

# PHYSIO FIRST FINAL AUDIT FOR ALLOCATION OF LEGAL BASIS

**By: Paul, Julia, Donna and Shannon**

**Date: 24.04.18**

## Introduction

Paul, Julia, Donna and Shannon having met on Tuesday 20<sup>th</sup> February and again on Wednesday 14<sup>th</sup> March 2018 to review and then allocate the Legal Basis for the personal data that Physio First collects and uses on its various Data Subjects that our team have identified as appropriate in accordance with the guidance they have looked at and the advice they have received, came to some conclusions that will help Julia and our Office Team to carry on with our endeavour to make Physio First GDPR compliant.

Our duty is essentially to ***“to document [our] decisions on legitimate interests so that [we] can demonstrate compliance under the new GDPR accountability principle [that we] must also include ... in [our] privacy notice”***.

The primary point coming out of these meetings is that the Legal Basis for processing the personal data of the Data Subjects that Physio First have identified (using the ICO audit template) as falling under “Business Function – Sales”, and under our MRM category MB100 which include Full, Affiliate, Honorary (Practicing and non-Practicing) and Deferred member as well as Journal Subscriber and CSP Visitor has been identified as “Legitimate Interests” where consent is not required, but where there are still some opt-out & opt back in options for the data subjects.

We understand that this Legal Basis is the most complex to test as it has the most elements to test.

The point of this audit is to articulate the steps that have to be taken in relation to this.

What follows are the questions that the ICO Guidance says that we must ask ourselves when considering the Legal Basis of “Legitimate Interest” together with our answers to each.

## Ultimate Objective

Under the GDPR Physio First, like all other organisations, will have to produce a Privacy Notice which in summary requires the publication of answers to the following 8 questions:

1. What information is being collected?	6. Who will it be shared with?
2. Who is collecting it?	7. What will be the effect of this on the individuals concerned?
3. How is it collected?	8. Is the intended use likely to cause individuals to object or complain?
4. Why is it being collected?	
5. How will it be used?	

## A summary of our thinking about “Legal Basis” under GDPR

What follows is a summary of our analysis of the “Legal Basis” under GDPR.

6 legal bases	Physio First comment on each re itself
<p><b>(1) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.</b></p>	<p>Originally, we thought it may be applicable to Physio First for what we had always called our “marketing activities” e.g. for our conference /courses / membership benefits / etc - to all our contacts: i.e. Members / Non-Members / Trade / Speakers/Authors/ Tutors. Having assessed it, we have found that “consent” does not apply to how we manage and use personal data for Full, Affiliate, Honorary (Practicing and non-Practicing) and Deferred members as well as for Journal Subscribers and CSP Visitors (see also below), as we have concluded that we can use “Legitimate Interest” as our legal basis for managing and processing this personal data and that we have a legitimate interest in undertaking what we had called “marketing” to existing, paying members, but which on analyses is really “communicating with” them in a way that they would reasonably expect to receive communications from us in relation to their being a member of an organisation of our type, with our constitution and our organisational statement of intent (vision).</p>
<p><b>(2) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.</b></p>	<p>This will most likely apply for contracts of employment/ our SLA contract with the PPEF and any to come re our being their data processor</p>
<p><b>(3) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).</b></p>	<p>Also applicable to Physio First for HR /payroll purposes e.g. sending details to Hawsons our accountants / HMRC</p>
<p><b>(4) Vital interests: the processing is necessary to protect someone’s life.</b></p>	<p>Applicable to Physio First from a HR perspective if an employee had an accident at work and info was needed form their Emergency contacts/ Medical form</p>
<p><b>(5) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.</b></p>	<p>Unlikely to apply to Physio First unless the law changes</p>
<p><b>(6) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)</b></p>	<p>This is the legal basis for Physio First’s managing and processing the personal data of our data subjects</p>

**Questions & Answers to ascertain whether the personal data of Data Subjects who fall under ICO classification “Business Function – Sales” and categorised by Physio First as MB100 i.e. Full, Affiliate, Honorary (Practicing and non-Practicing) and Deferred members as well as Journal Subscribers and CSP Visitors fall under GDPR Legal Basis “Legitimate Interest”.**

## **Section 1 – The Purpose test: are you pursuing a legitimate interest?**

### **1. Why do you want to process the data – what are you trying to achieve?**

Physio First wants to process their personal data to offer to:

**Full, Affiliate Non-Practising, Deferred and Honorary (Practicing and non-practicing) members – To manage your membership and to communicate:**

- information about and assistance with our member benefits
- the opportunity to attend our annual conference and periodic post-graduate education courses and, if practicing, to promote your practice through our Find a Physio online directory and other on-line directories, who manage your data as Physio First Data Processors.

