

Privacy Policy

Version of 15 September 2026.

This is an English translation of the Polish-language Privacy Policy of Optimals sp. z o.o. In the event of any discrepancy between the language versions, the Polish version prevails.

Below we set out how personal data is processed in respect of patients of the Optimals Health medical entity, persons authorised by them or acting on their behalf, users of the Optimals Health Application (available at <https://app.optimalshealth.com> and as a mobile application for iOS and Android), and visitors to the optimalshealth.com website.

These rules have been drawn up on the basis of 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), in force since 25 May 2018 (the "GDPR").

If you are both a patient and a user of the Application, data relating to healthcare services (medical history, a Specialist's recommendations, referrals, results of tests ordered by us, medical records) is processed under the rules described for patients, including where you view it in the Application. All other data in the Application (food diary, activity, data from devices, conversations with the AI assistant, communities) is processed under the rules described for users of the Application.

DATA CONTROLLER

The controller of your personal data is Optimals sp. z o.o., with its registered office in Warsaw, Aleja Solidarności 163/57, 00-877 Warsaw, Poland, entered in the register of entrepreneurs of the National Court Register (Krajowy Rejestr Sądowy) under KRS number 0001169942, REGON 541558246, NIP (tax identification number) 5361990570, hereinafter referred to as "PL". PL operates the Optimals Health medical entity and provides the Optimals Health Application.

PL is the "controller of personal data", which means that it determines the purposes and scope of processing and is responsible for the security of the data belonging to patients and users, that is to say "data subjects", who are entitled to a range of rights and freedoms.

PL applies appropriate technical and organisational measures to protect personal data against unauthorised access, loss or destruction.

In matters concerning the processing of your personal data, please contact the controller by e-mail at: office@optimalshealth.com

DATA PROTECTION OFFICER

PL has not appointed a Data Protection Officer.

PURPOSES OF PROCESSING

PL processes a patient's personal data for the purpose of:

1. taking steps, at the request of the patient or a person acting on their behalf, towards the

provision of healthcare services to them (including verifying the patient's identity, registering the patient, providing information about scheduled appointments and about the cancellation or rescheduling of an appointment) (Article 6(1)(b) and Article 9(2)(h) GDPR),

2. providing healthcare services to the patient (including making a medical diagnosis, providing health care, treatment and preventive healthcare) (Article 6(1)(b) and Article 9(2)(h) GDPR),
3. keeping and storing medical records (Article 6(1)(c) and Article 9(2)(h) GDPR),
4. giving effect to patients' rights (for example, in respect of authorising other persons to access medical records or to be given information about the patient's state of health) (Article 6(1)(c) and Article 9(2)(h) GDPR),
5. complying with other legal obligations incumbent on PL in connection with the medical activity it conducts (including keeping accounting books and meeting tax obligations) (Article 6(1)(c) and Article 9(2)(h) GDPR),
6. ordering laboratory tests from a co-operating laboratory and receiving their results (Article 6(1)(b) and Article 9(2)(h) GDPR),
7. establishing, pursuing or defending claims (Article 6(1)(f) and Article 9(2)(f) GDPR),
8. pursuing other legitimate interests of PL, namely marketing of the services offered by PL and internal administrative purposes of PL (Article 6(1)(f) GDPR),
9. protecting the vital interests of patients (Article 6(1)(d) and Article 9(2)(c) GDPR);
10. conducting communication through electronic channels (legal basis: Article 6(1)(a) GDPR),
11. marketing of the services offered by PL through electronic channels (legal basis: Article 6(1)(a) GDPR),
12. performing the contract, including the contract for the provision of services by electronic means, in accordance with the terms and conditions accepted by the patient (Article 6(1)(b) GDPR),
13. purposes to which the patient has consented (legal basis: Article 6(1)(a) GDPR).

On the first purchase of a service of the medical entity we ask for your PESEL number (the Polish national identification number) and your telephone number. This follows from the obligation to keep medical records to the extent specified in the Act on Patients' Rights and the Patients' Rights Ombudsman (ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta) and from the laboratory's requirements when a referral is issued.

