PRIVACY POLICY OF THE CORAZZDROWIEJ.PL WEBSITE

Table of contents

---

1) Definitions

GDPR: 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 controller (Article 4(7) GDPR): an entity that determines the purposes and means of processing personal data.

Processor (Article 4(8) GDPR): an entity that processes personal data on behalf of the controller.

Recipient (Article 4(9) GDPR): an entity to which personal data are disclosed. Recipients do not include public authorities that process data within the scope of their public tasks.

Service: the Website operating within CORAZ ZDROWIEJ's services supporting the management of medical entities. Within the Service, the necessary technical and organisational infrastructure is maintained to deliver and maintain the services, including network and server environments, as well as a team ensuring security and compliance of the services with technical and legal requirements.

---

2) Personal data controller and processing context

- The controller of personal data related to operating the Service is **CORAZ ZDROWIEJ sp. z o.o.** with its registered office in Krakow at ul. Bonarka 8, 30-415

Krakow, entered in the Register of Entrepreneurs of the National Court Register under KRS 0000960776; registry court where company records are kept: District Court in Rzeszow, 12th Commercial Division of the National Court Register; share capital: PLN 6,000; NIP: 8133876161; REGON: 521493568; email: kontakt@corazzdrowiej.pl.

- Medical entities using the Service under agreements concluded with CORAZ ZDROWIEJ are the controllers of medical data for data collected within the services delivered by the Service under those agreements; CORAZ ZDROWIEJ processes such data as a processor. CORAZ ZDROWIEJ, as part of services provided to a medical entity, enables that entity to place on the resources made available to it its own documents addressed to the owners of the data (patients). Those documents are not part of this Privacy Policy.
- Where CORAZ ZDROWIEJ participates in research experiments as part of clinical research conducted jointly with medical entities, and acts as the Sponsor of such research, it will act as controller for personal data for the purposes of initiating the clinical trial, managing it and organising its financing, as well as coded participant data received from the investigator in the form of clinical report forms (CRF). This Privacy Policy does not describe clinical trial scenarios, which will be handled each time by separate documentation provided by controllers to the persons whose data will be processed (parties to the tripartite agreement between the CRO, the Investigator and the Sponsor, and trial participants).

Joint controllership

- CORAZ ZDROWIEJ, when using analytics mechanisms within the Service (see the “Cookies and analytics” section), acts as one of the controllers of personal data.
- CORAZ ZDROWIEJ, when using external authentication mechanisms (Google, Facebook) to authorise access for users representing medical entities, is one of the controllers for data used to log in to the Service.

---

3) Contact details

The controller has appointed a **Data Protection Officer (DPO)**, who can be contacted regarding personal data processing at:

- email: iod@corazzdrowiej.pl
- postal address: CORAZZDROWIEJ, ul. Bonarka 8, 30-415 Krakow

Correspondence may also be delivered in person to the address above.

---

4) Purpose, legal basis and retention period of data processing on the Website

The controller may process personal data on the Website for the purposes, on the legal bases and for the retention periods described below.

A) Preparation for conclusion, conclusion and performance of an agreement between Coraz Zdrowiej and a medical entity using the Service

Legal basis

- GDPR Article 6(1)(b) and Article 49(1)(b): conclusion and performance of an agreement under the following laws:
    - Civil Code of 23 April 1964
    - Entrepreneurs' Law of 6 March 2018
    - Commercial Companies Code of 15 September 2000
- GDPR Article 6(1)(f): legitimate interest of the controller in processing personal data of persons designated by the medical entity to ensure ongoing performance of the agreement, including Service users.

Retention period

- For the period necessary to perform, terminate, or otherwise expire the agreement for providing the electronic service.