**Journal subscribers and CSP visitors – To:**

- Keep you informed about Physio First membership (if eligible)
- Send you clinical information through our Journal (i.e. if a Journal subscriber)
- Offer you the opportunity to attend our annual conference and periodic post-graduate education courses.

All of which enables Physio First, a not-for-profit trade association and professional network of the Chartered Society of Physiotherapy, to achieve our:

- Constitutional objectives which are:
  - 2.1 To promote the highest standards of clinical practice in physiotherapy generally and specifically in private practice*
  - 2.2 To promote the interchange of professional skills and ideas between individual practitioners*
  - 2.3 To encourage the Continuing Professional Development (CPD) of all members, ensuring that all members who actively practice physiotherapy participate in a recognised level of CPD annually*
  - 2.4 To market the private physiotherapy services provided by members in order to increase business and profit for those members*
  - 2.5 To provide large organisational benefits to individual members including guidance, support, education and representation at a national level with commercial organisations and within the healthcare marketplace*
  - 2.6 To encourage the highest standards of professional management within the context of private practice*
  - 2.7 To act as an advisory body to which members and the public can apply for advice concerning matters specific to physiotherapy in private practice*
  - 2.8 To strengthen and maintain the direct relationship between the Organisation and The Chartered Society of Physiotherapy*

For details see [here](#)
- Strategic reason to exist which is ***“to champion evidence-based cost effective private physiotherapy with Physio First members in the changing healthcare marketplace”***.

### **2. Who benefits from the processing? In what way?**

Every individual who falls under the Physio First category of Full, Affiliate, Honorary (Practicing and non-Practicing) and Deferred members and CSP Visitors are, by definition, Chartered Physiotherapists. Those who fall under the category “Journal Subscribers” whilst not required to be Chartered Physiotherapists are most likely to be as many convert to this as they retire from private practice. So, taking that entire context

into account, the people who benefit are Chartered Physiotherapists who have an interest in private physiotherapy through a combination of invitations to:

- join and/or remain a member of Physio First
- attend the Physio First annual conference or post graduate education courses that we provide or facilitate
- promote their practice through our on-line Find-A-Physio directory and other on-line directories, who manage their data as contracted Data Processors of Physio First
- safeguard their practitioners and patients – where necessary, through lawful checks e.g. DBS, who also manage their data as contracted Data Processors.

### 3. Are there any wider public benefits to the processing?

Wider public benefits to the processing of the personal data of:

- **Full, Affiliate, Honorary (Practicing) members** are the opportunity to search the Physio First Find-a-Physio section of our website and other on-line directories (where Physio First has a Data Controller / Data Processor agreement) where member details are displayed (where a member has opted in) that include:
  - Whether HCPC registered, as Physio First check all member HCPC registrations once a year i.e. if they are not HCPC registered their details would not appear and they would not be a member
  - The likelihood that they are individual members of the Chartered Society of Physiotherapy and therefore have Professional Liability Insurance cover of £7m, which comes with being a member of the CSP
  - Contact and geographical details that relate to how they can be contacted to provide treatment
  - Details of the particular physiotherapy treatment they provide and areas of speciality
  - The details of these physiotherapists who all receive a quarterly journal, the remit of which is to support the Physio First Quality Assured Practitioner scheme which is possibly the only third party MSK physiotherapist assessing quality system in the world.
- **Honorary (non-Practicing) members** are the opportunity for members to search for details of individuals who are non-physiotherapists or members who have ceased practicing as a Physiotherapist and who have been given (by our awards panel and full committee) an award to honour them for eminent service rendered to the Organisation.
- **Deferred members**, who, by definition, are Chartered Physiotherapists who are imminently about to start in private practice and who will, upon commencement, become a full member of an organisation that will (if specific consent is given) publicly display their details that will include:
  - Whether HCPC registered, as Physio First check all HCPC registrations once a year i.e. if they are not registered their details will not appear and they would not be a member
  - The likelihood that they are individual members of the Chartered Society of Physiotherapy and therefore have Professional Liability Insurance cover of £7m, which comes with being a member of the CSP
  - Contact and geographical details that related to how they can be contacted to provide treatment
  - Details of the particular physiotherapy treatment they provide and areas of speciality
  - The details of physiotherapists who receive a quarterly journal the remit of which is to support the Physio First Quality Assured Practitioner scheme which is possibly the only third party MSK physiotherapist assessing quality system in the world
- **CSP Visitors**, who, by definition, are Chartered Physiotherapists who are thinking about starting in private practice, and who if they should decide to, are likely to become a member of an organisation that will publicly display their details that will include:

- Whether HCPC registered, as Physio First check all HCPC registrations once a year i.e. if they are not their details will not appear and they would not be a member
- The likelihood that they are individual members of the Chartered Society of Physiotherapy and therefore have Professional Liability Insurance cover of £7m, which comes with being a member of the CSP
- Contact and geographical details that related to how they can be contacted to provide treatment
- Details of the particular physiotherapy treatment they provide areas of speciality
- The details of physiotherapists who receive a quarterly journal the remit of which is to support the Physio First Quality Assured Practitioner scheme which is possibly the only third party MSK physiotherapist assessing quality system in the world

#### 4. How important are those benefits?

The importance of the benefits to:

- **Full, Affiliate, Honorary (Practicing and non-Practicing) and Deferred members** are in not having to expend additional time and energy having to regularly re-consent to the processing of their personal data by an organisation of which they are a member and whose constitutional objectives and strategic priority are as set out in 2 above.
- **Journal Subscribers** are in not having to expend additional time and energy having to re-consent to receiving a quarterly journal and information from a not for profit organisation about opportunities to join or attend an annual conference and post graduate educational courses that all exist to support quality in private physiotherapy practice.
- **CSP Visitors** are in not having to expend additional time and energy having to re-consent to receiving information from a not-for-profit organisation about opportunities to join or attend an annual conference and post graduate educational courses that all exist to support quality in private physiotherapy practice.

#### 5. What would the impact be if you couldn't go ahead?

Ultimately the impact would be the cessation of Physio First as a properly constituted not-for-profit trade association whose membership is optional and that is run by volunteer members who are elected from its membership.

#### 6. Would your use of the data be unethical or unlawful in any way?

No as all data is given freely upon joining Physio First or signing up to be a CSP visitor and must be used in line with our constitutional objectives and strategic reason to exist as outlined in the answer to 1 above.

### Section 2 – The Necessity test.

#### 1. Does this processing actually help to further that interest?

Without the ability to process the personal data in the way described in Section 1 above of the Data Subjects identified there, Physio First would not be able to continue as a viable not-for-profit trade association and professional network of the Chartered Society of Physiotherapy.

#### 2. Is it a reasonable way to go about it?

On the basis that:

- 1) It is very difficult to think how else Physio First may go about it
- 2) Physio First has remained a responsible not-for-profit trade association and professional network of the Chartered Society of Physiotherapy since 1952

this is a reasonable way to go about it.

### 3. Is there another less intrusive way to achieve the same result?

No. There is no less intrusive way to enable Chartered Physiotherapists who have an interest in private physiotherapy to:

- join and/or remain a member of Physio First
- be alerted to or helped to use the member benefits provided
- become informed about the options to attend the Physio First annual conference or post graduate education courses that Physio First provides or facilitates
- have their practices promoted.

## Section 3 – The Balancing test. Consider the impact of your processing and whether this overrides the interest you have identified.

### 1. What is the nature of your relationship with the individual?

The individual Data Subjects identified in Section 1 Question 1 above are all HCPC Registered and Chartered physiotherapists with:

- **Full, Affiliate and Honorary (Practicing and non-Practicing)** being members
- **Deferred members** who are about to become self-employed and thus eligible to become members
- **Journal Subscribers** who choose to pay for and receive the Physio First quarterly journal whose remit is to support the Physio First Quality Assured Practitioner Scheme
- **CSP Visitors** who are interested to have limited non-member access to the website

of Physio First, a not-for-profit trade association and professional network of the Chartered Society of Physiotherapy, whose remit and activities are governed by its constitution and strategic intent.

