NHS Pando Processor Audit and Due Diligence Report

Authored: 23/02/2021
Updated: 16/01/2023(DPO)
Next review date: January 2024
Version 1.3

Version	Purpose	Date	Author	Authorised Date
1.1	Formalise supply chain audit	23/02/2021	Claire Robinson DPO	23/02/2021
1.2	Reintroduce Google Analytics	19/04/2021	Claire Robinson DPO	19/04/2021
1.3	Review as part of overall review of IG documents	16/01/2023	Claire Robinson	16/01/2023

Processor details (1):	
Processor Organisation Name	**Amazon Web Services** see AWS Privacy (amazon.com) (UK and EU compliant) The DPA forms part of the online terms and conditions see https://aws.amazon.com/blogs/security/tag/data-processing-agreement/ hence the DPA automatically applies.
Subject matter of the Processing	Infrastructure hosting provider for the Pando products and services.
Duration of the Processing	The Processing will take place over the duration of the relevant Service Instance, except that storage of any data item that may require retention for purposes of historical review or audit, shall be retained by Pando for a period which is no longer than is necessary for those purposes.
Nature and purposes of Processing	Secure message communications occur between parties' devices, data is encrypted in transit and at rest, and storage is solely in the UK or EEA. Amazon Web Services (AWS) Encryption Keys are held in the UK and AWS has no access to them by any technical means. Some metadata is collected to provide additional context about the way their service is being used and for safety and monitoring purposes. Data is required to fulfil the **contract.**
Type of Personal Data	Set by the user/data controller in terms of message data - see above. Users' email addresses and Trust are collected to facilitate logins.
Categories of Data Subjects	Users: Clinicians, affiliated personnel at a Trust Organisation administrative and support staff.
Plan for return and destruction of the data once the Processing is complete	At the controller's choice, at the end of the contract, Pando requires all sub processors to delete or return all the personal data it has been processing for it; and delete existing copies of the personal data unless UK law requires it to be stored. Deletion of personal data is done in a secure manner, in accordance with the security requirements of Article 32 of the GDPR.

Processor details (2):	
Processor Organisation Name	**Google Analytics** is a web analytics service offered by Google that tracks and reports website traffic, currently as a platform inside the Google Marketing Platform see **https://policies.google.com/privacy?hl=en-GB** DPA: https://www.google.com/analytics/terms/dpa/dataprocessingamendment_20130906.html
Subject matter of the Processing	Google Analytics is deployed to collect standard internet log information and details of visitor behaviour patterns. We do this to find out such things as the number of visitors to the various parts of the site. This information is only processed in a way that does not directly identify anyone. We do not make, and do not allow Google to make, any attempt to find out the identities of those visiting our website. It is categorised as “Analytics software”.
Duration of the Processing	The Processing will take place over the duration of the relevant Service Instance, except that storage of any data item that may require retention for purposes of historical review or audit, shall be retained by Pando for a period which is no longer than is necessary for those purposes.
Nature and purposes of Processing	Personal Data is collected for the purpose of providing the Services in order to improve the service delivered as part of the **contract.** The cookie preferences management software on the website collects advance **consent** for this processing.
Type of Personal Data	The type of information collected through the Google Analytics for Firebase implementation includes: ● Internet log information ● Visitor behaviour pattern ● Number of site visitors **Only Anonymised data is processed.**
Categories of Data Subjects	Clinicians, Affiliated personnel at a Trust Organisation Administrative and support staff Website users
Plan for return and destruction of the data once the Processing is complete	At the controller’s choice, at the end of the contract, Pando requires all processors to delete or return all the personal data it has been processing for it; and delete existing copies of the personal data unless UK law requires it to be stored. Deletion of personal data is done in a secure manner, in accordance with the security requirements of Article 32 of the GDPR.

Processor details (3):	
Processor Organisation Name	**Google Firebase** is a Backend-as-a-Service (Baas). It provides developers with a variety of tools and services to help them develop quality apps. Firebase is categorised as a NoSQL database program, which stores data in JSON-like documents (UK and EU compliant) see https://firebase.google.com/support/privacy DPA: https://firebase.google.com/terms/data-processing-terms
Subject matter of the Processing	Firebase is deployed to manage data about prospects and customers and their interactions with Beacon Medical Systems Ltd. trading as Pando. The Service falls in the global category of "Analytics software".
Duration of the Processing	The Processing will take place over the duration of the relevant Service Instance, except that storage of any data item that may require retention for purposes of historical review or audit, shall be retained by Pando for a period which is no longer than is necessary for those purposes.
Nature and purposes of Processing	Personal Data is collected for the purpose of providing the Services in order to fulfil the **contract.**
Type of Personal Data	The type of information collected through the Google Analytics for Firebase implementation includes: ● Number of users and sessions ● Session duration ● Operating systems ● Device models ● Geography ● First launches ● App opens ● App updates ● In-app purchases
Categories of Data Subjects	Clinicians, Affiliated personnel at a Trust Organisation Administrative and support staff
Plan for return and destruction of the data once the Processing is complete	At the controller's choice, at the end of the contract, Pando requires all processors to delete or return all the personal data it has been processing for it; and delete existing copies of the personal data unless UK law requires it to be stored. Deletion of personal data is done in a secure manner, in accordance with the security requirements of Article 32 of the GDPR.

Processor details (4):	
Processor Organisation Name	**Hubspot** as a CRM solution (UK and EU compliant) see https://legal.hubspot.com/privacy-policy DPA: https://legal.hubspot.com/dpa
Subject matter of the Processing	HubSpot is deployed to manage data about prospects and customers and their interactions with Beacon Medical Systems Ltd. trading as Pando. The Service falls in the global category of "Lead management and CRM software".
Duration of the Processing	The Processing will take place over the duration of the relevant Service Instance, except that storage of any data item that may require retention for purposes of historical review or audit, shall be retained by Pando for a period which is no longer than is necessary for those purposes.

