the audit reports with the development and implementation of a corrective action plan by the Provider's management.

13. Warranties

13.1 The Provider warrants and represents that:

(a) its employees, subcontractors, agents and any other person or persons accessing the Personal Data on its behalf are reliable and trustworthy and have received the required training on the Data Protection Legislation;

(b) it and anyone operating on its behalf will process the Personal Data in compliance with the Data Protection Legislation and other laws, enactments, regulations, orders, standards and other similar instruments;

(c) it has no reason to believe that the Data Protection Legislation prevents it from providing any of the Master Agreement's contracted services; and

(d) considering the current technology environment and implementation costs, it will take appropriate technical and organisational measures to prevent the accidental, unauthorised or unlawful processing of Personal Data and the loss or damage to, the Personal Data, and ensure a level of security appropriate to:

(i) the harm that might result from such accidental, unauthorised or unlawful processing and loss or damage;

(ii) the nature of the Personal Data protected; and

(iii) comply with all applicable Data Protection Legislation and its information and security policies, including the security measures required in Clause 5.1.

13.2 The Customer warrants and represents that the Provider's expected use of the Personal Data for the Business Purposes and as specifically instructed by the Customer will comply with the Data Protection Legislation.

14. Communication

All notices under this Agreement shall be in writing and be deemed duly given when sent, if transmitted by email.

ANNEX A Personal Data processing purposes and details

Subject matter of processing:

Cloud service offering Customers tools for corporate GDPR compliance

Duration of Processing:

During the Data Processing Agreement

Personal Data Categories:

- Personal details, including any information that identifies the data subject and their

personal characteristics, including: first name, last name, contact details (email);

- Employment data which may include: place of employment, work position, date and time of login to the software;
- Personal images;
- Location details including country, city, state and region;
- Login and technical details like passwords, tokens, device characteristics;
- Online identifiers and technical data like IP address.

Data Subject Types:

data subjects about whom personal data is transferred to the Provider in connection with the Processor Services by, at the direction of, or on behalf of Customer. This includes following Data Subjects:

- Customer's staff including volunteers, agents, temporary and casual workers
- Customer's Data Subject making Subject Access Requests
- Customer's Advisers, consultants and other professional experts

Approved Subcontractors:

IT Provide LLC (ООО «АйТи Провайд»)

Address: Russian Federation, 350051, Krasnodar, Ulitsa Dzerzhinskogo 49 office 28 (г. Краснодар, ул. Дзержинского, д. 49, пом. 28)

ANNEX B Security measures

1. KEY PRINCIPLES OF THE DATA PROTECTION BY DEFENDOCS LIMITED

1.1 All data stored on IT Systems are managed securely in compliance with all relevant parts of EU Regulation 2016/679 General Data Protection Regulation ("GDPR") and all other laws governing data protection whether now or in the future in force.

1.2 All data stored on IT Systems is available only to those Users with a legitimate need for access.

1.3 All data stored on IT Systems is protected against unauthorised access and processing.

1.4 All data stored on IT Systems is protected against loss and corruption.

1.5 All breaches of security pertaining to the IT Systems or any data stored thereon are reported and subsequently investigated by the IT Department.

2. SOFTWARE SECURITY MEASURES

2.1 All software in use on the IT Systems (including, but not limited to, operating systems, individual software applications, and firmware) are kept up-to-date and any and all relevant software updates, patches, fixes, and other intermediate releases are applied.

2.2 Where any security flaw is identified in any software that flaw is fixed immediately or the software may be withdrawn from the IT Systems until such time as the security flaw can be effectively remedied.

2.3 No DEFENDOCS LIMITED employees may install any software of their own, whether that software is supplied on physical media or whether it is downloaded, without the approval of the IT Manager. Any software must be approved by the IT Manager and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject.

2.4 Regular backups are taken of all data stored within the IT Systems at intervals no less than 1 month and such backups are stored at a suitable locations onsite and offsite.

