

Exhibit D

California Data Exhibit

1. This California Data Exhibit (this “Exhibit”), forms part of the DPA. Capitalized terms used and not otherwise defined herein shall have the meanings ascribed to them in the DPA or the Agreement (as applicable).
2. Definitions and Obligations.
 - a. In this Exhibit:
 - i. “Genetic Data” means any data, regardless of its format, that results from the analysis of a biological sample of a California resident, or from another source enabling equivalent information to be obtained, and concerns genetic material. Genetic material includes, but is not limited to, deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from analysis of the biological sample or other source, and any information extrapolated, derived, or inferred therefrom.
 - ii. “Health Insurance Information” means a California resident's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the California resident, or any information in a California resident's application and claims history, including any appeals records.
 - iii. “Medical Information” means any California Personal Data, in electronic or physical form, regarding a California resident’s medical history or medical treatment or diagnosis by a health care professional.
 - iv. “Sensitive California Personal Data” means any California Personal Data that constitutes either of the following: (A) California resident’s first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (I) social security number; (II) driver’s license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific California resident; (III) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an California resident’s financial account; (IV) Medical Information; (V) Health Insurance Information; (VI) Genetic Data; or (VII) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific California resident (except that unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes); or (B) a username or email address in combination with a password or security question and answer that would permit access to an online account. For the avoidance of doubt, Sensitive California Personal Data does not include publicly

available California Personal Data that is lawfully made available to the general public from federal, state, or local government records.

- v. The following terms have the meanings given in the California Privacy Laws: "business purpose", "personal information", "processing", "service provider", "contractor", "person", "share", "sharing", "shared", "sell", "selling", "sale" and "sold".
- b. This Section 2(b) shall apply only until the CPRA Effective Date. Except as otherwise required by applicable law, Company shall:
- i. process the California Personal Data for the business purpose of providing the Services or as otherwise permitted by the CCPA;
 - ii. implement and maintain commercially reasonable security procedures and practices appropriate to the nature of the Sensitive California Personal Data (if any) intended to protect such Sensitive California Personal Data from unauthorized access, destruction, use, modification, or disclosure;
 - iii. not retain, use or disclose California Personal Data for any purpose outside the scope of the business relationship of the parties and other than for the specific purpose of providing the Services, nor retain, use, or disclose the California Personal Data for a commercial purpose other than providing the Services, or as otherwise permitted by the CCPA as applicable to service providers;
 - iv. not collect or use California Personal Data except as reasonably necessary to provide the Services;
 - v. not sell California Personal Data;
 - vi. to the extent necessary, use commercially reasonable efforts to assist Customer, at Customer's expense, in Customer's fulfillment of Customer's obligation to respond to California residents' requests to exercise rights with respect to their California Personal Data under the CCPA; and
 - vii. use commercially reasonable efforts to assist Customer, at Customer's expense, to the extent necessary to support Customer's compliance with Customer's obligations under the CCPA.
- c. Company understands the restrictions provided in Sections 2(b)(iii) and 2(b)(v) and will comply with them. This Section 2(c) shall not apply from and after the CPRA Effective Date.
- d. This Section 2(d) shall apply only from and after the CPRA Effective Date. Except as otherwise required by applicable law, Company shall:
- i. not sell or share California Personal Data;
 - ii. not retain, use, or disclose California Personal Data for any purpose other than for the business purposes specified in this DPA and/or the Agreement for Customer, nor retain, use, or disclose California Personal Data for a commercial purpose other than the business purposes specified in this DPA and/or the Agreement, or as otherwise permitted by the CPRA;

- iii. not retain, use, or disclose California Personal Data outside of the direct business relationship between the parties;
- iv. not combine California Personal Data, which Company receives pursuant to the Agreement or from or on behalf of Customer, with personal information which it receives from or on behalf of another person or persons, or collects from its own interaction with the individual to whom such California Personal Data relates, except as otherwise expressly permitted by the CPRA;
- v. reasonably cooperate with Customer in responding to any requests from any individual regarding California Personal Data relating to such individual, including reasonably assisting Customer in deletion, correction, or limitation of the use of such California Personal Data where required under the CPRA, and including instructing Company's service providers and/or contractors (if any) to so reasonably cooperate in such response;
- vi. reasonably assist Customer through appropriate technical and organizational measures in Customer's complying with the requirements of subdivisions (d) to (f), inclusive, of Section 1798.100 of the CPRA, taking into account the nature of the California Personal Data processing by Company;
- vii. implement and maintain commercially reasonable security procedures and practices appropriate to the nature of the California Personal Data intended to protect such California Personal Data from unauthorized access, destruction, use, modification, or disclosure;
- viii. comply with all applicable obligations under the CPRA and provide the same level of privacy protection with respect to California Personal Data as required by the CPRA; and
- ix. notify Customer if Company determines it can no longer meet its obligations under the CPRA.

To the extent Company is a contractor, Company certifies that Company understands the restrictions provided in Sections 2(d)(i), 2(d)(ii), 2(d)(iii), and 2(d)(iv) and will comply with them.

- e. This Section 2(e) shall apply only from and after the CPRA Effective Date. Company acknowledges and agrees that the California Personal Data has been disclosed to it for the limited and specified purposes set forth in the Agreement and Company further acknowledges and agrees Customer shall have the right: (i) to take reasonable and appropriate steps to ensure that Company uses California Personal Data in a manner consistent with Customer's obligations under the CPRA; and (ii) upon notice from Customer to Company, to take reasonable and appropriate steps to stop and remediate unauthorized use of California Personal Data.
- f. This Section 2(f) shall apply only from and after the CPRA Effective Date. To the extent required by the CPRA and to the extent Company is a contractor, Company shall permit, subject to agreement of the parties, Customer to monitor Company's compliance with this Exhibit through measures, including, but not limited to, ongoing manual reviews and automated scans, and regular assessments, audits, or other technical and operational testing once every twelve (12) months (each, an "Audit"), upon reasonable prior notice from Customer, provided that no third-party auditor (each an "Auditor") shall be a competitor of Company, nor shall any Auditor be

compensated on a contingency basis, and provided further that in no event shall Customer have access to the information of any other client of Company and the disclosures made pursuant to this Section 2(f) ("Audit Information") shall be held in confidence as Company's confidential information and subject to any confidentiality obligations in the Agreement, and provided further that no Audit shall be undertaken unless or until Customer has requested, and Company has provided, information about Company's data protection practices and Customer reasonably determines that an Audit remains necessary to demonstrate material compliance with the obligations laid down in this Exhibit. Without limiting the generality of any provision in the Agreement, Customer shall employ the same degree of care to safeguard Audit Information that it uses to protect its own confidential and proprietary information and in any event, not less than a reasonable degree of care under the circumstances, and Customer shall be liable for any improper disclosure or use of Audit Information by Customer or its agents.

- g. This Section 2(g) shall apply only until the CPRA Effective Date. Nothing in this DPA shall prevent Company from engaging its own service providers in the processing of California Personal Data, provided that Company shall enter into contractual arrangements with such service providers requiring a substantially similar level of data protection compliance and information security as that provided in this Section 2 with respect to California Personal Data.
- h. This Section 2(h) shall apply only from and after the CPRA Effective Date. If Company engages any other person to assist Company in processing California Personal Data for a business purpose on behalf of Customer, Company shall notify Customer of such engagement, and the engagement shall be pursuant to a written contract binding the other person to observe substantially similar requirements to those set forth in this Exhibit. Company hereby notifies Customer that Company may engage the persons listed in Annex III of Exhibit A to this DPA to assist Company in processing California Personal Data for a business purpose on behalf of Customer.