Privacy Notice

pg40 Consulting Group GmbH
Privacy Notice

Version dated August31, 2019

The applicable version of this privacy notice can be downloaded as a PDF from download area on our website https://www.diafyt.de/german/diafyt-app/

1. INTRODUCTION

1.1 Responsible entity

1.1.1 pg40 Consulting Group GmbH, located in Leipzig at the business address Schwägrichenstr. 3, 04107 Leipzig, VAT 231/289/00535 and responsible tax office, Finanzamt Leipzig II ("**pg40**"), is the stated responsible entity under the data protection regulations. In other words we are the company that decides on the purpose and means of processing the personal data of our users ("**User Data**") and is therefore responsible for its security and compliance with the applicable laws.

1.1.2 As the responsible entity we are subject, for example, to information requirements that we wish to fulfill in connection with this privacy notice. We also provide additional information within our products, e.g. we may ask you for a new consent or explain the consequences of revocation. The information in our products does not contradict this privacy notice, but rather supplements it with brief and easily readable information so that you can make decisions more easily. This privacy notice and the additional information are easily accessible at any time from within our products.

1.2 Structure and consent concept

1.2.1 This privacy notice informs you about the purposes and scope of processing your User Data, as well as data transfers, and your extensive rights. As our offer is exclusively aimed at persons with diabetes, your use typically already provides information on your health condition. We therefore only process User Data as health data with your consent. We differentiate as follows:

1.2.1.1 "Necessary Processing" describes how we process the User Data required to fulfill the contract. Without this consent the use of our products is not possible from a legal and a factual point of view because our services depend on this processing.

1.2.1.2 "Processing for Marketing Purposes" describes how we contact you for marketing purposes, with your consent, e.g. by email, notifications etc. Here too you may use the products without consent but with your consent you will receive interesting information on our products or if, for example, your health insurance company covers new services.

1.2.1.3 In "General Information" we have assembled the information that applies to all of the above consents to avoid repetition.

The relevant categories are described in more detail below. You may provide the relevant consents upon registration or later via the account settings. You may revoke any consents at any time. For doing so please contact our support. In such an instance we will inform you about the consequences of the revocation. The lawfulness of the processing prior to revocation remains unaffected.

1.2.2 In some cases, the processing may take place independently of consent on the basis of statutory principles (e.g. medical device regulations). We will inform you accordingly in appropriate cases.

2. NECESSARY PROCESSING

If you grant your consent, we process the User Data listed below in order to be able to provide our services. If you do not consent to this necessary processing, you cannot use the services of pg40. You may provide your consents during the registration process and manage them in the account settings.

2.1 Necessary and optional User Data

2.1.1 In order to protect your User Data in diafyt Pro, our services can only be used in connection with a user

account. To create a user account we require and process the following User Data:

- Email address
- Closing date standing order
- Status of consents.

2.1.2 All other information is optional and self-explanatory in the input masks or rather collected in case of a support request. Such optional entries include:

Personal Master Data: first name, last name, address, date of birth/age, gender, telephone number.

Medical Master Data: diagnosis year, blood glucose target range, height, weight, type of insulin.

Commercial and Usage Data
App store download, purchase, invoices, payment status, payment method (credit card, bank account, etc.), diafyt Pro status, support queries.

Medical Data
App entries such as date/time/time zone/place, food intake/meal/ingredients, injections, blood glucose measurements, notes/text, weight, medication, imported values; sensor data such as start date/time, end date/time, time zone, sensor value, type; app settings.

2.1.3 If you wish, you can operate the user account under an assumed name (pseudonym), i.e. you do not have to state your real name. You can also enter any email address that you set up especially for us – however it must work so that we can send you important warnings.

The scope of the data recorded by pg40 depends on your use of our products. We only process the User Data that you actively and voluntarily provide to pg40. The entry of requested User Data is however a requirement for the comprehensive use of our products. If you do not enter optional data the associated functionality of our products is limited accordingly. For example diafyt Pro requires detailed (voluntary) entry of your data in order to ensure optimal use.

