



# Privacy Policy

## Version History

Date	Version	Reason for Change	Author
03/03/2026	5.1.0	Section(s) updated: 1,2,3	Adi Topaz
08/09/2025	5.0.0	Document structure changed	Adi Topaz
21/07/2025	4.0.0	Document structure changed	Adi Topaz
26/02/2025	3.3.0	Section(s) updated: 1,3	Adi Topaz
12/02/2025	3.2.0	Section(s) updated: 1,3	Adi Topaz
09/12/2024	3.1.0	Section(s) updated: 1,3	Kati Mizrahi
23/09/2024	3.0.0	Document structure changed	Naq
26/06/2024	2.1.0	Section(s) updated: 3	Adi Topaz
25/06/2024	2.0.0	Document structure changed	Adi Topaz
02/06/2024	1.3.0	Section(s) updated: 1,3	Adi Topaz
25/05/2024	1.2.0	Section(s) updated: 1,2,3	George Frey
10/05/2024	1.1.0	Section(s) updated: 1,2,3	Adi Topaz
10/05/2024	1.0.0	Initial generation	Adi Topaz



# Privacy policy

## Introduction

Cognishine Therapy and Education Ltd. respects the privacy of its customers, suppliers and partners. We have therefore formulated and implemented a policy on complete transparency regarding the processing of personal data, its purpose(s) and the possibilities to exercise your legal rights in the best possible way. For employees, we have formulated a separate privacy policy, available upon employment and upon request.

This privacy policy pertains to processing by Cognishine Therapy and Education Ltd. by means other than through the use of cookies. Cognishine Therapy and Education Ltd. has formulated a separate cookie policy, which can be found on our Cognishine Therapy and Education Ltd.'s websites: <https://cognishine.com/>

This policy applies to the Cognishine Therapy and Education Ltd. group consisting of Cognishine Therapy and Education Ltd. with subsidiaries:

<b>Cognishine therapy and education USA, Inc.</b>	
Subsidiary name:	Cognishine therapy and education USA, Inc.
Address:	600 North Broad Street, Suite 5 #33, 19709, Middletown, United States of America
Registration number:	32-0667566

This policy applies to the Cognishine Therapy and Education Ltd. group consisting of Cognishine Therapy and Education Ltd. with subsidiaries:

<b>Cognishine Therapy &amp; Education Deutschland GmbH</b>	
Subsidiary name:	Cognishine Therapy & Education Deutschland GmbH
Address:	c/o Startplatz Im Mediapark 5, 50733, Köln, Germany
Registration number:	HRB 120915

This policy applies to the Cognishine Therapy and Education Ltd. group consisting of Cognishine Therapy and Education Ltd. with subsidiaries:



<b>COGNISHINE THERAPY AND EDUCATION UK LIMITED</b>	
Subsidiary name:	COGNISHINE THERAPY AND EDUCATION UK LIMITED
Address:	77 East Road, Studio Shoreditch Bsl, N1 6AH, London, United Kingdom
Registration number:	16047742

## Definitions

- Party responsible for processing personal data: Cognishine Therapy and Education Ltd.; with registered address at 8 Neshor St. in Israel; company registration number 516061660 and Data Protection Officer George Frey who can be reached at [george.frey@cognishine.com](mailto:george.frey@cognishine.com) (the "Controller").
- Data Protection Authority: The Data Protection Authority of Israel.
- Data Protection laws:
  - For European citizens or residents, the EU GDPR 2018; the EU e-privacy directive 2002 (soon to be replaced by the EU e-privacy regulation);
  - For UK citizens or residents, the UK GDPR 2020 and the UK Data Protection Act 2018
  - and the national laws of the countries where we operate.

## Collection of data

- Your personal data will be collected by Cognishine Therapy and Education Ltd. and its data processors.
- Personal data means any information relating to an identified or identifiable natural person ('data subject').
- An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

