OceanBrowser Ltd (NZ)
www.oceanbrowser.com
privacy@oceanbrowser.com

OceanBrowser Ltd Privacy Policy

Last updated: August 2020
Version 1.5

This policy came into effect August 11th 2020.

1. Introduction

1.1. We are committed to safeguarding the privacy of our users.

1.2. This policy applies where we are acting as a data controller with respect to the personal data of our users; in other words, where we determine the purposes and means of the processing of that personal data.

1.3. This policy applies to delivery of our service to all customers and their users apart from Enterprise customers for whom other policies may apply.

1.3.1. Enterprise customers are optionally able request alterations to the provision of our services based on their requirements, such as specifying where data is located, conditions for access to accounts, or adjusting which components of our service are enabled ("enterprise access"). Our privacy policy for enterprise access will be adjusted to reflect the specific arrangements that pertain to the specific enterprise. If you are accessing our services through enterprise access, a version of this privacy policy specific to your enterprise will be provided, and you will be notified of the name of the Enterprise at the service login screen.

1.4. We use cookies on our website. In this document, we describe why they are necessary for the provision of our services. Our services including our website and delivered under our domains *.ob3.io and *.oceanbrowser.com domains – where "*" includes but is not limited to the domains https://use.ob3.io, https://www.ob3.io, and https://www.oceanbrowser.com.

1.5. Our service and all data hosted on our services may only be accessed using Hypertext Transfer Protocol Secure (HTTPS).

1.6. In this policy, "we", "us" and "our" refer to OceanBrowser Ltd. "Service" refers to OB3 and websites provided on our domains (see 1.5 above). For more information about us, see Section 14.

1.7. You may access the latest version of this policy online at https://www.ob3.io/privacy

1.8. We encourage users of our service who are interested in privacy issues to consider joining our privacy advisory group by emailing privacy@oceanbrowser.com subject "advisory group", or to send us questions or feedback on our Privacy policy to the same address.

1.9. It is important to us that our clients and users make informed decisions about privacy. We are developing privacy related educational resources. If you are interested in having early access to these resources, and providing us with feedback on these resources, please email privacy@oceanbrowser.com subject "privacy resources"

2. Credit

2.1. This document was created using a template from Docular (https://docular.net).

3. How we use your personal data

3.1. In this Section 3 we have set out:

3.1.1. the general categories of personal data that we may process;

3.1.2. the purposes for which we may process personal data; and

3.1.3. the legal bases of the processing.

3.2. We may process data about your use of our website and services ("usage data"). The usage data may include your IP address, geographical location, browser type and version, operating system, referral source, length of visit, page views and website navigation paths, as well as information about the timing, frequency and pattern of your service use. The sources of the usage data is Google Analytics using settings to anonymize your identity. This usage data may be processed for the purposes of analysing the use of the website. The legal basis for this processing is our legitimate interests, namely monitoring and improving our website and services, e.g. learning which path a user takes to find the information he or she is looking for, or learning about the browser to know which one should be supported.

3.3. We may process your account data ("account data"). The account data may include your name, service password (if you have chosen to use a password) and your email address. The account data may be processed for the purposes of operating our services, ensuring the security of our website and services, maintaining back-ups of our databases and communicating with you. The legal basis for this processing is our legitimate interests, namely the proper administration of our website and to offer you our services.

3.3.1. Your account data may be created automatically when you first access our service by following an LTI link to our service, from within a course hosted in within an LMS that is configured to use our service. Such LTI links enable personal information to be transferred from the LMS to our service including your name, your email address and details of your course enrolment. Such information can only and always be transmitted securely between the LMS and our service, and

does not include your LMS password details. By default your account on our service, when created by following an LTI link, will not have a password: it can only be accessed by you by following an LTI link within your course, from the LMS. You may optionally set a password to access our service directly.

3.3.2. As part of our automated support messaging to new users all users will be provided with a link to this policy along with a summary of their privacy rights and options for obtaining privacy-related support.

3.3.3. An existing user of our service may invite a new user to create an account by providing at a minimum an email address, and optionally a name for the user to be invited ("invited user"). This will result in an account activation message being sent to the invited user. If the recipient follows the link in the account activation message their account will be activated. As inviting a new user results in entering their private information in our service, such data will be deleted after a period of 365 days if the account is not activated. We may use this information to provide support to the invited user such as assistance with activating their account. The legal basis for this processing is our legitimate interests, namely processing of service data to enable you to invite a new user to be able to access shared content on our systems.

3.4. We may process your information included in your personal profile on our service ("profile data"). The profile data may include your real name (if provided), email address, and profile picture (if provided). The profile data may be processed for supporting communication among users of our service, and to provide you with information that you requested. The legal basis for this processing is our legitimate interests, namely processing of service data, course services, providing support to you, and enabling you to share content with other users on our systems.

3.5. We may process your personal data that is provided in the course of the use of our services ("service data"). The service data may include documents and other content such as digital files you have uploaded or embedded within documents in our systems, or other data that you have created within our platform, or support requests created within our support systems. Service data includes content that you have shared with other users of our system including discussion posts. We may process information contained in any enquiry you submit to us regarding our services, such data may be processed for the purposes of answering our users' enquiries and offering relevant support services to users. The service data may be processed for the purposes of operating our website and providing our services. The legal basis for this processing is our legitimate interests, namely the proper administration of our website and

business, and providing our services to you, and enabling building of a community around shared content provided within our services.

3.5.1. To assist us in providing support to you we have the ability to access all content within your account ("support data access"). All use of support data access is logged, monitored, and support data access is restricted to our staff who have a legitimate need to have such access. We have implemented security measures to limit how support data access can be accessed to prevent unauthorised access. We are implementing additional controls to allow you as a user to turn support data access off, or to selectively grant access to allow us to provide you with support. This policy will be updated when these controls are available. The legal basis for this processing is our legitimate interests, namely the ability to provide you with assistance with your account, to provide training and support, and to investigate and resolve issues with your account.

3.6. We may process information that is created in the form of a course to which other users can be invited to participate as course members (i.e. instructors or students) ("course data"). The course data may be processed for the purposes of enabling delivery of courses. When accessing a course users should understand that course administrators and instructors may have additional ability to access, or request access to, information to facilitate the delivery of their course. Where a course provider's institution has policies controlling access to course data, requests to access course data within our systems will be guided by any such rules. Upon request we will provide any user within a course, with a copy of those portions of any data supplied to a course provider that pertain to you. The legal basis for this processing is our legitimate interests, namely offering you our services, enabling you to complete your course-related study activities, and enabling us to deliver course services.

3.6.1. As a user within a course ("student") you may engage in collaborative activities such as discussions, creating documents, or contributing content within course documents such as collaboratively written pages or wiki-type pages. Our service is designed to support the creation of online communities of practice, which in the context of a course, may encompass currently enrolled students in a course, future enrolled students in a course, and alumni students. Content you contribute in a course may be accessed by current students, and in some cases may be accessed by future students and alumni students. In some courses you may be invited by your instructor to contribute content for access by future students in the course (for example a video on a topic you created as a student). Our service tracks all content you have created within our system. Please ask

your Instructor for details of how your course and its community of practice is configured. Upon request we can either delete, or anonymise, content that you have contributed within a course.

3.7. Your course provider may elect to provide you with alumni access to your completed course ("alumni content"). If you have alumni access you will be able to continue to access your completed course, or portions of your completed course, after you have completed your studies. Access to alumni course content is controlled by your course provider who may revoke, limit or change access to alumni content at any time and without notice. As an alumni student you can request to have any content you have created within an alumni course be either anonymised or deleted.

3.8. In some situations, where requested by a client, course data (or elements of course data) from our service may be embedded within, or accessed via, a client's Learning Management System such as (but not limited to) Canvas or Moodle LMS. The legal basis for this processing is our legitimate interests, namely offering you our services, enabling course providers to embed course content within their systems to facilitate delivery of courses.

3.9. Some courses may be delivered as part of a multi-institution or multi-client collaboration. In such instances course data including your data contributions within the course, may be accessed by staff from all institutions involved in delivery of the course.

3.10. Some courses may be delivered as part of work integrated learning programme where portions of your course may be accessible to partners drawn from industry – for example a company involved in mentoring a student project or group.

3.11. We may process course data to provide course instructors with learning analytics information ("learning analytics data"). Such data will only be provided on request and in accordance with any regulations an Instructor's Institution has regarding the use of learning analytics information. As a user of our service participating in a course, you may request a copy of any analytics information specifically related to you that has been supplied to your Instructor, within the scope of your enrolled course study activity. The legal basis for this processing is our legitimate interests, namely enabling us to support course providers to monitor and improve the delivery of their online courses, enabling Instructors within courses to identify students that may require learning support as part of their course activities, and offering you course-related services as a student.

3.12. We may process course data to provide course administrators with reporting data to assist with administration (“reporting data”). Reporting data does not contain personal information. Examples of reporting data include but are not limited to: exporting URL links to content within a course to facilitate LMS course configuration. The legal basis for this processing is our legitimate interests, namely enabling us to support course providers to facilitate delivery of their online courses, and offering you our services.

3.13. We may process course data to provide course administrators with course export data to assist with administration (“course export data”). Export data contains all content within a course, including if requested discussion posts, and content that has been co-created by users within the context of the course. The legal basis for this processing is our legitimate interests, namely enabling us to provide exported data to a course provider to facilitate backups or to migrate data to another service.

3.14. We may process information relating to our customer relationships, including customer contact information ("customer relationship data"). The customer relationship data may include your name, your employer, your job title or role, your contact details, and information contained in communications between us and you or your employer. The customer relationship data may be processed for the purposes of managing our relationships with you, communicating with you, keeping records of those communications and promoting our products and services to you. The legal basis for this processing is our legitimate interests, namely the proper management of our customer relationships.

3.15. We may process information that you provide to us for the purpose of subscribing to our email notifications and/or newsletters ("notification data"). The notification data may be processed for the purposes of sending you the relevant notifications and/or newsletters. You may control the delivery of notifications through your profile within our service. The legal basis for this processing is our legitimate interests, delivery of discussion post notifications, account problems, or informing you about our services, news and progress made.

3.16. We may process your personal data for the purposes of security and the prevention of fraud and other criminal activity. For example, we might analyse service log data and compare to profile data to verify access was legitimate which would involve processing personal data. The legal basis of this processing is our legitimate interests, namely the protection of our website, services and business, and the protection of others.

3.17. We may process information contained in or relating to any communication that you send to us ("correspondence data") including but not limited to via website contact forms, Intercom, or via email. The correspondence data may include the communication content and metadata associated with the communication. Our website will generate the metadata associated with communications made using the website contact forms. The correspondence data may be processed for the purposes of communicating with you and record-keeping. The legal basis for this processing is our legitimate interests, namely the proper administration of our website and business and efficient communications with you.

3.18. We may process any of your personal data identified in this policy where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure. The legal basis for this processing is our legitimate interests, namely the protection and assertion of our legal rights, your legal rights and the legal rights of others.

3.19. We may process customer relationship data in this policy in the event that it was necessary for the purposes of obtaining or maintaining insurance coverage, managing risks, or obtaining professional advice. The legal basis for this processing is our legitimate interests, namely the proper protection of our business against risks.

3.20. In addition to the specific purposes for which we may process your personal data set out in this Section 3, we may also process any of your personal data where such processing is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person.

3.21. Please do not supply any other person's personal data to us, unless we prompt you to do so.

4. Providing your personal data to others

4.1. We may disclose all personal data categories to our suppliers or subcontractors insofar as reasonably necessary for operating our services, ensuring the security of our website and services, maintaining back-ups of our databases and communicating with you, administration of our website and business, and providing our services to you.

4.2. Our suppliers or subcontractors are divided into principle suppliers and additional suppliers and subcontractors.

4.3. Principle suppliers

4.3.1. Our principle suppliers provide services that are critical to our operations. Our accounts with our principle suppliers are in every

case secured by two factor authentication. Where additional security and encryption options are provided by our principle suppliers as part of their service offering to us, we have enabled them.

4.3.2. **Digitalocean**

We use the infrastructure and services of DigitalOcean for hosting our services including but not limited to services on the domains www.ob3.io and use.ob3.io. They are located at 101 Avenue of the Americas, 10th Floor New York, NY 10013
GST Number: 128-573-283.

While hosting our website, DigitalOcean may process usage data, account data, profile data, service data, course data, learning analytics data, reporting data, alumni data, course export data, customer-relationship data, correspondence data, and notification data for the purposes mentioned in Section 3. For further information about how DigitalOcean processes data and how you can object, please consult their privacy policy (https://www.digitalocean.com/legal/privacy-policy/)

Our Digitalocean services are currently physically located in Singapore. We are in the process of transitioning away from DigitalOcean to AWS, with data and services to be located on AWS Sydney Australia region.

4.3.3. **Rackspace**

We use Rackspace to store your digital assets – file attachments, movies, images and other binary data that you upload to OB3. Digital Assets in our service are stored within Rackspace's Cloud Files service, with data located in London UK. Rackspace may process service data and course data for the purposes mentioned in Section 3. When users access digital assets in our service they will be loaded from Rackspace Cloudfiles to Rackspace's Content-Delivery-Network (CDN) causing that digital asset to be loaded (temporarily) to a server in the country where (or near to where) the user is located. For example a user accessing a movie in Australia would cause the movie to be loaded to the CDN server in Australia. This ensures high-speed access to content.

In order to provide file services, Rackspace may process service data and course data for the purposes mentioned in Section 3. For further information about how Rackspace processes data and how you can object, please consult their privacy policy (https://www.rackspace.com/managed-security-services/privacy-data-protection)

We are currently in the planning stage of transitioning away from Rackspace with currently stored on Rackspace moving to AWS S3 within AWS Sydney Australia region. This process will be completed no later than 1st October 2020.

4.3.4. Amazon Web Services (AWS)

We are currently migrating our DigitalOcean and Rackspace provided services to AWS with services to be provisioned in the AWS Sydney Australia region.

As part of our contingency planning in the event of a major failure with one or more of our other service providers we may at short notice deploy contingency services within AWS to ensure continuity of service. To prepare for contingencies we may store and process data on AWS including usage data, account data, profile data, service data, alumni data, course export data, course data, learning analytics data, reporting data, customer-relationship data, correspondence data, and notification data for the purposes mentioned in Section 3. For this purposes we store data where-ever possible in the AWS Sydney Australia Region. AWS Privacy policy may be viewed here (https://aws.amazon.com/privacy/)

4.3.5. Mailgun

All email delivered to you through our service is sent through Mailgun's service. We may provide profile data to Mailgun (112 E. Pecan St. #1135 San Antonio, TX 78205 US) for the purposes mentioned in section 3. Mailgun maintains transaction logs of mail sent for 5 days. Mailgun may process profile data, service data course data, correspondence data, and notification data for the purposes mentioned in Section 3, specifically in this context, the delivery of email notifications such as discussion posts, account reset emails and service notifications. For European users: Mailgun is Privacy-Shield certified and offers a guarantee to comply with European data privacy laws (https://www.privacyshield.gov/participant?id=a2zt0000000PCbmAAG&status=Active) For further information about how Mailgun processes data and how you can object, please consult their privacy policy (https://www.mailgun.com/privacy-policy/)

4.3.6. Slack

We use Slack to facilitate collaboration between our staff (and contractors) involved in the delivery, development and provision of our service. To facilitate our day to day operations certain data from our system is securely transmitted to and stored within our organisation's Slack account. Additionally information from our sub-contractors and service providers may be pushed to our Slack account, examples include Mailgun and Intercom. Access to specific areas of this content is restricted to only be available to staff or contractors who have a legitimate need to access this information. Examples of the way we use slack include: responding to support

requests and interactive chat requests from users, monitoring status of our systems, monitoring requests via our website at www.ob3.io, monitoring and assisting new users with account activation requests. Security of access to our organisation's Slack account is controlled by measures including two factor authentication. Slack may use account data, profile data, service data, course data, and correspondence data for the purposes mentioned in Section 3, specifically in this context, the monitoring of our systems, provision of support services, and provision of sales & marketing support to users enquiring via our website at www.ob3.io. For European users: Slack Technologies, Inc. ("We" or "Our") has certified with the EU-U.S. and Swiss-U.S. Privacy Shield with respect to the personal data we receive and process on behalf of our customers through our online workplace productivity tools and platform (https://slack.com/intl/en-nz/privacy-shield-notice). For further information about how Slack processes data and how you can object, please consult their privacy policy (https://slack.com/intl/en-nz/privacy-policy)

4.3.7. **Intercom**

We use Intercom to provide you with help and support services including: onboarding support messages, creating help requests, to engage in live help chat, and processing in-bound email requests to help@oceanbrowser.com. To do this we push certain events from our service to Intercom to help us provide appropriate support. For example, the first time you upload a video we might provide a message explaining how to use video features, or we may send an email notification message to assist you if we detect you are having problems logging in.

Additionally we may use Intercom to deliver activity completion messages such as certificates or email notifications on the completion of a learning activity.

