

## Privacy Policy for Customers

Nox Medical ehf (hereinafter “we”, “us” or “Nox Medical”) is committed to the protection of your personal data. Your personal data will be processed exclusively in accordance with the applicable data protection legislation, in particular the provisions of the European Data Protection Regulation (hereinafter: "GDPR"). In the light of this legislation, we would like to provide you with some information on the processing and protection of your personal data, as required by the GDPR. The term “**personal data**” covers any piece of information that refers to an identified or identifiable natural person (“**data subject**”). Furthermore, "personal data" or "processing" correspond to the definitions according to Article 4 GDPR. If you would like to take a look at the GDPR yourself, you can find it [here](#).

If you have any questions on the processing of your personal data or wish to exercise your rights as a data subject, please contact us using the contact details below.

### 1 Information about the Controller of the data processing

The joint controllers of the processing of your data within the meaning of Article 4 No. 7 GDPR is:

Nox Medical ehf  
Katrínartún 2  
105 Reykjavík  
Iceland

Tel: +(354) 570 7170  
E-Mail: [info@noxmedical.com](mailto:info@noxmedical.com)

Nox Health Group Inc.  
5000 Research Parkway, Suite 500  
Suwanee, GA 30024  
USA

Tel: 855-617-6691  
Fax: 678 669 2274  
E-Mail: [privacy@noxhealth.com](mailto:privacy@noxhealth.com)

If you have any questions on the processing of your data or wish to exercise your rights as a data subject (see section “Your rights as a data subject”), please contact us using the contact details above.

You can also contact our data protection officer directly at [dataprotection.nox@v-formation.gmbh](mailto:dataprotection.nox@v-formation.gmbh) or our postal address with the addition “Data protection officer / DPO”.

## 2 Processing of customer data

Within the following, we would like to give you an overview of the data processing that typically takes place within the scope of your customer relationship with Nox Medical.

Furthermore, there may always be situations, in which data processing might take place that is not mentioned here. In these cases, we will provide you with separate data protection information (e.g., privacy policy on our website) referring to the respective situation, as far as this is required by law.

### 2.1 Customer relationship system (CRM system)

Within your customer relationship with Nox, we store the personal data provided by you during your customer contact with us in our CRM system (hereinafter "HubSpot"). Furthermore, your data may be stored in HubSpot within the context of your registration for our newsletter or the registration to our webinars. For more information on the processing of your data in the context of our newsletter mailing or participation in our webinars, please refer to the dedicated data protection information, which we will provide you separately. For information on data processing in the context of participation in webinars, see under "Video conferencing / webinars".

#### 2.1.1 What categories of personal data do we process?

Within HubSpot we process the following data from you:

- Master data (first and last name, country/region, postal code, profession, organization)
- Contact data (email address, phone number)
- Product preferences (interests, registrations for webinars/newsletters, individual customer requests/notes)
- ...

#### 2.1.2 What are the purposes and legal basis for the data processing?

We process the data mentioned above for the following purposes and on the following legal basis:

- To ensure the management and maintenance of customer data on the basis of our legitimate interests in accordance with Article 6 (1) (f) GDPR.
- To provide online registration forms (e.g., for newsletters or webinars) on the basis of our legitimate interests in accordance with Article 6 (1) (f) GDPR.
- For the efficient performance of marketing measures on the basis of our legitimate interests in accordance with Article 6 (1) (f) GDPR and if applicable on the basis of your prior consent in accordance with Article 6 (1) (a) GDPR.

Our legitimate interests for the processing of your data are to ensure the management and maintenance of customer data and to conduct marketing measures as well as to ensure an efficient process design.

The data processed within HubSpot may be merged with data we have collected from you from different sources.

#### 2.1.3 Does a transfer of your data to third countries take place?

Within our customer relationship management, we use HubSpot, a service of Hubspot Inc., 25 First St., 2<sup>nd</sup> floor, Cambridge, Massachusetts 02141, USA (hereinafter "HubSpot"). We cannot exclude the possibility that your data will be transferred to HubSpot servers in the USA. Please note that currently no adequate level of data protection within the meaning of Article 45 GDPR can be guaranteed in the USA. Possible risks of processing your data in the USA are, that access to your data by governmental authorities, such as security agencies and/or intelligence services, cannot be excluded and that your data may be processed by them without your knowledge and without any enforceable legal remedies being available to you. Transfers of your data to HubSpot will be subject to the EU standard contractual clauses according to Article 46 (2) (c) GDPR available at <https://legal.hubspot.com/dpa>. For further information on data protection at HubSpot please visit <https://www.hubspot.com/data-privacy/gdpr> and/or <https://legal.hubspot.com/privacy-policy>.

## 2.2 Enterprise resource planning system (ERP system)

Within your customer relationship with Nox, we store the personal data provided by you during your customer contact with us in our ERP system. We use the Microsoft service "Dynamics 365 Business Central", also known as "Dynamics NAV", as ERP system. Within the ERP system we mainly process order and billing data, for the execution of our invoicing.

### 2.2.1 What categories of personal data do we process?

Within our ERP system, we process the following data from you:

- Contract data (contract number, conditions, billing modalities etc.)
- Master data (first and last name, organization, function/position)
- Contact data (email address, phone number, billing address)
- Billing data (bank details, credit card data, incoming payments, payment history etc.)

### 2.2.2 What are the purposes and legal basis for the data processing?

We process the data mentioned above for the following purposes and on the following legal basis:

- For the fulfillment of contracts with our customers on the basis of Article 6 para. 1 lit. b GDPR.
- To ensure the management and maintenance of customer data on the basis of our legitimate interests in accordance with Article 6 (1) (f) GDPR.
- To fulfill our statutory obligations regarding accounting and the preparation of annual financial statements on the basis of Article 6 (1) (c) GDPR in conjunction with ... .
- To ensure our corporate planning on the basis of our legitimate interests in accordance with Article 6 (1) (f) GDPR.

Our legitimate interests for the processing of your data are to ensure the management and maintenance of customer data and to ensure proper corporate planning.

### 2.2.3 Does a transfer of your data to third countries take place?

Within our customer relationship management, we use Dynamics 365 Business Central, a service of Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA (hereinafter "Microsoft"). We cannot exclude the possibility that your data will be transferred to Microsoft servers in the USA. Please note that currently no adequate level of data protection within the meaning of Article 45 GDPR can be guaranteed in the USA. Possible risks of processing your data in the USA are, that access to your data by governmental authorities, such as security agencies and/or intelligence services, cannot be excluded and that your data may be processed by them without your knowledge and without any enforceable legal remedies being available to you. Transfers of your data to Microsoft will be subject to the EU standard contractual clauses according to Article 46 para. 2 lit. c GDPR available at [https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.documentsearch.blob.core.windows.net%2Fprodv%2FMicrosoftProductandServicesDPA\(WW\)\(English\)\(Sept2022\)\(CR\).docx%3Fsv%3D2020-08-04%26se%3D2122-10-07T08%3A57%3A26Z%26sr%3Db%26sp%3Dr%26sig%3DQjvcuvCstdxi6b%252FBu9%252Fvr74Xwt5w7f8arm0P2FnHvoA%253D&wdOrigin=BROWSELINK](https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.documentsearch.blob.core.windows.net%2Fprodv%2FMicrosoftProductandServicesDPA(WW)(English)(Sept2022)(CR).docx%3Fsv%3D2020-08-04%26se%3D2122-10-07T08%3A57%3A26Z%26sr%3Db%26sp%3Dr%26sig%3DQjvcuvCstdxi6b%252FBu9%252Fvr74Xwt5w7f8arm0P2FnHvoA%253D&wdOrigin=BROWSELINK). For further information on data protection at Microsoft please visit <https://privacy.microsoft.com/en-us/privacystatement>.

## 2.3 Customer support

Regarding support matters, you can contact us via our ticket system, by telephone or email as well as via the dedicated contact form on our website. Within the support requests, you will be asked to provide the information necessary for the best possible handling of your request. Furthermore, you have the possibility to attach any relevant documents to your request. Depending on your country your support request will be assigned to the respective customer support agent. As part of handling your request, we will contact you by email. Moreover, we might contact you by telephone or carry out online support sessions if necessary to resolve the respective issue. Upon your prior consent, support sessions via telephone might be recorded by us. Within the online support sessions, our customer support agents might access your end device or system by screen sharing upon your prior consent in order to give you the best support possible. After all, we will ask you for feedback on our support service by email.

### 2.3.1 What categories of personal data do we process?

Within the scope of the handling of your support request as described above, we process the following data from you:

- Master data (first and last name, function/position, company, country, postcode)
- Contact data (email address, phone number)
- Information concerning your request (subject of the request, description of the issue, affected product, software version, information on your system and device, attached files e.g., screenshots or log file data)
- Information concerning the handling of your request (email conversations, information shared within support sessions, recordings of support phone calls, feedback on our support service)
- Ticket system account data (profile picture if applicable)

### 2.3.2 What are the purposes and legal basis for the data processing?

Within the scope of our customer support service, we process the data mentioned above for the following purposes and on the following legal basis:

- To ensure proper response to customer requests and communication on the basis of our legitimate interests in accordance with Article 6 (1) (f) GDPR.
- To ensure an efficient process design and the best possible handling of your request on the basis of your prior consent in accordance with Article 6 (1) (a) GDPR.
- To ensure the proper fulfillment of contracts with our customers on the basis of Article 6 (1) (b) GDPR.

Our legitimate interests for the processing of your data are to ensure a proper communication with customers and to answer customer requests as well as to ensure an efficient process design.

### 2.3.3 Does a transfer of your data to third countries take place?

In the course of our customer support, we use Zendesk, a service of Zendesk Inc., Market St. 989, CA 94103 San Francisco, USA (hereinafter "Zendesk") as well as Jira, a service of Atlassian Pty Ltd, 341 George Street, NSW 2000 Sydney, Australia (hereinafter "Atlassian"). We cannot exclude the possibility that your data will be transferred to Zendesk and/or Atlassian servers in the USA and Australia. Please note that currently no adequate level of data protection within the meaning of Article 45 GDPR can be guaranteed in the USA and Australia. Possible risks of processing your data in the USA are, that access to your data by governmental authorities, such as security agencies and/or intelligence services, cannot be excluded and that your data may be processed by them without your knowledge and without any enforceable legal remedies being available to you. Transfers of your data to Zendesk (USA) and/or Atlassian (Australia) will be subject to the EU standard contractual clauses according to Article 46 para. 2 lit. c GDPR. Please contact us using our contact details mentioned above to obtain a copy of the standard contractual clauses concluded with Zendesk and Atlassian.

## 2.4 Video conferencing / webinars

If you participate in our webinars or in a video call in the context of our customer support, your data will be processed. Webinars (outside of our customer support) are communicated e.g., via social media and newsletters. You can register to a webinar via a link to our website, where we provide a dedicated registration form. Upon your prior consent, some webinars might be recorded and published on our website, in order to provide the contents of the respective webinar to a wider audience. If we record webinars, this will be communicated to you before the start or displayed in the webinar and - if necessary - you will be asked for your consent. Consent can be given, for example, by a positive message in the chat. Your consent is always voluntary. If you do not want to be recorded on video and/or audio, you can leave the online meeting. You can also deactivate your camera and/or microphone or refrain from using the chat tool.

Apart from that, you can always freely choose to share your video or audio and/or to participate under a pseudonym. The scope of the data being processed depends on the information you provide before or when participating in a webinar or video call.

### 2.4.1 What categories of personal data do we process?

Typically, the following data are processed when participating in our webinars or video calls:

- Master data (first and last name, function/position, company, country)
- Contact data (email address, phone number)
- User account data (display name, profile picture)
- Image, video, sound and text data
- Online and meta data (IP address, information on end device, browser type, user ID, user settings, operating system, logfile data, date and time of video call, subject of video call etc.)

### 2.4.2 What are the purposes and legal basis for the data processing?

Within the scope of webinars and video calls, we process the data mentioned above for the following purposes and on the following legal basis:

- To ensure proper customer communication and generate services on the basis of our legitimate interests in accordance with Article 6 (1) (f) GDPR.
- To conduct marketing activities on the basis of your prior consent in accordance with Article 6 (1) (a) GDPR.
- To ensure the proper fulfillment of contracts with our customers on the basis of Article 6 (1) (b) GDPR.

Our legitimate interests for the processing of your data are to ensure a proper communication with customers and to answer customer requests as well as to ensure an efficient process design.

### 2.4.3 Does a transfer of your data to third countries take place?

To conduct our webinars or video calls we use video conferencing services from U.S. providers (e.g., Zoom, Webex, Loom, Google Meets). If you participate in our webinars or in a video call, we cannot exclude the possibility that your data will be transferred to the respective video conferencing tool provider. Please note that currently no adequate level of data protection within the meaning of Article 45 GDPR can be guaranteed in the USA. Possible risks of processing your data in the USA are, that access to your data by governmental authorities, such as security agencies and/or intelligence services, cannot be excluded and that your data may be processed by them without your knowledge and without any enforceable legal remedies being available to you. Transfers of your data to video conferencing providers based in the USA will be subject to the EU standard contractual clauses according to Article 46 para. 2 lit. c GDPR. Please contact us using our contact details mentioned above to obtain a copy of the relevant standard contractual clauses. In addition, technical data in particular may also be processed by the respective video conferencing provider itself. For details, please refer to the privacy policy of the respective video conferencing provider, which will be provided to you with in advance of the respective webinar or video call.

## 2.5 Evaluation of device usage

We create and evaluate reports that contain information about the use of our medical devices. The reports show, for example, how many tests the customer has performed with the medical device within a month and whether the test was successful or not (error rate). This data is relevant for us, especially for billing purposes. The data is also used for error detection and product improvement.

### 2.5.1 What categories of personal data do we process?

We process the following data from you within the evaluation of the medical device usage:

- Mater data (first and last name, organization)
- Usage data (tests performed per month, error rate)

### 2.5.2 What are the purposes and legal basis for the data processing?

We process the data mentioned above for the following purposes and on the following legal basis:

- For the fulfillment of contracts with our customers on the basis of Article 6 (1) (b) GDPR.
- For the steady improvement of our products on the basis of our legitimate interests in accordance with Article 6 (1) (f) GDPR.

Our legitimate interest for the processing of your data is to ensure the steady improvement of our products.

### 2.5.3 Does a transfer of your data to third countries take place?

For the evaluation of the medical device usage, we use Power BI, a service of Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA (hereinafter "Microsoft"). We cannot exclude the possibility that your data will be transferred to Microsoft servers in the USA. Please note that currently no adequate level of data protection within the meaning of Article 45 GDPR can be guaranteed in the USA. Possible risks of processing your data in the USA are, that access to your data by governmental authorities, such as security agencies and/or intelligence services, cannot be excluded and that your data may be processed by them without your knowledge and without any enforceable legal remedies being available to you. Transfers of your data to Microsoft will be subject to the EU standard contractual clauses according to Article 46 (2) (c) GDPR available at [https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwwwlpdocumentsearch.blob.core.windows.net%2Fprodv2%2FMicrosoftProductandServicesDPA\(WW\)\(English\)\(Sept2022\)\(CR\).docx%3Fsv%3D2020-08-04%26se%3D2122-10-07T08%3A57%3A26Z%26sr%3Db%26sp%3Dr%26sig%3DQjvcuvCstdxi6b%252FBu9%252Fvr74Xwt5w7f8arm0P2FnHvoA%253D&wdOrigin=BROWSELINK](https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwwwlpdocumentsearch.blob.core.windows.net%2Fprodv2%2FMicrosoftProductandServicesDPA(WW)(English)(Sept2022)(CR).docx%3Fsv%3D2020-08-04%26se%3D2122-10-07T08%3A57%3A26Z%26sr%3Db%26sp%3Dr%26sig%3DQjvcuvCstdxi6b%252FBu9%252Fvr74Xwt5w7f8arm0P2FnHvoA%253D&wdOrigin=BROWSELINK). For further information on data protection at Microsoft please visit <https://privacy.microsoft.com/en-us/privacystatement>.

## 2.6 Vigilance Process

In the event of reported patient harm due to quality problems with our medical devices or quality problems that could lead to potential patient harm, the medical device in concerned is investigated by us in coordination with the responsible regulatory authority. We prepare a corresponding assessment report. In the case of reportable incidents, we are required to submit a country-specific reporting form to the competent authorities of the countries in which the products are approved. As part of the preparation of the evaluation reports, you will be asked to provide us with the relevant information in order to evaluate the specific event.

### 2.6.1 What categories of personal data do we process?

Within the process mentioned above we process the following data from you:

- Mater data (first and last name, organization)
- Individual descriptions of the respective issue with our medical device

### 2.6.2 What are the purposes and legal basis for the data processing?

We process the data mentioned above for the following purposes and on the following legal basis:

- For the compliance with our legal obligations on the basis of Article 6 (1) (c) GDPR in conjunction with ... .
- For the enforcement and defense of legal claims on the basis of our legitimate interests in accordance with Article 6 (1) (f) GDPR, namely the enforcement and defense of legal claims.

### 3 How long will your data be stored?

In general, we process and store your data as long as it is required for the purpose of the respective data processing mentioned above, unless you have effectively objected to the processing of your data on the basis of our legitimate interests or effectively withdrawn any given consent. Insofar as statutory retention obligations exist - e.g., from commercial or tax law - we will store the data affected by this for the duration of the corresponding retention period.

### 4 Recipients of personal data

Your data will only be transferred to external recipients to the extent necessary to fulfill the above-mentioned purposes, we are legally obligated to transfer your data or you have given us your effective consent to do so. If necessary, your data will be transferred to external service providers which we use to fulfill the above-mentioned purposes and with whom we have concluded an agreement on the processing of your data in accordance with Article 28 GDPR. External service providers used by us process your data only for the intended purpose and within the scope of our instructions. External recipients of your personal data can be in particular:

- Affiliated companies;
- Service providers bound by instructions that we use to fulfill the above-mentioned purposes;
- Business partners (e.g., freelancers);
- Tax authorities;
- Tax consultants and auditors;
- Courts, arbitration tribunals, authorities or legal advisors, if this is necessary to comply with applicable law or to assert, exercise or defend legal claims.

### 5 Third country data transfers

While processing your personal data, especially when using cloud services, your personal data may be transferred to entities outside the European Union (EU) or the European Economic Area (EEA) (hereinafter referred to as "third countries"). In these cases, we will then provide you with separate information on data protection - related to the respective third country transfer - insofar as this is required by law. In any case, if your personal data is transferred to third countries, we will ensure that an adequate level of data protection exists in the third country concerned before transferring your personal data, apart from exceptional cases permitted by law. An adequate level of data protection can be guaranteed, for example, by the conclusion of EU standard contractual clauses or the existence of so-called binding corporate rules (BCR). Please contact us via the contact options provided to you as part of this privacy policy to obtain a copy of the specific guarantees for the transfer of your data to third countries.

## 6 Your rights as a data subject

As a data subject, you have the following rights within the statutory limits:

### *Right to information (Article 15 GDPR)*

You have a right to obtain information about the personal data concerning you that is processed by us.

### *Right to rectification (Article 16 GDPR)*

You have the right to request that we immediately correct inaccurate data and complete incomplete data, provided that the legal requirements are met.

### *Right to erasure (Article 17 GDPR)*

You have the right to request the erasure of your personal data, provided that the legal requirements are met and in particular if (1) your data is no longer necessary for the purposes stated in this privacy notice, (2) you have withdrawn your consent and there is no other legal basis for the processing, (3) your data has been processed unlawfully or (4) you have objected to the processing of your data and there are no overriding legitimate grounds for the processing.

### *Right to restriction of processing (Article 18 GDPR)*

You have the right to request that we restrict the processing of personal data concerning you, in particular if you dispute the accuracy of the data or if the processing of your data is unlawful and you request restriction instead of erasure.

### *Right to data portability (Article 20 GDPR)*

If your data is processed on the basis of a contract or on the basis of your consent, you have the right to receive your data in a structured, commonly used and machine-readable format or to have your data transferred to another controller, provided that the legal requirements for this are met.

### *Right to object (Article 21 GDPR)*

You have the right to object to the processing of your data at any time on grounds relating to your particular situation, insofar as the legal basis for our processing of your data is the maintenance of our legitimate interests or the legitimate interests of a third party pursuant to Article 6 (1) (f) GDPR. If you exercise your right to object, we will stop processing your data unless we can demonstrate compelling legitimate grounds for continuing the processing which override your interests, rights and freedoms, or the processing is for the purpose of asserting, exercising or defending legal claims.

### *Right of withdrawal (Article 7 para. 3 GDPR)*

If we process your data on the basis of your consent, you have the right to withdraw this consent at any time with effect for the future. This does not affect the lawfulness of the processing until the time of the withdrawal.

### *Right to lodge a complaint with a supervisory authority (Article 77 GDPR)*

Without prejudice to any other administrative or judicial remedy, you have the right to lodge a complaint with a supervisory authority if you consider that the processing of personal data concerning you infringes the GDPR. You may exercise this right with a supervisory authority in the member state of your ordinary residence, place of work or place of the alleged infringement or with the supervisory authority responsible for us. The supervisory authority responsible for us is the Icelandic data protection authority – Persónuvernd, Rauðarárstígur 10, 105 Reykjavík, Iceland.

To exercise your rights as a data subject, please contact us using the contact details under “Information about the Controller of the data processing”.

This privacy policy may be subject to change. The current version of this privacy policy applies.