DATAROBOT MASTER SUBSCRIPTION AGREEMENT

This Master Subscription Agreement (this "**Agreement**") between **DataRobot, Inc.**, a Delaware Corporation, with its principal place of business located at 225 FRANKLIN STREET, 13TH FLOOR, BOSTON, MASSACHUSETTS 02110, USA ("**DataRobot**") and the customer stated in the Order (as defined in Section 1) ("**Customer**") is effective as of the date DataRobot accepts the Order (the "**Effective Date**").

This Agreement supersedes any other agreement (including any click-through or electronic agreements within the Solution) between DataRobot and Customer with respect to the Solution. This Agreement applies to all future purchases of DataRobot software and services by Customer unless expressly agreed otherwise by Customer and DataRobot.

1 DEFINITIONS

Affiliate means in relation to a party, any entity that directly or indirectly controls, is controlled by, or is under direct or indirect common control with such party, or which is a wholly owned subsidiary of such party, where "**control**" means owning, directly or indirectly, at least 51% of the equity securities or equity interests of such entity.

Authorized Users means the employees, agents and independent contractors of Customer and of its Affiliates.

Customer Data means any code or data belonging to Customer which is uploaded into the Solution by or on behalf of Customer (including by DataRobot).

Documentation means the technical documentation for the Solution that is included in version of the Solution accessed by Customer, including all additions and modifications made by DataRobot from time to time in accordance with this Agreement.

Maintenance means the services and updates to the Solution as described in Appendix 1 (Support Policy).

Order means each order, order form or statement of work for the purchase of software or services from DataRobot.

Professional Services means training, enablement and/or other professional services.

SaaS means software as a service.

Solution means the DataRobot software products stated in the Order including all additions and modifications made by DataRobot from time to time in accordance with this Agreement.

Subscription Term means the period of Customer's subscription to the Solution that is stated in the Order.

Support means the technical support services described in Appendix 1 (Support Policy).

2 ORDERING AND LICENSE GRANT

2.1 This Agreement governs each Order unless the parties expressly agree otherwise in writing. Each Order will form a separate contract between the parties and will be deemed to be subject to the terms set out in this Agreement except to the extent that the Order provides for different or varied terms.

2.2 Subject to the terms of this Agreement, DataRobot grants to Customer, for the Subscription Term, a non-exclusive, non-transferable, non-sublicensable license to use the Solution together with the Documentation, for its internal business use and the purpose of the Solution as described in the Documentation.

3 AUTHORIZED USERS

3.1 Customer may permit its Authorized Users to use the Solution for the same purposes permitted for Customer under Section 2.2 provided that:

(a) only Customer may bring actions against DataRobot for any losses, damage or liabilities suffered or incurred by any Affiliate or Authorised User and Customer shall procure that no Affiliate or Authorised User commences or maintains any claim against DataRobot for any matter arising in connection with this Agreement (whether founded on breach of contract or tort or any other legal theory); and

(b) Customer shall procure that all Authorized Users comply with the terms of this Agreement and shall remain liable for all acts and omissions of its Affiliates or Authorized Users.

4 RESTRICTIONS ON USE

Customer shall not, and shall not permit any third party to, except as permitted under this Agreement:

(a) use the Solution other than in accordance with the Documentation;

(b) attempt to copy (other than for backup purposes where this is not an agreement for SaaS), modify, create derivative works from, or distribute any part of the Solution;

(c) attempt to de-compile, reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form any part of the Solution except to the extent the law in Customer's or an Affiliate's jurisdiction permits this where necessary for the purposes of integrating the operation of the Solution with the operation of other software or systems used by Customer or that Affiliate. Before carrying out such action, Customer shall give DataRobot no less than 30 days' written notice and the exception will not apply if DataRobot is prepared to carry out such action at a reasonable commercial fee or provides the information necessary to achieve such integration within a reasonable period;

(d) access any part of the Solution in order to build a competing product or service;

(e) use the Solution to provide services to third parties;

(f) license, lease, transfer, assign, disclose, or otherwise commercially exploit the Solution; or

(g) modify any proprietary rights notices that appear in the Solution.

5 EVALUATION USE

5.1 Customer may receive access to the Solution (or Solution features) as a no-fee, trial, alpha, beta or early access offering ("**Evaluation Software**"). Unless otherwise agreed, use of the Evaluation Software is only for Customer's internal evaluation for 30 days from the date Customer is first granted access to the Evaluation Software.

5.2 Any predictive models generated by Customer using the Evaluation Software may only be used to evaluate the features and functions of the Evaluation Software and not used to make decisions on any other Customer business issues. Upon conclusion of the evaluation, Customer shall cease use of and destroy all such predictive models unless Customer purchases the Solution within three months of access to the Evaluation Software ending.

5.3 DataRobot shall be entitled to cancel Customer's access to the Evaluation Software or modify the Evaluation Software at any time. No warranty, availability, Maintenance or Support obligations of DataRobot will apply to Evaluation Software.

5.4 Customer agrees to provide feedback related to the Evaluation Software as reasonably requested by DataRobot. Customer grants to DataRobot, without charge, the fully paid-up, perpetual right to exploit such feedback for development of its business, products and services so long as such exploitation does not identify Customer as the source of the feedback. The Evaluation Software is subject to the terms of Section 4 (Restrictions on Use) to the same extent as the Solution.

5.5 Other than for a breach of Section 4 (Restrictions on Use), and subject to Section 16.4 (Liability which cannot be excluded), each party's liability in connection with Customer's use of any Evaluation Software will be $25,000.

6 SUPPORT, MAINTENANCE AND AVAILABILITY

6.1 DataRobot shall provide Support and Maintenance.

6.2 If Customer has purchased access to the Solution as SaaS DataRobot shall comply with Appendix 2 (Availability).

7 PROFESSIONAL SERVICES

7.1 DataRobot shall provide Professional Services as described in an Order. Where DataRobot provides any other services at Customer's request in connection with an Order, such services shall be deemed to be Professional Services and chargeable at the rate given in the Order for such services or, where no rate is given, at the rate agreed to by the parties in advance.

7.2 Professional Services will be performed Monday through Friday, excluding national holidays, during working hours, in the location where the Professional Services are to be performed by DataRobot.

7.3 DataRobot grants to Customer, during the Subscription Term a non-exclusive, non-transferable, non-sublicensable license to use any training and other informational materials provided during or created in the performance of the Professional Services to the extent necessary to enable Customer's use of the Solution in accordance with the terms of this Agreement. Unless otherwise agreed in writing, if not used, pre-purchased Professional Services and expenses expire 12 months after the date purchased.

7.4 Customer shall provide reasonable access, cooperation and information as necessary to permit DataRobot to perform the Professional Services.

7.5 While on Customer premises, DataRobot personnel shall comply with any rules or policies of Customer that are made available to them in writing.

7.6 Customer will be charged at cost for travel and expenses incurred in providing the Professional Services (if any) unless stated otherwise on the Order.

8 EXPORT

Each party will comply with applicable laws and regulations governing the export, re-export, and transfer of the Solution and will obtain all required local and extraterritorial authorizations, permits or licenses.

9 TERM AND TERMINATION

9.1 This Agreement starts on the Effective Date and will continue until terminated in accordance with its terms.

9.2 Each Order shall continue for the Subscription Term unless terminated earlier in accordance with the terms of this Agreement.

9.3 Either party shall be entitled to terminate this Agreement and any or all Orders:

(a) for any material breach not cured within 30 days following written notice of the breach; or

(b) immediately upon written notice if the other party becomes the subject of any bankruptcy proceeding or any other proceedings relating to insolvency, administration, liquidation or assignment for the benefit of some or all of its creditors or enters into an agreement for the composition, extension, or readjustment of substantially all of its obligations.

9.4 DataRobot shall be entitled to immediately terminate this Agreement and any or all Orders upon written notice:

(a) upon Customer's breach of Section 4(c) (Restrictions on Use) and Section 12.5 or 12.6(a)(Customer Data); or

(b) if it believes that it is no longer legal or desirable to continue to operate its business or to offer the Solution for use in or access from the country where Customer is using or accessing the Solution.

9.5 Except as otherwise set out in this Agreement, this Agreement and any applicable Orders are non-cancellable and all fees are non-refundable.

9.6 On termination or expiry of this Agreement for any reason:

(a) this Section 9.6, Section 11 (Proprietary Rights), Section 13 (Confidentiality), Section 16 (Limitation of Liability), Section 19 (Entire Agreement) and Section 21 (General) will survive alongside any other clauses that are intended to survive termination or expiration or expiration of this Agreement in order to achieve the fundamental purposes of this Agreement;

(b) all licenses granted under this Agreement will immediately terminate and Customer shall immediately cease use of the Solution;

(c) each party shall return and make no further use of any equipment, property, documentation and other items (and all copies of them) belonging to the other party; and

(d) any rights, remedies, obligations or liabilities of the parties that have accrued up to the date of termination which existed at or before the date of termination will not be affected.

9.7 Termination or expiry of an Order shall not affect the validity of any other Orders or this Agreement.

10 FEES, PAYMENT AND TAXES

10.1 The fees for Maintenance and Support are included in the fees for the Solution.

10.2 All fees are exclusive of any sales, excise, export, import, value added or similar tax ("**Tax**"). DataRobot shall show any applicable Tax as a separate item on its invoice to Customer.