We soft delete users from Intercom who are not active in the last 30 days (soft deleted users can be restored in Intercom along with their profile data). Intercom deletes all detailed user data older than 90 days, but does retain some summary metadata information, see Intercom's privacy policy below for additional details.

Intercom may process usage data, account data, profile data, service data, course data, customer-relationship data, correspondence data, and notification data for the purposes mentioned in Section 3, specifically in this context the provision of the services outlined

above. For European users: Intercom, Inc. has certified its compliance with the EU-US Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use and retention of personal data from the EEA, the UK and Switzerland. Intercom, Inc. adheres to and commits to apply the Privacy Shield Principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement, and Liability. For further information about how Intercom processes data and how you can object, please consult their privacy policy (https://www.intercom.com/legal/privacy)

4.3.8. Fastmail

Fastmail is our mail hosting provider. When you send email to us it may be stored and delivered on our business email accounts hosted on Fastmail. Email to help@oceanbrowser.com will be forwarded on to Intercom.

In order to provide email services, Fastmail may process service data and data contained in emails you send to us for the purposes mentioned in Section 3. For further information about how Fastmail processes data please consult their privacy policy (https://www.fastmail.com/about/privacy/)

4.4. Additional Service providers

4.4.1. Transloadit

If you upload media files to our service these may be processed by Transloadit to prepare them for access by users. Transloadit only stores files temporarily while they are being processed – for a maximum of 24 horus. Transloadit may process service data and course data for the purposes mentioned in Section 3, specifically in this context, the processing of uploaded media files to prepare them for use within our service. For further information about how Transloadit processes data and how you can object, please consult their privacy policy (https://transloadit.com/legal/privacy/)

4.4.2. Iframely

If you embed media files within our service these will be processed by Iframely to determine the correct way to embed these for display. Iframely may service data and course data, for the purposes mentioned in Section 3, specifically in this context, the embedding of media content within our service. For further information about how Iframely processes data and how you can object, please consult their privacy policy (https://iframely.com/docs/privacy)

4.4.3. Vimeo

We may provide Vimeo with usage data in general, and we may provide usage data to Vimeo if and only if you or your organization have embed videos hosted on Vimeo within our service. Vimeo uses cookies, and with it we are providing usage data for the purposes mentioned in Section 3. The usage data that is created by viewing a Vimeo video on our service will generally be transferred to and stored on a server hosted by Vimeo in the USA. Note: you may prevent data being transferred to Vimeo by not using Vimeo and instead uploading your videos to our service directly. For European users: Vimeo has certified to the U.S. Department of Commerce that it adheres to the Privacy Shield Principles. To learn more about the Privacy Shield program, and to view Vimeo's certification, please visit https://www.privacyshield.gov. By making this certification, Vimeo is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission (FTC). Vimeo's privacy policy may be accessed here (https://vimeo.com/privacy)

4.4.4. Google and YouTube

We may provide Google Analytics with usage data in general, and we may provide usage data to YouTube if and only if you or your organization have embed videos hosted on YouTube within our service. Google Analytics and YouTube are services of Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. Google uses cookies, and as a result will be providing usage data to Google for the purposes mentioned in Section 3. The usage data that is created by using our website will generally be transferred to and stored on a server hosted by Google in the USA. Note: you may prevent data being transferred to YouTube by not using YouTube and instead uploading your videos to our service directly.
For European users: Google is Privacy-Shield certified and offers a guarantee to comply with European data privacy laws (https://www.privacyshield.gov/participant?id=a2zt000000001L5AAI) . For further information about how Google processes data and how you can object, please consult their privacy policy (https://policies.google.com/privacy and https://policies.google.com/technologies/ads).

4.4.5. Google reCAPTCHA

We use Google reCAPTCHA to prevent spam requests for the self-signup form on www.ob3.io. Google reCAPTCHA collects the following browser and user information:

All cookies placed by Google in the last 6 months
CSS information

The language/date
Installed plug-ins
All Javascript object

4.5. **Content by other online service providers embedded within pages in our service**
Our service enables users to embed content from over 500 online providers within pages in our service – by the process of copying a link from the 3rd party service and pasting it into a page in our service. Examples of 3rd party embeddable services include GoogleDocs, Twitter, Slideshare and many others. It is not possible for us to provide details of how all these services process data or ensure privacy. If you are creating content within our service, especially as part of a course, you should consider the privacy and data implications of any content you are embedding within our service. Please note that for common applications such as file uploads and video embeds you have the option to upload content directly to our service if you wish.

