PhysioTools and the EU General Data Protection Regulation (GDPR)

We would like to outline some major changes PhysioTools have made and will be making to comply with the EU General Data Protection Regulation (GDPR; 679/2016) by May 25, 2018, the date the legislation comes into force. The focus is on the processing of personal data on behalf of our PhysioTools Online customers. We also describe measures we have undertaken to comply with our role as controller of personal data.

General background on the GDPR

The GDPR lays down rules for the protection of natural persons with regard to the processing of personal data. It will strengthen and unify data protection for individuals within the EU. The legislation also comes into force in the United Kingdom.

GDPR obligates organisations such as PhysioTools to have in place clear and secure procedures for the processing of personal data. Processing is defined to include operations on personal data or sets of data by both manual and automated means. It includes amongst others the collection, structuring, storage, use and destruction of personal data. GDPR also requires us to have our processing procedures documented and available for PhysioTools' customers to see.

Personal data as defined by the GDPR means any information relating to an identified or identifiable natural person (data subjects). Identification can be based on, for instance, name, an identification number or location data. For instance, a first and a last name can be used to help identify a natural person and thus fall in the category of personal data.

Your role as part of the GDPR

You are considered the controller of any personal data entered into the PhysioTools software. You determine the purposes and means of processing personal data. It is your decision to either enter personal data into PhysioTools, for example, to fulfil legal obligations to document your therapy processes, or to use PhysioTools as a tool for creating exercise programs without associating them with an identifiable data subject.

What personal data can be input into PhysioTools software?

Our customers may choose to enter the following personal data that can be used to identify individuals:

- First name
- Surname
- Email address

PhysioTools' role as part of the GDPR

PhysioTools is providing services to you in the form of a software for creating personalised exercise programs. The service is offered online and personal data may be entered into the software by you. In this sense **PhysioTools is considered the processor of the data entered into the software and stored on its servers.** PhysioTools processes the data on your behalf based on a licence or similar agreement.

In where its own customer registers are concerned, PhysioTools acts in the role of data controller.

How is PhysioTools preparing for GDPR compliance?

One of the first steps to prepare for the change in legislation was to provide GDPR training for PhysioTools personnel. This has increased awareness of the upcoming changes and initiated the overall analysing and planning process in our company.

As part of its preparations to be compliant with GDPR, PhysioTools is **currently revising its legal agreements**. We will require all our online customers to have a Data Processing Agreement (DPA) in place with us, be it by accepting our DPA through the PhysioTools Online software or by additionally sending us their own written guidelines or agreements for data processors.

PhysioTools has undertaken steps to **document in an easily understandable way the processes related to the processing and controlling of personal data**. This includes documentation on the different data sources, collection, storage and deletion.

For processing personal data measures include the documenting and improving of technical and organisational measures to mitigate the risk of data breaches. On a general level our lawful base for processing personal data on your behalf is by a licence or similar agreement based on which we deliver the PhysioTools service to you. Access to the personal data we process on your behalf is restricted to situations where PhysioTools personnel are required to provide, for example, technical assistance to you. All PhysioTools personnel with access to personal data stored in our systems are subject to a non-disclosure agreement that extends also beyond the termination of their work contract.

For controlling personal data measures include revising website privacy policies and putting in place agreements with third party providers. We have also revised the way we seek, obtain and record, for example, your consent to receiving our e-newsletter. GDPR includes your right to be informed about the data we hold about you and your right to be forgotten – meaning the deletion of your personal data from our registers – under certain conditions. We have put in place procedures to ensure our ability to provide you with the required information in electronic and commonly used format. Please be aware that under GDPR you also have the obligation to inform us about any changes in your personal data and to rectify inaccurate information about you that comes to your attention.

PhysioTools has been and is still working on **putting the necessary procedures in place to detect, report and investigate personal data breaches** that come to our attention and to ensure we are in the position to document and describe them to the affected parties. GDPR defines personal data breaches as security breaches resulting in, e.g. the accidental or unlawful destruction, disclosure or alteration of personal data. We are also analysing the risks related to possible personal data breaches, accidental or unlawful destruction, disclosure or alteration of personal data. We are also analysing the risks related to possible personal data breaches.

PhysioTools **will comply with requests from its customers to help fulfil their legal obligations**. This might include providing assistance by giving information about data types and categories processed by us, or by providing background information on the way data is secured within our system.

We have evaluated the requirements for appointing a data protection officer but have concluded that this is not necessary for our organisation.

Please direct any request you would like to address to PhysioTools regarding our GDRP policies and compliances to info@physiotools.com**.**