2.2 Necessary purposes

2.2.1 All the necessary purposes of our processing are associated with providing our services:

Order, delivery, support, and billing of our products (including goods from our cooperation partners) require the entry and processing of certain data in order to process your order.

Installation of our apps leads to technical and device-related data recordings such as the device ID.

A standing order leads to the creation of an internal user-id.

The **provision of our services** requires you to voluntarily and actively enter data.

Communication from pg40 with you within our apps or via other electronic messaging services (e.g. email, messenger, telephone) where this is required to support or troubleshoot our products. This is how we process any comments and queries that you may have via various communication channels when using pg40. The most important example is our support service. Please therefore think about which information and data you want to give in your active communication with us - this is solely your decision. For our part, communication with users may be necessary either by email, in-app card, or push notification. This is how we inform you about updates to our products and provide important security advice as well as assistance associated with your usage. This support communication - as an essential part of our products - is sent to users notwithstanding whether they have subscribed to our Newsletter or not.

Therapy devices (e.g. blood glucose meters) can be paired with your device which enables data to be transferred to our apps.

2.2.2 Use of our apps and extensions requires you to actively and voluntarily enter data. You will find additional selection options in the settings of our apps. To resolve an error in the app we require, for example, crash reports that we can use for troubleshooting purposes to determine the circumstances of the problem. In addition, the key data of your device and your usage behavior are recorded as our contractual fulfillment, above all, means customizing our products. An automated analysis of user behavior is performed exclusively for the purpose of customizing your use when fulfilling the contract and has no legal effect for you.

3. PROCESSING FOR MARKETING PURPOSES

3.1 Newsletter

3.1.1 We would like to send you interesting information on products and services in addition to the contractual scope (including information from carefully selected partners) and invitations to participate in surveys or other sales promotions and marketing activities ("**Newsletter**").

3.1.2 You can select whether you want to subscribe to our Newsletter (opt in). You can revoke your consent at any time via the link in the Newsletter or the account settings.

3.2 Other types of marketing

3.2.1 Other consents, e.g. for surveys, notifications, or customized offers, are obtained as required when you are logged in. We always explain to you why we need certain data and also how you can revoke the consent.

3.2.2 Please be aware that we may show you offers within the app without processing your personal data. You will also see these non-customized advertisements if you have not provided your consent.

4. USAGE FOR STATUTORY PURPOSES

4.1 Scientific research and statistics

pg40 is committed to the science of all aspects of diabetes. Therefore, anonymous User Data may also be used for the purposes of research and statistics (always whilst complying with the recognized ethical scientific standards) and internal analyses. This is used mainly to determine and improve the effectiveness of techniques for controlling and treating diabetes. The legal basis for this is Article 9 (2) j) GDPR.

4.2 Enforcement of rights

The use of personal data may also be necessary to prevent abuse by users or to assert, exercise, or defend legal claims. We may be forced into disclosure due to binding laws, court or official decisions and instructions, criminal investigation, or in the public interest. In such cases, the storage and processing of your data are permitted by law without your consent. The legal basis for this is Article 9 (2) f) GDPR.

4.3 In accordance with medical device legislation

Finally, as the manufacturer or distributor of a medical device, we are subject to increased requirements for monitoring the functionality of our product. This vigilance system required for regulatory purposes may also involve the processing of personal data. The legal basis for this is Article 9 (2) i) GDPR.

5. GENERAL INFORMATION

5.1 Purpose limitation and security

5.1.1 pg40 uses your personal data exclusively for the purposes determined in this privacy notice and the relevant consents. We ensure that each processing is restricted to the extent necessary for its purpose.

5.1.2 Each processing always guarantees adequate security and confidentiality of your personal data. This covers protection from unauthorized and illegal processing, unintentional loss, unintentional destruction or damage using appropriate technical and organizational measures. We use strict internal processes, security features, and the latest encryption methods, always taking into account state-of-the-art technology and implementation costs.

5.2 Processors

5.2.1 pg40 transfers User Data to Processors exclusively within the framework of this privacy notice and only to fulfill the purposes stated in it. Processors work according to our specifications and instructions; they are not permitted to use the personal data of our users for their own or other purposes.

5.2.2 We use Processors offering sufficient guarantees that suitable technical and organizational measures are undertaken in a way that the processing of personal data complies with the statutory requirements and our privacy notice. The protection of the rights of our users is ensured by concluding binding contracts that meet the strict requirements of GDPR.

5.2.3 The third-party suppliers appointed by pg40 may only use other processors (subcontractors) with our prior

consent. If a subcontractor does not comply with the same data protection obligations and all of the appropriate security measures that we impose on our Processors, then we will prohibit the hiring of such a subcontractor.

5.3 Encryption, pseudonymization, and anonymization

5.3.1 Each data transfer, without exception and by default, is encrypted during transfer.

In addition, for the purposes of data security and minimization, we also use other processes for the encryption and pseudonymization of User Data. Of course this depends on the type, scope, and purpose of the relevant data processing and takes into account the latest technology. For example, we only disclose User Data that a Processor requires to carry out his tasks.

5.3.2 When a contractual relationship with a Processor is terminated, such Processor must, at pg40's discretion, either return all our User's Data or delete it if there are no statutory storage obligations.

5.3.3 Data that requires no personal reference for processing (e.g. for research and analysis) is subject to anonymization. This prevents a connection to a specific user being made in all cases.

5.4 EU and other countries

5.4.1 We primarily select cooperation partners who are based in or whose servers are located in the European Union (EU) or European Economic Area (EEA). Data transmission within the EU and EEA is unobjectionable because the GDPR applies in all member states.

5.4.2 In exceptional circumstances we appoint third-party suppliers who are located in or who have servers outside the EU, e.g. innovative companies in Silicon Valley, USA. However, even in these cases your personal data is subject to a high protection level in line with the GDPR – either through an EU adequacy decision, which considers data protection in certain third-party countries to be appropriate (e.g. Switzerland, Israel, and New Zealand), or through certain standard contractual clauses approved by the EU, which the contractual relationships with our contracted data processors are based on, or through comparable legal instruments permitted under the GDPR. In any case, all Processors are subject to the obligations in this privacy notice.

5.4.3 In addition, we ensure that our partners have additional security standards in place, such as individual security measures and data protection provisions or certifications under the GDPR. So, for example, if third-party suppliers are located in the USA they should be subject to the Privacy Shield Framework approved by the EU or comparable internationally recognized security standards.

5.5. Categories of recipients

5.5.1 Our cooperation partners are bound by the agreements signed with pg40 as well as by the GDPR and only process data according to our instructions. We provide our users' Data only to fulfill the contract:

Bookkeeping and payment service providers support us in the ongoing billing of our chargeable products.

Customer support services and their tools help our customer support to quickly and efficiently handle our users' inquiries. Here, for example, queries are recorded from various communication channels and grouped according to topics using ticket systems.

Analysis service providers and their tools help us to understand how users use our products in order for us to provide customized communication and product improvements in the future.

Marketing service providers support us in creating, sorting, customizing, and sending newsletters, emails, and other messages about our products to our users.

Hosting and cloud services and their tools are used to store data and to produce anonymized analyses (see section 2.4 above).

Reminder: the transfer of data to our Processors and service providers is protected by guarantees such as adequacy decisions, certifications (Privacy Shield) or standard contractual clauses.

5.5.2 Finally please note that you have the option to directly share certain data with a third party from within our products. This relates, for example, to reports generated in our apps and communication with your healthcare professional for therapy advice. You are solely responsible for such data transfers.

5.6 Cookies

We use cookies on our website. These are small files that your browser automatically creates and that are stored on your device (laptop, tablet, smartphone, etc.) when you visit our site. Cookies do not damage your device, do not contain viruses, Trojans or other malicious software.

In the cookie information is stored, each resulting in connection with the specific terminal used. However, this does not mean that we are immediately aware of your identity.