## The types of personal data we may process through third party applications:

Business process	Data	Legal basis
------------------	------	-------------



Compliance	Company - Non-PII data, Email Address, Home Address, Telephone Number Employees - Non-PII data, Email Address, Home Address, Telephone Number Suppliers - Non-PII data	Legal Obligation Compliance
Marketing	Customers - First Name, Last Name, Non-PII data	Legitimate Interests
Task Management	Customers - Date of Birth, First Name, Online Activity, Contracts, Gender, Job Title, Home Address, Subscription Data, Telephone Number, Last Name, Email Address Business Partners - Date of Birth, First Name, Online Activity, Contracts, Gender, Job Title, Email Address, Last Name, Telephone Number Users - First Name, User Name, Last Name, Email Address	Legitimate Interests
Technical Tool	Users - User Name, Non-PII data, Email Address, IP Address Customers - Non-PII data	Legitimate Interests
Document Storage	Employees - Email Address Customers - Date of Birth, First Name, Online Activity, Contracts, Gender, Job Title, Home Address, Subscription Data, Telephone Number, Last Name, Email Address Business Partners - Date of Birth, First Name, Online Activity, Contracts, Gender, Job Title, Email Address, Last Name, Telephone Number Users - First Name, User Name, Last Name, Email Address	Legitimate Interests
Office Management	Employees - Email Address	Legitimate Interests
Security	Employees - Email Address, Mobile Device Information, IP Address	Legitimate Interests
AI-Powered Tool	Users - User Name, Non-PII data, Email Address	Legitimate Interests



Accounting	<p>Customers - Contracts, First Name, Last Name, Email Address, Telephone Number, Home Address, Subscription Data, Non-PII data</p> <p>Suppliers - Email Address, First Name, Last Name, Non-PII data, Contracts, Telephone Number, Home Address</p> <p>Employees - First Name, Last Name, Email Address, Non-PII data, Telephone Number, Home Address</p> <p>Company - Contracts, Non-PII data</p>	Legal Obligation Compliance
Product Development	<p>Company - Non-PII data, Source Code, Intellectual Property</p> <p>Users - User Name, Non-PII data, Email Address, Online Activity</p>	Legitimate Interests
CRM	<p>Customers - Date of Birth, First Name, Online Activity, Contracts, Gender, Job Title, Home Address, Subscription Data, Telephone Number, Last Name, Email Address, Non-PII data</p> <p>Business Partners - Date of Birth, First Name, Online Activity, Contracts, Gender, Job Title, Email Address, Last Name, Telephone Number</p> <p>Users - First Name, User Name, Last Name, Email Address, Non-PII data</p>	Data Subject Consent
Bookkeeping	<p>Customers - First Name, Last Name, Home Address, Email Address, Non-PII data, Telephone Number</p>	Legal Obligation Compliance
Email	<p>Employees - Email Address</p> <p>Customers - Date of Birth, First Name, Online Activity, Contracts, Gender, Job Title, Home Address, Subscription Data, Telephone Number, Last Name, Email Address, Non-PII data</p> <p>Business Partners - Date of Birth, First Name, Online Activity, Contracts, Gender, Job Title, Email Address, Last Name, Telephone Number</p> <p>Users - First Name, User Name, Last Name, Email Address</p>	Legitimate Interests



Communication	<p>Employees - Email Address</p> <p>Customers - Date of Birth, First Name, Online Activity, Contracts, Gender, Job Title, Home Address, Subscription Data, Telephone Number, Last Name, Email Address</p> <p>Business Partners - Date of Birth, First Name, Online Activity, Contracts, Gender, Job Title, Email Address, Last Name, Telephone Number</p> <p>Users - First Name, User Name, Last Name, Email Address</p>	Legitimate Interests
Website Hosting	<p>Company - IP Address, Source Code, Online Activity, Subscription Data, First Name, Email Address, Last Name, Job Title, Browser Information, Mobile Device Information, Non-PII data, Home Address</p> <p>Customers - IP Address, Source Code, Online Activity, Subscription Data, First Name, Email Address, Last Name, Job Title, Browser Information, Mobile Device Information, Non-PII data</p> <p>Users - First Name, Email Address, Last Name, IP Address, Online Activity, User Name, Subscription Data, Mobile Device Information</p>	Legitimate Interests
Application Hosting	<p>Company - IP Address, Source Code, Online Activity, Subscription Data, First Name, Email Address, Last Name, Job Title, Browser Information, Mobile Device Information, Non-PII data</p> <p>Customers - IP Address, Source Code, Online Activity, Subscription Data, First Name, Email Address, Last Name, Job Title, Browser Information, Mobile Device Information, Non-PII data</p> <p>Users - First Name, Email Address, Last Name, IP Address, Online Activity, User Name, Subscription Data, Mobile Device Information</p>	Legitimate Interests
Legal	<p>Company - Non-PII data, Email Address, Home Address, Telephone Number</p> <p>Employees - Non-PII data, Email Address, Home Address, Telephone Number</p> <p>Suppliers - Non-PII data</p>	Legal Obligation Compliance
Payment	<p>Customers - First Name, Last Name, Home Address, Email Address, Non-PII data, Telephone Number</p>	Contract Performance