10.3 Customer will be invoiced for the fees for the Solution, Professional Services and any applicable Tax annually in advance unless otherwise set out in the Order. Customer shall pay invoices within 30 days of the invoice date unless disputed in good faith.

10.4 All amounts due under this Agreement shall be paid by Customer in full without any set-off, counterclaim, deduction or withholding.

10.5 Following no less than 14 days' written notice, DataRobot may suspend Customer's access to Support, Maintenance and the Solution if any payments are not received within 60 days of the date of invoice that has not been disputed in good faith on objectively reasonable grounds.

11 PROPRIETARY RIGHTS

11.1 The Solution and Documentation are the proprietary intellectual property of DataRobot and its licensors. Subject to any license granted in this Agreement, DataRobot retains sole and exclusive ownership of all right, title, and interest in and to the Solution, Documentation and any other technology used to provide them.

11.2 All enhancements, modifications, corrections and derivative works that are made in or through the Solution will be considered part of the Solution for the purposes of this Agreement and will be owned by DataRobot.

11.3 Customer retains all rights, title and interest in any (i) Customer Data, (ii) predictive models created by Customer and (iii) predictions data generated by Customer through processing Customer Data through the Solution.

11.4 DataRobot will own any intellectual property rights in anything provided or created by it in the performance of the Professional Services.

12 CUSTOMER DATA

12.1 Each party shall comply with Appendix 3 (Information Security) and Appendix 4 (Data Processing).

12.2 Customer shall comply with all laws and regulations applicable to its use of the Solution.

12.3 DataRobot shall only process Customer Data as necessary to perform its obligations under this Agreement.

12.4 Customer represents and warrants that it has the necessary rights and permissions to provide the Customer Data to DataRobot.

12.5 Customer shall not use or allow others to use the Solution:

(a) for any illegal or fraudulent activity;

(b) to violate the rights of others;

(c) to threaten, incite, promote, or actively encourage violence, terrorism, or other serious harm;

(d) for any content or activity that promotes child sexual exploitation or abuse;

(e) to violate the security, integrity, or availability of any user, network, computer or communications system, software application, or network or computing device.

12.6 Subject to Section 12.7, where Customer is using the Solution as SaaS, Customer shall not import or allow others to import into the Solution any:

(a) trojan horse, worm, virus or other code which does not serve a legitimate purpose, and which is designed to be destructive, disabling or harmful or enables unauthorized access to, or disclosure or corruption of information or software;

(b) data regulated by the Payment Card Industry Data Security Standards, or other financial account numbers or credentials;

(c) information regulated by the U.S. Health Insurance Portability and Accountability Act;

(d) social security numbers (or local equivalent), driver's license numbers or other government ID numbers;

(e) sensitive personal data (including special categories of personal data defined under Article 9 and criminal offence data defined under Article 10 of the E.U. and U.K. General Data Protection Regulation);

(f) personal data of individuals under 16 years old; or

(g) information subject to regulation or protection under the U.S. Gramm-Leach-Bliley Act, U.S. Children's Online Privacy Protection Act or similar foreign or domestic laws.

12.7 Personal data listed in 12.6 (b)-(g) that has been anonymized in accordance with the applicable regulatory regime may be imported into the SaaS Solution.

12.8 For the SaaS version of the Solution**,** DataRobot shall be entitled to delete any Customer Data or suspend Customer's access to the Solution:

(a) where Customer is in breach of Section 12.5 or 12.6;

(b) where removal or blocking of the Customer Data is necessary to protect the security, or integrity of the Solution, DataRobot, or any third party; or

(c) in order to respond to law enforcement or any other governmental authority.

12.9 DataRobot shall provide written notice of any action taken in accordance Section 12.8 as soon as possible unless prohibited by applicable law. DataRobot shall use reasonable endeavours to delete the offending Customer Data without suspending access to the Solution. If access to the Solution is suspended, DataRobot shall reinstate Customer's access as soon as possible after the offending Customer Data has been deleted.

13 CONFIDENTIALITY

13.1 "**Confidential Information**" means all information of a party or its Affiliates ("**Discloser**") disclosed to the other party ("**Recipient**") that is identified as confidential at the time of disclosure or should be reasonably known by the Recipient to be confidential due to the nature of the information and the circumstances surrounding the disclosure.

13.2 The Recipient shall:

(a) not use the Discloser's Confidential Information for any purpose outside of this Agreement;

(b) not disclose such Confidential Information to any person or entity other than on a need-to-know basis;

(c) ensure that anyone Confidential Information is disclosed to is bound by written obligations of confidentiality in place with the Recipient; and

(d) use reasonable measures to protect the confidentiality of such Confidential Information.

13.3 If the Recipient is required by applicable law, court order or the rules of a stock exchange on which it is listed to make any disclosure of such Confidential Information, it will first, if legally permitted, give written notice to the Discloser. To the extent within its control, the Recipient shall permit the Discloser to intervene in any relevant proceedings to protect its interests in its Confidential Information.

13.4 Confidential Information will not include information that the Recipient can show:

(a) was rightfully in its possession or known to it prior to receipt without any restriction on its disclosure;

(b) is or becomes publicly known through no breach of this Agreement;

(c) is independently developed without the use of the other party's Confidential Information; or

(d) is rightfully obtained from a third party without breach of any confidentiality obligation.

13.5 The Recipient acknowledges that unauthorized disclosure of the Discloser's Confidential Information could cause substantial harm to the Discloser for which damages would not be an adequate remedy.

14 WARRANTIES

14.1 DataRobot warrants that:

(a) during the first 90 days following the date of the applicable Order, the Solution will, in all material respects, conform to the functionality described in the then-current Documentation for the applicable software version;

(b) the Solution is not subject to any "copyleft" or other obligation or condition that: (i) requires or conditions the use, operation, publication, reproduction or distribution of the Solution or any Customer software used in conjunction with the Solution; (ii) requires the disclosure, licensing or distribution of the Solution or any Customer software used in conjunction with the Solution (including any source code); or (iii) otherwise imposes any limitation, restriction or condition on the right or ability of DataRobot to license the Solution to its customers;

(c) it shall comply with all laws applicable to the operation of its business; and

(d) the Professional Services will be provided in accordance with good industry standards by appropriately qualified personnel using reasonable skill and care.

14.2 In the event of a breach of Section 14.1(a), Customer's sole and exclusive remedy is that DataRobot shall use commercially reasonable efforts to correct any reproducible nonconformity. If such efforts are unsuccessful within 30 calendar days of written notice from Customer, Customer may terminate the license to the affected Solution. DataRobot shall then promptly provide a pro-rata refund of the license fees that have been paid in advance for the remainder of the Subscription Term for the applicable Solution, calculated from the date of termination.

14.3 The warranty in Section 14.1(a) will not apply to the extent any non-conformance is caused by:

(a) Customer using the Solution with an application or in an environment other than as described in the Documentation; or

(b) modifications made to the Solution that were not made by DataRobot, DataRobot's authorized representatives or with the express written authorization of DataRobot.

14.4 Customer acknowledges that the accuracy of the predictive models created by the Solution is dependent on the Customer Data used to build the predictive models. DataRobot gives no warranty as to the accuracy, correctness, or completeness in live operation of any predictive model used by the Solution or predictions made by the Solution.

14.5 DataRobot only gives the express warranties in this Agreement. All other conditions, warranties or other terms which might have effect or be implied or incorporated into this Agreement whether by statute, common law or otherwise are excluded to the fullest extent permitted by law.

15 INDEMNIFICATION

15.1 Subject to Section 15.3, DataRobot agrees to defend, at its cost, Customer against (or, at DataRobot's option, settle), any third party claim to the extent such claim asserts that the Solution infringes or misappropriates any patent, copyright, trademark or trade secret of that third party and DataRobot shall pay all costs and damages finally awarded against Customer by a court of competent jurisdiction as a result of any such claim.

15.2 If the use of the Solution is, or in DataRobot's sole opinion is likely to become, subject to such a claim, DataRobot shall be entitled to:

(a) replace the applicable Solution with functionally equivalent non-infringing technology;

(b) obtain a license for Customer's continued use of the applicable Solution; or

(c) terminate this Agreement or the license to the infringing Solution and provide a pro-rata refund of the license fees that have been paid in advance for the remainder of the Subscription Term for the applicable Solution, calculated from the date of termination.

15.3 The indemnity in Section 15.1 will not apply:

(a) if the Solution is modified by anyone other than DataRobot;

(b) if the infringement is caused by Customer combining the Solution with non-DataRobot applications, code, or products;

(c) in the event of continued use of an infringing version of the Solution after DataRobot has provided a non-infringing version; or

(d) to the extent breach of this Agreement caused the infringement claim.

15.4 The foregoing will be Customer's sole remedy for any claim of infringement of third party intellectual property rights.

15.5 Customer agrees to defend, at its cost, DataRobot against any third-party claim arising from Customer's breach of Sections 12.5 or 12.6 and Customer shall pay all costs and damages finally awarded against DataRobot by a court of competent jurisdiction because of any such claim.

15.6 An indemnifying party's obligations under this Section 15 only apply if:

(a) the other party notifies the indemnifying party of the indemnification claim in writing as soon as possible once it becomes aware of the claim;

(b) the indemnified party makes no admission of liability or fault;

(c) the indemnifying party is given sole control over the defense of the claim and settlement of it; and

(d) the indemnified party provides all reasonable assistance to the indemnifying party.

16 LIMITATION OF LIABILITY

16.1 Subject to Section 16.4, except for any loss or damage to Customer caused directly by the Solution's failure to operate in accordance with the Documentation, DataRobot shall have no liability related to Customer's reliance on predictions made by the Solution.

16.2 Subject to Section 16.4, in no event will either party be liable for any: (a) loss of revenues or profits; (b) loss of or damage to business reputation; (c) loss of use or business interruption; (d) loss of wasted management time or staff time; (e) loss of data; or (f) indirect, incidental, special, punitive or consequential damages, whether in an action in contract or tort (including negligence), even if the other party has been advised of the possibility of such damages.

16.3 Subject to Sections 16.1, 16.2 and 16.4, each party's liability for any damages payable to the other party or, in the case of DataRobot, liability for damages payable to Customer or in respect of any Affiliate, (whether for breach of contract, misrepresentations, negligence, strict liability, other torts or otherwise) under or in connection with this Agreement and all Orders shall be limited as follows. Each party's liability for damages in any complete calendar year following execution of this Agreement will not exceed 100% of the total fees paid (plus fees payable) to DataRobot during the immediately preceding calendar year. In respect of any damages becoming payable in respect of the first such calendar year, the sum shall be the total amount payable in the first year of the Subscription Term.

16.4 Nothing in this Agreement will limit or exclude either party's liability for:

(a) any matter which by law may not be excluded or limited;

(b) in the case of Customer, for: (i) breach of Sections 4 (Restrictions on Use) or 12.5 or 12.6 (Customer Data); and (ii) payment of fees.

17 RESELLERS

17.1 If Customer makes any purchases through an authorized partner of DataRobot ("**Partner**"):

(a) instead of paying DataRobot, Customer will pay the applicable amounts to the Partner, as agreed between Customer and the Partner; and

(b) Customer order details (e.g., the Solution Customer is entitled to use, how Customer's entitlements are measured, the Subscription Term, etc.) will be as stated in the order placed between Partner and Customer and communicated to DataRobot.

17.2 Partners are not authorized to modify this Agreement or make any promises or commitments on DataRobot's behalf, and DataRobot is not bound by any obligations to Customer other than as set out in this Agreement or in writing by an authorized DataRobot representative.

17.3 The amount paid or payable by the Partner to DataRobot for Customer's use of the applicable Solution under this Agreement will be deemed the amount actually paid or payable under this Agreement for purposes of calculating the liability cap in Section 16.3 (Limitation of Liability).

18 DATAROBOT DATA

18.1 When customers use the Solution DataRobot may collect, and process data related to the use of the Solution as detailed in this Section 18. To the extent that this data includes personal data, DataRobot is a data controller under the GDPR and the UK GDPR and complies with applicable privacy laws and DataRobot's Privacy Policy.

18.2 User Metrics: Where customers use the SaaS version of the Solution, DataRobot may collect and analyze data about customers' usage of the Solution, including technical logs, account and login information, frequency of logins, the

volume of data uploaded, and number of models deployed, feature usage and engagement. DataRobot uses this data to review user trends and performance, improve and develop products, to provide Support and assist customers with deployment and adoption of the Solution. When usage data is used for purposes other than Support, it is anonymized of customer data and personal data in accordance with applicable law.

18.3 Metadata: Where customers use the SaaS version of the Solution, we may also collect and analyze customer metadata that describes customer models and projects. Metadata may include, for example, data points such as dataset summary statistics, dataset size, project type, model accuracy metrics, run times, project and model flags or errors, which models and blueprints were run, and the parameters of those models and blueprints. Customer metadata is used to improve the overall performance of DataRobot AI models. Metadata is anonymized of any customer data and personal data in accordance with applicable law, and does not include any Customer Data.

18.4 Contact Data: DataRobot collects personal data from employees and personnel of customers while doing business with customers, including as necessary for access to the Solution and Support. Contact data collected includes contact information and employment information such as employer and job title. Contact data is used for administrative and account management purposes, to provide and bill for the Solution, advise customers of new products and product updates, and comply with our contractual and legal obligations. Contact data is processed in accordance with our Privacy Policy.

19 ENTIRE AGREEMENT

19.1 This Agreement and any documents referred to in it are the complete and exclusive statement of the parties' agreement and supersede all proposals or prior arrangements, understandings or agreements between the parties relating to the subject matter of this Agreement.

19.2 Each party acknowledges that, in entering into this Agreement, it has not relied on, and will have no right or remedy in respect of, any statement, representation, assurance, understanding or warranty (whether in writing or not) of any person (whether party to this Agreement or not) other than as expressly set out in this Agreement.

20 NOTICES

20.1 All notices required to be given under this Agreement shall be in writing and delivered by hand, email, first class prepaid mail or recorded delivery mail.

20.2 Notices for DataRobot shall be sent to legal@datarobot.com or DataRobot Inc., 225 Franklin St.; 13th Floor, Boston, MA 02110, U.S.A., Attn: Legal.

20.3 Notices for Customer shall be sent to the bill to address on the Order or address at the top of this Agreement.

20.4 Notice will be deemed given:

(a) when received, if delivered by hand or email; or

(b) the next business day after it is sent, if sent by first class prepaid mail or recorded delivery;

(c) five business days following postage if sent internationally.

21 GENERAL

21.1 Unless it expressly states otherwise, this Agreement does not give rise to any rights for a third party to enforce any term of this Agreement.

21.2 If this Agreement conflicts with any of the terms of any Order, then the terms of the Order will control solely with respect to the Solution and Professional Services covered by the Order. Any purchase orders issued by Customer shall be deemed to be for Customer's convenience only and, notwithstanding acceptance of purchase orders by DataRobot, shall in no way change, override, or supplement this Agreement.

21.3 Any waiver or modification of the provisions of this Agreement will only be effective if in writing and signed by both parties.

21.4 If the whole or any part of a provision of this Agreement is held invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions will be unaffected. If any invalid, unenforceable or illegal provision would be valid, enforceable or legal if part of it were deleted, the provision shall apply with whatever modification is necessary to give effect to the commercial intention of the parties.

21.5 No failure or delay by a party to exercise any right or remedy provided under this Agreement or by law will constitute a waiver of that or any other right or remedy, nor will it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of such right or remedy will prevent or restrict the further exercise of that or any other right or remedy.

21.6 DataRobot is an independent contractor and not an employee of Customer. At no time shall either party make any commitments or incur any charges or expenses for or in the name of the other party, or be considered the agent, partner, joint venture, employer or employee of the other party.

21.7 Customer may not assign this Agreement without the prior written approval of DataRobot.

21.8 Neither the Uniform Commercial Code (UCC), the United Nations Convention on Contracts for the International Sale of Goods nor the Uniform Computer Information Transactions Act (UCITA) will apply to this Agreement.

21.9 As defined in U.S. Federal Acquisition Regulation (FAR) section 2.101, the Solution and Documentation are "commercial items" and according to U.S. Defense Federal Acquisition Regulation Supplement (DFARS) section 252.227 7014(a)(1) and (5) are deemed to be "commercial computer software" and "commercial computer software documentation." Consistent with DFARS section 227.7202 and FAR section 12.212, any use modification, reproduction, release, performance, display, or disclosure of such commercial software or commercial software documentation by the U.S. Government will be governed solely by the terms of this Agreement and will be prohibited except to the extent expressly permitted by the terms of this Agreement.

21.10 Neither party will be responsible for any failure to perform its obligations under this agreement due to causes beyond its reasonable control including acts of any government or government agency such as blocking internet traffic or any webpage (each a "**Force Majeure Event**"). The time for performance will be extended for a period equal to the duration of the Force Majeure Event. If a Force Majeure Event continues for more than 30 days then either party may terminate the relevant Order by giving written notice to the other party.

21.11 Customer agrees that DataRobot may refer to Customer by its trade name and logo, and may briefly describe Customer's business, in DataRobot's marketing materials and website.

21.12 Each party represents that its signatory whose signature appears on the Order is duly authorized by all necessary corporate or other appropriate action to execute this Agreement.

21.13 Except as may be stated in relation to any SCCs (as defined in Appendix 4) agreed by the parties in respect of the international transfer of Personal Data under Appendix 4, this Agreement and any dispute (whether contractual or non-contractual) arising out of or in connection with this Agreement, its subject matter or formation will be governed by and interpreted and construed in accordance with the laws of the Commonwealth of Massachusetts, without regard to conflict of law principles, and will be subject to the exclusive jurisdiction of the federal and state courts located in Boston, Massachusetts. Each party consents to the exclusive personal jurisdiction and venue of such courts.

Appendix 1

Support Policy

This Appendix 1 (Support Policy) describes the support services provided by DataRobot to Customer.

1. DEFINITIONS

"Business Day" means Monday through Friday (Customer Local Time), excluding public holidays in the country where Customer is based.

"Business Hours" means 9:00 a.m. to 5:00 p.m. (Customer Local Time) on Business Days.

"**GA Release**" means the current generally available Major Release of the Solution plus the previous Major Release (e.g. Vers. 7.2 and 7.1).

"**LTS Release**" means each x.1 release of the Solution;

"**Maintenance Release**" means an Upgrade to the Solution bringing fixes and security updates to an existing Major Release;

"**Major Release**" means each new release of the Solution where the number after the decimal point changes e.g. Vers 7.1, 7.2.

"Support Contact" means Authorized Users registered in the DataRobot Support Portal account.

"**Upgrades**" all new versions, updates, and upgrades of the Solution made generally available to DataRobot's customer base.

2. TECHNICAL SUPPORT CONTACT INFORMATION

The number of Support Contacts that may contact DataRobot technical support will be as set out in the Order. If the Order contains no limit, the number of Support Contacts will be unlimited. Customer's Support Contacts may contact DataRobot technical support by opening a case via the DataRobot Support Portal (support.datarobot.com).

3. SUPPORT SERVICES OBLIGATIONS

3.1 Customer shall use the DataRobot Support Portal to report any failure of the Solution to operate in accordance with its Documentation ("**Error**"). DataRobot shall use commercially reasonable efforts, commensurate with the severity of the Error, to correct the Error.

3.2 Customer shall conduct reasonable and adequate research with respect to any claimed Error prior to contacting the DataRobot Support Portal. Customer will respond promptly to all reasonable DataRobot requests for information and assistance regarding an Error.

3.3 Each reported Error will be logged and assigned a tracking identifier which will be provided to Customer. Customer may suggest the severity level when submitting an Error. DataRobot shall be entitled to adjust the severity based on the definitions in Paragraph 3.5. Any support for Upgrades will be designated as Severity 3.

3.4 DataRobot does not provide Support for any customizations of the Solution nor any scripts, extensions, APIs or similar that are created for Customer unless agreed otherwise in writing.

3.6 If Customer contacts DataRobot about a version of the Solution that was released more than 24 months before the most current LTS Release, DataRobot's support obligations will be limited to assisting with queries related to matters covered by the Documentation and requests to install Upgrades.

3.7 DataRobot shall use commercially reasonable efforts to deliver a solution or an action plan to correct any reported Error as follows:

SEVERITY	DATAROBOT RESPONSIBILITIES	CUSTOMER RESPONSIBILITIES	DEFINITION
Severity 1	Resources available 24x7 until a resolution or workaround is in place.	Designated resources available 24x7 until a resolution or workaround is in place. Ability to provide necessary diagnostic information.	A condition in which all or a critical portion of the Solution is not operating.
Severity 2	Resources available Monday through Friday during Business Hours until a resolution or workaround is in place.	Resources available Monday through Friday during local Business Hours until a resolution or workaround is in place. Ability to provide necessary diagnostic information.	A condition in which the Solution is degraded, but there is some capacity to operate the Solution by a majority of Customer's users.
Severity 3	Resources available Monday through Friday during Business Hours until a resolution or workaround is in place.	Resources available Monday through Friday during Business Hours until a resolution or workaround is in place. Ability to provide necessary diagnostic information.	A condition whereby Customer has experienced a partial, non-critical loss of functionality of the Solution.
Severity 4	Solid understanding of Customer request documented in DataRobot systems for review by Product Management.	Use cases for the feature request and specifics on requested functionality	A condition whereby functionality of the Solution is not affected, but a change is desired solely for

			aesthetic, “look and feel,” or similar reasons.

SEVERITY	INITIAL RESPONSE TARGET	UPDATE FREQUENCY TARGET
Severity 1	Within 1 hour	Continuous effort with written updates every 4 hours
Severity 2	Within 2 Business Hours	Updated every Business Day
Severity 3	Within 8 Business Hours	Updated every 3 Business Days
Severity 4	Within 2 Business Days	N/A, feature request

3.6 For a Severity 1 Error, the parties agree to activate a management call-out and escalation list for the purpose of problem resolution.

3.7 With Customer’s written permission, DataRobot may access error logs and application logs held by Customer for the sole purpose of providing proactive support and fixes to the affected Solution. This may require a connection to Customer’s system, or Customer can establish a means of getting this information to DataRobot personnel in a manner conducive to providing efficient support (e.g., posting logs to a secure ftp site).

4. MAINTENANCE

4.1 This paragraph 4 details the Maintenance provided to Customer.

4.2 DataRobot shall make Upgrades available to Customer without additional charge.

4.3 For the on-premise version of the Solution, Customer may download and install an Upgrade once the Upgrade is released.

4.4 For Customers using the on-premise version of the Solution, DataRobot will provide Maintenance Releases for each GA Release. Each LTS Release will receive Maintenance Releases until the release of the next LTS Release.

4.5 For the SaaS version of the Solution, DataRobot shall be entitled to perform maintenance to the Solution or any elements of its hardware or infrastructure as DataRobot deems necessary for the provision of the Solution and Upgrades will be automatically applied to the Solution. DataRobot shall give Customer no less than 14 days’ notice of any scheduled Maintenance (“**Scheduled Maintenance**”) and as much notice as possible for any other Maintenance. Notice of Scheduled Maintenance will be given at https://status.datarobot.com/. Customer can subscribe to email updates to the page using the subscribe function on the page. During Maintenance, Customer may not be able to access the Solution. DataRobot shall use commercially reasonable efforts to keep the frequency and duration of impeded access during Maintenance to a minimum.

4.6 DataRobot shall be entitled to update the Documentation to reflect Upgrades or at any other time for any other reason.

5. EXCLUSIONS

This Support Policy does not apply to any software, equipment, or solutions not purchased from DataRobot. This Support Policy does not apply if Customer is in material breach of this Agreement or payment is overdue for any undisputed invoice.

6. CHANGES TO SUPPORT

DataRobot is continually seeking to improve the service it provides to customers, including technical support. DataRobot shall be entitled to update this Support Policy at any time and the version applicable will be the then current version. DataRobot will provide no less than 30 days' written notice if any update to the Support Policy will have a material adverse effect on your use of the Solution or DataRobot’s obligations under this Support Policy. In such circumstances, Customer shall be entitled to terminate the relevant Order by giving written notice to DataRobot within 60 days of the notice date on DataRobot’s notice of changes to this Support Policy. If Customer terminates, DataRobot will promptly provide a pro-rata refund of the license fees that have been paid in advance for the remainder of the Subscription Term for the applicable Solution, calculated from the date of termination.

Appendix 2

Availability Terms

This Appendix 2 will only apply if Customer has purchased the SaaS version of the Solution, as indicated in the Order.

1. AVAILABILITY

1.1 Definitions

"**Available**" means Customer can:

(a) log into the Solution (see Website);

(b) create a Project within the Solution (see AutoML & API);

(c) ingest data into its Projects (see DataPrep and AI Catalog and DataIngest);

(d) run an AutoPilot (see AutoML & API);

(e) deploy a chosen predictive model; (see AutoML & API)

(f) make predictions based on a deployed predictive model (see Predictions);

(g) where applicable, monitor the deployed predictive model for accuracy and drift (see MLOps).

"**Exclusions**" means any time the Solution is not accessible because of:

(a) any Scheduled Maintenance performed by DataRobot.

(b) failure of the internet backbone itself and the network by which Customer connects to the internet backbone;

(c) any network unavailability outside of the data center located router that provides the outside interface of each of DataRobot's WAN connections to its backbone providers;

(d) misconfigurations, proxies or firewalls of Customer;

(e) Customer using, combining or merging the Solution with any hardware or software not supplied by DataRobot or not identified by DataRobot in the Documentation as being compatible with the Solution; or

(f) Customer's or any third party's use of the Solution in an unauthorized or unlawful manner.

"**Project**" means a project of all predictive models built with a dataset imported into the Solution. See here for more details.

"**Quarterly Uptime**" the percentage of time the Solution is Available in a calendar quarter measured by the following formula: (n - y)/n *100, where:

(a) "n" is the total number of minutes in a calendar quarter;

(b) "y" is the total number of minutes in a calendar quarter that the Solution was not accessible to Customer ; and

(c) "y" will not include any minutes where the Solution was not accessible because of an Exclusion.

1.2 DataRobot shall make the Software Available to Customer with a Quarterly Uptime of at least 99.95%.

1.3 Quarterly Uptime will be determined by a DataRobot health monitoring system. Notice of availability is provided at https://status.datarobot.com/.

2. REMEDIES FOR MISSING QUARTERLY UPTIME

2.1 If Quarterly Uptime falls below 99.95% in a calendar quarter, DataRobot shall pay Customer a service credit as follows ("**Service Credit**"):

Availability	**Service Credit**
97.0% - 99.94%	5 percent of the fees for the affected Solution for the applicable calendar quarter
95.0% - 96.9%	10 percent of the fees for the affected Solution for the applicable calendar quarter
Less than 95%	20 percent of the fees for the affected Solution for the applicable calendar quarter

2.2 To receive Service Credits, Customer shall submit a written request to DataRobot at legal@DataRobot.com within 30 days after the end of the quarter in which Quarterly Uptime was less than 99.9% or Customer's right to receive Service Credits will be waived. Customer's notice must include the date and time period for each instance where the Solution was not Available and any relevant calculations.

2.3 Such Service Credit will be issued as a credit against any fees owed by Customer for the calendar quarter of the Subscription Term after the request for a Service Credit, or, if Customer does not owe any additional fees, then DataRobot shall pay Customer the amount of the applicable Service Credit within 30 days after the end of the calendar month in which Customer has requested the Service Credit. The remedies stated in this Appendix 2 are Customer's sole and exclusive remedy for service interruption or unavailability.

3. CHANGES TO AVAILABILITY

DataRobot is continually seeking to improve the service it provides to customers, including around service availability. DataRobot shall be entitled to update these Availability Terms at any time and the version applicable will be the then current version. DataRobot will provide no less than 30 days' written notice if any update to the Availability Terms will have a material adverse effect on your use of the Solution or DataRobot's obligations under this Support Policy. In such circumstances, Customer shall be entitled to terminate the relevant Order by giving written notice to DataRobot within 60 days of the notice date on DataRobot's notice of changes to these Availability Terms. If Customer terminates, DataRobot will promptly provide a pro-rata refund of the license fees that have been paid in advance for the remainder of the Subscription Term for the applicable Solution, calculated from the date of termination.

Appendix 3

DataRobot Information Security Exhibit

This Appendix 3 describes the technical and organizational security measures implemented by DataRobot to secure the Solution and Customer Data where Customer purchases the SaaS version of the Solution. DataRobot may update or change its controls from time to time but will never materially decrease the level of security as set out in this Appendix 3.

1. Definitions

Unless otherwise defined herein, all capitalized terms have the meaning given to them in the body of the Agreement.

"Customer Data" means data that is imported into the Solution by Customer or provided to DataRobot to import into the Solution on Customer's behalf.

"Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data.

"Personal Data" means any Customer Data relating to an identified or identifiable natural person or household.

"Supervisory Authority" means any regulator or regulatory body or supervisory authority in any country.

2. General Security Practices

DataRobot has implemented and shall maintain appropriate technical and organizational measures designed to protect Customer Data against accidental loss, destruction, alteration, unauthorized disclosure or access, or unlawful destruction, including the policies, procedures and internal controls as set forth in this Appendix 3.

3. Information Security Organization

3.1 **Information Security Program.** DataRobot shall maintain a comprehensive written information security program ("**Program**") that encompasses administrative, technical and physical controls designed to protect the confidentiality, security, integrity, and availability of Customer Data and with the aim of protecting against Data Breaches. DataRobot shall ensure the Program is consistent with global industry standards and appropriately tailored to the types of data processed by DataRobot.

3.2 **Information Security Personnel.** DataRobot's Program shall be led by its Chief Information Security Officer ("**CISO**"), who is responsible for its direction, governance and oversight. To administer the Program, the CISO shall direct a team of highly qualified personnel with training and certifications specialized in information security.

3.3 **Information Security Review.** DataRobot's Program and approach to managing information security shall be reviewed regularly and whenever significant changes occur, by appropriate internal and external assessors.

3.4 **Information Security Governance.** DataRobot shall establish and maintain an Enterprise Security Steering Committee as a cross-functional leadership team to shape security programs and drive executive alignment in all security initiatives. DataRobot shall also designate a Security Advisory Council to meet regularly to foster communication between operational teams and ensure security is considered in all projects.

3.5 **Policies and Procedures.** DataRobot shall maintain policies and procedures related to information security, confidentiality and integrity. These shall be reviewed and updated at least annually and made available to employees via the DataRobot intranet. Employees must review and acknowledge these policies at onboarding and on an annual basis.

4. Human Resources Security

4.1 **General.** DataRobot shall ensure all personnel are subject to written confidentiality obligations and the DataRobot Code of Conduct and Business Ethics, and shall inform personnel of the consequences of violation. Personnel who violate these shall be subject to disciplinary action up to and including termination.

4.2 **Training and Awareness.** DataRobot shall ensure that mandatory information security and data privacy training is provided to employees at onboarding and on a regular basis throughout employment to aid in the prevention of unauthorized or

unintended disclosure of Customer Data. Training shall be regularly reinforced by security awareness communications, events and phishing campaigns.

4.3 **Background Checks.** DataRobot shall conduct background checks on personnel in compliance with applicable law, including employment history, foreign employment, criminal background, credit check (when applicable), education verification, sex offender register, OFAC/Global Sanctions, SSN Tracing.

4.4 **Third Party Security.** DataRobot shall implement a vendor management program to assess and monitor risk associated with service providers that process Customer Data. Service providers shall be evaluated prior to onboarding and periodically throughout their engagement, and are contractually obligated to security and confidentiality requirements.

5. Business Continuity Management

5.1 **Business Continuity Management Program.** DataRobot shall maintain a Business Continuity Management Program ("**BCM Program**") designed to manage significant disruptions to operations and infrastructure, including cybersecurity incident response. The BCM Program shall include the following elements:

(a) defined global and regional governance bodies and executive ownership;

(b) full-time BCM professionals responsible for creating, managing and monitoring preparedness;

(c) defined crisis management organizations and escalation protocols;

(d) established crisis communications strategies for all stakeholders;

(e) identification of critical activities and planned recovery time objectives;

(f) thorough risk and impact assessments of locations and processes, including critical suppliers;

(g) testing on at least an annual basis of all related systems and components, including staff recovery, and tracked remediation for any issues identified during testing; and

(h) continued maintenance and review of arrangements to respond to changing business requirements and risks.

5.2 **Data Recovery.** Where and as applicable, DataRobot shall design redundant storage and procedures for recovering data in its possession or control in a manner sufficient to reconstruct Customer Data in its original state on the last recorded backup.

6. Physical Controls

6.1 **Physical Access to Facilities.** DataRobot shall limit access to all office locations to authorized individuals. All office building entryways shall be monitored by building security personnel and/or CCTV and shall be access controlled at all times.

(a) All personnel shall be issued entry and identification badges which must be carried at all times. Badges shall be deactivated upon employment termination.

(b) All office visitors shall be logged and accompanied throughout the office.

6.2 **Physical Access to Equipment.** All DataRobot server rooms shall implement badge entry access controls to limit access to authorized personnel only.

6.3 **Protection from Disruptions.** DataRobot shall implement appropriate measures designed to protect against loss of data due to power supply failure or line interference.

7. Audits

7.1 **General.** DataRobot shall cooperate with reasonable requests by Customer for legally required audits of DataRobot's security and privacy practices. The time, duration, place, scope and manner of the audit must be mutually agreed by the parties.

7.2 **Audit Procedure.** On written request from Customer, DataRobot shall answer Customers' written questions about DataRobot's security and privacy practices and shall provide Customer with information necessary to demonstrate DataRobot's compliance with the terms of Appendices 3 and 4. Customer may make one request per calendar year except if a Data Breach has occurred.

7.3 **Certifications.** DataRobot shall make available to Customer, upon written request and without undue delay, copies of any third-party audit reports or evidence of certifications it maintains (such as SSAE 16 –SOC2, attestations or ISO 27001:2013 certifications, or their equivalent under any successor standards) that apply to the Solution. DataRobot shall maintain SSAE 16 – SOC2 and ISO 27001:2013 certifications, or equivalent successor standards, for the duration of the Agreement.

7.4 **Regulatory Compliance.** Taking into account the nature of the request and to the extent reasonably feasible from a technical perspective, DataRobot shall provide Customer with any information necessary to enable Customer to comply with any applicable law or any request from a Supervisory Authority.

7.5 **Cooperation with Supervisory Authorities.** If a Supervisory Authority wishes to carry out an audit of DataRobot or its activities under the Agreement, Customer shall provide DataRobot with no less than 10 business days' notice, unless the Supervisory Authority has given less notice to Customer. DataRobot shall cooperate with the Supervisory Authority as they require.

8. Customer Data

8.1 Where Customer Data includes Personal Data, the parties will comply with their obligations in Appendix 4.

8.2 **Cloud Data Storage.** Other than for the Zepl and Algorithmia products, DataRobot's SaaS product is hosted on AWS servers located in the United States and Ireland. Customers based in the United States will be provisioned on the United States AWS instance and customers based in the European Economic Area, Switzerland and the UK will be provisioned on the Ireland AWS instance. Customers located in other countries will be provisioned on either the Ireland or US AWS instance. To review AWS's security documentation, please visit https://aws.amazon.com/compliance/data-center/controls/. The Zepl and Algorithmia products are hosted with the cloud provider and in the region stated on the Order.

8.3 **Data Backups.** AWS Elastic Block Store (EBS) volumes are backed up using EBS Snapshots. Backups shall be automated, encrypted, and performed multiple times daily.

8.4 **Logging and Monitoring.** DataRobot shall maintain logs of administrator and operator activity and data recovery events.

8.5 **Data Encryption.** DataRobot shall encrypt all Customer Data residing in or transiting to or from the Solution. Customer Data in transit is encrypted using HTTPS (TLS 1.2/AES-256). Data at rest in AWS S3 buckets is encrypted with SSE-S3 object level data encryption (AES-256).

8.6 **Return of Data**. Customer may export its data from the Solution at any time during the Subscription Term in accordance with the instructions in the Documentation.

8.7 **Data Disposal.** Within 30 days of termination of Subscription Term, DataRobot will delete all Customer Data that is not required to be retained by law. Any Customer Data that is retained will be managed in accordance with the terms of this Appendix 3 and Appendix 4 (where applicable) and deleted according to our retention policy. For data stored in the Zepl product, DataRobot shall delete such Customer Data within 14 days of a written request from Customer.

9. Access Controls

9.1 **Access Management**. DataRobot shall employ access control mechanisms to prevent unauthorized access to Customer Data and systems that have access to Customer Data. DataRobot shall restrict access to Customer Data only to personnel whose access is necessary to provide the Solution.

(a) DataRobot shall maintain a record of personnel authorized to access Customer Data and review user access rights at regular intervals.

(b) DataRobot shall have controls designed to avoid personnel assuming access rights beyond those that they have been assigned to limit unauthorized access to Customer Data.

(c) At Customer's reasonable request, DataRobot shall promptly suspend or terminate access rights to Customer Data for DataRobot personnel reasonably suspected of breaching any of the provisions of this Appendix 3. DataRobot shall remove access rights of all personnel upon termination of their employment.

9.2 **Secure Access Protocols.** DataRobot shall use secure access protocols and solutions such as LDAP, firewalls, and VPN to enforce logical access in the internal network environment.

9.3 **Application Password Management.** For users attempting to access the Solution, DataRobot shall require complex user passwords with length, character complexity, and non-repeatability requirements. DataRobot shall ensure that deactivated or expired login credentials are not granted to other individuals. User passwords shall be encrypted and salted using PBKDF2 (SHA512+128bit salt).

9.4 **Application Authentication Controls.** Other than for the Zepl product, DataRobot shall monitor repeated failed attempts to gain access to the Solution and shall lock out user accounts after five failed authentication attempts. DataRobot shall ensure that two factor authentication is available for user accounts, and provide for unique user API tokens. DataRobot shall allow for Single Sign On (SSO) authentication with any standard SAML 2.0 identity provider.

9.5 **Role Based Access.** DataRobot shall provide granular user application privilege controls. User administrative accounts shall have the ability to assign user and group roles with varying levels of access privileges based on the user's or group's use of the Solution.

10. Data Breaches

DataRobot shall maintain procedures to ensure a timely and efficient response to a Data Breach.

DataRobot shall:

(a) notify Customer without undue delay but no later than 48 hours after becoming aware of a Data Breach;

(b) provide assistance and available information to Customer as reasonably requested to enable Customer to investigate, mitigate the effects of and remediate the Data Breach and comply with any breach notification obligations that apply to Customer under applicable law;

(c) take steps to identify the cause of any Data Breach and put in place measures and take steps that DataRobot deems necessary to mitigate the effects of and remediate the Data Breach;

(d) retain appropriate information and records about any Data Breach for a reasonable period of time;

(e) cooperate with Customer, law enforcement and any appliable Supervisory Authorities as reasonably required in relation to a Data Breach;

(f) not reference or identify Customer when making any notification to a third party about a Data Breach unless required to do so by applicable law.

11. Communications Security

11.1 **Networks.** DataRobot shall use the following controls designed to secure its networks that access or process Customer Data:

(a) Network traffic shall pass through firewalls, which are monitored at all times. DataRobot shall implement intrusion detection and/or prevention systems.

(b) Network devices used for administration shall utilize industry standard cryptographic controls when processing Customer Data.

(c) Anti-spoofing filters and controls shall be enabled on routers.
Network, application and server authentication passwords shall have complexity requirements.
DataRobot shall have a policy prohibiting the sharing of user IDs, passwords or other login credentials.

(d) Firewalls shall be deployed to protect the perimeter of DataRobot's networks.

11.2 **Virtual Private Networks.** DataRobot shall employ the following controls when remote connectivity to DataRobot's network is required for processing Customer Data:

(a) Connections shall be encrypted using industry standard cryptography (i.e. a minimum of 256 bit encryption);

(b) Connections shall only be established using VPN servers;

(c) Multifactor authentication shall be required for access.

12. Secure Development

12.1 **Development Requirements.** DataRobot shall have policies for secure development, system engineering, change control, and support. DataRobot shall conduct appropriate tests for system security as part of acceptance testing processes. DataRobot shall supervise and monitor the activity of outsourced system development.

12.2 **Change Management.** DataRobot shall follow industry best practices for the tracking of application projects and source code changes. Task tracking software shall be used to provide an audit trail of all software changes and pull requests. All code shall be subject to extensive testing, stakeholder signoffs, and code review prior to release.

12.3 **Application Code Security Analysis.** DataRobot shall adhere to the OWASP Top 10 for secure coding practices. Static, dynamic and software composition analysis scans shall be performed on each major application release. If the scans reveal any material deficiencies or weaknesses, DataRobot shall promptly take such steps as may be required, in DataRobot's reasonable discretion, to remediate, taking into consideration their criticality based on their nature, severity and likelihood.

12.4 **Application Environment Security Analysis.** For each major application release, DataRobot shall perform static and dynamic analysis scans and container environment scans. If the scans reveal any material deficiencies or weaknesses, DataRobot shall promptly take such steps as may be required, in DataRobot's reasonable discretion, to remediate, taking into consideration their criticality based on their nature, severity and likelihood.

12.5 **Supply Chain Management.** DataRobot shall manage and regularly scan its software supply chain libraries for vulnerabilities and license compliance. DataRobot shall promptly remediate any material vulnerabilities or instances of noncompliance that are identified.

13. Security Testing and Monitoring

13.1 **Testing and Monitoring Requirements.** DataRobot shall maintain policies and procedures for the ongoing testing and monitoring of DataRobot environments by internal and/or external parties, using industry standard tools and methodologies.

13.2 **Threat Management.** DataRobot shall maintain a threat management program to monitor both malicious and non-malicious threats**.** Identified issues shall be reviewed and investigated.

13.3 **Penetration Testing.** On at least an annual basis, DataRobot shall engage a trusted third-party security vendor to perform penetration tests to detect corporate infrastructure and network vulnerabilities. Any and all identified vulnerabilities or weaknesses shall undergo a risk assessment process and shall be mitigated as appropriate.

13.4 **Remediation.** If the testing and monitoring described in this Section 13 reveal any material deficiencies or weaknesses, DataRobot shall promptly take such steps as may be required, in DataRobot's reasonable discretion, to remediate, taking into consideration their criticality based on their nature, severity and likelihood.

Appendix 4

DataRobot Data Processing Clauses

This Appendix 4 provides additional terms that apply where DataRobot Processes Personal Data as a Processor on behalf of Customer when providing the Solution to Customer pursuant to the Agreement. DataRobot may update or change this agreement from time to time but will never materially decrease the level of security or privacy rights as set out in this Appendix 4.

SECTION I - DEFINITIONS

Unless otherwise defined herein, all capitalized terms have the meaning given to them in Appendix 3 or the body of the Agreement.

"CCPA" means the California Consumer Privacy Act of 2018.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"Data Subject" means the individual to whom Personal Data relates.

"Data Protection Laws" means, to the extent they are applicable, (a) the UK GDPR; (b) the GDPR; and (c) the CCPA.

"GDPR" means the General Data Protection Regulation ((EU) 2016/679), as it has effect in EU law.

"**Process**" or **Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"**Processor**" means the entity which processes Personal Data on behalf of the Controller.

"**SCCs**" means, where the GDPR applies, the Controller to Processor Standard Contractual Clauses adopted under the GDPR that are attached at Appendix 5 (GDPR Controller to Processor SCCs), and, where the UK GDPR applies, the Controller to Processor Standard Contractual Clauses adopted under Data Protection Directive 95/96/EC that are attached at Appendix 6 (UK GDPR Controller to Processor SCCs).

"**Subprocessor**" means a third-party entity engaged by DataRobot as a Data Processor under this Appendix 4.

"Third Country" means (a) to the extent that the GDPR applies to the processing, a country outside the European Economic Area or Switzerland not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR); (b) to the extent the UK GDPR applies to the processing, a country outside the United Kingdom not recognized by the UK Government as providing an adequate level of protection for personal data (as described in the UK-GDPR).

"UK GDPR" has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018.

Clause 1

Purpose and Scope

a. The purpose of these Data Processing Clauses ("**Clauses**") is to ensure compliance with the Data Protection Laws as they may be amended, replaced or supplemented from time to time.

b. Customer and DataRobot have agreed to these Clauses in order to ensure compliance with the Data Protection Laws.

c. These Clauses apply to the Processing of Personal Data as specified in Annex II.

d. Annexes I to III are an integral part of these Clauses.

e. These Clauses are without prejudice to obligations to which Customer is subject by virtue of the Data Protection Laws.

f. To the extent that the Processing of Personal Data is within the scope of the CCPA, Customer shall be considered the "Business" and DataRobot shall be considered the "Service Provider."

Clause 2

Interpretation

a) These Clauses shall be read and interpreted in the light of the provisions of the Data Protections Laws, to the extent that they apply.

b) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in the Data Protection Laws or in a way that prejudices the fundamental rights or freedoms of the Data Subjects.

Clause 3

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

SECTION II - OBLIGATIONS OF THE PARTIES

Clause 4

Description of Processing

The details of the Processing, in particular the categories of Personal Data and the purposes of Processing for which the Personal Data is Processed on behalf of Customer, are specified in Annex II.

Clause 5

Obligations of the Parties

5.1 Instructions

a. DataRobot shall Process Personal Data only on documented instructions from Customer, unless required to do so by applicable local law to which DataRobot is subject. In this case, DataRobot shall inform Customer of that legal requirement before Processing, unless the law prohibits this. Subsequent instructions may also be given by Customer throughout the duration of the Processing of Personal Data. These instructions shall always be documented.

b. DataRobot shall immediately inform Customer if, in DataRobot's opinion, instructions given by the Customer infringe the Data Protection Laws or the applicable local law data protection provisions.

c. To the extent that the Processing of Personal Data is within the scope of the CCPA, DataRobot shall not retain, use or disclose Personal Data for any purposes other than to perform the services specified in the Agreement, or as otherwise required under applicable law. DataRobot shall not sell Personal Data as "selling" is defined in the CCPA.

