Privacy policy

We are thedocyard which is a business of an entity called thedocyard Pty Ltd (**tdy**). In this document, when we say "we", "us", "our" etc we are referring to tdy. When we say you, your etc. we mean you, the person (or organisation) registering for and using our Product, all of your employees that use the Product and any third party you allow to use the Product (such as a client). You promise to us that you have the authority to bind all relevant third parties to this document and that you are also acting as their authorised agent for this purpose and when using our Product. We are going to rely on these promises. This privacy policy explains how we manage personal information. If you are from or your business is domiciled in the European Economic Area (EEA) please read and understand the schedule to this privacy policy headed EEA Data Terms. The EEA Data Terms take precedence over any other term in this document or our terms of use document to the extent of any inconsistency.

What is personal information?

Personal information includes any information or opinion, about an identified individual or an individual who can be reasonably identified from their information. The information or opinion will still be personal information whether it is true or not and regardless of whether we have kept a record of it. The information that we seek to collect about you will depend on the products or services that we provide. If you do not allow us to collect all of the information we request, we may not be able to deliver all of those services effectively.

What kinds of personal information do we collect and hold?

When you register with us or use our products or services we most likely will ask for or collect personal information. Throughout the life of your connection to us we may collect and hold additional personal information about you or others. This could include transaction information, information in documents held by us or making a record of queries or complaints you make.

For what purposes do we collect, hold, use and disclose personal information?

The main reason we collect, use, hold and disclose personal information is to provide you with products and services. This includes:

- registering you
- providing the product or service, and
- helping manage the product or service.

We may also use information to comply with legislative or regulatory requirements in any jurisdiction, prevent fraud, crime or other activity that may cause harm in relation to our products or services and to help us run our business. We may also use your information to report to you on how you use our products and services and tell you about products or services we think may interest you. Please note the section further down in this document under the heading "Do we use or disclose personal information for marketing?" which gives you more specific detail about that use of personal information.

How do we collect personal information?

We collect most personal information directly from you. Mainly via our online portal. We also collect information from you electronically. For instance, browsing data, IP addresses, pages you visit on our sites, when you visited us and devices you use when you visit us. We use technology called cookies when you visit our site. Cookies are small pieces of information stored on your computer. They can record information about your visit to the site, allowing it to remember you the next time you visit and provide a more meaningful experience. The

main reasons for using cookies is to offer you a better experience.

How do we hold personal information?

All of the information we hold will be stored electronically in secure data centres that are located, at your selection, in Western Europe or Australia.

Who do we disclose your personal information to, and why?

In the main, third party service providers who help us deliver our products and services to you. To protect personal information, we enter into contracts with our service providers that require them to comply with our privacy standards. These contracts oblige them to only use the personal information we disclose to them for the specific role we ask them to perform. The sorts of third parties include (but are not limited to):

- our agents, contractors and external service providers (for example, mailing houses and technology service providers)
- payment systems operators
- our advisers or auditors
- fraud bureaus or other organisations to identify, investigate or prevent fraud or other misconduct
- external dispute resolution schemes, and
- regulatory bodies, government agencies and law enforcement bodies in any jurisdiction.

We may also disclose personal information where we are required or authorised by law or where we have a public duty to do so; you may have expressly consented to the disclosure or the consent may be reasonably inferred from the circumstances; or we are otherwise permitted to disclose the information under relevant and applicable laws.

Do we disclose personal information overseas?

We host the data in the geo-location that you select. We do not control where you send data though, so keep that in mind. You are responsible for where you send data.

Security

We take extensive security measures and use a host of security technologies to protect personal information from loss and misuse, and from unauthorised access, modification or disclosure. Your information is located on a secured server behind a firewall however; there are risks in transmitting information across the internet. While we strive to protect such information, we cannot ensure or warrant the security of any information transmitted to us online and individuals do so at their own risk. We use 256 bit SSL encryption on data.

Do we use or disclose personal information for marketing?

Yes. We will use your personal information to offer you products and services we believe may interest you, but we will not do so if you tell us not to. These products and services may be offered by us or someone outside of our group. We may offer you products and services by various means, including by mail, telephone, email, SMS or other electronic means, such as through social media or targeted advertising websites. We may also disclose your personal information to companies outside our group who assist us to market our products and services to you. If you don't want to receive marketing offers from us please tell us.