## The types of personal data we may process through suppliers:

Business process	Data	Legal basis
Sales	Company - First Name, Email Address, Home Address, Non-PII data Customers - First Name, Email Address, Home Address, Non-PII data, Last Name, Job Title, Telephone Number, Contracts, Subscription Data	Legitimate Interests
Training	Company - Subscription Data, Contracts, Email Address, First Name, Non-PII data Employees - Subscription Data, Contracts, Email Address, First Name, Non-PII data	Data Subject Consent
Legal	Company - Email Address, Contracts, Subscription Data, First Name, Non-PII data Employees - Email Address, Contracts, Subscription Data, First Name, Non-PII data Stakeholders - Age or Age Group, First Name, Contracts, Last Name, Email Address, Copy of ID	Legal Obligation Compliance
Security	Company - Email Address, Telephone Number, Home Address Employees - Email Address, Telephone Number, Home Address Suppliers - Email Address, Telephone Number	Legitimate Interests
Product Development	Company - Non-PII data, Contracts, First Name, Home Address, Email Address, Source Code	Legitimate Interests
IT Supplier	Company - First Name, Date of Birth, Last Name, Job Title, Email Address, Telephone Number, Home Address, User Name, Mobile Device Information, IP Address Employees - First Name, Date of Birth, Last Name, Job Title, Email Address, Telephone Number, Home Address, User Name, Mobile Device Information, IP Address	Legitimate Interests



Accountancy	Company - Bank account or creditcard number, Salary Information, Job Title, Email Address, Contracts Employees - Bank account or creditcard number, Salary Information, First Name, Last Name, Date of Birth, Email Address, Copy of ID Customers - Email Address, Subscription Data, Contracts Suppliers - Email Address, Subscription Data	Legal Obligation Compliance
Insurance	Company - Bank account or creditcard number, Email Address, First Name, Home Address, Non-PII data, Subscription Data, Contracts	Legal Obligation Compliance
Marketing	Company - Email Address	Data Subject Consent
Website Development	Company - Contracts, First Name, Home Address, Non-PII data	Legitimate Interests
Consultancy	Company - Subscription Data, Contracts, Email Address, First Name, Non-PII data, Telephone Number, Home Address Employees - Subscription Data, Contracts, Email Address, First Name, Non-PII data, Telephone Number, Home Address Suppliers - Email Address, Telephone Number	Contract Performance

## Purposes

Cognishine Therapy and Education Ltd. processes personal data for one or more of the following purposes:

- Customer, employee, contractor, partner or supplier management
- Business and financial administration
- Direct marketing
- Delivery of goods or services
- Work planning

## How we collect, store or otherwise process your data:

The following business processes describe how we may collect, store or otherwise process the types of personal information:



- Collection of cookies, subscription to newsletter or filling out the contact form on the website(s);
- Analyse trends and profiles, for our legitimate interest to aim to enhance, modify, personalise and improve our services and communications for the benefit of our customers;
- Process and respond to support requests, enquiries and complaints received from you through use of business email;
- Provide services and products requested and/or purchased by you and to communicate with you about such services and/or products. We do this as necessary in order to carry out a contract with you and in accordance with our legitimate interest to operate a business;
- Carry out administrative activities such as invoicing and collecting payments either locally on devices or using cloud-services;
- Store and exchange personal information contained in documents through email and cloud-services;
- Marketing and customer acquisition through email or using cloud-services.

## Sharing data with third parties

We may have to share your data with third parties, including third-party service providers. We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your Personal Data outside Israel. If we do, you can expect a similar degree of protection in respect of your Personal Data.

We will only share your Personal Data with third parties in accordance with the GDPR and as outlined in the legal justification table above.

We share your personal data with the following enterprise third parties. We also share your data with SME third parties, details of which are available upon request. You will be notified when we have engaged with a new third party recipient of your personal data.

### Microsoft Office 365

<b>Function</b>	<b>Communication, Document Storage, Email, Office Management</b>
<b>Data categories</b>	<b>Email Address</b>
<b>Data subjects</b>	<b>Employees</b>



<b>Security measures</b>	<b>Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.</b>
--------------------------	---

## **Monday.com**

<b>Function</b>	<b>Communication, CRM, Document Storage, Email, Task Management</b>
<b>Data categories</b>	<b>Contracts, Date of Birth, Email Address, First Name, Gender, Home Address, Job Title, Last Name, Online Activity, Subscription Data, Telephone Number, User Name</b>
<b>Data subjects</b>	<b>Business Partners, Customers, Users</b>



<b>Security measures</b>	<b>Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.</b>
--------------------------	---

## Naq Cyber

<b>Function</b>	<b>Compliance, Legal</b>
<b>Data categories</b>	<b>Email Address, Home Address, Non-PII data, Telephone Number</b>
<b>Data subjects</b>	<b>Company, Employees, Suppliers</b>
<b>Security measures</b>	<b>Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.</b>

## AWS

<b>Function</b>	<b>Application Hosting, Website Hosting</b>
-----------------	---



<b>Data categories</b>	<b>Browser Information, Email Address, First Name, IP Address, Job Title, Last Name, Mobile Device Information, Non-PII data, Online Activity, Source Code, Subscription Data, User Name</b>
<b>Data subjects</b>	<b>Company, Customers, Users</b>
<b>Security measures</b>	<b>Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.</b>

## **Github**

<b>Function</b>	<b>Product Development</b>
<b>Data categories</b>	<b>Email Address, Intellectual Property, Non-PII data, Online Activity, Source Code, User Name</b>
<b>Data subjects</b>	<b>Company, Users</b>



<b>Security measures</b>	<b>Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.</b>
--------------------------	---

## Grammarly

<b>Function</b>	<b>AI-Powered Tool, Technical Tool</b>
<b>Data categories</b>	<b>Email Address, Non-PII data, User Name</b>
<b>Data subjects</b>	<b>Users</b>
<b>Security measures</b>	<b>Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.</b>

## Rivhit

<b>Function</b>	<b>Bookkeeping, Payment</b>
<b>Data categories</b>	<b>Email Address, First Name, Home Address, Last Name, Non-PII data, Telephone Number</b>
<b>Data subjects</b>	<b>Customers</b>



<b>Security measures</b>	<b>Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.</b>
--------------------------	---

### Michpal

<b>Function</b>	<b>Accounting</b>
<b>Data categories</b>	<b>Contracts, Email Address, First Name, Home Address, Last Name, Non-PII data, Subscription Data, Telephone Number</b>
<b>Data subjects</b>	<b>Company, Customers, Employees, Suppliers</b>
<b>Security measures</b>	<b>Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.</b>

### Mail Express

<b>Function</b>	<b>Email, Marketing</b>
-----------------	-------------------------



<b>Data categories</b>	<b>First Name, Last Name, Non-PII data</b>
<b>Data subjects</b>	<b>Customers</b>
<b>Security measures</b>	<b>Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.</b>

## Iubenda

<b>Function</b>	<b>Technical Tool</b>
<b>Data categories</b>	<b>IP Address, Non-PII data</b>
<b>Data subjects</b>	<b>Users</b>
<b>Security measures</b>	<b>Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.</b>

## MongoDB Cloud

<b>Function</b>	<b>Technical Tool</b>
<b>Data categories</b>	<b>Non-PII data</b>



<b>Data subjects</b>	<b>Customers</b>
<b>Security measures</b>	<b>Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.</b>

## **Apollo**

<b>Function</b>	<b>CRM</b>
<b>Data categories</b>	<b>Email Address, First Name, Home Address, Job Title, Last Name, Non-PII data, Subscription Data, Telephone Number</b>
<b>Data subjects</b>	<b>Customers, Users</b>
<b>Security measures</b>	<b>Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.</b>

## **Webflow**

<b>Function</b>	<b>Website Hosting</b>
-----------------	------------------------



<b>Data categories</b>	<b>First Name, Home Address, Non-PII data</b>
<b>Data subjects</b>	<b>Company</b>
<b>Security measures</b>	<b>Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.</b>

## SentinelOne

<b>Function</b>	<b>Security</b>
<b>Data categories</b>	<b>Email Address, IP Address, Mobile Device Information</b>
<b>Data subjects</b>	<b>Employees</b>
<b>Security measures</b>	<b>Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.</b>

## International data transfers

The third parties we have engaged for the abovementioned business process may transfer your personal information to outside of your jurisdiction. Cognishine Therapy and Education Ltd.'s third



party processors take all necessary measures to ensure the confidentiality, availability and integrity of personal data and to comply with the GDPR with regards to international data transfers. The international nature of its compliance certifications, as well as far-reaching technical security measures (including but not limited to encryption of the personal data, making the data illegible to an unauthorised recipient) are sufficient to ensure that the data subjects continue to benefit from the fundamental rights they are entitled to under the GDPR.

Where Cognishine Therapy and Education Ltd. transfers data to third countries, it relies on the following legal grounds for international data transfers:

- An Adequacy Decision in accordance with article 45 of the GDPR
- In the absence of an Adequacy Decision, appropriate safeguards in the form of Standard Contractual Clauses or Binding Corporate Rules.

In the event that Cognishine Therapy and Education Ltd. is reliant on Standard Contractual Clauses for the legality of its international data transfer, it ensures that the Processor or Subprocessor takes supplementary security measures to safeguard the international data transfer with one or more of the following measures:

- Encryption;
- Anonymisation;
- Pseudonymisation.

## **Storage and protection of data**

Your data is protected by Cognishine Therapy and Education Ltd. and its processors in pursuance to all legal requirements set by the relevant data processing laws. Cognishine Therapy and Education Ltd. has taken technical and organizational security measures to protect your data and requires its data processors to meet the same requirements. Cognishine Therapy and Education Ltd. has signed processing agreements with its processors to ensure an adequate level of data protection.

The following security measures are taken by Cognishine Therapy and Education Ltd. to protect your personal data in the course of the listed business processes:

## **Organisational security measures**

### **Staff**

Cognishine Therapy and Education Ltd. staff members are required to conduct themselves in a manner consistent with Cognishine Therapy and Education Ltd.'s guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. All staff members



undergo appropriate background checks prior to hiring and sign a confidentiality agreement outlining their responsibility in protecting customer data.

We continuously train staff members on best security practices, including how to identify social hacks, phishing scams, and hackers.

## **Access controls**

Cognishine Therapy and Education Ltd. maintains your data privacy by allowing only authorized individuals access to information when it is critical to complete tasks for you. Cognishine Therapy and Education Ltd. staff members will not process customer data without authorization.

## **Data hosting**

As a rule, data is hosted within countries and areas that provide a substantially similar level of protection as data subjects have under the GDPR. To ensure this, we rely on Adequacy Decisions as a legal basis for our international data transfers. In exceptional circumstances, where data is transferred to a country or area not subject to an Adequacy Decision, we rely on Standard Contractual Clauses with the recipient and take supplementary security measures to secure this data transfer, such as anonymisation.

## **Physical security**

The data centres on which personal data is hosted are secured and monitored 24/7 and physical access to facilities is strictly limited to select staff.

## **Technical security measures**

All devices which are used to access personal data for which we are responsible are secured with antivirus software, firewalls, encryption and access management. We regularly update operating systems and software to ensure vulnerabilities cannot be exploited.

We carry out regular vulnerability scanning of our website and have engaged credentialed external auditors to verify the adequacy of our security and privacy measures.

## **Your rights regarding information**

Each data subject has the right to information on and access to, and rectification, erasure and restriction of processing of their personal data, as well as the right to object to the processing and the right to data portability. You also have the right to request that you are not made subject to decision making based solely on automated processes, including profiling, if these decisions would have a significant effect on you.



You can exercise these rights by contacting us at the following email address: [info@cognishine.com](mailto:info@cognishine.com). If we have any doubts as to your identity, we may request you to provide us with proof of identification, such as through sending us a copy of your valid ID. Ensure that you write "Data Request" in the subject line of your email.

Within one month of the submitted request, you will receive an answer from us. We will not charge you for submitting your request unless the request is manifestly unfounded or otherwise unreasonable in its nature. Depending on the complexity and the number of the requests this period may be extended to two months.

## Marketing

- You may receive commercial offers from Cognishine Therapy and Education Ltd.. If you do not wish to receive them (anymore), please send us an email to the following address: [info@cognishine.com](mailto:info@cognishine.com) and ensure that you write "Data Opt-Out" in the subject line of your email.
- Your personal data will not be used by our partners for commercial purposes.
- If you encounter any personal data from other data subjects while visiting our website, you are to refrain from collection, any unauthorized use or any other act that constitutes an infringement of the privacy of the data subject(s) in question. The collector is not responsible in these circumstances.

## Data retention

The collected data are used and retained for the duration determined by law. You may, at any time, request your data to be deleted from any Cognishine Therapy and Education Ltd. account, system or other data processing medium in accordance with the process described above.

## Applicable law

These conditions are governed by the laws and regulations of the country where we are headquartered. The court in the district where we are headquartered has the sole jurisdiction if any dispute regarding these conditions may arise, save when a legal exception applies.

## Children's Data

We do not knowingly process children's data, unless specifically stated in this Privacy Policy. If you have concerns about or knowledge of a child using our services, products, websites or apps without parental consent, please contact our DPO via [george.frey@cognishine.com](mailto:george.frey@cognishine.com) to ensure we can take appropriate action as soon as possible.



## Contact

For questions about this privacy policy, product information or information about the website itself, please contact: [info@cognishine.com](mailto:info@cognishine.com).

## International data transfers

### Third Party Applications

#### Microsoft Office 365

<b>Third party headquarter address</b>	1 Microsoft Way, Redmond, WA 98052-6399, United States of America
<b>The primary location of processing is the United States of America.</b>	Personal data collected by Microsoft Office 365 may be stored and processed in any country where Microsoft Office 365 or its affiliates, subsidiaries, or service providers operate facilities.
<b>Safeguards (art. 45 GDPR)</b>	Standard Contractual Clauses
<b>Additional safeguards</b>	<ul style="list-style-type: none"><li>• Encryption</li><li>• Anonymisation where possible</li><li>• Pseudonymisation where possible</li></ul>
<b>For more information, see Microsoft Office 365's Privacy Policy</b>	<a href="https://privacy.microsoft.com/en-ca/privacystatement">https://privacy.microsoft.com/en-ca/privacystatement</a>

#### Naq Cyber

<b>Third party headquarter address</b>	Vlamingstraat 4, 2712BZ, Zoetermeer, The Netherlands
<b>The primary location of processing is the The Netherlands.</b>	Personal data collected by Naq Cyber may be stored and processed in any country where Naq Cyber or its affiliates, subsidiaries, or service providers operate facilities.
<b>Safeguards (art. 45 GDPR)</b>	Standard Contractual Clauses



<b>Additional safeguards</b>	<ul style="list-style-type: none"><li>• Encryption</li><li>• Anonymisation where possible</li><li>• Pseudonymisation where possible</li></ul>
<b>For more information, see Naq Cyber's Privacy Policy</b>	<a href="https://www.naqcyber.com/policies/privacy-policy">https://www.naqcyber.com/policies/privacy-policy</a>

## AWS

<b>Third party headquarter address</b>	410 Terry Ave. North, Seattle, WA, 98109-5210, United States of America
<b>The primary location of processing is the United States of America.</b>	Personal data collected by AWS may be stored and processed in any country where AWS or its affiliates, subsidiaries, or service providers operate facilities.
<b>Safeguards (art. 45 GDPR)</b>	Standard Contractual Clauses
<b>Additional safeguards</b>	<ul style="list-style-type: none"><li>• Encryption</li><li>• Anonymisation where possible</li><li>• Pseudonymisation where possible</li></ul>
<b>For more information, see AWS's Privacy Policy</b>	<a href="https://aws.amazon.com/privacy/">https://aws.amazon.com/privacy/</a>

## Github

<b>Third party headquarter address</b>	88 Colin P. Kelly Jr. Street, San Francisco, CA 94107, United States of America
<b>The primary location of processing is the United States of America.</b>	Personal data collected by Github may be stored and processed in any country where Github or its affiliates, subsidiaries, or service providers operate facilities.
<b>Safeguards (art. 45 GDPR)</b>	Standard Contractual Clauses



<b>Additional safeguards</b>	<ul style="list-style-type: none"><li>• Encryption</li><li>• Anonymisation where possible</li><li>• Pseudonymisation where possible</li></ul>
<b>For more information, see Github's Privacy Policy</b>	<a href="https://docs.github.com/en/github/site-policy/github-privacy-statement">https://docs.github.com/en/github/site-policy/github-privacy-statement</a>

## Grammarly

<b>Third party headquarter address</b>	548 Market Street, #35410 San Francisco, CA 94104, United States of America
<b>The primary location of processing is the United States of America.</b>	Personal data collected by Grammarly may be stored and processed in any country where Grammarly or its affiliates, subsidiaries, or service providers operate facilities.
<b>Safeguards (art. 45 GDPR)</b>	Standard Contractual Clauses
<b>Additional safeguards</b>	<ul style="list-style-type: none"><li>• Encryption</li><li>• Anonymisation where possible</li><li>• Pseudonymisation where possible</li></ul>
<b>For more information, see Grammarly's Privacy Policy</b>	<a href="https://www.grammarly.com/privacy-policy">https://www.grammarly.com/privacy-policy</a>

## Mail Express

<b>Third party headquarter address</b>	23 Center St., Middletown, NY, 10940, United States of America
<b>The primary location of processing is the United States of America.</b>	Personal data collected by Mail Express may be stored and processed in any country where Mail Express or its affiliates, subsidiaries, or service providers operate facilities.
<b>Safeguards (art. 45 GDPR)</b>	Standard Contractual Clauses



<b>Additional safeguards</b>	<ul style="list-style-type: none"><li>• Encryption</li><li>• Anonymisation where possible</li><li>• Pseudonymisation where possible</li></ul>
<b>For more information, see Mail Express's Privacy Policy</b>	<a href="https://help.mailexpress.com/hc/en-us/articles/1260803228570-Privacy-Policy">https://help.mailexpress.com/hc/en-us/articles/1260803228570-Privacy-Policy</a>

## Iubenda

<b>Third party headquarter address</b>	Via San Raffaele, 1 - 20121 Milan, Italy
<b>The primary location of processing is the Italy.</b>	Personal data collected by Iubenda may be stored and processed in any country where Iubenda or its affiliates, subsidiaries, or service providers operate facilities.
<b>Safeguards (art. 45 GDPR)</b>	Standard Contractual Clauses
<b>Additional safeguards</b>	<ul style="list-style-type: none"><li>• Encryption</li><li>• Anonymisation where possible</li><li>• Pseudonymisation where possible</li></ul>
<b>For more information, see Iubenda's Privacy Policy</b>	<a href="https://www.iubenda.com/privacy-policy/252372">https://www.iubenda.com/privacy-policy/252372</a>

## MongoDB Cloud

<b>Third party headquarter address</b>	1633 Broadway, 38th Floor New York, NY 10019, United States of America
<b>The primary location of processing is the United States of America.</b>	Personal data collected by MongoDB Cloud may be stored and processed in any country where MongoDB Cloud or its affiliates, subsidiaries, or service providers operate facilities.
<b>Safeguards (art. 45 GDPR)</b>	Standard Contractual Clauses



<b>Additional safeguards</b>	<ul style="list-style-type: none"><li>• Encryption</li><li>• Anonymisation where possible</li><li>• Pseudonymisation where possible</li></ul>
<b>For more information, see MongoDB Cloud's Privacy Policy</b>	<a href="https://www.mongodb.com/legal/privacy-policy">https://www.mongodb.com/legal/privacy-policy</a>

## Apollo

<b>Third party headquarter address</b>	440 N Barranca Ave #4750, Covina, CA 91723, United States of America
<b>The primary location of processing is the United States of America.</b>	Personal data collected by Apollo may be stored and processed in any country where Apollo or its affiliates, subsidiaries, or service providers operate facilities.
<b>Safeguards (art. 45 GDPR)</b>	Standard Contractual Clauses
<b>Additional safeguards</b>	<ul style="list-style-type: none"><li>• Encryption</li><li>• Anonymisation where possible</li><li>• Pseudonymisation where possible</li></ul>
<b>For more information, see Apollo's Privacy Policy</b>	<a href="https://www.apollo.io/privacy-policy">https://www.apollo.io/privacy-policy</a>

## Webflow

<b>Third party headquarter address</b>	398 11th Street, 2nd Floor, San Francisco, CA 94103, United States of America
<b>The primary location of processing is the United States of America.</b>	Personal data collected by Webflow may be stored and processed in any country where Webflow or its affiliates, subsidiaries, or service providers operate facilities.
<b>Safeguards (art. 45 GDPR)</b>	Standard Contractual Clauses



<b>Additional safeguards</b>	<ul style="list-style-type: none"><li>• Encryption</li><li>• Anonymisation where possible</li><li>• Pseudonymisation where possible</li></ul>
<b>For more information, see Webflow's Privacy Policy</b>	<a href="https://webflow.com/legal/privacy">https://webflow.com/legal/privacy</a>

## SentinelOne

<b>Third party headquarter address</b>	444 Castro St #400, Mountain View, CA 94041, United States of America
<b>The primary location of processing is the United States of America.</b>	Personal data collected by SentinelOne may be stored and processed in any country where SentinelOne or its affiliates, subsidiaries, or service providers operate facilities.
<b>Safeguards (art. 45 GDPR)</b>	Standard Contractual Clauses
<b>Additional safeguards</b>	<ul style="list-style-type: none"><li>• Encryption</li><li>• Anonymisation where possible</li><li>• Pseudonymisation where possible</li></ul>
<b>For more information, see SentinelOne's Privacy Policy</b>	<a href="https://www.sentinelone.com/legal/privacy-policy/">https://www.sentinelone.com/legal/privacy-policy/</a>

