Personal data breach notification policy

1. Introduction

1.1 This policy sets out the policies and procedures of GGPM Limited t/a focusonmy.life (the "**company**") with respect to detection of personal data breaches, responding to personal data breaches and notification of personal data breaches to supervisory authorities, data controllers and data subjects.

1.2 When dealing with personal data breaches, the company and all company personnel must focus on protecting individuals and their personal data, as well as protecting the interests of the company.

2. Definitions

2.1 In this policy:

(a) "**appointed person**" means the individual primarily responsible for dealing with personal data breaches affecting the company, being the data protection officer of the company;

(b) "**data controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

(c) "**data processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(d) "**data subject**" means an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(e) "**personal data**" means any information relating to a data subject;

(f) "**personal data breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed by the company (including any temporary or permanent loss of control of, or inability to access, personal data); and

(g) "**supervisory authority**" means the Information Commissioner's Office of the United Kingdom.

3. Detection of personal data breaches

3.1 The company has put in place technological measures to detect incidents which may result in personal data breaches. As at the date of this policy, those measures include those measures set on it the company's Privacy Policy.

3.2 The company has put in place organisational measures to detect incidents which may result in personal data breaches.

3.3 The company shall regularly review the technical and organisational measures it uses to detect incidents which may result in a personal data breach. Such reviews shall be carried out at least annually.

4. Responding to personal data breaches

4.1 All personnel of the company must notify the appointed person immediately if they become aware of any actual or possible personal data breach.

4.2 The appointed person is primarily responsible for investigating possible and actual personal data breaches and for determining whether any notification obligations apply. Where notification obligations apply, the appointed person is responsible for notifying the relevant third parties in accordance with this policy.

4.3 All personnel of the company must cooperate with the appointed person in relation to the investigation and notification of personal data breaches.

4.4 The appointed person must determine whether the company is acting as a data controller and/or a data processor with respect to each category of personal data that is subject to a personal data breach.

4.5 The steps to be taken by the appointed person when responding to a personal data breach may include:

(a) ensuring that the personal data breach is contained as soon as possible;

(b) assessing the level of risk to data subjects as soon as possible;

(c) gathering and collating information from all relevant sources;

(d) considering relevant data protection impact assessments;

(e) informing all interested persons within the the company of the personal data breach and the investigation;

(f) assessing the level of risk to the company; and

(g) notifying supervisory authorities, data controllers, data subjects and others of the breach in accordance with this policy.

4.6 The appointed person shall keep a full record of the response of the company to a personal data breach, including the facts relating to the personal data breach, its effects and the remedial action taken. This record shall form part of the personal data breach register of the company.

5. Notification to supervisory authority

5.1 This section 5 applies to personal data breaches affecting personal data with respect to which the company is acting as a data controller.

5.2 The company must notify the supervisory authority of any personal data breach to which this section 5 applies without undue delay and, where feasible, not later than 72 hours after the company becomes aware of the breach, save as set out in subsection 5.4.

5.3 Personal data breach notifications to the supervisory authority must be made by the appointed person using the form set out in schedule 1 (Notification of personal data breach to supervisory authority). The completed form must be sent to the supervisory authority by secure and confidential means. The appointed person must keep a record of all notifications, and all other communications with the supervisory authority relating to the breach, as part of the personal data breach register of the company.

5.4 The company will not notify the supervisory authority of a personal data breach where it is unlikely to result in a risk to the rights and freedoms of natural persons. The appointed person shall be responsible for determining whether this subsection 5.4 applies, and the appointed person must create a

record of any decision not to notify the supervisory authority. This record should include the appointed person's reasons for believing that the breach is unlikely to result in a risk to the rights and freedoms of natural person. This record shall be stored as part of the personal data breach register of the company.

5.5 To the extent that the company is not able to provide to the supervisory authority all the information specified in schedule 1 (Notification of personal data breach to supervisory authority) at the time of the initial notification to the supervisory authority, the company must make all reasonable efforts to ascertain the missing information. That information must be provided to the supervisory authority, by the appointed person, as and when it becomes available. The appointed person must create a record of the reasons for any delayed notification under this subsection 5.5. This record shall be stored as part of the personal data breach register of the company.

5.6 The company must keep the supervisory authority informed of changes in the facts ascertained by the company which affect any notification made under this section 5.

6. Notification to data controller

6.1 This section 6 applies to personal data breaches affecting personal data with respect to which the company is acting as a data processor.

6.2 The company must notify the affected data controller(s) of any personal data breach to which this section 6 applies without undue delay.

6.3 Personal data breach notifications to the affected data controller(s) must be made by the appointed person using the form set out in schedule 2 (Notification of personal data breach to data controller). The completed form must be sent to the affected data controller(s) by secure and confidential means. The appointed person must keep a record of all notifications, and all other communications with the affected data controller(s) relating to the breach, as part of the personal data breach register of the company.

7. Notification to data subjects

7.1 This section 7 applies to personal data breaches affecting personal data with respect to which the company is acting as a data controller.

7.2 Notifications to data subject under this section 7 should, where appropriate, be made in consultation with the supervisory authority and in accordance with any guidance given by the supervisory authority with respect to such notifications.