On the one hand, the use of cookies serves to make the use of our offer more pleasant for you. For example, we use so-called session cookies to recognize that you have already visited individual pages on our website. These are automatically deleted after leaving our page.

In addition, to improve usability, we also use temporary cookies that are stored on your device for a specified period of time. If you visit our site again to use our services, it will automatically recognize that you have already been with us and what inputs and settings you have made, so you do not have to re-enter them.

On the other hand, we use cookies to statistically record the use of our website and to evaluate it for the purpose of optimizing our offer (see section 5). These cookies allow us to automatically recognize when you visit our site again that you have already been with us. These cookies are automatically deleted after a defined time.

The data processed by cookies are for the purposes mentioned in order to safeguard our legitimate interests as well as third parties pursuant to Art. 6 para. 1 sentence 1 lit. f DSGVO required.

Most browsers accept cookies automatically. However, you can configure your browser so that no cookies are stored on your computer or a note always appears before a new cookie is created. However, disabling cookies completely may mean that you can not use all features of our website.

5.7 Usage data

5.7.1 Google Analytics

We use Google Analytics, a web analytics service provided by Google Inc. (https://www.google.com/intl/en/about/) (1600 Amphitheater Parkway, Mountain View, CA 94043, for the purpose of customizing and continually optimizing our pages. USA, hereafter "Google"). In this context, pseudonymised usage profiles are created and cookies (see point 4) are used. The information generated by the cookie about your use of this website such as:

- Browser type / version,
- used operating system,
- Referrer URL (the previously visited page),
- Host name of the accessing computer (IP address),
- Time of server request,

are transferred to a Google server in the US and stored there. The information is used to evaluate the use of the website, to compile reports on website activity, and to provide other services related to website activity and internet usage for the purpose of market research and customization of these websites. This information may also be transferred to third parties if required by law or as far as third parties process this data in the order. Under no circumstances will your IP address be merged with any other data provided by Google. The IP addresses are anonymized, so that an assignment is not possible (IP masking).

You can prevent the installation of cookies by setting the browser software accordingly; however, we point out that in this case not all features of this website may be fully exploited.

You can also prevent the collection of data generated by the cookie and related to your use of the website (including your IP address) and the processing of this data by Google by downloading and installing a browser add-on (https: // tools.google.com/dlpage/gaoptout?hl=de).

As an alternative to the browser add-on, especially for browsers on mobile devices, you can prevent the collection by Google Analytics by clicking on this link. An opt-out cookie will be set which prevents the future collection of your data when you visit this website. The opt-out cookie is only valid in this browser and only for our website and is stored on your device. If you delete the cookies in this browser, you must set the opt-out cookie again.

For more information about privacy related to Google Analytics, see the Google Analytics Help Center (https://support.google.com/analytics/answer/6004245?hl=en).

5.7.2 Google Adwords Conversion Tracking

To statistically record the use of our website and to evaluate it for the purpose of optimizing our website, we also use Google conversion tracking. In doing so, Google Adwords will set a cookie (see section 4) on your computer, provided that you have reached our website via a Google ad.

These cookies lose their validity after 30 days and are not used for personal identification. If the user visits certain pages of the Adwords customer's website and the cookie has not yet expired, Google and the customer can recognize that the user clicked on the ad and was redirected to this page.

Each Adwords customer receives a different cookie. Cookies can not be tracked via the websites of Adwords customers. The information gathered using the conversion cookie is used to generate conversion statistics for Adwords customers who have opted for conversion tracking. Adwords customers hear the total number of users who clicked on their ad and were redirected to a conversion tracking tag page. However, they do not receive any information that personally identifies users.

If you do not want to participate in the tracking process, you can also refuse the required setting of a cookie - for example, via a browser setting that generally deactivates the automatic setting of cookies. You can also disable cookies for conversion tracking by setting your browser to block cookies from the domain "www.googleadservices.com". Google's privacy policy on conversion tracking can be found here (https://services.google.com/sitestats/en.html).