## Suppliers

### Naq

<b>Country where data is processed or sent to</b>	United Kingdom
<b>Safeguards (art. 45 GDPR)</b>	Standard Contractual Clauses
<b>Additional safeguards</b>	<ul style="list-style-type: none"><li>• Encryption</li><li>• Anonymisation where possible</li><li>• Pseudonymisation where possible</li></ul>



## KiM Kommunikation im Mittelpunkt GmbH

Country where data is processed or sent to	Germany
Safeguards (art. 45 GDPR)	Standard Contractual Clauses
Additional safeguards	<ul style="list-style-type: none"><li>• Encryption</li><li>• Anonymisation where possible</li><li>• Pseudonymisation where possible</li></ul>

## Amwins Global Risk Ltd

Country where data is processed or sent to	United States of America
Safeguards (art. 45 GDPR)	Standard Contractual Clauses
Additional safeguards	<ul style="list-style-type: none"><li>• Encryption</li><li>• Anonymisation where possible</li><li>• Pseudonymisation where possible</li></ul>

## Cleverdev

Country where data is processed or sent to	India
Safeguards (art. 45 GDPR)	Standard Contractual Clauses
Additional safeguards	<ul style="list-style-type: none"><li>• Encryption</li><li>• Anonymisation where possible</li><li>• Pseudonymisation where possible</li></ul>

## The Babel Group

Country where data is processed or sent to	United States of America
Safeguards (art. 45 GDPR)	Standard Contractual Clauses



<b>Additional safeguards</b>	<ul style="list-style-type: none"><li>• Encryption</li><li>• Anonymisation where possible</li><li>• Pseudonymisation where possible</li></ul>
------------------------------	---

## Favoured

<b>Country where data is processed or sent to</b>	United Kingdom
<b>Safeguards (art. 45 GDPR)</b>	Standard Contractual Clauses
<b>Additional safeguards</b>	<ul style="list-style-type: none"><li>• Encryption</li><li>• Anonymisation where possible</li><li>• Pseudonymisation where possible</li></ul>

## IS Connecting

<b>Country where data is processed or sent to</b>	Brazil
<b>Safeguards (art. 45 GDPR)</b>	Standard Contractual Clauses
<b>Additional safeguards</b>	<ul style="list-style-type: none"><li>• Encryption</li><li>• Anonymisation where possible</li><li>• Pseudonymisation where possible</li></ul>

## Grupo Damosal

<b>Country where data is processed or sent to</b>	Mexico
<b>Safeguards (art. 45 GDPR)</b>	Standard Contractual Clauses
<b>Additional safeguards</b>	<ul style="list-style-type: none"><li>• Encryption</li><li>• Anonymisation where possible</li><li>• Pseudonymisation where possible</li></ul>



## Agerite

Country where data is processed or sent to	Australia
Safeguards (art. 45 GDPR)	Standard Contractual Clauses
Additional safeguards	<ul style="list-style-type: none"><li>• Encryption</li><li>• Anonymisation where possible</li><li>• Pseudonymisation where possible</li></ul>

## Einat Sandler Leib

Country where data is processed or sent to	Canada
Safeguards (art. 45 GDPR)	Standard Contractual Clauses
Additional safeguards	<ul style="list-style-type: none"><li>• Encryption</li><li>• Anonymisation where possible</li><li>• Pseudonymisation where possible</li></ul>

## MD5 Consulting

Country where data is processed or sent to	United States of America
Safeguards (art. 45 GDPR)	Standard Contractual Clauses
Additional safeguards	<ul style="list-style-type: none"><li>• Encryption</li><li>• Anonymisation where possible</li><li>• Pseudonymisation where possible</li></ul>

## Best Suited Ltd

Country where data is processed or sent to	United Kingdom
Safeguards (art. 45 GDPR)	Standard Contractual Clauses



<b>Additional safeguards</b>	<ul style="list-style-type: none"><li>• Encryption</li><li>• Anonymisation where possible</li><li>• Pseudonymisation where possible</li></ul>
------------------------------	---

## South Med Supply, LLC

<b>Country where data is processed or sent to</b>	United States of America
<b>Safeguards (art. 45 GDPR)</b>	Standard Contractual Clauses
<b>Additional safeguards</b>	<ul style="list-style-type: none"><li>• Encryption</li><li>• Anonymisation where possible</li><li>• Pseudonymisation where possible</li></ul>