5.2. Purpose limitation

DataRobot shall process Personal Data only for the specific purpose(s) of the Processing, as set out in Annex II, unless it receives further instructions from Customer.

5.3. Duration of the Processing of Personal Data

Processing by DataRobot shall only take place for the duration specified in Annex II.

5.4. Security of Processing

a. DataRobot shall at least implement the technical and organizational measures specified in Annex III to ensure the security of Personal Data. This includes protecting Personal Data against a Data Breach. In assessing the appropriate level of security,

the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for Data Subjects.

b. DataRobot shall grant access to Personal Data undergoing Processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the Agreement. DataRobot shall ensure that persons authorised to Process Personal Data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5.5. Sensitive Data

If the Processing involves Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("**Sensitive Data**"), DataRobot shall apply specific restrictions and/or additional safeguards. The collection of Sensitive Data is prohibited under the Agreement.

5.6. Documentation and Compliance

a. The Parties shall be able to demonstrate compliance with these Clauses.

b. DataRobot shall deal promptly and adequately with inquiries from Customer about the Processing of Personal Data in accordance with these Clauses.

c. DataRobot shall make available to Customer all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and/or stem directly from the Data Protection Laws. At Customer's request, DataRobot shall also permit and contribute to audits of the Processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, Customer may take into account relevant certifications held by DataRobot.

d. Customer may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of DataRobot if mutually agreed and shall, where appropriate, be carried out with reasonable notice.

e. The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

f. Customer chooses to conduct any audit or inspection it has the right to request or mandate on its own behalf by instructing DataRobot to carry out an audit in accordance with the terms of Section 7 (Audits) of Appendix 3 (DataRobot Information Security Exhibit). If Customer wishes to change this instruction regarding the audit or inspection, Customer has the right to request a change to this instruction by sending DataRobot written notice as provided for in the Agreement. If DataRobot declines to follow any instruction requested by Customer regarding audits, including inspections, Customer is entitled to terminate the Agreement in accordance with its terms.

5.7. Use of Subprocessors

a. DataRobot has Customer's general authorisation for the engagement of Subprocessors posted on www.datarobot.com/privacy/subprocessors. Customer may subscribe on that webpage to be notified of any intended changes of that list through the addition or replacement of Subprocessors at least ten days in advance.

b. Where DataRobot engages a Subprocessor for carrying out specific Processing activities (on behalf of Customer), it shall do so by way of a contract which imposes on the Subprocessor, in substance, the same data protection obligations as the ones imposed on DataRobot in accordance with these Clauses. DataRobot shall ensure that the Subprocessor complies with the obligations to which DataRobot is subject pursuant to these Clauses and to the Data Protection Laws.

c. At the Customer's request, DataRobot shall provide a copy of such a Subprocessor agreement and any subsequent amendments to Customer. To the extent necessary to protect business secrets or other confidential information, including Personal Data, DataRobot may redact the text of the agreement prior to sharing the copy.

d. DataRobot shall remain fully responsible to Customer for the performance of the Subprocessor's obligations in accordance with its contract with DataRobot. DataRobot shall notify Customer of any material failure by the Subprocessor to fulfil its contractual obligations to process Customer's Personal Data in accordance with these Clauses.

e. This Section 5.7(e) shall apply only where the GPDR or the UK GDPR applies to the Processing of the Personal Data:

1. Customer may object to DataRobot's use of a new Subprocessor on reasonable grounds related to the protection of the Personal Data by notifying DataRobot in writing within ten business days after notice of an updated Subprocessor List. In that event, DataRobot shall use commercially reasonable efforts to make available to Customer a change in the Solution or recommend a commercially reasonable change to Customer's use of the Solution to avoid Processing of Personal Data by the objected-to new Subprocessor. Any change to Customer's use of the Solution must not unreasonably burden Customer.

2. If DataRobot is unable to make such change within a reasonable period of time and cannot come to a mutually agreed upon solution, Customer may give written notice to terminate those parts of the Solution which cannot be provided by DataRobot without the use of the objected-to new Subprocessor. Promptly following termination, DataRobot shall provide a pro-rata refund of the license fees that have been paid in advance for the remainder of the Subscription Term for the applicable Solution, calculated from the date of termination.

3. DataRobot shall agree a third-party beneficiary clause with the Subprocessor whereby in the event DataRobot has factually disappeared, ceased to exist in law or has become insolvent - the Customer shall have the right to terminate the Subprocessor contract and to instruct the Subprocessor to erase or return the Personal Data.

5.8. International Transfers

a. This section 5.8 shall apply only where the GDPR or the UK GDPR applies to DataRobot's Processing of the Personal Data.

b. Any transfer of Personal Data to a Third Country or to an international organization by DataRobot shall be done only on the basis of documented instructions from Customer or in order to fulfil a specific requirement under applicable local law to which DataRobot is subject and shall take place in compliance with the GDPR or the UK-GDPR (as applicable). DataRobot may transfer Personal Data to its Affiliates or its Subprocessors located in a Third Country, subject to the notification requirements of Clause 5.7.

c. Customer agrees that where DataRobot engages a Subprocessor in accordance with Clause 5.7. for carrying out specific Processing activities (on behalf of the Customer) and those Processing activities involve a transfer of Personal Data, either directly or via onward transfer, to any Third Country, DataRobot and the Subprocessor can ensure compliance with the GDPR or the UK-GDPR (as applicable) using the relevant SCCs, provided the conditions for the use of those SCCs are met. The parties shall use reasonable efforts to agree any relevant changes to the SCCs, or replacement clauses, including sharing relevant information to complete any applicable transfer risk assessments, to enable the continued transfer of Personal Data as intended by the parties under this Agreement.

d. The SCCs attached at Appendix 5 (GDPR Controller to Processor SCCs) shall apply between Customer and DataRobot only when Personal Data is transferred, either directly or via onward transfer, from the European Economic Area and Switzerland to any Third Country. When this section 5.8 (d) applies, the following terms shall also apply:

1. For the purposes of Clause 8.5 of the SCCs, (Duration of processing and erasure or return of data), data erasure and return shall be performed in accordance with the terms of Section 8.6 (Return of Data) and Section 8.7 (Data Disposal) of Appendix 3.

2. For the purposes of Clause 8.6 (c) and (d) of the SCCs (Security of processing), data breaches shall be managed in accordance with the terms of Section 10 (Data Breaches) of Appendix 3.

3. For the purposes of Clause 8.9 of the SCCs (Documentation and compliance), audits shall be performed in accordance with the terms of Section 7 (Audits) of Appendix 3.

4. For the purposes of Clause 9 of the SCCs (Subprocessors) Subprocessors shall be managed in accordance with the terms of Section 5.7 of this Appendix 4.

5. For purposes of Clause 12 of the SCCs (Liability) liability of a party to the other party for breach of these Clauses shall be capped in accordance with the terms of Section 16 (Limitation of Liability) of the Agreement, to the extent permitted by law.

6. For purposes of Clause 15 of the SCCs (Obligations of the data importer in case of access by public authorities) requests shall be managed in accordance with DataRobot's Government Data Request Policy (available at https://www.datarobot.com/trustcenter/government-data-request-policy/).

7. For purposes of Clauses 17 and 18 of the SCCs (Governing Law), the governing law named therein shall apply to the SCCs and the Agreement, including this Appendix 4, to give full effect to the Agreement in respect of the enforcement of any rights or obligations, or any claims under the SCCs.

e. The SCCs attached at Appendix 6 (UK GDPR Controller to Processor SCCs) shall apply between Customer and DataRobot only when Personal Data is transferred, either directly or via onward transfer, from the United Kingdom to any Third Country. When this section 5.8(e) applies, the following terms shall also apply:

1. For the purposes of Clause 5(f) of the SCCs (Obligations of the data importer), audits shall be performed in accordance with Section 7 (Audits) of Appendix 3.

2. For purposes of Clause 11 of the SCCs (Subprocessing), Subprocessors shall be managed in accordance with the terms of Section 5.7 of this Appendix 4.

3. For purposes of Clause 12(1) of the SCCs (Obligations after termination of personal data processing services), data erasure and return shall be performed in accordance with the terms of Section 8.6 (Return of Data) and Section 8.7 (Data Disposal) of Appendix 3.

4. For the purposes of Clause 9 of the SCCs (Governing Law), the governing law named therein shall apply to the SCCs and the Agreement, including this Appendix 4, to give full effect to the Agreement in respect of the enforcement of any rights or obligations, or any claims under the SCCs.

f. The parties agree that the terms of this section 5.8 are not intended to amend or modify the SCCs. These provisions provide clarity in terms of DataRobot's business processes for complying with the SCCs. In the event of any conflict between the terms of this Appendix 4 and the provisions of the SCCs, the SCCs shall prevail.