### 2. Is any of the data particularly sensitive or private?

Article 9 GDPR says that the “*processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited*”. Article 4 GDPR defines ‘*personal data*’ as “*any information relating to an identified or identifiable natural person*” but it does not define “*private*” or “*particularly sensitive*” data. But taking all of the above into account, our assessment of what “*particularly sensitive or private*” data that Physio First holds or processes on the Data Subjects described in Section 1 above is:

- Date of Birth (DoB)
- Gender
- Visual impairment or disability
  - o Given in relation to an enquiry
  - o Submitted in response to surveys
- Bank account number and sort code for those paying by direct debit

### 3. Would people expect you to use their data in this way?

We judge that the data that we hold on the Data Subjects described in Section 1 would expect Physio First to use their personal data in the way described by Physio First, as it is given freely and now fully described in our privacy policy.

#### 4. Are you happy to explain it to them?

Physio First is very happy to and has done so in our Privacy Notice i.e. which itself has to answer the 8 questions, namely:

1. What information is being collected?	6. Who will it be shared with?
2. Who is collecting it?	7. What will be the effect of this on the individuals concerned?
3. How is it collected?	8. Is the intended use likely to cause individuals to object or complain?
4. Why is it being collected?	
5. How will it be used?	

#### 5. Are some people likely to object or find it intrusive?

As Physio First we judge this to be unlikely, but we provide specific opt-outs for those who might change their preferences i.e. they can opt out of:

- receiving our quarterly journal In Touch
- receiving any electronic communications from us (sent from our MRM system database)
- receiving email alerts from us (sent from our MRM database via MailChimp)
- having their details posted on our Find-a-Physio section of our website
- having their details posted on any on-line directory with whom Physio First has a Data Processor agreement.

#### 6. What is the possible impact on the individual?

From the way that Physio First describes the personal data that it obtains and processes from the Data Subjects described in Section 1 i.e. Full, Affiliate, Honorary (Practicing and non-Practicing) and Deferred members as well as Journal Subscribers and CSP Visitors, as Physio First we judge there to be no negative impact.

#### 7. How big an impact might it have on them?

See answer to Section 3 number 6 above.

#### 8. Are you processing children's data?

No, as all Data Subjects identified in Section 1 above, must be over 18.

#### 9. Are any of the individuals vulnerable in any other way?

No, as all Data Subjects identified in Section 1 must be Chartered Physiotherapists, registered with the HCPC, and their data is given freely to us.

#### 10. Can you adopt any safeguards to minimise the impact?

All data is protected – see our separate data protection audit.

#### 11. Can you offer an opt-out?

Physio First can and does offer this and in reverse an opt back in option – see our answer to question 5 above.

## Physio First decision about whether “legitimate interests” is an appropriate “Legal basis” for processing the data of the Data Subjects identified in Section 1 above

The ICO Office guidance advises that once the questions above (see Sections 1, 2 and 3) have been answered that we must make a decision about whether we still think legitimate interests is an appropriate basis.

<b>They also advise that:</b>	<b>Physio First responses:</b>
<ul style="list-style-type: none"> <li>- There’s no fool proof formula for the outcome of the balancing test – but that we must be confident that our legitimate interests are not overridden by the risks we have identified.</li>   <li>- We keep a record of our LIA (i.e. Legitimate Interests Assessment) and the outcome.</li>   <li>- There is no standard format for this, but it’s important to record our thinking to help show we have proper decision-making processes in place and to justify the outcome.</li>   <li>- We keep our LIA under review and refresh it if there is a significant change in the purpose, nature or context of the processing.</li>   <li>- If we are not sure about the outcome of the balancing test, it may be safer to look for another lawful basis.</li>   <li>- Legitimate interests will not often be the most appropriate basis for processing data which is unexpected or high risk.</li>   <li>- If our LIA identifies significant risks, consider whether we need to do a DPIA to assess the risk and potential mitigation in more detail. See our guidance on DPIAs for more on this.</li> </ul>	<ul style="list-style-type: none"> <li>- We are confident that Physio First’s legitimate interests do not override the risks we have identified i.e.               <ul style="list-style-type: none"> <li>- We have a legitimate interest in communicating with members who would reasonably expect to receive communications from us in relation to their membership and our organisation.</li> <li>- We support the first principal of GDPR, i.e. lawful and transparent processing by communicating both digitally and in hard copy to our data subjects and in providing a clear mechanism for opting out of such processing</li> </ul> </li>   <li>- See Sections 1 to 3 above</li>   <li>- See Physio First’s proper decision-making processes above, sections 1 to 3.</li>   <li>- We will write office procedures to ensure that this happens</li>   <li>- We feel confident about the basis of or LIA</li>   <li>- We have not found any of our data processing to be “unexpected” or “high risk”</li>   <li>- We have not found “significant” risk.</li> </ul>