

## **MYOKARDIA EMPLOYEE PRIVACY NOTICE: PROCESSING OF PERSONAL DATA**

MyoKardia is committed to protecting the privacy and security of your personal data. As your employer, we collect your personal data and are the "controller" under the applicable data protection laws.

This notice is to help you understand what personal data we collect about you, why we collect it and what we do with it.

### **1 Contact details**

Your personal data is collected by MyoKardia, Inc. and MyoKardia Netherlands B.V. ("we"/"us"/"our"). You can contact us via email at [privacy@myokardia.com](mailto:privacy@myokardia.com) or by telephone at +1 (650) 741 0900. If you have any questions or complaints in relation to the use of your personal data or this Employee Notice, you can contact our Data Protection Officer ("DPO") at [dpo@myokardia.com](mailto:dpo@myokardia.com).

### **2 Personal data collected**

We collect, store, and use the personal data in relation to your employment or engagement with us as listed in Schedule 1 to this Employee Privacy Notice.

If you fail to provide certain personal data when requested, we may not be able to perform all our legal and contractual obligations or carry out all activities regarding your employment or engagement such as payroll, benefits, tax and insurance and to ensure health and safety.

It is important that the personal data we hold about you is accurate and up to date. Please keep us informed if your personal data changes during your working relationship with us.

### **3 Sources of personal data**

Your personal data is either (a) provided by you; (b) obtained from third parties (e.g. in relation to background checks and trainings); or (c) created by us in the course of job-related activities during your employment/engagement with us.

### **4 Why we use your personal data and what is the legal basis for using your personal data**

We will use personal data collected from you because: (1) it is necessary for our performance and compliance with your employment contract or other applicable engagement contract with us or in order to take steps prior to entering into that contract; (2) we need to process your personal data to comply with a regulatory obligation; (3) we or a third party have a legitimate interest to: (a) ensure effective administration and management of your employment or engagement, benefits, management of the business and business continuity; (b) ensure our assets are protected, kept confidential, and not used for inappropriate or unlawful purposes; (c) prevent, detect, or investigate unauthorised use of our systems and ensure we comply with law and our policies; (d) check if you are legally entitled to work in the Netherlands, manage performance and promotion processes; (e)

manage training and development requirements; (f) deal with disputes and accidents and take legal or other professional advice; and (g) ensure network and information security.

Please find below an overview of each of the purposes and the legal basis relied upon.

<b>Purpose</b>	<b>Legal basis</b>
Management of employees, both at a local level and group level	Legitimate interest, namely to ensure effective administration and management of your employment/engagement, benefits, management of the business and business continuity
Identification of employees on IT tools available to employees	Legitimate interest, namely IT and network security
Management of professional e-mail accounts	Legitimate interest, namely IT and network security
Protection of MyoKardia's information systems	Legitimate interest, namely IT and network security
Monitoring the use of e-mail and internet	Legitimate interest, namely IT and network security
Management of expense accounts	Legitimate interest, to manage your expense account
Management of mobile equipment	Legitimate interest, namely to manage the mobile equipment available
Management of whistleblowing channel	Legitimate interest, namely to investigate possible fraud or other malpractices
Training and career management	Legitimate interests, namely to manage your trainings and career development
Use of collaborative digital platforms	Legitimate interest, namely providing you and the rest of the company with digital platforms
Measuring employee engagement	Legitimate interest, namely to measure the engagement of our employees
Creating reports in order to implement relevant change management actions, including training needs and functional upgrade	Legitimate interest, namely for the process of our change management
Meeting fiscal and other European statutory requirements	Necessary to comply with a legal obligation

<b>Purpose</b>	<b>Legal basis</b>
Meeting fiscal and other US statutory requirements	Legitimate interest, namely to comply with US laws
Keeping and maintaining adequate administration of employees	Legitimate interest, namely to ensure effective administration and management of our employees
Payroll management	Necessary for our performance and compliance with your employment contract
Monitoring of compliance with the corporate policies and code of ethics	Legitimate interests, namely to prevent fraud and prevent, detect, or investigate other malpractices (based on corporate policies and code of ethics)

## **5 Personal data that we share**

We will share your personal data with the following third parties for the purposes of effective administration and management of your employment/engagement, benefits, management of the business and business continuity: (1) recruitment and employment agencies; (2) payroll providers (3) employee benefits vendors; (4) expense reimbursement vendors; (5) travel vendors; (6) IT administrators; (7) future and prospective employers; (8) regulators and competent authorities.

We will also share your personal data within our group for the purposes of consulting, administration, accounting and reporting purposes.

## **6 Retention of your personal data**

We will retain your personal data for the duration of your employment/engagement and for a maximum period of two years after your employment/engagement has ended. Besides that, we will retain your personal data for the length of any applicable limitation period for claims that might be brought against us later. The following types of personal data require to be retained for a certain period by law. We retain payroll administration that is of fiscal importance for a period of seven years after your employment/engagement has ended. Regarding income tax declaration and a copy of proof of identity, this personal data will be retained for a period of five years after your employment/engagement has ended.

In some circumstances, we may anonymize your personal data so that it can no longer be associated with you, in which case we may use such personal data without further notice to you.

## **7 Where your personal data will be held**

Your personal data will be stored on servers in the United States. In accordance with Article 46 GDPR, we have concluded the Standard Contractual Clauses for the transfer of personal data from the Netherlands (MyoKardia Netherlands B.V.) to the United States (MyoKardia Inc.).

## 8 Your rights

In accordance with the applicable laws in the European Union, you have the right of access, the right to rectification, the right to erasure, the right to restriction of processing, the right to data portability and the right to object. Please note that most of these rights are not absolute and subject to exemptions in the law, may only apply to certain types of personal data or processing. Below we set out your rights in more detail and give personal data on how you can exercise your rights. We will respond to your request within one month, but have the right to extend this period to two months. If we extend the response period, we will let you know within one month from your request.

- **Access:** you are entitled to ask us if we are processing your personal data and, if we are, you can request access to your personal data (commonly known as a "**data subject access request**"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it. If your request is clearly unfounded or excessive we reserve the right to charge a reasonable fee or refuse to comply in such circumstances.
- **Correction:** you are entitled to request that any incomplete or inaccurate personal data we hold about you is corrected.
- **Erasure:** you are entitled to ask us to delete or remove personal data in certain circumstances. There are certain exceptions where we may refuse a request for erasure, for example, where the personal data is required for compliance with law or in connection with claims.
- **Restriction:** you are entitled to ask us to suspend the processing of certain of your personal data about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Transfer:** you may request the transfer of certain of your personal data to another party. You have the right to ask that we provide your personal data in an easily readable format to another company.
- **Objection:** where we are processing your personal data based on a legitimate interest (or those of a third party), you may object to processing on this ground. However, we may be entitled to continue processing your personal data based on our legitimate interests.

In the limited circumstances where you may have provided your consent to the collection and processing of your personal data for a specific purpose, you have the right to withdraw your consent for that specific processing at any time without affecting the lawfulness of processing based on consent before its withdrawal.

If you want to exercise any of these rights, or to withdraw your consent, please contact our DPO in writing at [dpo@myokardia.com](mailto:dpo@myokardia.com).

## 9 Right to lodge a complaint

You also have a right to lodge a complaint with a supervisory authority, in particular in the Member State in the European Union where you are habitually resident, where you work or where an alleged infringement of Data Protection law has taken place. In the Netherlands

you can make a complaint to the *Autoriteit Persoonsgegevens* (tel. +31 70 888 8500 or at <https://autoriteitpersoonsgegevens.nl/en>).

## 10 Questions or complaints

If you would like to receive additional information specified in this Employee Privacy Notice or have any questions how we handle your personal data or would like to make any complaints, please contact our DPO at [dpo@myokardia.com](mailto:dpo@myokardia.com).

## 11 Changes to this notice

This Notice will be changed from time to time.

If we change anything important about this Notice (the personal data we collect, how we use it or why), we will notify you.

---

I have read and fully understood the **MYOKARDIA EMPLOYEE PRIVACY NOTICE**.

Name:

(Signature)

Date:

## Schedule 1

### Personal data relating to you

- 1 *Personal identifiers*, such as title, name, date of birth, age, home address, personal email address, telephone number, passport number, citizen service number (*BSM*) and where applicable, driver's licence and ID card.
- 2 *Resume/CVs*, which will include personal data on your education and training details such as qualifications, academic records, schools, training record, professional expertise.
- 3 *Personnel records*, which includes offer letters, recommendations, notice acknowledgements, employment agreements, promotion records, termination and resignation letters, exit interview notes performance evaluations and reviews, leave requests and absence records and training records.
- 4 *Personal data provided as part of the recruitment process*
- 5 *Employment details*, such as employment status, job title(s) and description, whether full time or part time, work location, hire/start date, termination date, individual photo, and organisational details such as name of company, work phone number and email.
- 6 *Financial personal data*, such as salary and compensation history, benefits, documentation summarising enrolment and participation on benefit programs, general employee communications related to benefits), travel expenses, pay cheque personal data, bank account personal data and pensions personal data.
- 7 *Records generated by and in relation to investigations* of misconduct allegations or for the general purpose of collecting facts or other personal data.

### Personal data relating to your use of our information and communications systems

- 8 Records of your use of our IT systems including email, internet systems, computers, laptops (including via remote access) telephone systems and mobile devices.

### Special categories of personal data

We may also collect, store and use the following "**special category**" of personal data:

- 9 *Data regarding criminal convictions* (criminal background checks, as part of the employee screening process for an HR, Legal or Vice President position).
- 10 *Personal data relating to criminal offences* to the extent collected in relation to the whistleblower hotline.