3. ANTI-VIRUS SECURITY MEASURES

3.1 DEFENDOCS LIMITED IT Systems (including all computers and servers) are protected with suitable anti-virus, firewall, and other suitable internet security software. All such software is kept up-to-date with the latest software updates and definitions.

3.2 All DEFENDOCS LIMITED IT Systems protected by anti-virus software are subject to a full system scan at least once a week.

3.3 All physical media (e.g. USB memory sticks or disks of any kind) used by employees for transferring files must is virus-scanned before any files may be transferred. Such virus scans are performed by the IT Staff Manager**.**

3.4 DEFENDOCS LIMITED employees are permitted to transfer files using cloud storage systems only with the approval of the IT Manager. All files downloaded from any cloud storage system are scanned for viruses during the download process.

3.5 Any files being sent to third parties outside the DEFENDOCS LIMITED, whether by email, on physical media, or by other means (e.g. shared cloud storage) are scanned for viruses before being sent or as part of the sending process.

3.6 Where any virus is detected by a User this must be reported immediately to the IT Department (this rule shall apply even where the anti-virus software automatically fixes the problem). The IT Department shall promptly take any and all necessary action to remedy the problem. In limited circumstances this may involve the temporary removal of the affected computer or device. Wherever possible a suitable replacement computer or device will be provided immediately within 1 day to limit disruption to the User.

3.7 All IT Systems with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) shall be protected, where possible, with a password protected screensaver that will activate after 5 minutes of inactivity. This time period cannot be changed by Users and Users may not disable the screensaver. Activation of the screensaver will not interrupt or disrupt any other activities taking place on the computer (e.g. data processing).

3.8 All mobile devices (including, but not limited to, laptops, tablets, and smartphones) provided by the Company shall be set to lock, sleep, or similar, after 5 minutes of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake, or similar. Users may not alter this time period.

4. HARDWARE SECURITY MEASURES

4.1 DEFENDOCS LIMITED IT Systems are located in rooms which are securely locked (with authorised Users being granted access by means of a smart card).

4.2 All IT Systems not intended for normal use by Users (including, but not limited to, servers, networking equipment, and network infrastructure) are located in secured, climate-controlled rooms in locked cabinets which may be accessed only by designated members of the IT Department.

5. ACCESS SECURITY

5.1 Access privileges for all IT Systems is determined on the basis of employee levels of authority within DEFENDOCS LIMITED Company organization structure and the requirements of their job roles. Employees are not granted access to any IT Systems or electronic data which are not reasonably required for the fulfilment of their job roles.

5.2 All IT Systems (and in particular mobile devices including, but not limited to, laptops, tablets, and smartphones) are protected with a secure password or passcode, or such other form of secure log-in system as the IT Department may deem appropriate and approve.

5.3 All passwords are covered with the following security measures:

a) Are at least 8 characters long;

b) Contain a combination of upper and lower case letters,numbers, symbols;

c) Not obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events, or places etc.); and

d) Created by individual Users.

6. DATA STORAGE SECURITY

6.1 All data stored electronically on physical media, and in particular personal data, is stored securely in a locked box, drawer, cabinet, or similar.

6.2 No data, and in particular personal data, is transferred to any computer or device personally belonging to an employee unless the employee in question is a sub-processor working on behalf of DEFENDOCS LIMITED.

7. DATA PROTECTION

1.1 All personal data (as defined in the GDPR) collected, held, and processed by the Company is collected, held, and processed strictly in accordance with the principles of the GDPR.

1.2 All Users handling data for and on behalf of the Company shall be subject to, and must comply with security measures at all times. In particular, the following shall apply:

a) All emails containing personal data are marked “confidential”;

b) Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted under any circumstances;

8. SUBPROCESSOR SECURITY

Before onboarding Subprocessors, DEFENDOCS LIMITED conducts an audit of the security and privacy practices of Sub-processors to ensure Sub-processors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide.