Data Processing Agreement

Ashford Orthodontics Ltd

Document Ref.	**Ashford**
Version:	**1**
Dated:	**09 May 2018**

1 Parties to the Agreement

The Controller: Practice name

The Processor: Ashford Orthodontics Ltd

2 Scope and Roles

2.1 This agreement applies to the processing of Personal Data, within the scope of the GDPR, by the Processor on behalf of the Controller.

2.2 For purposes of this agreement, [Controller Name] and Ashford Orthodontics Ltd agree that [Controller Name] is the Controller of the Personal Data and Ashford Orthodontics Ltd is the Processor of such data. In the case where [Controller Name] acts as a Processor of Personal Data on behalf of a third party, [Processor Name] shall be deemed to be a Sub-Processor.

2.3 These Terms do not apply where Ashford Orthodontics Ltd is a Controller of Personal Data.

3 Definitions

3.1 For the purposes of this Agreement, the following definitions shall apply:

Agreement	This data processing agreement
GDPR	means 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, and repealing Directive 95/46/EC (General Data Protection Regulation)
Personal Data	means that data, meeting the definition of "personal data" as defined in Article 4 of the GDPR, that is provided by [Controller Name] to Ashford Orthodontics Ltd in order to perform the processing as defined in Schedule 1 of this Agreement.
Sub-Processor	means a natural or legal person, public authority, agency or body other than the data subject, Controller and Processor who, under the direct authority of the Processor, are authorised to process Personal Data for which [Controller Name] is the Controller

Terms used but not defined in this Data Processing Agreement (e.g., “processing”, “controller”, “processor”, “data subject”) shall have the same meaning as in Article 4 of the GDPR.

4 The Processing

4.1 The subject matter, duration, nature and purpose of the Processing, and the types of Personal Data and categories of data subjects shall be as defined in Schedule 1 of this Agreement.

5 Obligations and rights of the controller

5.1 Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the Controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that Processing is performed in accordance with the GDPR. Those measures shall be reviewed and updated where necessary.

5.2 Where proportionate in relation to Processing activities, the measures referred to in paragraph 5.1 shall include the implementation of appropriate data protection policies by the Controller.

5.3 The Controller shall implement appropriate technical and organisational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the Processing are processed. That obligation applies to the amount of Personal Data collected, the extent of their Processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default Personal Data are not made accessible without the individual's intervention to an indefinite number of natural persons.

6 Obligations of the Processor

6.1 The Processor shall:

6.1.1 process the Personal Data only on documented instructions from the Controller;

6.1.2 ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

6.1.3 take all measures required pursuant to Article 32 of the GDPR, namely to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk to the rights and freedoms of natural

persons including, as a minimum, the measures set out in Schedule 2 of this Agreement;

6.1.4 respect the conditions referred to in paragraphs 2 and 4 of Article 28 of the GDPR for engaging another Processor, namely that the Processor may not engage another Processor (Sub-Processor) without the prior authorisation of the Controller. Those Sub-Processors that are authorised by the Controller at the date of this agreement are listed in Schedule 3. In cases where another Processor is engaged, the Sub-Processor must be subject to the same contractual terms as described in this Agreement;

6.1.5 assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR;

6.1.6 assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, relating to security of Processing, Personal Data Breaches and data protection impact assessments;

6.1.7 at the choice of the Controller, delete or return all the Personal Data to the Controller after the end of the provision of services relating to Processing, and delete existing copies unless applicable law requires storage of the Personal Data;

6.1.8 make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller;

7 Duration and Applicable Law

7.1 This Agreement shall continue in effect for so long as the Processor is processing Personal Data on behalf of the Controller.

7.2 This Agreement shall be governed by the laws of England and Wales and subject to the exclusive jurisdiction of the courts of England and Wales.

8 Signatures

Signed for and on behalf of [Controller Name]:

Signature	
Name	
Title	
Date	

Signed for and on behalf of Ashford Orthodontics Ltd.

Signature	
Name	Craig Stevens
Title	Director
Date	11/5/2018

SCHEDULE 1 – Description of the Processing

Subject matter and duration of the Processing	The processing relates to patient data from the controller which may consist of name or patient id number, the data is kept indefinitely.
Nature and purpose of the Processing	The purpose of the process is to enable both parties to identify impressions or scans for production of appliances or for invoicing
Type of Personal Data and categories of data subjects	The personal data created is in accordance to this agreement satisfies the requirements of article 5 of the general data protection regulations 2016

SCHEDULE 2 – Technical and Organisational Measures

The following security measures shall be implemented by the Processor, as a minimum:

Section 1. Ashford Orthodontics Ltd

What data does Ashford store? Ashford Orthodontics Ltd stores data some on your behalf the database of your orders, customers, invoices. The personal data we need to protect is your; Customer names and email addresses, Patient details (if present) on orders.

Where is the data stored? Primarily the data is stored in our lab offices on the Labtrac database, this is protected by us and procedures are in place to secure our computer systems. The Labtrac cloud backup service which takes a copy of our database and stores it offsite uses the Microsoft Azure Datacentre in the UK, these files are also encrypted when they are stored. We also have the Labtrac cloud platform which has a synced copy of your data to run the applications like https://app.labtrac.com and https://dashboard.labtrac.com , this also uses the Microsoft Azure services within the UK and the highest level of security and data encryption when transferring the data.

Does Labtrac use any subcontractors or suppliers? Labtrac uses a number of software vendors to provide your systems. Each one of these is GDPR compliant. Currently these providers are:

- Microsoft Azure
- SendGrid (sending emails)
- Trello (stores your support requests)
- Teamviewer (remote support)

What does Labtrac use the data for? We only use data to provide the systems and services that you buy from us. We don't sell or forward on the data to any other parties. Each of the Labtrac systems has up to date terms and conditions that confirm how we use the data.

Using Teamviewer? Labtrac uses Teamviewer for our remote support. They have made the steps to be GDPR compliant https://community.teamviewer.com/t5/Knowledge-Base/TeamViewer-and-GDPR/tap/33344 We don't store any of your personal data or your customer data on TeamViewer, it is simply used to remote connect to your desktop. We are changing the way we use TeamViewer passwords, from now on we will change the password setting on each of your desktop computers to give a new password every time we need to connect. You will then have tel us this password when we help you with a support request. This makes TeamViewer as secure as possible and we recommend you insist on this policy for all of your suppliers.

Digital 3D data storage. Digital data is primarily stored on Ashford Orthodontics main office site, all relevant internal data protection policies are in

place to protect any giving data received from the controller no personal patient data is received and we do advice practices to use patient numbers and not names for further protection.

Data is also backed up on the cloud platform this is done using Amazon S3 servers. As of this writing, there are fourteen regions where data is stored : US East (Northern Virginia), US East (Ohio), US West (Oregon), US West (Northern California), AWS GovCloud (US)
(Oregon), EU (Frankfurt), EU (Ireland), Asia Pacific (Seoul), Asia Pacific (Mumbai), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), China (Beijing), and South America (Sao Paulo (b) they are managed by a 3rd party entity and they are ISO27001 certified and compliant.

SCHEDULE 3 – Sub-Processors

As at the date of this agreement, the Sub-Processors we use have been notified by the Processor to the Controller with respect to the Processing: