



Privacy Notice

Published on 11th January 2021.

What does this notice cover:

You can either scroll down to read this notice in its entirety, or click on one of the links below to go straight to the section you are interested in.

1. [About us and our apps](#)
2. [Purpose of this notice](#)
3. [Data Protection Legislation](#)
4. [Data protection roles and responsibilities](#)
5. [Our use of patients' data as a data processor on behalf of our customers](#)
 1. [The personal data we collect](#)
 2. [How we collect personal data](#)
 3. [How and why we use personal data](#)
 4. [Who we share personal data with](#)
 5. [How long we keep personal data](#)
 6. [Information security](#)
6. [Our use of patients' data as the data controller on our own behalf](#)
 1. [The personal data we collect](#)
 2. [How we collect personal data](#)
 3. [How and why we use personal data](#)
 4. [Who we share personal data with](#)
 5. [How long we keep personal data](#)
 6. [Information security](#)
 7. [Data protection rights](#)
 8. [Complaints](#)

1. About us and our apps

Who we are

We are Appy Solutions Ltd, a company incorporated and registered in England and Wales with company number 12099226. Our registered office is at 71-75 Shelton Street, Covent Garden, London, United Kingdom, WC2H 9JQ.

About us and our apps

We provide mobile apps for use by licensed clinics and their patients. Our apps are used by clinics to provide pre-operative and post-operative information and advice to their patients in respect of surgical procedures (for example, hair transplants). This includes non-medical information (for example, location, travel and accommodation) and medical care instructions. The clinics use our apps to deliver daily instructions to their patients, so that their patients know exactly what they need to do, when they need to do it and what they can't do.

How to contact us

If you have any questions, comments or complaints in regard to this notice or our processing of patients' personal data, please contact us at support@hairtransplant.app, using the support buttons within the app, or the above address.

[Back to Contents](#)

2. Purpose of this notice

This document serves as our transparency notice on data protection. It sets out how we process the personal information of patients using our apps. It is aimed at clinics and patients using our apps.

Personal data means information that relates to an identified or an identifiable individual.



[Back to Contents](#)

3. Data Protection Legislation

Our use of personal data is subject to data protection laws applicable in the United Kingdom. On the date of the publication of this notice, these laws include the EU General Data Protection Regulation (**GDPR**), the UK Data Protection Act 2018, and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (together **Data Protection Legislation**).

Even though the United Kingdom has left the European Union, the EU General Data Protection Regulation continues to apply in the United Kingdom during the transition period, until the end of 2020.

[Back to Contents](#)

4. Data protection roles and responsibilities

Our use of patients' data as a data processor on behalf of clinics

We offer our apps to clinics. They are our customers and, for the purposes of the Data Protection Legislation, they the **data controllers** of the personal data of their patients (**data subjects**) processed through our apps. This means that the clinic is responsible for determining the purposes and means of processing their patient's data.

When a clinic chooses to use our app and creates a user account for their patient on our app, they engage us to process the personal data of their patient on their behalf and in accordance with their instructions, as their **data processor**.

The Data Protection Legislation specifies that the processing of personal data by a data processor must be governed by a written contract with the data controller and it must comply with Article 28 of the GDPR. Our use of patients' data is governed by our contract with the clinic. That contract includes appropriate terms mandated by the GDPR, which ensure that we can only process patients' information as instructed by the clinic.

For further information about our processing of patients' information as a data processor, see section 5 of this notice.

Our use of patients' data as the data controller on our own behalf

When our customer's patient signs up to our app for the first time, they must agree to our [End User Licence Agreement](#). That document is a contract between us and the patient. It provides information, which we are required by consumer law to disclose to users, and sets out the terms and conditions on which we permit them to use our app. For example, it covers the acceptable use restrictions aimed at protecting our apps, systems and other users of our apps.

If a patient breaches those terms and conditions, we might have to take action to enforce them against that patient. For example, if a patient uses our app in an inappropriate way, we may have to block their access to the app. We may also need to use patients' information, such as their login credentials or the way they use our app, to protect our app and business (for example, for user authentication or troubleshooting). When we use personal data of patients in these ways, we do that for our own purposes as the **data controllers**.

For further information about our processing of patients' information as the data controller, see section 6 of this notice.

[Back to Contents](#)

5. Our use of patients' data as a data processor on behalf of our customers



This section provides privacy information in respect of our use of personal information of patients as data processors acting on behalf of clinics – the data controllers. See section 4 of this notice for an explanation of what this means.

[Back to Contents](#)

1. The personal data of patients processed through our apps

Types of personal data	Examples
Identity data	name; gender;
Contact data	email address; language; time zone;
Surgery data	surgery date; details of the clinic undertaking the surgery; pre-surgery documents provided by the clinic (for example, confirmation letter);
Health data	pre-operative and post-operative care information and instructions provided by the clinic to the patient (including instructional videos); mobile notification reminders from the clinic to the patient; messages from the clinic to the patient.

[Back to Contents](#)

2. How we collect personal data

Most of the information set out in in section 5.1 above will be inputted onto our apps by the clinic looking after the patient. They will create an account for their patient on our app and will invite that patient to use it. The clinic will provide the in-app information and instructions for the patient and send messages to the patient using the app.

[Back to Contents](#)

3. How and why we use personal data

Under the Data Protection Legislation, data controllers can only use personal data if they have a lawful basis to do so under Article 6 of the GDPR. These include: consent, contract, legal obligation, vital interests, public task or legitimate interests. It is the clinic's responsibility to determine the lawful bases they rely on when using personal information of their patients on our apps. This includes all purposes that the clinic may decide to use our app for, whether it is surgery aftercare or clinic's marketing communication.

We process that data in order to provide our app services to the clinic.

[Back to Contents](#)

4. Who we share personal data with

The personal data set out in section 5.1 of this notice is directly shared only with the clinic responsible for the patient.

We use the following third party suppliers to operate our apps. These are:



- Amazon Web Services (AWS), a US company that provides data hosting services to us. AWS host our data in France; and
- Bright Idea, a company based in Croatia that provides app development services to us.

These suppliers act as **sub-processors** on behalf of the clinics. We impose contractual obligations on our suppliers compliant with Article 28 of the GDPR to ensure that the personal data of patients is protected.

We do not transfer personal data to suppliers based outside the European Economic Area.

[Back to Contents](#)

5. How long we keep personal data

We will only keep the personal data set out in section 5.1 of this notice for the purposes set out in section 5.3 of this notice until:

- the clinic instructs us to stop; or
- the patient closes their account on our app,

whichever is earlier. However, if a patient closes their account on our app but the clinic instructs us to retain their data for a longer period of time, we will have to comply with the clinic's instructions, because they are the controller of that data.

[Back to Contents](#)

6. Information security

We have appropriate security measures to prevent personal data from being accidentally lost, or used or accessed unlawfully. We limit access to personal data of individuals to those who have a genuine business need to access it. Those processing personal data will do so only in an authorised manner and are subject to a duty of confidentiality. We also have procedures in place to deal with any suspected data security breach.

[Back to Contents](#)

7. Data protection rights

Where we act as a data processor and receive a request from a patient in respect of the exercise of their data protection rights (for example, the rights of access or data erasure), we will notify the data controller (the clinic responsible for that patient's personal information). We will then follow the data controller's instructions in respect of that patient's request.

[Back to Contents](#)

6. **Our use of patients' data as the data controller on our own behalf**

This section provides privacy information in respect of our use of personal information of patients as the data controllers acting on our own behalf. See section 4 of this notice for an explanation of what this means.

1. The personal data we collect through our app

Types of personal data	Examples
Identity data	name;



Contact data	email address; language; time zone;
Contract data	version of our End User Licence Agreement accepted by the patient and date when it was accepted;
Usage data	login credentials; features of our app accessed by the patients; enquires received from the patient (for example, using our in-app help support buttons);
Technical data	app permissions; login data; internet protocol (IP) address; device ID; IMEI number; browser type and version; time zone setting; device type; operating system and platform and other technology on the devices used to access the app.

Anonymised data

We may also collect, use, and share anonymised, aggregated data such as statistical or demographic data for any purpose. Anonymised data may be derived from your personal data but is not considered personal information in law as this information does not directly or indirectly reveal your identity. For example, we may aggregate information on how users use our app to calculate the percentage of users accessing a specific app feature.

[Back to Contents](#)

2. How we collect personal data

Type of source	Examples
User's use of our app	when a patient user signs up to and uses our app; as they interact with our app, we may automatically collect technical data about their device and usage of our app;
Direct interactions with users	when they contact us.

[Back to Contents](#)

3. How and why we use personal data

Under the Data Protection Legislation, we can only use personal data if we have a lawful basis to do so under Article 6 of the General Data Protection Regulation, for example: consent, contract, legitimate interests or legal obligation.

- a) **Contract.** We will use personal data of users (patients) where it is necessary for the performance of our obligations under our [End User Licence Agreement](#). For example, if we need to enable users to use our app features or respond to their queries.
- b) **Legitimate interests.** We may process users' personal data when we (or a third party) have a legitimate reason to use it, so long as this is not overridden by that user's rights and interests. For example:



- to administer and protect our app, systems and business (including troubleshooting, data analysis, system maintenance, support, reporting and hosting of data);
 - to create anonymous aggregated data derived from the users' personal data and use it to improve or increase our business;
 - to ensure information security and proper functioning of our app;
 - for the prevention and detection of fraud and spam; and
 - for the establishment, exercise or defence of legal claims.
- c) **Legal obligation.** We may process personal data of users to comply with our legal obligations. For example:
- to notify users about changes to this Privacy Notice or our End User Licence Agreement;
 - to address a data protection request or complaint; or
 - to comply with a request of a competent authority.