4.6. **Financial transactions** relating to our website and services may be handled by our payment services providers in the future. We will share transaction data with our payment services providers only to the extent necessary for the purposes of processing your payments, refunding such payments and dealing with complaints and queries relating to such payments and refunds. Note that as of August 2020 we do not process Financial Transactions via our website. If we begin processing financial transactions at a future point in time we will update this policy to provide details.

4.7. In addition to the specific disclosures of personal data set out in this Section 4, we may disclose your personal data where such disclosure is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person. We may also disclose your personal data where such disclosure is necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

6. International transfers of your personal data

6.1 In this Section 6, we provide information about where data on our service is located and the circumstances under which we will transfer it internationally.

6.2 Our business and offices are based in New Zealand and operate under New Zealand law. We have a parent (IP holding and investment company) based in the UK – see section 14 for details. We do not currently provide our service to customers based in the UK or Europe, but we do provide our service to individual users based in the UK and Europe. This

policy document will be updated when and if we provide our service to customers based in the UK and Europe.

6.4 The locations of our suppliers and sub-contractors are described in Section 4, which also describes data which may be transferred to our suppliers and sub-contractors to enable provision of our service.

6.5 Access to our service is restricted to users with accounts on our service. You acknowledge that personal data and service data that you create within our services may be available to users of our system, via the internet, around the world.

5. Retaining and deleting personal data

5.1. This Section 5 sets out our data retention policies and procedure, which are designed to help ensure that we comply with our legal obligations in relation to the retention and deletion of personal data.

5.2. Personal data that we process for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

5.3. We will retain your personal data until you request deletion. Our reason for retaining your personal data until you request deletion is to enable us to provide lifelong access to your content, as our service is designed as a platform for lifelong learning. Examples of content include alumni course content, eportfolio content, group collaborative content, and your personal documents created in our service.

5.4. Notwithstanding the other provisions of this Section 5, we may retain your personal data where such retention is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person.

6. Visiting www.ob3.io

6.1. If you are browsing www.ob3.io and are not signed in to OB3, we may track some aspects of your usage via Intercom and Google Analytics for the purposes of providing support and marketing of OB3. This may include for example asking you via Intercom if you would like assistance, which may optionally allow you to provide your name and email address to facilitate communication with you.

7. Amendments

7.1. We may update this policy from time to time by publishing a new version on our website. This document will always include at the top the date at which it was last modified

7.2. We will notify all active users of OB3, via alert in OB3, when this policy is updated, along with a user friendly summary of what has been changed and why

7.3. You may request to be notified by email in the event of any change to this policy by emailing privacy@oceanbrowser.com subject subscribe-updates

8. Your rights

8.1. In this Section 8, we have summarised the rights that you have under data protection law. Some of the rights are complex, and not all of the details have been included in our summaries. Accordingly, you should read the relevant laws and guidance from the regulatory authorities for a full explanation of these rights.

8.2. Our company is based in New Zealand and complies with the New Zealand Privacy Act 1993 (the Act) when dealing with personal information. Users based in the UK or Europe may have additional rights under European law. We do not currently provide our service to customers based in the UK or Europe, this policy will be updated if we decide to provide our service to customers in the UK or Europe.

8.3. We are currently transitioning to provide all our users with the equivalent individual rights as those that pertain for European-based users under the provisions of GDPR (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/). During this transition period we will action requests under this section on a best effort basis. There may be delays in fulfilling your request. In the event of a potential delay, we will keep you fully informed of the status of your request and when we will be able to action it. This policy document will be updated at the end of the transition period. Users who are residents of Europe, and who are entitled by law to these rights, will have requests actioned according to the requirements of GDPR.

8.4. These individual rights are:

1. the right to access;
2. the right to rectification;
3. the right to erasure;
4. the right to restrict processing;
5. the right to object to processing;
6. the right to data portability;
7. the right to complain to a supervisory authority; and
8. the right to withdraw consent.

8.5. You have the right to confirmation as to whether or not we process your personal data and, where we do, access to the personal data, together with certain additional information. That additional information includes details of the purposes of the processing, the categories of personal data

concerned and the recipients of the personal data. Providing the rights and freedoms of others are not affected, we will supply to you a copy of your personal data.

