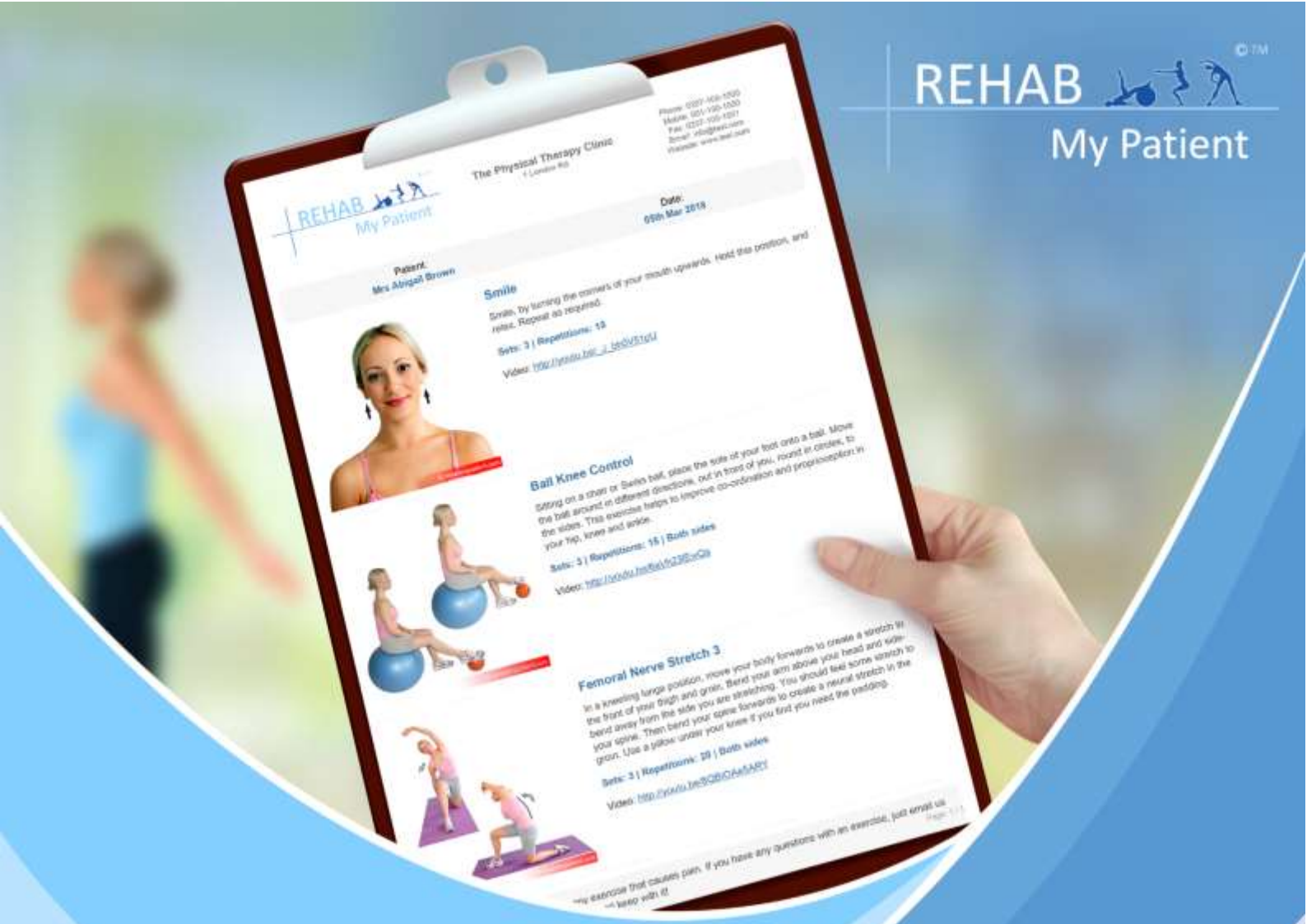


GDPR

Compliance Report

Rehab My Patient GDPR Compliance Report

Part I. Processing roles

1. Overview of the data processing roles

There are three important roles in the GDPR world:

Data subject - natural person that is identified or could be identified based on certain information (personal data). In your case data subjects will be the subscriber (medical professionals) and the patients.

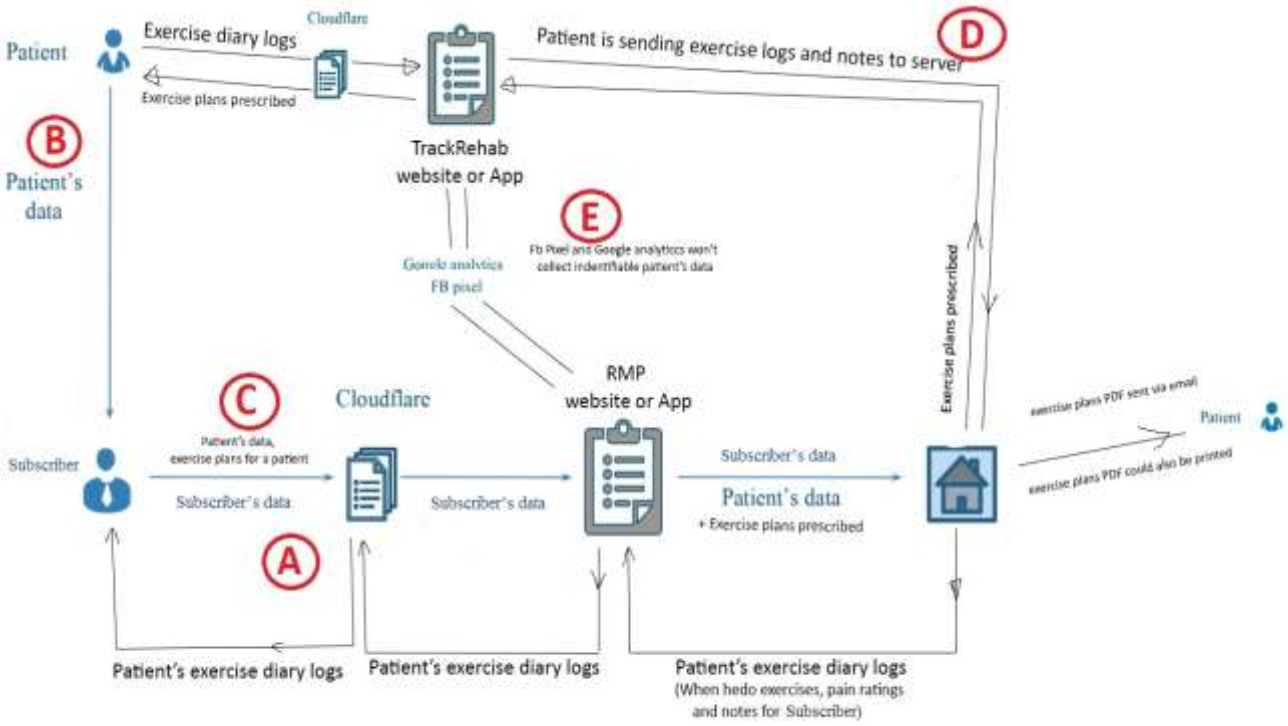
Data controller - this will be the entity or the natural person who collects data and determines the purposes and the means of the processing of personal data.

Data processor – this is the subject who processes personal data on behalf of the controller.

It is essential to determine the processing role of the Rehab My Patient website (RMP), considering the difference in the obligations of the processor and the controller under the GDPR. One entity may be considered as controller for part of its relations and as processor for other part, so the role of RMP should be clarified for all of its activities.

2. What is the data processing role of RMP?

There are five main groups of data processing activities that we can identify based on the provided information and on the final version of the data mapping (marked on the data mapping image below from A to E), as following:



A. Subscriber - RMP

The first data processing activity is the collection of the personal data of the subscriber in order to create and manage his account. The role of RMP here is without any doubt the role of **Controller**.

This is because RMP meets all prerequisites in order to be qualified as a controller - has a degree of control over the collected personal data, collects the data in order to provide specific service and most importantly determines the purposes (creating of an account, access to the RMP services) and the means of processing the personal data of the subscriber.

B. Subscriber - Patient

The subscriber has the role of **Controller** for the personal data of his patients.

C. RMP – Patient's data

The most complex and hard to determine role is the role of RMP in regard to the processing of the patient's data. The role of RMP in this case may be each one of the three processing roles: Controller, Co-controller and Processor.

The role of RMP is important for its obligations towards the patients to be determined and also because patient related data can be qualified as health data. The health data is subject to special protection under the GDPR.

This is because any data related to the physical health of a natural person, including information related to the provision of health care services is qualified as health data and may be processed only when certain conditions are met.

What is the role of the RMP?

The role of RMP in this case is the role of **Processor** because RMP will process the personal data of the patients only under the instructions of the subscriber.
For example:

- The subscriber enters the patient's data in the RMP system (RMP processes the data as storing it upon instructions by the subscriber).
- The subscriber compiles exercise plan by using the functionalities of RMP (RMP processes the data to provide different features for the compilation of the exercise plans again upon instructions by the subscriber).

RMP is constrained in any intervention with the data and has no say about its content. RMP only provides predefined content of exercises that become related to a natural person under the actions of the subscriber when an exercise plan is compiled by the subscriber.
The subscriber determines the purpose of processing (for compiling of an exercise plan) and the means (RMP website).
The subscriber determines whether to delete or to amend patient data.

Is RMP perceived as controller of patient's data?

RMP took legal advice to consider if the supervisory authority may perceive RMP as Controller or Co-controller of the patient's data.

The risk derives from opinions of the advisory body on the GDPR (Article 29 Data Protection Working Party).

After taking into account the guidelines and the opinions of Article 29 Data Protection Working Party and the recitals of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, we have come to the conclusion that RMP process patient's data only in the capacity of a processor. The overwhelming argument for this is that without any doubt such data is processed only on behalf and upon instructions by the subscriber and that RMP has no intervention in the content of this data or by any means determines the purposes of processing.

D. Patient – RMP website or App

This processing activity encompasses the sending of exercise plans via RMP to the patient. RMP will also collect data from the patient, such as frequency of performing exercises, and pain rating, and this data will be presented to the subscriber. For this activity RMP should be treated as a **Controller** considering that RMP determines the purposes of the collection of the data and the means of processing (RMP presents the data to the subscriber). RMP does not use the data in any other way, other than to present the data to the subscriber. However, RMP also seeks consent from the patient before information is entered by the patient, advising them that the data will be shared with the subscriber.

E. RMP – Google analytics, FB pixel

RMP will have the role of **Controller** in regard to the data of the subscriber and patients who visit the site, so RMP will need to notify them about the using of systems for Monitoring of the Consumer Behavior.

Part II. GAPs and Remedy actions

Item (A-E)	GDPR Guidelines	Processes
A Subscriber - RMP	According to the GDPR principle of transparency, subscribers should be informed of the existence of processing operations concerning their own personal data, its extent and its purposes. GDPR requires that the information is specific and is communicated to the data subjects prior to the initiation of the processing. In addition, any information and	The information is provided in writing by electronic means so an online form like popup notice and there is an easy accessible section in your terms and conditions. Each notice includes the following information: ► The identity and the contact details of the controller;

	communication relating to the processing of those personal data should be comprehensive, easily accessible and understandable. So you should take appropriate measures to provide any required information to the data subject in a concise, transparent and intelligible form, using clear and plain language.	► The contact details of the data protection officer, if you appoint one (currently not required). ► The explicit and legitimate purposes of the processing and the use for which the personal data are intended as well as the legal basis for the processing (in this case the legal basis will be performance of a contract); ► The types of personal data collected (including sensitive data); ► The period for which the personal data will be stored; ► The sources and the collection methods; ► The recipients of the data and explanations as to whether, when and why the data subjects' personal information may be transferred to third parties (including the hosting company) as well as the legal basis of the transfer. Whenever possible, it is advisable to provide a link to the Privacy Notices of third parties with whom data subjects' personal information will be shared; ► The data subjects' right to request access to collected personal information, submit a privacy-related complaint, data portability, rectification or erasure of personal data or restriction of processing concerning the data subject, object to processing, obtain confirmation of personal data processing, withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; ► Description of the data subjects' available choices to indicate preferences about

		whether their personal information is disclosed to third parties and preferences regarding the frequency, subject matter and / or format of communications; ► In case the personal data are collected from the data subject, it is clear whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and what the possible consequences of failure to provide such data are, as listed in the privacy policy; ► The existence of automated decision-making, including profiling, as well as the significance and the envisaged consequences of such processing for the data subject.
A	Pursuant to Article 30 from the GDPR, the data controller is required to maintain a record of processing activities under his responsibility. The record should be kept in writing, including electronic form, and should be made available to the supervisory authority upon request.	The obligation shall not apply to an enterprise employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, or the processing is not occasional. RMP does track all processing activities and is deemed compliant.
B Subscriber - Patient	A privacy notice and legal ground for sharing of the health data with RMP.	The subscriber can notify the patient for its intention to share data with RMP as processor and should also obtain the explicit consent of the patient as this is the only applicable legal ground for transferring the data to RMP. RMP has a consent box that can be ticked to ensure that the patient has given their consent for their data to be added.
C	Currently the relations between subscriber and RMP are governed by the Licence Agreement and Terms and Conditions of	RMP does meet the requirements of the GDPR. Specification of the roles -

RMP – Patient's data	Use of the website, and the privacy policy, as well as a Data Processing Agreement. Processing by a processor (RMP) must be governed by a contract signed between the processor and the controller (the subscriber). Article 28 of the GDPR stipulates that such agreements must include clauses such as: - Clear documented instructions provided by the controller; - Confidentiality arrangements; - Security of processing measures; - Conditions under which the processor may engage another processor (sub-processor); - Technical and organizational measures, with which the processer must assist the controller; - Clauses regarding deletion, return and retention periods	explicitly stipulate that RMP is a data processor, executing activities under the instructions of the client, which acts as a data controller for the patient's data. 1. As more detailed instructions regarding the processing is included in the agreements. 2. All mandatory clauses under Article 28 of the GDPR are included. 3. Policies for reaction and notification in the event of a breach or leakage of personal data is included. 4. Detailed policies regarding the distribution of responsibilities and obligations in cases where data subjects exercise their rights under the GDPR (right of access, right of erasure etc.) is included. 5. Retention policies and terms is included. 6. These details are clearly laid out in the privacy policy and the Data Processing Agreement between RMP and the subscriber.
C	There are records of data processing activities. The processing activities performed by the processor on behalf of the controller are differentiated. The registers for each processing activity meet the requirements and include the information set in Article 30 of the GDPR.	From compliance and practical perspective it is appropriate to keep separate registers of processing activities per each subscriber. This is achieved as a structure the register in different sections for each subscriber. The requirement for registers of data processing is applicable due to the processing of health data. Records kept in writing, including electronic form, could be made available to the supervisory authority upon request.
C	Processing of sensitive data (health data).	Additionally, to curb its exposure to potential liabilities towards the patients or to

	Although the legitimacy of the data processing (grounds for processing, compliance with information obligations, etc.) must be satisfied by the controller (the subscriber), RMP, nevertheless, make sure that its activities as a data processor comply with the GDPR requirements, as a higher level of protection of sensitive data is awarded thereunder (e.g. higher security requirements in terms of technical and organizational measures).	administrative sanctions, RMP has a comprehensive contractual mechanisms to ensure adequate warranties of the controller.
D Patient - RMP	Privacy notice to patients when they enter their data in the system.	Susbcribers and patients are provided with privacy notice that contain all information required under the GDPR. Details about cookies, how they are used, why they are used, and third parties are also provided.
D	Explicit consent for the collecting of health data.	Explicit consent of the patients in order to process their health data is taken by RMP.
E	Privacy notice for the Monitoring of the Consumer Behavior. Monitoring of the Consumer Behavior can be used to track the behavior of consumers, which is considered as personal data.	The Monitoring of the Consumer Behavior is in your privacy notices. Customers have the option to opt out from such monitoring.
Other GDPR Guidelines		
Storing of the data	Data is stored for six (6) years after the subscription is ended.	The limitation period for such type of contracts in UK is 6 years. Considering this all data collected in the capacity of controller for six years after the end of your contractual relation with the subscriber. The data that RMP processes in the capacity of processor shall be stored in accordance with the instructions of the subscriber. This also applies for the exercise plans.
Hosting provider	Contract with hosting provider. Permission for using of sub processor.	RMP has a contract with DigitalOcean, and CloudFlare, as hosting providers to RMP.

		RMP gains permission by the subscriber for using of sub processor, this permission may be granted in your contracts. This is in the terms and conditions, privacy policy and data processing agreement.
Terms and conditions	The RMP Licence agreement / terms and conditions meets GDPR guidelines especially with regards to who owns the data.	9. Data agreement is notified in the terms and conditions (licence agreement) as follows: 9.1 You agree that RMP and persons supplying maintenance, web hosting and other services will have, from time to time, access to all data supplied by you as a Subscriber or Patient, solely for the purpose operating, updating, maintaining, testing or otherwise improving the Website. The Website, all underlying programs, text, video and images shall remain the property of RMP. 9.2 The patient's data will be entirely controlled by the subscriber so it cannot be property of RMP. The data of the subscriber will still remain their own data and they have specific rights under the GDPR in order to dispose with it (right of access, right of rectification, right of erasure, right to be forgotten). 9.3 RMP shall keep patient's data according to the instructions of the subscriber, for a period of six (6) years after the subscription has ended.