Access to and correction of personal information

You can request access to the personal information we hold about you. You can also ask for corrections to be made. To do so, please contact us. There is no fee for requesting that your personal information is corrected or for us to make corrections. There are some circumstances in which we

are not required to give you access to your personal information. If we refuse to give you access to or to correct your personal information we will give you a notice explaining our reasons except where it would be unreasonable to do so. If we refuse your request to correct your personal information, you also have the right to request that a statement be associated with your personal information noting that you disagree with its accuracy. If we refuse your request to access or correct your personal information, we will also provide you with information on how you can complain about the refusal.

Resolving your privacy concerns and complaints – your rights

If you are concerned about how your personal information is being handled by us, please contact us. We will acknowledge your complaint as soon as we can after receipt of your complaint. We will let you know if we need any further information from you to resolve your complaint. We aim to resolve complaints as quickly as possible. In Australia you may complain to the Office of the Australian Information Commissioner about the way we handle your personal information. The Commissioner can be contacted at:

GPO Box 5218 Sydney NSW 2001
Phone: 1300 363 992
Email: enquiries@oaic.gov.au
Web: www.oaic.gov.au

If you are outside Australia please contact your local privacy regulator.

Contact us

You can contact us by emailing us on:
admin@thedocyard.co

Changes to the Privacy Policy

We may change the way we handle personal information from time to time for any reason. If we do so, we will update this privacy policy. So please check back every now and then to make sure you are up to date with our latest position on privacy.

Schedule – EEA Data Terms

This Schedule will apply where tdy processes personal data of data subjects that are located in the European Economic Area or where tdy processes personal data on your behalf where you are established in the European Economic Area and will take priority over any other provision of our privacy policy and terms of use of our Product to the extent of any conflict or inconsistency between them. You and we (Parties both, Party singular) will comply with all applicable obligations under this Schedule and under European Data Protection Law with respect to the types of personal data it processes and according to its responsibilities as a controller or processor (as appropriate) for the relevant personal data. Without limiting the foregoing, the Parties agree that: tdy will be a controller with respect to the processing of CRM Data and User Data; and you will be the controller of and tdy will be a processor of Content Data (unless you are acting as a processor of Content Data on behalf of a third party, in which case you will be a processor and tdy will be sub-processor of the Content Data, but for the purposes of this Schedule you will be treated as a controller and tdy will be treated as a processor).

Controller obligations

Whenever a Party is acting in a capacity as a controller in relation to personal data, it will comply in all respects with European Data Protection Law including: by processing such data fairly and lawfully; by implementing appropriate technical and organisational measures to protect such personal data against Data Security Incidents; by obtaining any consents required for its processing of personal data, particularly where sensitive personal data or special categories of personal data are processed; and by complying with its obligations with respect to data subject rights. As the controller with respect to Content Data, you accept full responsibility for obtaining all consents necessary for, and otherwise for having lawfully grounds to process, Content Data that is processed in connection with tdy's performance and delivery of the Product.

Where tdy is processing personal data on your behalf, whether as a processor or sub-processor, but not as a controller or joint controller, the following provisions will apply:

(A) Purpose limitation
tdy will process the personal data as necessary: (i) to perform its obligations under any written agreement with you; and (ii) to comply with its obligations under Applicable Law (the "Permitted Purpose"). In no event will tdy process the personal data for its own purposes or those of any third party.

(B) Documented instructions
tdy will process the personal data only on documented instructions from you, which may include the instructions set out in an agreement with us and we will immediately inform you if we know an instruction infringes European Data Protection Law.

(C) Categories of personal data
The Parties agree that the written agreements between us set out the categories of personal data, including Content Data, that are processed in connection with your use of the Product. It is the controller's responsibility to determine if any further details of tdy's processing of such personal data need to be recorded in an agreement with us to comply with European Data Protection Law and tdy will act in good faith to cooperate with any reasonable request to do so.

(D) Confidentiality of processing
tdy will ensure that any person that it authorises to process the personal data (including tdy's staff, agents and subcontractors) (each an "Authorised Person") will be under an obligation (whether under contract or statute) to keep the personal data confidential.