5.7.3 Matomo

We use Matomo open-source software for analysis and statistical analysis of website usage. Cookies are used for this purpose (see paragraph 4). The information generated by the cookie about the use of the website is transmitted to our servers and summarized in pseudonymous usage profiles. The information is used to evaluate the use of the website and to enable a needs-based design of our website. The information will not be passed on to third parties.

In no case will the IP address be associated with any other data concerning the user. The IP addresses are anonymized, so that an assignment is not possible (IP masking).

Your visit to this website is currently covered by the Matomo web analytics. Click here (https://matamo.org/docs/privacy/) to stop your visit.

5.8. Storage and deletion

5.8.1 Your User Data is stored on your device. This data is also stored on our servers. We only use systems that meet GDPR requirements.

5.8.2 By default your data are stored on servers in the European Union (EU). Regardless of the storage location we ensure that the high protection level pursuant to the GDPR is guaranteed; naturally this also applies to data that is stored temporarily at another location or is transferred for processing.

5.8.3 As a rule, pg40 only stores your personal data for the duration of the contract. In exceptional cases, longer storage may be required in order to fulfill post-contractual obligations or to comply with statutory storage obligations or disclosure duties, or to assert, exercise, or defend legal claims (limitation periods).

5.9. Minors

Minors, below the age of sixteen are only permitted to use our products with the consent of a parent/guardian (see section 3.2.4 of our General Terms & Conditions – T&C). This also applies to processing their personal data, which is only legal if and to the extent to which the consent has been obtained by and through the parent/guardian. Otherwise use of our products is prohibited.

5.10. Data protection officer

5.10.1 Our data protection officer is available to answer all data protection questions. The data protection officer monitors independently and not bound by instructions compliance with all data protection regulations and is subject to strict statutory secrecy and confidentiality obligations.

5.10.2 The data protection officer is widely involved in all questions associated with protecting the personal data of our users. As a trained expert, he monitors our processing on an ongoing basis, informs and regularly advises the entire pg40 team in order to ensure the best possible protection of your User Data.

5.11. Changes

5.11.1 As technology and processes in the Internet as well as data protection legislation are constantly being developed, we have to undertake changes from time to time. We will inform you of changes by appropriate means whilst granting an appropriate advance notice period and if necessary obtaining new consents.

5.11.2 Unless otherwise provided by this privacy notice, the same definitions apply in our General Terms and Conditions - T&Cs.

6. YOUR RIGHTS

6.1. Revocation of consents

If we process your User Data based on your consent, you may revoke the consent at any time. However, this will not affect the lawfulness of the processing before the revocation. We will continue to provide our services if they do not depend on the consent that has been revoked.

6.2. Information, correction, and restriction

6.2.1 Each user has the right to request information on the processing of their personal data. To do so, please contact us at any time.

6.2.2 Your right to information covers information on the processing purposes, data and recipient categories, storage time, origin of your data, and your rights under the data protection regulations. You can find all of this information in this privacy notice and we are happy to provide it to you in an electronic form.

6.2.3 Should some of your personal data be incorrect, you can request that your data is corrected or completed at any time. You can correct most data yourself in our apps. You have the right to restrict data processing for the duration of any investigation review that you have requested.

6.3 Deletion (“right to be forgotten”)

Each user has the right to request the deletion of their personal data. To do so, please contact our support.

6.4 Ability to transfer data

Finally each user has the right to request that we provide an overview of their personal data to another responsible party, if this is technically feasible.

6.5 Complaints

6.5.1 If you feel we are not protecting your data protection rights adequately, please contact our support at any time or contact our data protection officer. We will handle your request immediately.

6.5.2 Any user has the right to submit a complaint with following Data Protection Authority in Saxony, Germany, responsible for pg40 at Datenschutzbeauftragter in Sachsen, 01067 Dresden, Devrienstr. 1, if they believe that the processing of their personal data is not in compliance with data protection regulations. In addition, the user has a right to complain to a supervisory authority in the EU member state in which they are resident, in which their workplace is located, or which is the location of a suspected infringement.

THANK YOU FOR YOUR CONFIDENCE IN US!