Clause 6

Assistance to the Customer

a. DataRobot shall promptly notify Customer of any request it receives from Data Subjects. It shall not respond to the request itself, unless authorized to do so by Customer.

b. DataRobot shall assist Customer in fulfilling its obligations to respond to Data Subjects' requests to exercise their rights, taking into account the nature of the Processing. In fulfilling its obligations in accordance with (a) and (b), DataRobot shall comply with Customer's instructions.

c. In addition to DataRobot's obligation to assist Customer pursuant to Clause 6(b), DataRobot shall furthermore assist Customer in ensuring compliance with the following obligations, taking into account the nature of the Processing and the information available to DataRobot:

1. The obligation to carry out an assessment of the impact of the envisaged Processing on the protection of Personal Data (a "**Data Protection Impact Assessment**") where a type of Processing is likely to result in a high risk to the rights and freedoms of natural persons;

2. the obligation to consult the competent supervisory authority/ies prior to Processing where a Data Protection Impact Assessment indicates that the Processing would result in a high risk in the absence of measures taken by Customer to mitigate the risk;

3. the obligation to ensure that Personal Data is accurate and up to date, by informing Customer without delay if DataRobot becomes aware that Personal Data it is Processing is inaccurate or has become outdated;

4. the obligations in the Data Protection Laws.

d. The Parties shall set out in Annex III the appropriate technical and organizational measures by which DataRobot is required to assist Customer in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 7

Notification of Data Breach

In the event of a Data Breach, DataRobot shall cooperate with and assist the Customer for the Customer to comply with its obligations under the Data Protection Laws, taking into account the nature of Processing and the information available to DataRobot.

7.1 Data Breach concerning Personal Data Processed by the Customer

a. In the event of a Data Breach concerning Personal Data Processed by the Customer, DataRobot shall assist the Customer:

1. in notifying the Data Breach to the competent supervisory authority/ies, without undue delay after Customer has become aware of it, where relevant and unless the Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons;

2. in obtaining the following information which, pursuant to the Data Protection Laws, shall be stated in Customer's notification, and must at least include:

A. the nature of the Personal Data including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

B. the likely consequences of the Data Breach;

C. the measures taken or proposed to be taken by Customer to address the Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

b. Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

c. In complying, pursuant to the Data Protection Laws, with the obligation to communicate without undue delay the Data Breach to the Data Subject, when the Data Breach is likely to result in a high risk to the rights and freedoms of natural persons.

7.2 Data Breach Concerning Personal Data Processed by DataRobot

a. In the event of a Data Breach concerning Personal Data processed by DataRobot, DataRobot shall notify Customer in accordance with the terms of Section 10 (Data Breaches) of Appendix 3 (DataRobot Information Security Exhibit).

b. The Parties shall set out in Annex III all other elements to be provided by DataRobot when assisting Customer in the compliance with Customer's obligations under the Data Protection Laws.

SECTION III - FINAL PROVISIONS

Clause 8

Non-Compliance with the Clauses and Termination

a. These Clauses will continue in force until the termination of the Agreement.

b. Without prejudice to any provisions of the Data Protection Laws, in the event that DataRobot is in breach of its obligations under these Clauses, Customer may instruct DataRobot to suspend the Processing of Personal Data until the

latter complies with these Clauses or the Agreement is terminated. DataRobot shall promptly inform Customer in case it is unable to comply with these Clauses, for whatever reason.

c. Customer shall be entitled to terminate the Agreement insofar as it concerns Processing of Personal Data in accordance with these Clauses if:

1. The Processing of Personal Data by DataRobot has been suspended by the Customer pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension or another mutually agreed time period;

2. DataRobot is in substantial or persistent breach of these Clauses or its obligations under the Data Protection Laws;

3. DataRobot fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to the Data Protection Laws.

d. DataRobot shall be entitled to terminate the Agreement insofar as it concerns Processing of Personal Data under these Clauses where, after having informed Customer that its instructions infringe applicable legal requirements in accordance with Clause 5.1 (b), Customer insists on compliance with the instructions.

e. Following termination of the Agreement, DataRobot shall delete all Personal Data processed on behalf of Customer in accordance with the terms of Section 8.7 (Data Disposal) of Appendix 3 (DataRobot Information Security Exhibit), unless applicable local law requires storage of the Personal Data, and certify to Customer that it has done so, at Customer's request. Prior to termination of the Agreement, Customer may export their Personal Data in accordance with the terms of Section 8.6 (Return of Data) of Appendix 3 (DataRobot Information Security Exhibit). Until the Personal Data is deleted or returned, DataRobot shall continue to ensure compliance with these Clauses.

ANNEX I

List of parties

Customer(s):

For Customer details and accession date refer to the named “Customer” on the signed or accepted Order or Agreement.

DataRobot(s):

For DataRobot details and accession date refer to “DataRobot” on the signed or accepted Order or Agreement.

ANNEX II

Description of the processing

Categories of data subjects whose personal data is processed

The customer has sole control over the categories of data subjects whose personal data may be imported into DataRobot's software product.

Categories of personal data processed

Subject to Section 12.6 of the Agreement, the customer may import personal data into DataRobot's software product at their sole discretion.

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Sensitive personal data is restricted from upload into DataRobot's software product pursuant to Section 12.6 of the Agreement.

Nature of the processing

DataRobot processes any personal data uploaded into DataRobot's software product in order to provide the customer with AI predictive models.

Purpose(s) for which the personal data is processed on behalf of the Customer

To provide the Solution.

Duration of the processing

For the subscription term and for up to 30 days after until deleted in accordance with Section 8.7 (Data Disposal) of Appendix 3 (DataRobot Information Security Exhibit).

For processing by Subprocessors, also specify subject matter, nature and duration of the processing

Please see https://www.datarobot.com/privacy/subprocessors/ for details on Subprocessors.

ANNEX III

Technical and organizational measures including technical and organizational measures to ensure the security of the data

A description of the information security controls implemented by DataRobot to protect personal data is set forth in Appendix 3 (DataRobot Information Security Exhibit).

Appendix 5

GDPR Controller to Processor Standard Contractual Clauses

SECTION I

Clause 1

Purpose and scope

a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

b. The Parties:

i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer'),

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

ii. Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

iii. Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

iv. Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

v. Clause 13;

vi. Clause 15.1(c), (d) and (e);

vii. Clause 16(e);

viii. Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Optional Docking Clause Removed

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

a. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

b. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of

the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

b. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

c. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

d. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data

concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

a. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

b. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

c. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

d. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

e. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

a. GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least ten days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

b. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

c. The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

d. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

e. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

a. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

b. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

c. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

b. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

c. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

   i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

   ii. refer the dispute to the competent courts within the meaning of Clause 18.

d. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

e. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

f. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

b. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

c. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

d. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

e. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

f. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

g. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

a. Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

b. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

c. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

d. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received

(in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

ii. the data importer is in substantial or persistent breach of these Clauses; or

iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non- compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer

warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third- party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

b. The Parties agree that those shall be the courts of Ireland.

c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

d. The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: The named "Customer" on the signed or accepted Order or Agreement.

Address: The address associated with Customer on the signed or accepted Order or Agreement.

Contact person's Name, position and contact details: The contact details associated with Customer on the signed or accepted Order or Agreement.

Activities relevant to the data transferred under these Clauses:
Relevant activities are specified in Annex II of Appendix 4.

Signature and date: Refer to the signed or accepted Order or Agreement.

Role (controller/processor): Controller

Data importer(s):

Name: "DataRobot" as named on the signed or accepted Order or Agreement.

Address: The address associated with DataRobot on the signed or accepted Order or Agreement.

Contact person's Name, position and contact details: The contact details associated with DataRobot on the signed or accepted Order or Agreement.

Activities relevant to the data transferred under these Clauses:
Relevant activities are specified in Annex II of Appendix 4.

Signature and date: Refer to the signed or accepted Order or Agreement.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred
Categories of data subjects are specified in Annex II of Appendix 4.

Categories of personal data transferred
Categories of personal data transferred are specified in Annex II of Appendix 4.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.
Sensitive personal data is specified in Annex II of Appendix 4.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Customer has sole control over the frequency of transfer.

Nature of the processing

Nature of the processing is specified in Annex II of Appendix 4.

Purpose(s) of the data transfer and further processing

The purpose of the transfer is specified in Annex II of Appendix 4.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The duration of the processing specified in Annex II of Appendix 4.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Details on subprocessors are as specified in Annex II of Appendix 4.

C. COMPETENT SUPERVISORY AUTHORITY MODULE

Identify the competent supervisory authority/ies in accordance with Clause 13

The competent supervisory authority will be determined in accordance with the GDPR.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

A description of the information security controls implemented by DataRobot to protect personal data is set forth in Appendix 3 (DataRobot Information Security Exhibit).

Appendix 6

UK GDPR Controller to Processor SCCs

Commission Decision C(2010)593 Standard Contractual Clauses (Processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:
Refer to the named "**Customer**" on the signed or accepted Order or Agreement (the **data exporter**)
And

Name of the data importing organisation:
Refer to "**DataRobot**" on the signed or accepted Order or Agreement (the **data importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the **Clauses**) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1
Definitions

For the purposes of the Clauses:

(a) ***'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'*** **and** ***'supervisory authority'*** shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) **'*the data exporter*'** means the controller who transfers the personal data;

(c) ***'the data importer'*** means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) ***'the subprocessor'*** means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e **'*the applicable data protection law*'** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) ***'technical and organisational security measures'*** means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2
Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3
Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of

which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4
Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5
Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6
Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8
Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9
Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10
Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11
Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12
Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation

imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Data exporter
Refer to the named "Customer" on the signed or accepted Order or Agreement.

Data importer
Refer to "DataRobot" on the signed or accepted Order or Agreement.

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):

Refer to Annex II of Appendix 4.

Categories of data
The personal data transferred concern the following categories of data (please specify):

Refer to Annex II of Appendix 4.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):

Refer to Annex II of Appendix 4.

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):

Refer to Annex II of Appendix 4.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

For a description of the technical and organisational security measures please refer to Appendix 3.