Data Processing Addendum

This Data Processing Addendum (DPA) amends and supplements the Terms of Service, being an inseparable part of it. This DPA describes the agreement between you and Caphyon with regards to processing Personal Data in the course of accessing or using the Service and/or the Website. Service, Website and other capitalized terms used herein will have the meaning given to them in the Terms of Service or in the applicable Data Protection legislation.

This Customer Data Processing Agreement reflects the requirements of the European Data Protection Regulation ("GDPR") as it comes into effect on May 25, 2018. Caphyon's products and services offered in the European Union are GDPR ready and this DPA provides you with the necessary documentation of this readiness. If you do not agree with the provisions herein, please do not use the Service or the Website.

This DPA will not replace any other Data Processing Agreement that you and Caphyon may have executed separately.

1. DEFINITIONS

- "Caphyon", "We", "Us" or "Our" means Caphyon S.R.L., Str. Ana Ipatescu Nr. 51, Dolj, Craiova, 200340, European Union, Romania.
- "You" or "Your" means the individual or legal person that Registers to use the Service.
- "Party" or "Parties" means Caphyon and/or You, depending on the context.
- "EEA" means the European Economic Area which includes all 28 EU Member States plus Iceland, Liechtenstein, and Norway.

- “Data Subjects” means the individuals residing in the European Union, EEA, Switzerland and/or the United Kingdom, who access and/or use the Service under this DPA.
- “Personal Data” means any information related to a Data Subject, that can be used to directly or indirectly identify the Data Subject and is subject to Data Protection Legislation. Some examples include the name, email, address, billing information, IP location. Personal Data does not include User Data processed anonymously.
- “Data Protection Legislation” means all applicable data protection legislation, including the EU Data Protection Directive 95/46/EC and General Data Protection Regulation (EU) 2016/679.
- “Controller” means an individual or a legal person that controls and is responsible for determining the purpose and means of the Personal Data processing.
- “Processor” means an individual or a legal person that processes the Personal Data on behalf of the Controller.
- “Sub-processor” means any external supplier engaged by Caphyon as Processor to assist in performing its obligations for providing the Service under the Terms of Service.
- “Processing” means collecting, storing, using, structuring, amending, transferring, or deleting Personal Data.
- “Data Incidents” means a confirmed security incident in which confidential, sensitive, protected personal data was accessed by, or disclosed to an unauthorized entity.

2. DESCRIPTION OF PERSONAL DATA PROCESSING

The Parties herein agree that Personal Data will be treated as confidential, in compliance with the Data Protection legislation in force. When registering for accessing and using the Service, you are generally considered the Controller, whereas Caphyon is generally considered the Processor. Personal Data provided to Caphyon in the course of using the Service remains the property of the Controller and/or the relevant Data Subjects.

Categories of Data Subjects include, without limitation, Controller's personnel, collaborators, suppliers, customers, prospects and subcontractors, and any individual who transfers Personal Data to the Controller. Caphyon will process the Personal Data only for the technical scope of our business. Types of Personal Data include, without limitation, contact information which is determined by the Controller, Website and Service navigation data, and User Data as defined in the Terms of Service. Personal Data involved in the provision of the Service to the Controller is subject only to Processing activities and duration covered by the Terms of Service and Privacy Policy.

3. DATA SECURITY UNDERTAKINGS

Controller Responsibility. You agree to comply with obligations as a Controller under Data Protection Legislation in force regarding Personal Data that you provide to the Caphyon for Processing.

As the Controller, you understand that Caphyon will not assess the content that you provide as Personal Data or User Data. It is the Controller's responsibility to verify that it has the necessary rights to provide the Personal Data and/or User Data of the Data Subjects to the Processor, in the course of accessing and/or using the Service.

The Controller is responsible to make sure that it has obtained the required consent from Data Subjects, and that it has provided Data Subjects with the relevant notifications, as required by the Data Protection Legislation.

Processor Responsibility. Caphyon agrees to comply with obligations as a Processor under Data Protection Legislation in force, regarding the Personal Data from the Controller. As the Processor, Caphyon will process

Personal Data strictly within the scope of our business, performing our obligations in accordance with the Terms of Service and Privacy Policy.

The Processor is responsible for implementing and maintaining a data security program as described in the Terms of Service, with appropriate technical and organizational measures to protect Private Data against Data Incidents.

The Processor is responsible for storing the Personal Data in accordance with Data Protection Legislation in force. For this purpose, Personal Data subject to this DPA is stored on data centers based in the European Union and EEA, under the EU Data Protection Directive 95/46/EC and General Data Protection Regulation (EU) 2016/679.

To the extent of Processing Personal Data in the course of using the Service, Personal Data may be transferred to authorized US-based sub-processors, who are engaged directly in Processing activities. Under the Data Protection Legislation in force, it is the Processor's responsibility to ensure that the transfer of Personal Data subject to this DPA to US-based Sub-processors is made under the appropriate level of security, and the US-based Sub-processors have certified compliance with the GDPR and EU / Switzerland Privacy Shield Framework.

The Processor will ensure that the Personal Data subject to this DPA is accessed and handled only by Caphyon authorized employees and/or authorized Sub-processor staff, who are engaged directly in Processing activities and are subject to privacy, security, and confidentiality contractual obligations. For this purpose, the Processor will ensure the appropriate training for the employees engaged in Processing activities.

4. SUB-PROCESSORS

As the Controller, you understand that Caphyon may engage external suppliers as Sub-processors, for the scope of Processing Personal Data on behalf of the Controller.

Sub-processors currently engaged by Caphyon, without limitation, are listed herein:

Sub-processor	Scope of Processing Personal Data	Location	Security Certifications
Heroku Services, a Salesforce company	Infrastructure	The U.S.	Privacy Policy GDPR Compliance Statement Privacy Shield
Google LLC	Analytics and Remarketing	The U.S.	Privacy Policy GDPR Compliance Statement DPA Privacy Shield
MongoDB, Inc.	Database storage	The U.S.	Privacy Policy GDPR Compliance Statement Privacy Shield

Sub-processor responsibility. As Sub-processor, an external supplier of Caphyon, engaged in Processing Personal Data under this DPA, performs

its obligations in accordance with written agreements on data protection and confidentiality. Caphyon will remain responsible for the acts and omissions of external suppliers, as Sub-processors, to the same extent it would be if performing directly the external services engaged in Processing activities under this DPA, subject to Limitation of Liability (Section 14 of the Terms of Service).

5. DATA INCIDENTS

Caphyon will make reasonable efforts to implement and enhance an appropriate security program as well as organizational measures, ensuring the security and confidentiality of Personal Data subject to this DPA.

As the Processor, should we become aware of a Data Incident with an impact on Personal Data Processing, we will notify the Controller regarding the incident in a timely manner, no later than 72 hours, as required by the Data Protection Legislation in force. As the Controller, it is your responsibility to provide information reasonably sufficient and up to date to allow Caphyon to contact you, such as an email address or telephone number.

6. DATA SUBJECT RIGHTS

Caphyon will make reasonable efforts to assist you to fulfill obligations as Controller in regards to the rights of Data Subjects, in accordance with the Data Protection Legislation in force. For this purpose, we will respond to written requests with any information reasonably necessary to confirm Caphyon's compliance with Personal Data Processing under this DPA.

7. MISCELLANEOUS

The Parties acknowledge and agree that, except for the changes made by the DPA herein, the Terms of Service remains unchanged and in full force and effect. If there are conflicts between the Terms of Service and this DPA, to the extent of that conflict this DPA will prevail.