(E) Security
tdy will implement appropriate technical and organisational measures to protect the personal data from Data Security Incidents. Such measures will have regard to the state of the art, the costs of

implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

(F) **Subprocessing**

tdy will be authorised to engage third parties to process personal data on behalf of the controller, provided that it notifies you of such engagement (each, an "Authorised Sub-Processor"). tdy will ensure that there is in place a written contract between tdy and the Authorised Sub-Processor that specifies the Authorised Sub-Processor's processing activities and imposes on the Authorised Sub-Processor equivalent terms as those imposed on tdy in this Schedule. tdy will remain responsible for the acts and omissions of Authorised Sub-Processors in respect of their processing of personal data as if they were its own. Where tdy is instructed by you to grant access to personal data to a third party who is contracted to you (a "Contracted Third Party"), the Contracted Third Party will not be a sub-processor of tdy for the purposes of this Schedule and you will have sole responsibility for putting in place an appropriate data processing agreement with the Contracted Third Party that complies with European Data Protection Law.

(G) **Cooperation**

tdy will: (a) taking into account the nature of the processing, assist you by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising data subjects' rights, provided that tdy will not be required to comply with any requests to access, amend, update, erase or restrict processing of any Content Data to the extent that you can access, amend, update, erase or restrict the processing of the Content Data using the functionality and settings made available in connection with the Product; (b) assist the controller in implementing appropriate technical and organisational measures against Data Security Incidents, completing data protection impact assessments and notifying Data Security Incidents to the competent supervisory authority or to the data subjects concerned, as required by European Data Protection Law and taking into account the nature of the processing and the information available to tdy. If compliance with this Schedule requires: (i) a change to the Product, (ii) a change to an agreement between the Parties, or (iii) the expenditure of material effort or cost that is not provided in any agreement between the Parties, then either Party may raise this in accordance with the change control procedure or, in the absence of any such change control procedure, by discussing the same in good faith. For the avoidance of doubt, tdy will not be required to provide any assistance to you that would result in any change to the Product or an agreement or tdy incurring any expense, except if and to the extent that a suitable change is agreed to between the Parties in writing.

(H) **Data protection impact assessments**

If tdy believes or becomes aware that its processing of personal data is likely to result in a high risk to the data protection rights and freedoms of data subjects, we will inform you and provide you with assistance to conduct a data protection impact assessment.

(I) **Data Security Incidents**

Upon becoming aware of a Data Security Incident, tdy will inform you without undue delay and will provide such timely information and assistance in accordance with this Schedule as you may reasonably require in order to fulfil your data breach reporting obligations under European Data Protection Law and to mitigate the effects of the Data Security Incident. You understand

and accept that the delivery by tdy of the Product may carry a risk to you of loss or corruption of data. tdy's obligations in respect of data backup or retention are set out in the terms of use of the Product. You understand and accept that, save to the extent of any obligations detailed in a written agreement with us, you will bear full responsibility for the loss or corruption of data that may result from a Data Security Incident.

(J) **Subject access requests**
tdy will promptly notify you if it receives a request from a data subject to exercise their rights in respect of their personal data and will provide such assistance to you as may be required in accordance with this Schedule.

(K) **Deletion or return of personal data**
Upon termination of your use of the Product, tdy will (at the other Party's election) destroy or return to the other Party all personal data (including all copies of the personal data) contained in Content Data in its possession or control (including any personal data that is processed by an Authorised Sub-Processor) or alternatively make such facilities available to you using the functionality or settings for the Product to enable you to delete the personal data in question. This requirement will not apply to the extent that tdy is required by any Applicable Law to retain some or all of the personal data, in which event tdy will isolate and protect the personal data from any further processing except to the extent required by such Applicable Law. tdy will be entitled to render charges or recover such costs associated with destroying or returning personal data to the controller or joint controller (as appropriate) that are reasonable and which tdy can evidence.

(L) **Information and audit**
tdy will make available to you all information necessary to demonstrate compliance with the obligations set out in this Schedule and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller, except if and to the extent that providing such information or permitting such an audit would place tdy in breach of Applicable Law or cause it to infringe the rights (including rights in intellectual property or confidential information) of any of tdy's other customers. No more than one audit may be carried out in any calendar year, except if and when required by instruction of a competent data protection authority. tdy will be entitled to recover its costs of complying with any such audit. Where tdy has appointed a third party auditor to assess any of its technical or organisational measures to protect against Data Security Incidents for the purposes of any industry certification or otherwise (such as ISO 27001 compliance), tdy may share a copy of the auditor's certificate and an executive summary of its findings, in lieu of providing other information or allowing for other audits by the controller or another auditor under this Schedule. tdy will not be required to comply with any requests for Content Data to the extent that such Content Data can be accessed using the Product or the functionality or settings made available by tdy.

Data transfers outside of the EEA

The Parties acknowledge that tdy is located in a territory outside of the EEA that is not an Adequate Territory. The appropriate form of the Model Clauses will be incorporated into your written agreements with us by reference and will apply to the processing of any personal data that is transferred from you to tdy as follows:
(a) you will be the data exporter and will be deemed to have entered into the Model Clauses in its own name and on its own behalf in relation to the personal data disclosed to tdy;

(b) tdy will be deemed to have entered into the Model Clauses in its own name and on its own behalf in relation to the personal data disclosed to it by you and will also be deemed to have entered into the Model Clauses on behalf of any related entities in its corporate group that are also located in a territory outside of the European Economic Area that is not an Adequate Territory;
(c) the descriptions of the categories of personal data that are transferred under a written agreement with us will be incorporated based on the definitions in that agreement (that is, CRM Data, User Data and Content Data, as appropriate);
(d) the provisions of any security measures agreed in written agreement with us will be deemed to be set out in Appendix 2 to the Model Clauses;
(e) the optional illustrative indemnification clause will be deemed to have been deleted; and
(f) where and to the extent that the Model Clauses apply pursuant to this Schedule, if there is any conflict between any written agreement between you and us and the Model Clauses, the Model Clauses will prevail.

Where tdy is acting as a processor, it will not permit any onward transfer of personal data to a third country located outside European Economic Area (other than the place in which tdy is established) unless:
(a) tdy first puts in place adequate transfer mechanisms to ensure the transfer is in compliance with European Data Protection Law;
(b) tdy or the relevant Authorised Sub-Processor is required to transfer the personal data to comply with Applicable Law, in which case tdy will notify you of such legal requirement prior to such transfer unless such Applicable Law prohibits such notice from being given to you; or
(c) tdy is entitled to rely on a permitted derogation under European Data Protection Law in order to transfer the personal data outside of the European Economic Area, which may include circumstances where (among other things):
(i) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
(ii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person; or
(iii) the transfer is necessary for the establishment, exercise or defence of legal claims.

For the purposes of this Schedule, the adequate transfer mechanisms may include:
(i) transferring the personal data to a recipient in an Adequate Territory,
(ii) transferring the personal data to a recipient that has achieved binding corporate rules authorisation in accordance with European Data Protection Law, or
(iii) transferring the personal data to a recipient that has executed Model Clauses.

In this Schedule:

"Adequate Territory" means a territory outside of the European Economic Area that has been designated by the European Commission as ensuring an adequate level of protection pursuant to EU Privacy Law.

"Applicable Law" means applicable law, statute, bye-law, regulation, order, regulatory policy, guidance or industry code, rule of court or directives or requirements of any regulatory body, delegated or subordinate legislation or notice of any regulatory body.

"Content Data" means the content (comprising any speech, music, sounds, visual images or data of any description) created, provided, posted, hosted, uploaded, stored, communicated or displayed when using the Product.

"CRM Data" means any personal data of staff or representatives of a Party which is processed by the other Party for the purposes of managing the Product, administering an agreement between the Parties or marketing products or services to that Party.

"Data Security Incident" means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or

access to, personal data transmitted, stored or otherwise processed.

"Effective Date" is the date you enter into an agreement to use the Product.

"European Data Protection Law" means:
(a) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
(b) on and after 25 May 2018, the GDPR; and
(c) Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications.

"European Economic Area" means the Member States of the European Economic Area as it is made up from time to time, comprising the Member States of European Union and such other countries that are party to the agreement on the European Economic Area that entered into force on 1 January 1994, including the United Kingdom.

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

"Model Clauses" means model clauses for the transfer of personal data to Controllers or Processors (as appropriate) established in third countries approved by the European Commission from time to time (available online at http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm), as such model clauses may be amended or superseded by the European Commission from time to time.

"User" means any end user or administrator of a Service.

"User Data" means personal data regarding Users which is not Content Data or CRM Data. Such personal data include user IDs, passwords, authenticators, addresses (including MAC addresses, IP addresses and email addresses) and telephone numbers.