PL processes the personal data of persons authorised by the patient or acting on their behalf (for example, statutory representatives) for the purpose of:

1. establishing that person's entitlement, including their entitlement to act on the patient's behalf (Article 6(1)(c) GDPR),
2. keeping and storing medical records (Article 6(1)(c) GDPR),
3. complying with other legal obligations incumbent on PL in connection with the medical activity it conducts (including keeping accounting books and meeting tax obligations) (Article 6(1)(c) GDPR),
4. establishing, pursuing or defending claims (Article 6(1)(f) GDPR),
5. conducting communication through electronic channels (legal basis: Article 6(1)(a) GDPR).

Patients' health data may be processed for the purpose of marketing and promoting PL's services solely on the basis of the patient's explicit consent (Article 9(2)(a) GDPR).

PL processes the personal data of users of the Application for the purpose of:

1. concluding and performing contracts in connection with the services offered in the Application, including the operation of a plan or subscription, the shop and lab-test credits

- (Article 6(1)(b) GDPR),
2. performing the contract and providing services involving the processing of health data which the user enters into the Application or imports from devices (Article 9(2)(a) GDPR, explicit consent given on registration; its withdrawal means that use of the Application comes to an end),
 3. maintaining an individual user account (Article 6(1)(b) GDPR),
 4. analysis using artificial intelligence: estimating the nutritional values of a meal from a photograph or description, reading test results from uploaded documents, preparing lifestyle guidance and summaries, and operating the AI assistant (Article 6(1)(b) and Article 9(2)(a) GDPR),
 5. sending push notifications and e-mails of a technical nature and relating to use of the Application (reminders, summaries), which the user may switch off in the settings (Article 6(1)(b) and (f) GDPR),
 6. delivering marketing content concerning the controller and carrying out analytics of the Application and the website in connection with the use of cookies and similar technologies (Article 6(1)(a) GDPR),
 7. complying with legal obligations incumbent on PL (including keeping accounting books and meeting tax obligations) (Article 6(1)(c) GDPR),
 8. establishing, pursuing or defending claims (Article 6(1)(f) and Article 9(2)(f) GDPR),
 9. pursuing other legitimate interests of PL, namely ensuring security, error diagnostics, preventing abuse, recording acceptance of terms and conditions, marketing of the services offered by PL and internal administrative purposes of PL (Article 6(1)(f) GDPR),
 10. conducting communication through electronic channels (Article 6(1)(a) GDPR),
 11. marketing of the services offered by PL through electronic channels (Article 6(1)(a) GDPR); health data is not used for this purpose without separate explicit consent (Article 9(2)(a) GDPR),
 12. improving the Application on the basis of anonymised or aggregated data (anonymisation on the basis of Article 6(1)(f) GDPR),
 13. purposes to which the user has consented (legal basis: Article 6(1)(a) GDPR).

The data of users of the Application includes, in particular: account data (e-mail address, first name and surname, password in hashed form, Google account identifier where Google sign-in is used), profile and goal data (date of birth, sex, height, body weight, health goal, answers to questionnaires), diary data (photographs and descriptions of meals, estimated nutritional values, water, supplements, activity and workouts, sleep, symptoms, wellbeing, habits and challenges), test results and measurements entered by the user, data from Apple HealthKit and Android Health Connect, conversations with the AI assistant and messages with a Specialist, content in communities, payment data (customer identifier at the payment provider, purchase history, credit balance; without the full card number), technical data (IP address, device, browser, push notification identifiers, events in the Application, error messages) and a record of the documents and consents accepted.

Content that a user publishes in a community, together with their first name and their standing in the leaderboard, is visible to the other members of that community. A user joins a community voluntarily by means of an invitation code and may leave it at any time.

PL may process personal data within its social media profiles, such as Facebook, Instagram, LinkedIn, TikTok and X. This is data such as first name, surname, username, likeness, the content of comments or information sent through chat. PL processes the data of persons who have subscribed to a fan page by clicking the "Like", "Follow" or a similar icon, have used chat, or have published a comment under a post placed on the profile.

This data is obtained from the platform owner (for example, Meta Platforms Ireland Ltd. in the case of Facebook and Instagram) and from the person's public profile on the given platform. This data is used for the purpose of administering and managing social media profiles, communicating and delivering marketing content (Article 6(1)(f) GDPR). As regards page statistics on Facebook and Instagram, PL and Meta Platforms Ireland Ltd. are joint controllers.

DATA FROM APPLE HEALTHKIT AND ANDROID HEALTH CONNECT

If a user enables the import in the Application, PL reads the following categories of data from the Health app (iOS) or Health Connect (Android): step count, resting heart rate, sleep (duration and stages), body weight and workout sessions (type, duration, calories burned, distance). Reading requires the user's consent, given in a system dialog, separately for each category. PL reads data solely within the scope to which the user has consented, and only up to 30 days retrospectively on the first import, and on an ongoing basis thereafter. The import is one-way: PL does not write anything to HealthKit or Health Connect.

Imported data is stored on PL's servers in the EEA together with the remaining account data and is used solely for the functions of the Application: presenting activity, sleep and body weight, counting progress in challenges and creating guidance. PL does not use it for advertising, does not sell it, does not transfer it to data brokers, advertising networks or insurers, and does not use it to assess creditworthiness. Apart from the user, it is accessible only to a Specialist, if the user uses the services of the medical entity. It is transferred to the provider of the artificial intelligence models solely to the extent necessary to prepare guidance and summaries. The import may be switched off at any time in the settings of the Application or by withdrawing consent in the system settings; from that moment PL does not read any new data. The user may delete previously imported data in the Application, and all of it together with the account. The use of this data is additionally subject to the rules of Apple (HealthKit) and Google (Health Connect Permissions Policy), with which PL complies.

RECIPIENTS OF PERSONAL DATA

The personal data of a patient, a user of the Application and of persons authorised by the patient or acting on their behalf may be disclosed by PL to the following recipients or categories of recipients:

1. other medical entities co-operating with PL in the provision of healthcare services,
2. the laboratory performing tests ordered by PL, Diagnostyka S.A., as a separate controller in respect of performing the test: first name and surname, PESEL number, telephone number, scope of tests, results,
3. entities providing PL with IT solutions and technical and organisational support enabling the provision of healthcare services and the management of PL, listed in the table below,
4. entities providing marketing services to PL,
5. entities providing legal or advisory services to PL,
6. other entities to which PL has entrusted the processing of personal data,
7. other entities authorised to receive personal data on the basis of the applicable law,
8. Meta Platforms Ireland Ltd. in respect of measuring the effectiveness of advertising (the Meta pixel and the Conversions API), solely where marketing consent has been given; in

this respect PL and Meta are joint controllers on the terms set out at facebook.com/legal/controller_addendum,

9. on the basis of the patient's consent, PL may disclose their data to third parties carrying out health-promoting initiatives, for example conducting clinical trials or scientific research, or offering health-promoting services.

Entities processing data on PL's instructions (under data processing agreements):

Entity	Purpose	Data	Registered office and place of processing
Hetzner Online GmbH	hosting of the Application's server and database	all data stored in the Application, including health data	Germany; data centres in the EEA
Google Cloud EMEA Limited (Vertex AI, Gemini models)	analysis of meal photographs and descriptions, generating guidance and summaries, the AI assistant, reading test results from uploaded documents	content entered by the user, including health data and photographs	Ireland; processing solely in the EU region (Vertex AI); Google does not use this data to train models
Cloudflare, Inc.	file storage (photographs, documents, test results) and content delivery network	uploaded files, technical connection data	USA; files stored solely in the EU region; DPF
PostHog, Inc.	analytics of the use of the Application and the website, session recordings with full text masking, feature testing, error diagnostics	user identifier, events in the Application, technical device data, error messages; in session recordings, textual content is masked	USA; data stored in the EEA (eu.posthog.com)
Vercel Inc.	hosting of the interface layer of the Application and the website (without account data and without health data)	technical connection data (IP address, browser)	USA; DPF; servers in the EU region (Frankfurt)
Google Ireland Limited (Google Workspace: Gmail, Drive, Docs, Google Meet, Calendar)	e-mail, storage of documentation, e-visits, Specialists' calendars	contact data, medical records, image and sound of an e-visit (not recorded)	Ireland; EEA

Entity	Purpose	Data	Registered office and place of processing
Stripe Payments Europe Limited	payments, subscriptions, invoices	first name and surname, e-mail, payment data (provided directly to Stripe), payment history	Ireland; the Stripe group in the USA on the basis of the DPF or standard contractual clauses
Brevo (Sendinblue SAS)	sending transactional and marketing e-mails, delivery statuses	e-mail, first name, message content, delivery events	France; EEA
Apple Inc. (App Store, APNs) and Google Ireland Limited (Google Play, Firebase Cloud Messaging)	distribution of the mobile application, delivery of push notifications	device identifier for notifications, notification content (without health data), store diagnostic data	USA / Ireland; DPF

PL does not sell personal data and does not transfer it to data brokers or advertising networks for the purpose of profiling advertising, beyond the measurement of advertising effectiveness described above.

RETENTION PERIOD

PL stores the personal data of patients, users of the Application and persons authorised by the patient or acting on their behalf for no longer than is necessary for the purposes for which it was collected.

In the case of steps taken towards the provision of, or the provision of, healthcare services: until those services have been completed, and thereafter for the period and to the extent required by law or necessary to secure any claims of PL.

In the case of personal data processed in connection with the conclusion and performance of a contract: for the duration of the contract, and thereafter for the period required by law and the period necessary to establish and pursue claims or to defend against claims (no later than the expiry of the limitation period or the conclusion of proceedings).

In the case of an account in the Application: for the duration of the contract; once deletion of the account has been requested, the data is permanently deleted after 7 days (the period during which deletion may be reversed). An account that has been created but is unconfirmed and unused is deleted after 14 days. An account into which the user has not logged in for 24 months may be deleted by PL upon prior notice. Data from HealthKit and Health Connect is stored for as long as the account, and is deleted earlier on request. Content transferred for AI analysis and conversations with the AI assistant are stored for as long as the account; on Google's side (Vertex AI) they are not stored once the request has been handled, nor used to train models. Data relating to healthcare services (medical records) is not deleted together with the account. Data processed on the basis of consent will be processed for the time necessary to achieve the

purpose to which the consent relates, or until the consent is withdrawn. To the extent necessary, the data may additionally be stored for the period necessary to establish and pursue claims or to defend against claims (no later than the expiry of the limitation period or the conclusion of proceedings).

Data processed on the basis of the controller's legitimate interest will be processed for the time necessary to achieve the purpose for which it was processed, or until an objection is raised. To the extent necessary, the data may additionally be stored for the period necessary to establish and pursue claims or to defend against claims (no later than the expiry of the limitation period or the conclusion of proceedings). Analytics data: 12 months; session recordings: 30 days.

Technical logs: up to 90 days.

If a patient uses the contact form, their data and the content of the message will be stored for the time necessary to process the request, for no longer than one year, unless the content of the message is of a kind that by law requires longer storage (for example, in order to pursue or defend against claims we store the data until the expiry of the limitation period or the conclusion of proceedings).

Data processed in order to comply with legal obligations will be processed for the period resulting from the relevant provisions, for example, in the case of the storage of medical records, in most cases for a period of 20 years counted from the end of the calendar year in which the last entry was made; in some cases the law imposes on PL an obligation to store records for a longer period (for example, 30 years in the event of the patient's death) or a shorter one (for example, 2 or 5 years in the case of referrals); in the case of keeping accounting books and meeting tax obligations, for a period of 5 years counted from the end of the calendar year in which the tax obligation arose.

Data stored in order to protect the vital interests of patients will be stored for the period necessary to ensure that protection.

RIGHT TO WITHDRAW CONSENT

Where PL processes personal data solely on the basis of consent given by, or on behalf of, the data subject, that person has the right to withdraw that consent at any time. Withdrawal of consent does not affect the lawfulness of processing carried out on the basis of the consent before its withdrawal.

Consents to cookies and marketing may be changed in the settings of the Application, consent to data from devices in the system settings, and the remaining ones by e-mail. Withdrawal of consent to the processing of health data in the Application means that use of the Application comes to an end.

RIGHT TO OBJECT

A natural person whose data is processed by PL has the right to object at any time, on grounds relating to their particular situation, to the processing of their data for the performance of a task carried out in the public interest or for the purposes of the legitimate interests pursued by PL, including profiling. In such a case PL may process that person's data provided that it demonstrates the existence of compelling legitimate grounds for the processing which override the interests, rights and freedoms of that person, or grounds for the establishment, exercise or defence of legal claims (Article 21(1) GDPR).

Where personal data is processed for direct marketing purposes, the data subject has the right

to object at any time to the processing of their personal data for such marketing, including profiling, to the extent that the processing is related to such direct marketing (Article 21(2) GDPR).

OTHER RIGHTS

A natural person whose data is processed by PL has the right to:

1. obtain confirmation as to whether their data is processed by PL, as well as the right of access to their data (Article 15 GDPR);
2. rectification and completion of their data (Article 16 GDPR);
3. erasure of their data (Article 17 GDPR), subject to data which PL is required to store as medical records or on the basis of other provisions of law;
4. request the restriction of the processing of their data (Article 18 GDPR);
5. portability of their data to another controller (Article 20 GDPR); in the Application the user may download an export of their diary.

PL responds to requests within one month. In the Application the user may themselves correct their profile data, download an export of their diary and delete their account.

RIGHT TO LODGE A COMPLAINT

A natural person whose data is processed by PL has the right to lodge a complaint with the supervisory authority, that is, with the President of the Personal Data Protection Office (Prezes Urzędu Ochrony Danych Osobowych).

SOURCE OF THE DATA

The source of a patient's personal data is the patient or a person acting on their behalf. The results of tests ordered by PL come from the laboratory.

The source of the personal data of persons authorised by the patient or acting on their behalf is the patient or the data subject.

The source of the personal data of a user of the Application is the user themselves: registration, entries, photographs and documents that they upload, and their devices, if they enable the import from Apple HealthKit or Android Health Connect. Where sign-in with a Google account is used, PL receives from Google the e-mail address, first name and surname, and profile picture.

CONSEQUENCES OF NOT PROVIDING DATA

The provision of data by a patient, including health data, is voluntary.

However, if it is not provided, PL may refuse to provide the patient with any or with particular healthcare services.

The provision by the patient of the data of persons authorised by the patient or acting on their behalf is voluntary, but is a condition of giving effect to the authorisation or of acting on the patient's behalf. The patient acknowledges that PL's request for their personal data follows from the legal obligation to keep medical records properly and from the minimum scope of medical records under the provisions of the Act on Patients' Rights and the Patients' Rights Ombudsman.

The provision of data by a user of the Application, including health data, is voluntary. Without an e-mail address an account cannot be created, and without consent to the processing of health data the Application cannot deliver its functions. The remaining data (for example, meal photographs, data from devices) is provided by the user at their discretion; the absence of it limits only the corresponding functions.

PROFILING

PL does not take decisions in relation to you based solely on automated processing, including profiling, which would produce legal effects concerning you or similarly significantly affect you (Article 22(1) and (4) GDPR).

In the Application, PL uses artificial intelligence models for: estimating the nutritional values of a meal from a photograph or description, reading test results from uploaded documents, preparing lifestyle guidance and summaries, and operating an assistant which answers the user's questions on the basis of the data they have entered. The outputs of these models are informational in nature and do not produce legal effects concerning the user, nor do they similarly significantly affect them within the meaning of Article 22 GDPR. Personalisation of content (for example, matching guidance to a health goal) constitutes profiling within the meaning of the GDPR, but does not produce such effects. PL does not use users' photographs, entries or health data to train artificial intelligence models, and the terms of use of Vertex AI exclude such use on Google's side.

ADDITIONAL INFORMATION

In order to ensure the highest quality of service we use the services of other providers, for example in the area of IT support, listed in the section on recipients of data. Account data, diary data, test results, photographs, data from devices, conversations with the AI assistant and medical records are stored and processed by us solely within the European Economic Area: on Hetzner servers in Germany, in Cloudflare R2 files in the EU region, in the European PostHog instance and in Gemini models run through Vertex AI in the EU region. Health data does not leave the EEA.

Outside the EEA, to providers in the United States, only data that does not relate to health is transferred: advertising effectiveness measurement data to Meta (only where marketing consent has been given), technical connection data to Vercel, device identifiers for notifications to Apple and Google, and payment data within the Stripe group. In such cases the transfer of data takes place on the basis of a European Commission adequacy decision (the EU-US Data Privacy Framework) in respect of providers certified thereunder, or on the basis of an appropriate agreement containing the standard data protection clauses adopted by the European Commission (Article 46(2)(c) GDPR). A copy of the safeguards applied may be obtained by writing to office@optimalshealth.com.

COOKIES

When you use our websites and applications we may store or read cookies and similar technologies (for example, local storage) on your device. The mobile application does not use cookies, but stores a session token and analytics identifiers on the device on the same terms. We use them for the following purposes:

1. ensuring the basic operation and security of the services (necessary cookies);
2. remembering user interface settings (functional/preference cookies);
3. measuring the use of the services and improving them (analytics), where this is required on the basis of your consent; this includes session recording with masking of all text content entered and displayed;
4. measuring the effectiveness of our advertising on Meta services (marketing), on the basis of your consent.

On your first visit to the Website or the Application you see a consent bar in which you may agree to all optional technologies (analytics, marketing and session recording) or reject them all and use only the necessary technologies. Technologies necessary for operation and security are always applied. Merely closing the bar does not constitute consent. Once signed in, you may change or withdraw each of these consents separately in the settings of the Application (the Privacy tab). Consent given on the Website may be withdrawn by deleting cookies and changing the settings in your browser. Consent given in the Application is saved to your account, so it applies across all of your devices. Please note, however, that disabling cookies may cause difficulties in using the website, as well as many other websites that use cookies. Cookies are small files saved on your device. They enable the Website to be displayed correctly, all of its functionalities to be used, and statistics on visits to the Website to be kept by us. In addition, cookies make it possible to remember your visits to the Website. Cookies do not cause configuration changes on your device or in the software installed on it. You can read more about how cookies work at <http://www.allaboutcookies.org> or <http://wszystkoociasteczkach.pl>.

Cookies are divided into session cookies and persistent cookies. Session cookies operate for the period during which you have the Website open, and are then deleted. Persistent cookies are stored also after the Website is closed, and even after the browser or the entire computer is switched off.

Cookies may also be divided into first-party cookies and those originating from third parties. First-party cookies are above all the necessary cookies of the Website, which enable it to function correctly and securely.

You may manage cookies in your browser settings at any time.

Disabling necessary cookies may cause parts of the service to malfunction.

Information about the cookies we use:

Name / pattern	Provider	Purpose	Category	Retention period	Type
token	Optimals (first party)	User authentication , maintaining the session, account security	Necessary	Up to 30 days (session renewed)	HTTP cookie
Consent cookie	Optimals (first party)	Remembering your choices in the consent bar	Necessary	12 months	Cookie / local storage
ph_* (for	PostHog	Analytics: use	Analytics	Up to 1 year	Cookie /

Name / pattern	Provider	Purpose	Category	Retention period	Type
example, PostHog cookies)	(processor)	of the website, events, product development, session recordings, feature testing	(optional where consent is required)	(the provider's default configuration may differ)	similar technology
_fbp, _fbc	Meta Platforms Ireland Ltd. (joint controller)	Measuring advertising effectiveness, conversion matching	Marketing (with consent)	90 days	HTTP cookie
__stripe_mid, __stripe_sid	Stripe (processor)	Fraud prevention at payment	Necessary (only on payment pages)	12 months / session	HTTP cookie

CHANGES TO THE POLICY

We update the Policy when our services, our providers or the law change. We will notify you of material changes by e-mail or in the Application. The version and the date from which it applies are stated at the beginning of the document; previous versions are made available on request.