

## Privacy Policy

Last updated: September 2023

STATEMENT OF CONSENT TO THE PRIVACY POLICY FOR THE MyIUS app.

By consenting to the processing of your health-related data, I hereby grant my consent to the processing of my data when using the MyIUS app in accordance with the applicable Privacy Policy and Terms and Conditions for Use.

I can withdraw my consent for future data processing at any time. To exercise my right to withdraw consent, I must simply delete the app from my smartphone.

### PRIVACY POLICY FOR USING THE “MyIUS” APP

Through this Privacy Policy, we wish to inform you of the legal grounds and purposes for which we process personal data that we collect from you or that you provide to us when using the MyIUS app. We also wish to inform you of your rights under data protection law.

For specific categories of data processing, additional privacy policy provisions may apply; for example, when using the MyIUS app to participate in a study.

The MyIUS app is classified as a medical device within the sense of Regulation (EU) 2017/745 (“Medical Device Regulation”).

For more information, see the Terms and Conditions for Use.

MyIUS will process your personal data in strict confidence and only for the specified purpose. Your health-related data is processed using an algorithm hosted on the servers of Amazon AWS.

#### **1. Who is the data controller and who can I contact?**

The data controller, as defined by the General Data Protection Regulation (GDPR) is:

BAYOOCARE GmbH  
Europaplatz 5  
64293 Darmstadt, Germany

You can contact our company data protection officer by writing to the address above or by e-mail at: [dataprivacy@bayoocare.com](mailto:dataprivacy@bayoocare.com)

## 2. What is personal data?

Personal data is defined as any information that refers to an identified or identifiable natural person.

When using the MyIUS app, we do not require your name or other contact information. Your data is stored on your smartphone without any reference to your name (pseudonymously).

## 3. Which data does MyIUS collect?

### 3.1. data concerning health

MyIUS is a digital support tool for women using the intrauterine systems Kyleena, Jaydess or Mirena. It collects the following health-related data:

- Input parameters:
  - Weight and height
  - Past contraceptive methods
  - Pregnancies and births
- Daily bleeding pattern after insertion of the IUS
- Optional: data related to physical and mental discomfort (e.g. mood)

### 3.2. Usage data that we collect about the use of our app

#### 3.2.1. Microsoft App Center

Microsoft App Center collects data on the use of the app, specifically with regard to system crashes and errors. It uses information about your device (including the UUID), the installed app version and other information that can help resolve errors, especially with regard to the user's software and hardware. <https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/>

#### 3.2.2. Google Firebase

Google Firebase, a tool for reporting and analysing the use of the app. It uses information about the device (including the UUID), the app version installed, and other information that can help troubleshoot, especially related to the user's software and hardware. If you agree, information about your usage behaviour is recorded and stored. <https://firebase.google.com/support/privacy>

#### 3.2.3. Amazon Web Services (AWS).

AWS provides information about supported operating system and app versions in order to warn the user about non-validated version combinations as well as to be able to completely block the use of the app in case of misbehavior of the app under certain version combinations. To retrieve this information, a request is sent to an AWS server, which obtains knowledge of the IP address of the requesting device. [https://aws.amazon.com/compliance/eu-us-privacy-shield-faq/?nc1=h\\_ls](https://aws.amazon.com/compliance/eu-us-privacy-shield-faq/?nc1=h_ls)

#### **4. Where do we store your personal data?**

When using this app, data may be transferred to countries outside of the European Economic Area ("EEA") as part of the use of the Google Firebase service. On 10<sup>th</sup> of July 2023, the European Commission adopted the adequacy decision for the EU-US Data Privacy Framework ([https://ec.europa.eu/commission/presscorner/detail/en/ip\\_23\\_3721](https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721)) However, this does not imply a general adequate level of data protection for transfers to organisations in the US. Organisations to which transfers are made must be certified under the Data Privacy Framework. Otherwise, further transfer instruments or additional measures will be required. A list of certified entities is published on the U.S. Department of Commerce website (<https://www.dataprivacyframework.gov/s/participant-search>). Google is listed as such a certified organization (<https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt000000001L5AAI&status=Active>).

Other data processing takes place exclusively inside the EU and is performed by contracted service providers who act on our orders.

Your health-related data is stored on your smartphone when you use the app properly and for its intended purpose. To determine a prediction, the health-related data is sent to a server of Amazon AWS where it is processed but not stored.

If you change to a new smartphone or use the data export function, your health-related data will be sent temporarily (for up to 24 hours) as an encrypted file to a server of Amazon AWS to make your input available the first time you use your new smartphone. After the data is successfully imported to your new smartphone, the temporary data export is deleted.

#### **5. Why do we process your data (purpose of processing) and on what legal grounds?**

We process personal data in compliance with the provisions of the European General Data Protection Regulation (GDPR) and the German Federal Data Protection Act (BDSG):

##### **5.1. For the purpose of fulfilling contractual obligations (art. 6.1.b of the GDPR).**

MyIUS processes contractually relevant data to render and allocate the contractually agreed services to you and to provide the data to the correct recipients.

Your data is used in pseudonymous form for scientific and statistical purposes and to continually improve the app and the algorithm. It is not possible/no longer possible to identify the data subject based on the data used.

##### **5.2. To process personal health-related data based on your consent (art. 6. 1.a of the GDPR; art. 9. 2.a of the GDPR)**

the first time you start the MyIUS app, you grant consent for the processing of your health-related data by placing a checkmark in the appropriate check box. Based on your consent, we process your health-related data to make a prediction of your personal bleeding pattern.

5.3. To exert or defend legal claims (art. 9.2.f of the GDPR)

If necessary, we process your data to initiate, exert or defend legal claims.

**6. To whom is my personal data transferred?**

In general, within MyIUS, data is only accessible to persons who require such access for the fulfilment of our contractual and/or legal obligations. Service providers and vicarious agents we use may also receive data from us for these purposes. This refers in particular to our ISO 27001-certified host, Amazon AWS.

You are free to transfer the predictions generated by the app to third parties.

**7. Am I required by law or contract to provide personal data?**

You are not obligated to provide the aforementioned personal data to us.

**8. How long is my data stored?**

In general, we do not store your personal data. This data is stored exclusively on your smartphone. When using the prediction function, after 90 days, the parameters you have input along with your bleeding pattern log book will be transferred to an algorithm hosted by Amazon AWS for processing. Neither the input parameters nor the bleeding pattern log book will be stored on the Amazon AWS server.

**9. Your rights as a data subject**

Every person who is a subject of our personal data processing (data subject) has the right to be informed under art. 15 of the GDPR, the right to data correction under art. 16 of the GDPR, the right to data deletion under art. 17 of the GDPR, the right to limitation of processing under art. 18 of the GDPR, and the right to withdraw consent under art. 21 of the GDPR as well as the right to data portability under art. 20 of the GDPR. The right to information and the right to data deletion are subject to the limitations of sections 34 and 35 of the BDSG. You also have the right to file a complaint with a data protection oversight authority in accordance with art. 77 of the GDPR and section 19 of the BDSG.

MyIUS is not capable of identifying users. MyIUS lacks sufficient identifying characteristics to allocate health-related data to any specific user. In such cases, articles 15 through 20 do not apply.

**10. Information about your right to withdraw consent under art. 21 of the GDPR**

10.1. Incident-specific right to withdraw consent

You have the right to withdraw consent to the processing of your personal data collected on the grounds of art. 6.1.f of the GDPR (data processing on the basis of legitimate interests) at any time, and for reasons resulting from your specific situation; this also applies, if present, to any profiling based on this provision (as defined by art. 4.4 of the GDPR). See also section 3.4 specifically.

If you withdraw consent, your personal data will no longer be processed unless we can demonstrate compulsory, legally protected reasons for processing it which outweigh your interests, rights and freedoms, or the processing is required for the initiation, exertion of defense of legal claims.

If you withdraw consent for processing your data for the purpose of direct marketing, we will no longer use your personal data for this purpose.

#### 10.2. Withdrawal of consent

You can at any time withdraw the consent you have granted us.

This also applies to the withdrawal of the declarations of consent that have been issued prior to the enactment of the EU General Data Protection Regulation (i.e. before 25 May, 2018). Your withdrawal of consent has no further implications for the legality of the processing that took place at your consent prior to your withdrawal of consent.

#### 10.3. Exercising your right to withdraw/ revoke granted consent

You can withdraw consent by sending an email in any form to [dataprivacy\(at\)bayoocare.com](mailto:dataprivacy(at)bayoocare.com).

For any matters related to your data protection rights, directly contact the data protection officer.

### **11. Subject to change**

MyIUS is entitled to change this Privacy Policy at any time; specifically it can modify them to adjust to changes in legislation or jurisprudence. The latest version of this Privacy Policy is always available in the app. Changes to the Privacy Policy take effect immediately on the day they are published.