B) Charging and settling payments, issuing invoices, and keeping accounting records

Legal basis

- GDPR Article 6(1)(c) and Article 49(1)(b), including in particular:
    - Article 74(2) of the Accounting Act of 29 September 1994
    - Banking Law Act of 29 August 1997 (to the extent it regulates bank settlements and enables use of banking institutions)
    - Payment Services Act of 19 August 2011 (to the extent it enables use of payment institutions)

Commentary from the policy: this processing purpose in the GDPR context applies primarily where the party is a natural person conducting a sole proprietorship. For partnerships and capital companies, the processed data concern legal persons, and the information obligation is addressed exclusively to natural persons.

Retention period

- 5 years, counted from the beginning of the year following approval of the financial statements.

C) Handling disputes (complaints) and pursuing claims between the parties

Legal basis

- GDPR Article 6(1)(b), Article 6(1)(f) and Article 49(1)(e): legitimate interest of the controller (protection of own assets, tangible and intangible). The scope of data follows in particular from:
    - Civil Code of 23 April 1964
    - Accounting Act of 29 September 1994
    - Entrepreneurs' Law of 6 March 2018
    - Commercial Companies Code of 15 September 2000
      and concerns parties to the agreement and/or their representatives, as well as Service users.

Retention period

- Until expiry of potential claims relating to non performance or improper performance of the service/agreement.

D) Direct marketing to Service users and persons visiting the website

This includes promoting CORAZ ZDROWIEJ services and encouraging use of the offer, including expanding its scope by persons targeted with marketing.

Legal basis

- GDPR Article 6(1)(f) and Recital 47: legitimate interest of the controller, performed in line with Article 398 of the Electronic Communications Law (PKE), in particular taking into account obtaining the subscriber/end user consent, also by obtaining an electronic address for receiving marketing content.

Retention period

- For the duration of the controller's legitimate interest in direct marketing, but no longer than until the data subject objects or withdraws consent previously granted under Article 398 PKE.

E) Ensuring proper functioning of the Service (cookies mechanism)

Including adapting the Service parameters/mode of operation to the needs of visitors and users.

Legal basis

- GDPR Article 6(1)(f): legitimate interest.

Retention period

- For the duration of the legitimate interest, but no longer than the limitation period for the controller's claims against the data subject arising from business activity. The policy notes that the basic limitation period for claims related to business activity is three years.

F) Business assessment of promotional effectiveness and security monitoring, including analytics (for example, Google Analytics)

Including keeping statistics and analysing traffic on the Website.

Legal basis

- GDPR Article 6(1)(f): legitimate interest.

Retention period

- For the duration of the legitimate interest in traffic statistics and analysis, but no longer than until the data subject objects.

---

5) Data recipients on the Website

Below are categories of recipients and the context in which personal data may be disclosed.

A) Preparation for conclusion, conclusion and performance of an agreement

Recipients (categories)

- Providers supplying the controller with technical, IT and organisational solutions
- Facebook or Google for user authentication in the Service
- Entities authorised to perform inspections
- Postal service providers under postal law services

Context

- Data are disclosed during negotiation and conclusion of the agreement (within the Service and additionally via email and traditional correspondence) and during SaaS service configuration.
- For Facebook or Google, data are disclosed each time the user logs in to the Service.

B) Payments, invoices and accounting records

Recipients (categories)

- Accounting, legal, advisory and debt collection service providers
- Banks of the contracting parties
- Domestic payment institutions
- Entities authorised to perform inspections

Context

- Data are processed by accounting firms using their own IT systems.
- Data are transferred within a secure IT infrastructure (including encryption, access based at least on authorisation, and integrity safeguards) among stakeholders, including banks and payment institutions.

C) Disputes and claims

Recipients (categories)

- State entities within their tasks entrusted to them (for example tax office, common courts, public prosecutor's office)
  Note: the policy explains that such entities are not formally "recipients" within the meaning of Article 4(9) GDPR; however, they are listed to reflect the data flow.
- Courier companies
- Entities providing IT services (website maintenance and accounting system support)

Context

- Reporting and resolving claims between parties, including legal compliance issues
- Delivering correspondence to the parties
- Documenting and delivering information about events

D) Direct marketing

Recipients (categories)

- Providers supplying the controller with technical, IT and organisational solutions
- Entities authorised to perform inspections

Context

- Data are disclosed as part of using external entities to operate functionalities offered by the Website.

E) Ensuring proper functioning of the Service (cookies and social media plug-ins)

Recipients (categories)

- Meta Platforms Ireland Ltd for login related functionality
- Providers supplying the controller with technical, IT and organisational solutions
- Providers of social plug-ins, scripts and similar tools embedded on the Website, enabling the visitor's browser to download content from such providers (including Meta Platforms Ireland Ltd)
- Entities authorised to perform inspections

Context

- Within the use of persistent and session cookies, as described in the “Cookies and analytics” section.

F) Analytics and advertising effectiveness assessment (for example, Google Analytics)

Recipients (categories)

- Google, within Google Analytics tools
- Providers supplying the controller with technical, IT and organisational solutions
- Entities authorised to perform inspections

Context

- Meta Platforms Ireland Ltd and Google provide their services in exchange for their own benefits related to collecting information about users of CORAZ ZDROWIEJ’s Website. Those benefits mainly include delivering ads based on profiling user preferences. The policy refers to the privacy rules published by Meta and Google.

---

6) Transfers to third countries and profiling

This section describes whether data are transferred outside the European Economic Area (EEA) and whether profiling is used, depending on the processing purpose.

A) Agreement related processing

- Personal data are not transferred to third countries outside the EEA, except where users use social login (for example Facebook or Google).
- In such cases, personal data may be transferred to the providers of those services located outside the EEA for the purpose of authenticating the user.
- Other data processing services, including data storage, computing capacity and software, are provided within the EEA.
- Profiling is not used for this purpose.

B) Payments, invoices and accounting

- Data are not transferred outside the EEA.
- Profiling is not used for this purpose.

C) Disputes and claims

- Data are not transferred outside the EEA (except situations resulting from the presence of a party to the agreement/service outside the EEA).
- Profiling is not used for this purpose.

D) Direct marketing

- Personal data may be transferred to third countries outside the EEA, including the United States, in connection with the use of social media and advertising services (for example Facebook or Google).
- Personal data may be used for profiling for marketing purposes.

E) Cookies and social media plug-ins

- Data may be transferred to third countries outside the EEA, including the United States, in connection with the use of social media and advertising services (for example Facebook or Google).
- Profiling may be used for marketing purposes as part of these services.

F) Analytics (for example, Google Analytics)

- Personal data may be transferred to third countries outside the EEA, including the United States, in connection with the use of analytics services (for example Google Analytics).
- Profiling on the Website involves automated analysis or prediction of a person's behaviour on the Website, including analysis of the history of actions taken on the Website.

The policy refers readers to the privacy and data transfer framework statements published by Meta and Google.

---

7) Rights of the data subject

Depending on the purpose and legal basis, the data subject may have the following rights under the GDPR:

- **Article 15 GDPR**: right of access to data
- **Article 16 GDPR**: right to rectification and completion of data
- **Article 17 GDPR**: right to erasure of data where the purpose of processing has ceased
- **Article 18 GDPR**: right to restriction of processing, including safeguarding data, for example where data accuracy is contested for the time needed to verify, or where the purpose has ceased
- **Article 19 GDPR**: right to be informed, upon request, about recipients to whom the controller has communicated rectification, erasure, or restriction of processing
- **Article 20 GDPR**: right to data portability and to receive data in a structured, commonly used format, to the extent data are processed in an IT system used to manage agreements
- **Article 21 GDPR**: right to object to processing, including profiling (in particular relevant to processing based on legitimate interests such as direct marketing)

Necessity of providing data (as described in the policy)

- For concluding and performing an agreement: providing data is necessary to conclude and perform the agreement.
- For accounting and tax obligations: providing data is necessary to fulfil legal duties related to accounting books and tax documentation.
- For disputes/claims: no additional data are collected beyond data already collected for other purposes.
- For direct marketing: providing data is not necessary; the controller processes data on the basis of consent granted under Article 398 PKE.
- For cookies/analytics: providing data is voluntary (through mechanisms described in the “Cookies and analytics” section), but refusing may limit certain Website functionalities and make full use of the Service more difficult.

How to exercise rights

To exercise the above rights, contact the Data Protection Officer (DPO) as indicated in section 3 of this Policy. Fulfilment of a request will be preceded by verification of your identity in a manner individually adapted to the request.

Right to lodge a complaint

If you consider that the processing of your personal data by CORAZ ZDROWIEJ violates the GDPR, you have the right to lodge a complaint with the President of the Personal Data Protection Office (PUODO), ul. Stawki 2, 00-193 Warsaw, Poland.

---

8) Cookies and analytics on the Website

1. The controller uses cookies, meaning small text files stored on the user’s device, used among other things to optimise use of the Website and to collect anonymous statistical data. Information on disabling or managing cookies can be found in the settings of the internet browser used.
2. Depending on function and purpose, cookies used by the Website can be divided into categories:

By provider

- first party cookies (created by the controller’s Website)
- third party cookies (belonging to entities other than the controller)

By storage duration

- session cookies (stored until logout or browser closure)
- persistent cookies (stored for a defined time, as set by cookie parameters, or until manually deleted)

By purpose

- necessary (enable proper functioning of the Website)
- functional/preference (adapt the Website to visitor preferences)
- analytics and performance (collect information on how the Website is used)
- advertising/marketing/social (collect information to display ads, measure their effectiveness, and personalise ads, including when visitors browse other websites within advertising networks)

3. During use of the Website, the controller or joint controllers may process information stored in cookies for specific purposes, including:

- identifying users as logged in and showing they are logged in (necessary cookies)
- remembering items added to the basket for placing an order (necessary cookies)
- remembering data entered in forms, surveys or login data (necessary and/or functional cookies)
- adapting Website content to user preferences and optimising Website use (functional cookies)
- producing anonymous statistics about use of the Website (analytics/performance cookies)
- displaying and rendering ads, limiting frequency, ignoring unwanted ads, measuring ad effectiveness, and personalising ads through anonymous analysis of activity (for example repeated visits, keywords), including within Google and Meta advertising networks (marketing/advertising/social cookies)

4. The policy describes how to check in popular browsers which cookies are currently sent by the Website, including their lifetime and provider (instructions for Chrome, Firefox, Internet Explorer, Opera, Safari). It also references external tools for cookie inspection.
5. Most browsers accept cookies by default. Users can change settings to partially restrict or completely block cookies, which may affect certain Website functions (for example the order process). Under applicable law, browser settings regarding cookies may be treated as consent to their use. The policy indicates that detailed instructions are available in the browser help resources.
6. The controller uses Google Analytics and Universal Analytics services provided by Google Ireland Limited (Gordon House, Barrow Street, Dublin 4, Ireland). These services help compile statistics and analyse Website traffic. Data are processed to generate aggregated statistics helpful for administering the Website and analysing traffic. The controller collects, among other things: acquisition sources and medium, behaviour on the Website, device and browser information, IP and domain, geographic data, and demographic data (age, gender) and interests.
7. The policy indicates that a visitor can block sharing information about their activity with Google Analytics, for example by installing a browser add on provided by Google.
8. The policy notes that full information about Google's rules for processing data of Website visitors (including information stored in cookies) is available in Google's published privacy documentation related to partner sites and technologies.

---

9) Final provisions

1. The Website may contain links to other websites. The controller encourages visitors, after moving to other websites, to read the privacy policy established there. This Privacy Policy applies only to the controller’s Website.