Nature and purposes of Processing	Personal Data is collected for the purpose of providing the Services in order to fulfil the **contract.**
Type of Personal Data	Name Email Address, Work address (in some cases) Phone Number
Categories of Data Subjects	Clinicians, Affiliated personnel at a Trust Organisation Administrative and support staff
Plan for return and destruction of the data once the Processing is complete	At the controller's choice, at the end of the contract, Pando requires all processors to delete or return all the personal data it has been processing for it; and delete existing copies of the personal data unless UK law requires it to be stored. Deletion of personal data is done in a secure manner, in accordance with the security requirements of Article 32 of the GDPR.

Processor details (5):	
Processor Organisation Name	**Intercom** for live chat (UK and EU compliant) see Privacy Policy | Intercom **https://www.intercom.com/help/en/articles/1385437-how-intercom-complies-with-gdpr**
Subject matter of the Processing	Intercom is deployed as a messaging application for providing online user support.
Duration of the Processing	The Processing will take place over the duration of the relevant Service Instance, except that storage of any data item that may require retention for purposes of historical review or audit, shall be retained by Pando for a period which is no longer than is necessary for those purposes.
Nature and purposes of Processing	Personal Data is collected for the purpose of providing the Services in order to provide support services necessary to fulfil the **contract.**
Type of Personal Data	Name Employer/Trust Name Email Address
Categories of Data Subjects	Clinicians, Affiliated personnel at a Trust Organisation Administrative and support staff
Plan for return and destruction of the data once the Processing is complete	At the controller's choice, at the end of the contract, Pando requires all sub processors to delete or return all the personal data it has been processing for it; and delete existing copies of the personal data unless UK law requires it to be stored. Deletion of personal data is done in a secure manner, in accordance with the security requirements of Article 32 of the GDPR.

Processor details (6): Complete the rows below for each Processor involved in the above processing – the entries will typically be a subset of the information provided above. If you do not use any Processors, state "None used".	
Processor Organisation Name	**Mixpanel** see GDPR - Mixpanel performance improvement [UK and EU compliant] **DPA Link: https://mixpanel.com/legal/dpa/**

Subject matter of the Processing	Mixpanel is deployed for performance improvement
Duration of the Processing	The Processing will take place over the duration of the relevant Service Instance, except that storage of any data item that may require retention for purposes of historical review or audit, shall be retained by Pando for a period which is no longer than is necessary for those purposes.
Nature and purposes of Processing	Performance improvement as part of the contract**.**
Type of Personal Data	Anonymised user data.
Categories of Data Subjects	Clinicians, Affiliated personnel at a Trust Organisation Administrative and support staff but data is anonymised.
Plan for return and destruction of the data once the Processing is complete	At the controller's choice, at the end of the contract, Pando requires all sub processors to delete or return all the personal data it has been processing for it; and delete existing copies of the personal data unless UK law requires it to be stored. Deletion of personal data is done in a secure manner, in accordance with the security requirements of Article 32 of the GDPR.

Processor details (7): Complete the rows below for each Processor involved in the above processing – the entries will typically be a subset of the information provided above. If you do not use any Processors, state "None used".	
Processor Organisation Name	**Slack** see **https://slack.com/intl/en-gb/trust/compliance/gdpr** [UK and EU compliant] **DPA Link: https://slack.com/intl/en-gb/terms-of-service/data-processing**
Subject matter of the Processing	Slack is deployed as a messaging application to allow Pando's teams to manage support requests from users.
Duration of the Processing	The Processing will take place over the duration of the relevant Service Instance, except that storage of any data item that may require retention for purposes of historical review or audit, shall be retained by Pando for a period which is no longer than is necessary for those purposes.
Nature and purposes of Processing	Personal Data is collected for the purpose of providing the Services in order to provide support services necessary to fulfil the **contract.**
Type of Personal Data	Name Employer/Trust Name Email Address
Categories of Data Subjects	Clinicians, Affiliated personnel at a Trust Organisation Administrative and support staff
Plan for return and destruction of the data once the Processing is complete	At the controller's choice, at the end of the contract, Pando requires all sub processors to delete or return all the personal data it has been processing for it; and delete existing copies of the personal data unless UK law requires it to be stored. Deletion of personal data is done in a secure manner, in accordance with the security requirements of Article 32 of the GDPR.

Processor details (8):

Processor Organisation Name	**Wootric** see **http://help.wootric.com/en/articles/1832588-wootric-and-gdpr-compliance** performance improvement, customer experience improvement [UK and EU compliant] **DPA Link: see above.**
Subject matter of the Processing	Wootric is deployed to assist the full cycle of CX management to benefit the users' experience. Providing such feedback is entirely voluntary.
Duration of the Processing	The Processing will take place over the duration of the relevant Service Instance, except that storage of any data item that may require retention for purposes of historical review or audit, shall be retained by Pando for a period which is no longer than is necessary for those purposes.
Nature and purposes of Processing	Experience improvement and feedback under contract although there is no obligation to provide data on the part of a user.
Type of Personal Data	Email address.
Categories of Data Subjects	Clinicians, Affiliated personnel at a Trust Organisation Administrative and support staff but data is anonymised.
Plan for return and destruction of the data once the Processing is complete	At the controller's choice, at the end of the contract, Pando requires all sub processors to delete or return all the personal data it has been processing for it; and delete existing copies of the personal data unless UK law requires it to be stored. Deletion of personal data is done in a secure manner, in accordance with the security requirements of Article 32 of the GDPR.