8.6. You have the right to have any inaccurate personal data about you rectified and, taking into account the purposes of the processing, to have any incomplete personal data about you completed.

8.7. In some circumstances you have the right to the erasure of your personal data without undue delay. Those circumstances include: the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; you withdraw consent to consent-based processing; you object to the processing under certain rules of applicable data protection law; the processing is for direct marketing purposes; and the personal data have been unlawfully processed. However, there are exclusions of the right to erasure. The general exclusions include where processing is necessary: for exercising the right of freedom of expression and information; for compliance with a legal obligation; or for the establishment, exercise or defence of legal claims.

8.8. In some circumstances you have the right to restrict the processing of your personal data. Those circumstances are: you contest the accuracy of the personal data; processing is unlawful but you oppose erasure; we no longer need the personal data for the purposes of our processing, but you require personal data for the establishment, exercise or defence of legal claims; and you have objected to processing, pending the verification of that objection. Where processing has been restricted on this basis, we may continue to store your personal data. However, we will only otherwise process it: with your consent; for the establishment, exercise or defence of legal claims; for the protection of the rights of another natural or legal person; or for reasons of important public interest.

8.9. You have the right to object to our processing of your personal data on grounds relating to your particular situation, but only to the extent that the legal basis for the processing is that the processing is necessary for: the performance of a task carried out in the public interest or in the exercise of any official authority vested in us; or the purposes of the legitimate interests pursued by us or by a third party. If you make such an objection, we will cease to process the personal information unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing is for the establishment, exercise or defence of legal claims.

8.10. You have the right to object to our processing of your personal data for direct marketing purposes (including profiling for direct marketing

purposes). If you make such an objection, we will cease to process your personal data for this purpose.

8.11. You have the right to object to our processing of your personal data for scientific or historical research purposes or statistical purposes on grounds relating to your particular situation, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

8.12. To the extent that the legal basis for our processing of your personal data is:

0. consent; or
1. that the processing is necessary for the performance of a contract to which you are party or in order to take steps at your request prior to entering into a contract, and such processing is carried out by automated means, you have the right to receive your personal data from us in a structured, commonly used and machine-readable format. However, this right does not apply where it would adversely affect the rights and freedoms of others.

8.13. If you consider that our processing of your personal information infringes data protection laws, you have a legal right to lodge a complaint with a supervisory authority responsible for data protection. In New Zealand this is the New Zealand Privacy Commissioner (https://www.govt.nz/browse/consumer-rights-and-complaints/privacy-complaints/)

8.14. To the extent that the legal basis for our processing of your personal information is consent, you have the right to withdraw that consent at any time. Withdrawal will not affect the lawfulness of processing before the withdrawal.

8.15. You may exercise any of your rights in relation to your personal data by written notice to us. See below section 14 for contact details.

9. About cookies

9.1. A cookie is a file containing an identifier (a string of letters and numbers) that is sent by a web server to a web browser and is stored by the browser. The identifier is then sent back to the server each time the browser requests a page from the server.

9.2. Cookies may be either "persistent" cookies or "session" cookies: a persistent cookie will be stored by a web browser and will remain valid until its set expiry date, unless deleted by the user before the expiry date; a session cookie, on the other hand, will expire at the end of the user session, when the web browser is closed.

9.3. Cookies do not typically contain any information that personally identifies a user, but personal information that we store about you may be linked to the information stored in and obtained from cookies.

10. Cookies that we use

10.1. We use cookies for the following purposes:

0. authentication - we use cookies to identify you when you visit our website and as you navigate our website (cookies used for this purpose are set by OceanBrowser Ltd);
1. status - we use cookies to help us to determine if you are logged into our website (cookies used for this purpose are set by OceanBrowser Ltd);
2. personalisation - we use cookies to store information about your preferences and to personalise the website for you;
3. security - we use cookies as an element of the security measures used to protect user accounts, including preventing fraudulent use of login credentials, and to protect our website and services generally;
4. analysis - we use cookies to help us to analyse the use and performance of our website and services unless disabled by your organization ; and
5. cookie consent - we may use cookies to store your preferences in relation to the use of cookies more generally in the future.

11. Cookies used by our service providers

11.1. Our service providers use cookies and those cookies may be stored on your computer when you visit our website.

11.2. We use Google Analytics to analyse the use of our website. Google Analytics gathers information about website use by means of cookies. The information gathered relating to our website is used to create reports about the use of our website. Google's privacy policy is available at: https://www.google.com/policies/privacy/.

