Exhibit 2 (c) – Specific Jurisdiction Provisions for Data Transfer Agreement

1. Australia

a. The following provisions apply to all transfers of Personal Data where:
   i. The Personal Data is received or accessed by the Vendor from an Elanco Affiliate that is located in Australia; or
   ii. Elanco notifies the Vendor that the Personal Data is subject to these Processing requirements.

b. For the purposes of these Australia Specific Jurisdiction Provisions, "Sensitive Information" also includes Personal Information about an Individual's membership of a professional or trade association in addition to the types of information identified in the DTA.

c. The following requirement apply in addition to any Processing requirements in the Agreement.
   i. Anonymity/Pseudonymity. Where the Vendor is informed that the Data Subject wishes to be dealt with on an anonymous or pseudonymous basis, the Vendor will handle the request in accordance with (DTA)
   ii. Note of use of disclosure for enforcement purposes. If the Vendor uses or discloses Personal Data for one or more enforcement activities conducted by, or on behalf of, an enforcement body, the Vendor must keep a written record of the use and disclosure and promptly provide a copy of the record to Elanco, unless such notice is prohibited by law applicable to Vendor.
   iii. Collection of Personal Data. Where Elanco's instruction to the Vendor requires the Vendor to collect Personal Data on behalf of Elanco the Vendor must:
      1. Seek instructions from Elanco regarding:
         a. Any information that must be provided to the Data Subject in connection with the collection of the Data Subject's Personal Data; and
         b. Any opt-in consents required for direct marketing purposes; and
      2. Not collect any Sensitive Information without the consent of the Data Subject.
   iv. Australian government related identifiers. Where the Personal Data includes Australian government related identifiers the Vendor must not:
      1. Adopt the Australian government related identifier for an Individual as its own identifier on the Individual unless expressly directed to do so by Elanco; or
      2. Use or disclose the Australian government related identifier except where it is reasonably necessary to verify the identity of the Individual, or where directed to do so by Elanco.

2. Colombia

a. These provisions apply to all transfers of Personal Data controlled by Elanco in Colombia.

b. Vendor will only Process Personal Data in accordance with the Information Processing Policy communicated to Data Subjects, as instructed by Elanco.

c. Vendor will update its records with any updated Personal Data provided by Elanco within five (5) business days from its receipt unless the parties have agreed in writing to a shorter period.

3. Japan

a. The following provisions apply to all transfers of Personal Data controlled by Elanco in Japan.

b. Vendor will take the following measures to protect Personal Data relating to employment management as provided by Ministry of Health, Labor and Welfare ("MHLW") Employment Management Guidelines. Vendor will:

i. Ensure that its employees will not divulge or misappropriate the Personal Data learned through their employment;

ii. Obtain prior written consent for Elanco if Vendor discloses or transfers Personal Data to any third party (including an Affiliate) that is not party to this Agreement.

iii. Cease Processing and return or appropriately and definitively destroy Personal Data in its possession when it has achieved the purpose for which it was collected; and

iv. Not copy or reproduce Personal Data except for backup purposes.

4. South Korea

a. The following provisions apply to all transfers of Personal Data provided only for purposes specified in the relevant contract or policies or as clearly agreed upon in advance between the relevant parties.

b. Vendor will limit access to Personal Data to those Vendor Personnel who reasonably require such access for the purpose of the Processing; and Vendor will establish and maintain safeguards as per Section 5 of the SPS, including: (i) internal procedures for secure handling of Personal Data; (ii) technical safeguards such as firewalls, anti-virus and anti-malware software; (iii) physical access restrictions, such as locks; (iv) measures to prevent alteration or falsification of access logs or records of Processing; (v) measures to security store and transmit Personal Data, such as encryption of Personal Data where required by the Personal Information Protection Act (PIPA), the Enforcement Regulations of PIPA, the Act on Promotion of Information and Communications Network Utilization and Protection of Information (PICNU), the Utilization and Protection of Credit information Act (UPCIA) or other Korean Law. For purposes of these Specific Jurisdiction Provisions relating to Korea, Korean Law will be understood to require encryption of resident registration numbers, driver's license numbers, and passport numbers (collectively, "Peculiar Identification Data"), and passwords and bio data (e.g., biometric data), when: (a) any of such information is transmitted through an information or communications network; (b) any of such information is stored on portable storage media or peripherals; (c) any password or bio data is stored in any form; and (d) any Peculiar Identification Data is stored by Vendor on any external computer network, or in a demilitarized zone, or on any personal computer; provided that Peculiar Identification data stored on Vendor's internal network will also be encrypted If Vendor's systems fail to meet a risk assessment with criteria specified by Elanco.

c. In relation to Section 2.5 of the DTA, where Vendor will disclose or transfer Personal Data Information to a third-party data processor, Vendor will information Elanco reasonable in advance of such disclosure. Upon Elcano's request, Vendor will provide the following information; (a) the Processing activities to be subcontracted; (b) the identity of the third-party data processor; and (c) any changed to (a) and (b).