We do not use patients' information set out in section 6.1 of this notice for direct marketing purposes.

[Back to Contents](#)

4. Who we share personal data with

We may share personal data of our app users set out in section 6.1 of this notice with third parties for the purposes set out in section 6.3 of this notice.

Suppliers. We use the following third party suppliers to operate our apps. These are:

- Amazon Web Services (AWS), a US company that provides data hosting services to us. AWS host our data in France; and
- Bright Idea, a company based in Croatia that provides app development services to us.

These suppliers act as our **processors** on our behalf. We impose contractual obligations on our suppliers compliant with Article 28 of the GDPR to ensure that the personal data of our app users is protected.

We do not transfer personal data to suppliers based outside the European Economic Area.

Other sharing. We may also:

- share personal data with members of our staff;
- disclose personal data to professional advisers (e.g. lawyers, accountants, auditors or insurers) who provide professional services to us;
- disclose and exchange certain information with law enforcement agencies and regulatory bodies to comply with our legal obligations; and
- share some personal data with other parties, such as potential and actual investors or buyers of some or all of our business or during a re-structuring.

Such data recipients will be bound by confidentiality obligations.

[Back to Contents](#)



5. How long we keep personal data

We will only retain the personal data set out in section 6.1 of this notice for the purposes set out in section 6.3 of this notice for as long as reasonably necessary to fulfil the purposes it was collected for. This will usually be only until the user closes their account on our app. We may retain an individual's personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with that individual.

We may also anonymise personal data for analytics, research or statistical purposes, in which case we may use this information indefinitely without further notice.

[Back to Contents](#)

6. Information security

We have appropriate security measures to prevent personal data from being accidentally lost, or used or accessed unlawfully. We limit access to personal data of individuals to those who have a genuine business need to access it. Those processing personal data will do so only in an authorised manner and are subject to a duty of confidentiality. We also have procedures in place to deal with any suspected data security breach.

[Back to Contents](#)

7. Data protection rights

Our app users have a number of rights in relation to their personal data, which allow them to access and control their information in certain circumstances. They can exercise these rights free of charge, unless their request is manifestly unfounded or excessive (in which case we may charge a reasonable administrative fee or refuse to respond to such request).

Your right	Explanation
Access	The right to receive a copy of the personal data we hold about the individual and to check that we are lawfully processing it.
Rectification	The right to require us to correct any inaccuracies in personal data.
Erasure (to be forgotten)	The right to require us to delete personal data in certain situations.
Restriction of processing	The right to require us to restrict processing of personal data in certain circumstances (e.g. if the individual contests the accuracy of the data we hold).
Data portability	The right to receive, in certain situations, the personal data provided to us by the individual, in a structured, commonly used and machine-readable format and/or transmit that data to a third party.
To object	The right to object at any time to the personal data of an individual being processed for direct marketing (including profiling) or, in certain other situations, to our continued processing of your personal data (e.g. processing carried out for the purpose of our legitimate interests).



Not to be subject to automated individual decision-making	The right not to be subject to a decision based solely on automated processing (including profiling) that produces legal effects concerning you, or similarly significantly affects you.
---	--

If you would like to exercise any of those rights in respect of the information we process as the data controller (as set out in section 6 of this notice), please contact us by email at support@hairtransplant.app. Please let us know what right you want to exercise and the information to which your request relates.

If you would like to exercise any of those rights in respect of the information we process as a data processor on behalf of your clinic, you should contact the clinic directly. If you send your request to us, we will forward it to the clinic and follow their instructions.

[*Back to Contents*](#)

8. Complaints

If we process your personal data, we hope that we can resolve any query or concern you may raise about our use of that information. You may contact us by using any of the contact methods set out in section 1 of this notice.

The Data Protection Legislation also gives you a right to lodge a complaint with a supervisory authority, in particular in the UK or in the European Union (or the European Economic Area) state where you work, normally live or where any alleged infringement of data protection laws has occurred. The supervisory authority in the UK is the Information Commissioner, who may be contacted at <https://ico.org.uk/make-a-complaint/>, telephone on 0303 123 1113, or by post to: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. We would, however, appreciate the chance to deal with your concerns before you approach your supervisory authority, so please contact us in the first instance.

[*Back to Contents*](#)