11.3. We use Vimeo to allow you to access videos hosted on Vimeo within our service. You'll only get cookies from Vimeo if you embed or view Vimeo videos embedded within our service. You may view Vimeo's cookie policy here (https://vimeo.com/cookie_policy). Blocking the Vimeo cookies is not possible for us without blocking the entire Vimeo video, however you may elect not to use Vimeo by uploading video content directly to our service.

11.4. We use YouTube to offer you the ability to embed YouTube videos or embed YouTube videos within our service. You'll only get cookies from YouTube if you embed videos (or access embedded videos embedded by others within our service) which use YouTube. The YouTube service may use cookies for displaying advertisements that will be relevant to you. You can view the privacy policy of this service provider at https://policies.google.com/privacy. YouTube cookies are only set when viewing content that includes a YouTube video. Blocking the YouTube cookies is not possible for us without blocking the entire YouTube video, however you may elect not to use YouTube by uploading video content directly to our service.

11.5. We use Google's reCAPTCHA for preventing spam requests on our self-signup form. reCAPTCHA checks to see if the computer or mobile device has a Google cookie placed on it. A reCAPTCHA-specific cookie gets placed on the user's browser, and a complete snapshot of the user's browser window is captured.

11.6. Our service enables content from many 3rd party online content providers to be embedded within our service. Viewing content from 3rd party providers may cause cookies to be created with their content is loaded and displayed. See above 4.4 for additional information.

12. Protecting your privacy

12.1. You may be able to enhance your privacy through careful selection of the browser which you use. Some browsers, such as Firefox may offer privacy related features. We encourage you to familiarise yourself with browser privacy features such as private browsing options, and to read the privacy policies for the browser you commonly use. Links to several popular browsers privacy policies are provided:

0. Firefox privacy policy (https://www.mozilla.org/en-US/firefox/privacy/products/)
1. Safari privacy policy (https://www.apple.com/legal/privacy/en-ww/)
2. Chrome privacy policy (https://www.google.com/chrome/privacy/)

12.2. Users with special privacy and anonymity needs may wish to consider connecting to our service using the Tor Browser (https://www.torproject.org/)

12.3. You may be able to restrict the duration that cookies are stored on your computer by opening OB3 within a private browsing window within your browser. When closing a private browsing window, any cookies associated with the window will typically be deleted.

13. Managing cookies

13.1. Most browsers allow you to refuse to accept cookies and to delete cookies. The methods for doing so vary from browser to browser, and from version to version. You can however obtain up-to-date information about blocking and deleting cookies via these links:

0. Chrome: https://support.google.com/chrome/answer/95647?hl=en
1. Firefox: https://support.mozilla.org/en-US/kb/enable-and-disable-cookies-website-preferences
2. Opera: http://www.opera.com/help/tutorials/security/cookies/
3. Internet Explorer: https://support.microsoft.com/en-gb/help/17442/windows-internet-explorer-delete-manage-cookies
4. Safari: https://support.apple.com/kb/PH21411 and
5. Edge: https://privacy.microsoft.com/en-us/windows-10-microsoft-edge-and-privacy

13.2. Blocking all cookies will have a negative impact upon the usability of many websites.

13.3. If you block cookies, you will not be able to use all the features on our website.

14. Our details

14.1. This service and associated websites is owned and operated by OceanBrowser Ltd (New Zealand) company number 1485398, established in 2004.

14.2. OceanBrowser Ltd (NZ) is a wholly owned subsidiary of OceanBrowser Ltd (United Kingdom) being our investment and IP holding company. OceanBrowser Limited (UK) company number is 9435787.

14.3. We do not currently provide our service to customers in the UK or Europe. For individual UK and European-based users of our service: in the United Kingdom we are registered with the Information Commissioner's Office Data Protection Registry, registration number ZA347160.

14.4. Our registered office and principal place of business is: 44 Melville Street, Dunedin 9016, Dunedin, New Zealand. Our postal address is OceanBrowser Limited PO Box 2247, Dunedin 9044, Otago, New Zealand.

14.5. You can contact us:
by post, to the postal address given above;
by email, using the email address published on our website.

15. Data protection officer

15.1. Our Data Protection Officer can be contacted at privacy.officer@oceanbrowser.com