



# BIOMÉRIEUX CUSTOMER COMPLAINT HANDLING

## Data Processing Terms (Global)

### 1. APPLICABILITY

These BIOMÉRIEUX CUSTOMER COMPLAINT HANDLING Data Processing Terms (Global) (“**Data Processing Terms**”) shall govern Processing activities relating to Personal Data that is processed by bioMérieux or its Sub-Processors for Customer Complaint Handling. These Data Processing Terms shall include any applicable Annex 1 setting forth information regarding Processing and Sub-Processors.

### 2. DEFINITIONS

These terms as defined shall apply to these Data Processing Terms, inclusive of any applicable annexes.

- 2.1 “**Applicable Law**” shall have the meaning set forth in the General Terms.
- 2.2 “**Applicable Terms**” shall mean the General Terms and any applicable Additional Terms, or any other applicable underlying agreement.
- 2.3 “**Affiliate**” shall have the meaning set forth in the General Terms.
- 2.4 “**Additional Terms**” shall have the meaning set forth in the General Terms.
- 2.5 “**bioMérieux**” shall have the meaning set forth in the General Terms.
- 2.6 “**bioMérieux System**” shall have the meaning set forth in the General Terms.
- 2.7 “**Controller**” shall have the meaning ascribed to “controller” under GDPR, or to the equivalent or corresponding term as defined in any other applicable Data Privacy Laws.
- 2.8 “**Customer**” shall have the meaning set forth in the General Terms.
- 2.9 “**Customer Complaint Handling**” shall mean the activities carried out to support Customers’ complaints and investigations in the context of its use of bioMérieux System.
- 2.10 “**Data Privacy Laws**” shall have the meaning set forth in the General Terms.
- 2.11 “**Data Subject**” shall mean an identified or identifiable natural person to whom the Personal Data relates. It shall have the same meaning ascribed to “data subject” under GDPR, or to the equivalent or corresponding term as defined under Data Privacy Laws applicable in the applicable jurisdiction.
- 2.12 “**Data Subject Access Request**” shall mean an inquiry made by a Data Subject in exercise of rights granted to the Data Subject under applicable Data Privacy Laws. These rights include, but are not limited to, access to personal data, rectification of inaccurate data, erasure (right to be forgotten), restriction of processing, data portability, and the right to object to certain types of data processing.
- 2.13 “**EU**” shall mean the European Union, and any of its member states as may be constituted from time to time.
- 2.14 “**GDPR**” shall mean 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, and repealing Directive 95/46/EC (Data Protection Directive).
- 2.15 “**General Terms**” shall mean the bioMérieux General Maintenance and Repair Conditions.
- 2.16 “**Patient**” shall mean an individual who is seeking, is receiving, or has received medical care or services from Customer.
- 2.17 “**Personal Data**” shall have the meaning set forth in the General Terms.
- 2.18 “**Personal Data Breach**” shall have the meaning ascribed to “personal data breach” under GDPR, or to the equivalent or corresponding term as defined under Data Privacy Laws in the applicable jurisdiction.
- 2.19 “**Pseudonymized Data**” shall have the meaning set forth in the Annex 1 (if applicable).
- 2.20 “**Processing**” shall have the meaning ascribed to “processing” under GDPR, or to the equivalent or corresponding term as defined under Data Privacy Laws applicable in the applicable jurisdiction. “**Processes**” and “**Process**” shall be construed accordingly.
- 2.21 “**Processor**” shall have the meaning ascribed to “processor” under GDPR, or to the equivalent or corresponding term as defined under Data Privacy Laws applicable in the applicable jurisdiction.
- 2.22 “**Sub-Processor**” shall mean a natural or legal person, public authority, agency or other body appointed by or on behalf of Processor to process Personal Data on behalf of the Controller or shall have the meaning ascribed to the equivalent or corresponding term as defined in any other applicable Data Privacy Laws.

### 3. PROCESSING OF PERSONAL DATA

3.1 **Customer Responsibilities.** As Controller, Customer shall direct processing of Personal Data in accordance with Data Privacy Laws and these Data Processing Terms, including providing all requisite notices or obtaining all requisite consents, and obtaining all requisite rights to use and disclose the Personal Data including establishing applicable legal bases, where applicable.

#### 3.2 **Customer Instructions.**

- (a) bioMérieux and its Sub-Processors shall process Personal Data in accordance with Customer’s documented instructions solely as necessary for the purposes of bioMérieux fulfilling its obligations under the Applicable Terms. Customer shall be responsible for communicating instructions to bioMérieux and agrees that these Data Processing Terms, the Applicable Terms, and any other instructions agreed to in writing between Customer and bioMérieux shall comprise Customer’s complete instructions to bioMérieux regarding the Processing of Personal Data. Any additional or alternate instructions must be agreed to between Customer and bioMérieux in writing.
- (b) Customer shall, at all times, remain responsible for making sure that all instructions comply with Data Privacy Laws and these Data Processing Terms. bioMérieux and its Sub-Processors shall not bear responsibility for determining whether Customer’s instructions are compliant with Data Privacy Laws and these Data Processing Terms. However, if bioMérieux and/or its Sub-Processors are of the opinion that a Customer instruction violates applicable Data Privacy Laws or these Data Processing Terms, bioMérieux shall notify Customer as soon as reasonably practicable and shall not be required to comply with any non-compliant instruction pending further discussion with Customer.



## BIOMÉRIEUX CUSTOMER COMPLAINT HANDLING

### Data Processing Terms (Global)

**3.3 Details of Processing.** Details of the subject matter of the Processing, its duration, nature and purpose, and the type of Personal Data and Data Subjects are specified in the Annex 1.

**3.4 Compliance with Data Privacy Laws.** Customer and bioMérieux shall comply with their respective obligations under Data Privacy Laws. Customer shall retain sole responsibility for complying with Data Privacy Laws, as applicable to a Controller, regarding the lawfulness of the Processing of Personal Data prior to disclosing, transferring, or otherwise making available, any Personal Data to bioMérieux or its Sub-Processors. To the extent that the Data Privacy Laws, including any subsequent changes to Data Privacy Laws as may be implemented from time to time, impose additional mandatory obligations on Customer and/or bioMérieux in their respective roles as outlined in these Data Processing Terms, Customer and bioMérieux agree to comply with their respective additional mandatory obligations.

## 4. SUB-PROCESSORS

### 4.1 Use of Sub-Processors.

- (a) Customer consents and gives general authorization to bioMérieux allowing for Personal Data to be processed to or by bioMérieux Affiliates and Sub-Processors as mentioned in Section 4.2 below, subject to the following conditions:
  - (i) access to Personal Data shall only be granted by Customer to bioMérieux, its Affiliates and its Sub-Processors for the strict purposes of these Data Processing Terms; and
  - (ii) the Personal Data shall be strictly limited to what is necessary for bioMérieux, its Affiliates and its Sub-Processors to perform under these Data Processing Terms.
- (b) bioMérieux may use Sub-Processors with the Customer's general written authorization. Customer authorizes bioMérieux to appoint and use Sub-Processors to Process Personal Data in connection with Applicable Terms provided that bioMérieux puts in place a contract in writing with each Sub-Processor that imposes obligations that are: (a) relevant to the services to be provided by the Sub-Processors and (b) materially similar to the rights and/or obligations imposed on bioMérieux under these Data Processing Terms.
- (c) bioMérieux shall ensure that the Sub-Processor shall be subject to confidentiality obligations that limit the process of Personal Data to its employees or its contractors and its own Sub-Processors with a need to know and who are subject to obligations of confidentiality no less onerous than those set forth in these Data Processing Terms or the General Terms.
- (d) Where a Sub-Processor fails to fulfil its data protection obligations as specified above, bioMérieux shall be liable to the Customer for the performance of the Sub-Processor's obligations, subject to any applicable limitation of liability provision in the Applicable Terms.
- (e) bioMérieux shall oblige any Sub-Processor to notify without undue delay bioMérieux' Global Data Protection Officer (i) when a Personal Data Breach occurs, or (ii) if it is asked by any person or entity to take any action which may violate Data Privacy Laws or these Data Processing Terms.

### 4.2 List of Sub-Processors.

- (a) Customer acknowledges and agrees that the method by which bioMérieux will inform Customer of its Sub-Processors, and updates thereto, will be via the list of Sub-Processors identified in the applicable Annex 1 to these Data Processing Terms.
- (b) Where permitted under Data Privacy Laws, Customer may reasonably object to any changes concerning addition or replacement of the Sub-Processors. Customer shall object in writing by sending the objection by email to bioMérieux's Data Protection Officer at [privacyofficer@biomerieux.com](mailto:privacyofficer@biomerieux.com). Such objection must be made within 10 days from the date on which the notification is sent. In the event of an objection, bioMérieux shall provide information aimed at resolving these objections. If the Customer maintains its objection, the Parties agree to meet and negotiate in good faith regarding the continuation of their contractual relationship.

## 5. CROSS-BORDER DATA TRANSFERS

**5.1 Transfers of Personal Data from European Economic Area (EEA) Countries to Third Countries.** If bioMérieux's Affiliates and/or Sub-Processors are located outside the EU (and/or Iceland, Liechtenstein and Norway, which are part of the EEA), the processing of Personal Data shall only be granted to such Affiliates and/or Sub-Processors for which the recipient country shall:

- (a) offer an adequate level of protection within the meaning of Article 45 of GDPR, or
- (b) prior to any such export towards third countries that do not offer an adequate level of data protection (including for onward transfers):
  - (i) the exporter of the Personal Data shall, where required, conduct a Transfer Impact Assessment ("**TIA**") to ensure that the Personal Data (and Data Subjects) remain protected to the required standard and to share the TIA with the requesting party; and
  - (ii) the importer and the exporter of the Personal Data (according to the meaning given to these expressions in European law) shall execute the standard contractual clauses of the European Commission ("**SCC**").
- (c) If bioMérieux is the exporter of the Personal Data, bioMérieux shall conduct, prior to any transfer of said data, a TIA with the importer (Affiliates or any third-party Sub-Processors).
- (d) bioMérieux shall comply with all Processor obligations set forth in the Module 1 Controller to Processor and/or Module 3 Processor to Processor SCCs used as the basis of transfer under GDPR of Personal Data outside the EU/EEA.
- (e) In the event that any of the transfer mechanisms set forth above are declared invalid by a Court or other body of competent jurisdiction, Customer and bioMérieux agree that they shall undertake all necessary steps in order to put in place an alternative transfer mechanism acceptable under Data Privacy Laws and regulations.

**5.2 Transfers of Personal Data from Non-EEA Countries to Other Countries.** For jurisdictions other than those located within the EU/EEA, bioMérieux shall not transfer Personal Data outside of the jurisdiction where the Personal Data is obtained from unless such transfer is permitted under applicable Data Privacy Laws or as instructed by Customer.

## 6. PERSONAL DATA BREACH

As required by Data Privacy Laws, bioMérieux shall notify Customer without undue delay after becoming aware of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed. Taking into account the nature of processing and the information available, bioMérieux shall provide Customer with such cooperation and assistance as may be required to mitigate against the effects of, and comply with any reporting obligations which may apply in respect of, any such breach.



## BIOMÉRIEUX CUSTOMER COMPLAINT HANDLING

### Data Processing Terms (Global)

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

#### 7. DELETION OF PERSONAL DATA

bioMérieux shall delete all Personal Data of the Customer as Controller upon termination or expiry of the Applicable Terms as described in the Annex 1 and shall do so unless Applicable Law requires otherwise. To the extent that any Applicable Law or any agreement between bioMérieux and Customer requires retention of such Personal Data, the provisions of these Data Processing Terms shall continue to apply to the retained Personal Data.

#### 8. COOPERATION

**8.1 Data Subject Access Requests.** Where required under Data Privacy Laws, bioMérieux shall assist Customer in providing Data Subjects access to their Personal Data, and allowing Data Subjects to make Data Subject Access Requests to the extent the Data Subject may do so under Data Privacy Laws. bioMérieux shall promptly notify Customer of any Data Subject Access Request that it receives. The Parties agree that such requests will be addressed in collaboration between the relevant teams of both bioMérieux and Customer. Unless otherwise agreed to in writing, Customer shall be solely responsible for responding to such Data Subject Access Requests. bioMérieux reserves the right to charge Customer for such assistance if the cost of assisting exceeds a nominal amount.

**8.2 Privacy Impact Assessments and Prior Consultation.** Where required by Data Privacy Laws and taking into account the nature of processing and the information available, bioMérieux shall provide reasonable assistance to Customer (a) to carry out a data protection impact assessment in relation to Processing of Personal Data by bioMérieux or (b) as part of any required prior consultation(s) with supervisory authorities.

#### 9. DEMONSTRATING COMPLIANCE

bioMérieux shall, upon reasonable prior written request from Customer, provide Customer such information as may be reasonably necessary to demonstrate compliance by bioMérieux and, as applicable, the pertinent Sub-Processor(s) of their obligations under Data Privacy Laws and these Data Processing Terms. bioMérieux shall allow for and assist Customer with audits, reviews or inspections conducted by a data protection authority, or similar regulator, to the extent that bioMérieux assistance is required under Data Privacy Laws and upon mutually agreeable terms as described in the General Terms. bioMérieux reserves the right to charge Customer for such assistance if the cost of assisting exceeds a nominal amount.

#### 10. INFORMATION SECURITY MEASURES

##### **10.1 Technical and Organizational Security Measures.**

- (a) bioMérieux shall assist Customer in meeting its own obligations in relation to the security of Processing taking into account the nature of processing and the information available to bioMérieux.
- (b) bioMérieux undertakes to set up, from the beginning of the operations, appropriate devices and safety procedures, so as to guarantee the availability, the integrity, the confidentiality and the traceability of Personal Data.
- (c) Taking into account industry standards, the costs of implementation, the nature, scope, context and purposes of the Processing, and any other relevant circumstances relating to Processing of Personal Data on Processor systems, bioMérieux shall implement appropriate technical and organizational security measures to ensure that the security, confidentiality, integrity, availability and traceability of the systems involved in Processing of Personal Data are commensurate with the risk to such Personal Data. Under Customer's request, bioMérieux shall provide written details of such measures.
- (d) bioMérieux shall implement at a minimum the following security measures:
  - (i) **Physical Access Controls:** bioMérieux has implemented reasonable measures to prevent unauthorized persons from gaining access to Personal Data.
  - (ii) **System Access Controls:** bioMérieux has taken reasonable measures to prevent Personal Data from being used without authorization. These controls vary based on the nature of Processing undertaken and may include, among other controls, password-protected individual accounts, password policies, electronic or multi-factor authentication methods, audit trails, and traceability mechanisms.
  - (iii) **Data Access Controls:** bioMérieux has taken reasonable measures to provide that Personal Data is accessible and manageable only by properly authorized employees, database query access is controlled, and application access rights are established and enforced to ensure that employees entitled to use a Processing system only have access to Personal Data to which they have privilege of access, and that personal data cannot be read, copied, modified or removed without authorization in the course of Processing. bioMérieux has taken reasonable measures to implement an access policy under which access to system environments, Personal Data and other data is limited to authorized personnel only.
  - (iv) **Transmission Controls:** bioMérieux has taken reasonable measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during transmission. These controls include encryption of data transmission using either 128-bit Symmetric Encryption keys or the then-current but no less secure industry standard encryption.
  - (v) **Input Controls:** bioMérieux has taken reasonable measures to guard against any unauthorized inclusion, modification or deletion of Personal Data from databases. bioMérieux has taken reasonable measures to ensure that the source of Personal Data is under the control of Customer at the time of Personal Data collection, and that Personal Data exported into bioMérieux databases are managed by secure and encrypted file transfer from Customer to bioMérieux.
- (e) bioMérieux shall periodically:
  - (i) test and monitor the effectiveness of the safeguards, controls, systems and procedures, and
  - (ii) identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of Personal Data, and ensure that the risks are addressed.

##### **10.2 Restricted Access.** bioMérieux shall ensure that persons authorized to access and/or process Personal Data:

- (a) have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- (b) process Personal Data only upon documented instructions, unless required to do so pursuant to Applicable Law; and
- (c) have received appropriate training on their responsibilities, specifically pertaining to security and privacy measures.

**10.3 Data Sharing.** The Customer agrees to use the tools provided by bioMérieux to share Personal Data with bioMérieux or its Sub-processors. In case the Customer intends to use a different tool, it shall ensure that the tool complies with Applicable Law and implements appropriate technical and organizational measures to ensure a level of security appropriate to the risk.