7.3 The company must notify the affected data subjects of any personal data breach to which this section 7 applies if the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, save as set out in subsection 7.5.

7.4 Personal data breach notifications to the affected data subjects must be made by the appointed person in clear and plain language using the form set out in schedule 3 (Notification of personal data breach to data subject). The completed form must be sent to the affected data subjects by appropriate means. The appointed person must keep a record of all notifications, and all other communications with the affected data subjects relating to the breach, as part of the personal data breach register of the company.

7.5 The company has no obligation to notify the affected data subject of a personal data breach if:

(a) the company has implemented appropriate technical and organisational protection measures (in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption), and those measures have been applied to the personal data affected by the personal data breach;

(b) the company has taken subsequent measures which ensure that a high risk to the rights and freedoms of data subjects is no longer likely to materialise;

(c) it would involve disproportionate effort (in which case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner),

providing that the appointed person shall be responsible for determining whether this subsection 7.5 applies, and the appointed person must create a record of any decision not to notify the affected data subjects. This record should include the appointed person's reasons for believing that the breach does not need to be notified to the affected data subjects. This record shall be stored as part of the personal data breach register of the company.

7.6 If the company is not required by this section 7 to notify affected data subjects of a personal data breach, the company may nonetheless do so where such notification is in the interests of the company and/or the affected data subjects.

8. Other notifications

8.1 Without affecting the notification obligations set out elsewhere in this policy, the appointed person should also consider whether to notify any other third parties of a personal data breach. Notifications may be required under law or contract. Relevant third parties may include:

(a) the police;

(b) other law enforcement agencies;

(c) insurance companies; and/or

(d) regulatory authorities.

SCHEDULE 1 (NOTIFICATION OF PERSONAL DATA BREACH TO SUPERVISORY AUTHORITY)

1. Introduction

This personal data breach notification is made by [*[INDIVIDUAL NAME]* of *[address]*] OR [*[COMPANY NAME]*, a company incorporated in England and Wales (registration number *[registration number]*) having its registered office at *[address]*] OR [*[PARTNERSHIP NAME]*, a partnership established under the laws of England and Wales having its principal place of business at *[address]*].

2. Description of personal data breach

[Describe circumstances of personal data breach, including date and time when data controller became aware of the breach]

3. Categories of data subject affected

[Specify categories of data subject affected]

4. Number of data subjects affected

[Insert number or approximate number of data subjects affected]

5. Categories of personal data concerned

[Specify categories of personal data concerned]

6. Number of records concerned

[Insert number or approximate number of records concerned]

7. Likely consequences of breach

[Identify likely consequences of breach]

8. Measures taken to address breach

[Describe measures taken to address breach]

9. Has breach been notified to data subjects?

The breach [has] OR [has not] been notified to affected data subjects. The reason for not notifying affected data subjects is *[specify reason]*.

10. Late report of breach

The breach is being reported more than 72 hours after the data controller became aware of the breach because *[give reasons]*.

11. Contact details

The name of the person responsible for handling the breach is *[insert name]*, and [his] OR [her] contact details are as follows: *[insert contact details]*.

SCHEDULE 2 (NOTIFICATION OF PERSONAL DATA BREACH TO DATA CONTROLLER)

1. Introduction

This personal data breach notification is made by [*[INDIVIDUAL NAME]* of *[address]*] OR [*[COMPANY NAME]*, a company incorporated in England and Wales (registration number *[registration number]*) having its registered office at *[address]*] OR [*[PARTNERSHIP NAME]*, a partnership established under the laws of England and Wales having its principal place of business at *[address]*].

2. Description of personal data breach

[Describe circumstances of personal data breach, including date and time when data controller became aware of the breach]

3. Categories of data subject affected

[Specify categories of data subject affected]

4. Number of data subjects affected

[Insert number or approximate number of data subjects affected]

5. Categories of personal data concerned

[Specify categories of personal data concerned]

6. Number of records concerned

[Insert number or approximate number of records concerned]

7. Likely consequences of breach

[Identify likely consequences of breach]

8. Measures taken to address breach

[Describe measures taken to address breach]

9. Contact details

The name of the person responsible for handling the breach is *[insert name]*, and [his] OR [her] contact details are as follows: *[insert contact details]*.

SCHEDULE 3 (NOTIFICATION OF PERSONAL DATA BREACH TO DATA SUBJECT)

1. Introduction

This personal data breach notification is made by [*[INDIVIDUAL NAME]* of *[address]*] OR [*[COMPANY NAME]*, a company incorporated in England and Wales (registration number *[registration number]*) having its registered office at *[address]*] OR [*[PARTNERSHIP NAME]*, a partnership established under the laws of England and Wales having its principal place of business at *[address]*].

2. Description of personal data breach

[Describe circumstances of personal data breach, including date and time when data controller became aware of the breach]

3. Categories of personal data concerned

[Specify categories of personal data concerned]

4. Likely consequences of breach

[Identify likely consequences of breach]

5. Measures taken to address breach

[Describe measures taken to address breach]

6. Steps to mitigate breach

[Insert details of steps data subject may take to mitigate personal data breach]

7. Contact details

The name of the person responsible for handling the breach is *[insert name]*, and [his] OR [her] contact details are as follows: *[insert contact details]*.