PRIVACY POLICY

Effective date: 1 August 2026

Version: 2

Last reviewed: 28 July 2026

CONTENTS

1. About this Policy

1.1 **Who we are.** Ithaca Technologies (Pty) Ltd, registration number 2025/641148/07, is a company incorporated in the Republic of South Africa. We provide technology solutions and services, including the **ODIN** platform, to clients within and outside South Africa. In this Policy, "we", "us" and "our" refer to Ithaca Technologies (Pty) Ltd, and "you" refers to the person whose personal information we process.

1.2 **What this Policy covers.** This Policy explains what personal information we collect, why we collect it, what we do with it, who we share it with, how long we keep it, and what rights you have. It applies to the Website, to our associated applications, and to information you give us when you deal with us as a client, supplier, business contact or enquirer.

1.3 **What this Policy does not cover.** This Policy does not deal with:

(a) personal information processed inside ODIN on behalf of a Client. Section 8 explains our limited role there, and the Client, not Ithaca, is responsible for giving notice to the people whose information it puts into ODIN;

(b) personal information of our employees, contractors and job applicants, which is dealt with separately and does not fall under this Policy; and

(c) the privacy practices of any third-party website that we link to.

1.4 **Read this with.** This Policy must be read together with our PAIA Manual, available at www.ithaca.co.za.

1.5 **Changes.** We may amend this Policy from time to time. Check this page periodically so that you are aware of the current version.

1.6 **Questions.** Contact details for our Information Officer are in Section 18.

2. Definitions

In this Policy:

"Client" means a business that has contracted with us to use ODIN.

"Client Data" means data, information, files and content provided by a Client, or generated through a Client's use of ODIN, excluding our own proprietary data.

"Data Subject" means the person to whom personal information relates.

"De-identify" has the meaning given in POPIA, being the deletion of information that identifies a Data Subject, or that can be used by a reasonably foreseeable method to identify or to re-identify a Data Subject.

"Information Officer" means the person designated by us under POPIA and PAIA, whose details are in Section 18.

"ODIN" means our proprietary software platform used by Clients to support the operational and management requirements of Emergency Medical Services businesses.

"PAIA" means the Promotion of Access to Information Act 2 of 2000.

"Personal Information" has the meaning given in POPIA.

"POPIA" means the Protection of Personal Information Act 4 of 2013.

"Process" and **"Processing"** have the meanings given in POPIA.

"Operator" has the meaning given in POPIA, being a person who processes personal information for a Responsible Party in terms of a contract or mandate, without coming under the direct authority of that Responsible Party.

"Regulator" means the Information Regulator of South Africa established under POPIA.

"Responsible Party" has the meaning given in POPIA, being a person who determines the purpose of and means for Processing Personal Information.

"Security Compromise" means a circumstance in which there are reasonable grounds to believe that Personal Information has been accessed or acquired by an unauthorised person.

"Special Personal Information" has the meaning given in section 26 of POPIA, and includes information concerning a person's health, biometrics, race, religious beliefs and criminal behaviour.

"Website" means www.ithaca.co.za and its associated applications.

3. The Capacity in Which We Process Your Information

3.1 **Two roles.** POPIA distinguishes between a Responsible Party, which decides why and how information is processed, and an Operator, which processes information on a Responsible Party's instruction. We act in both capacities, depending on the information concerned. Which capacity applies determines who you deal with and who carries the obligation.

3.2 **How the capacities apply:**

Information	Whose information	Our capacity	Who to contact
Website and enquiry data	Website visitors, enquirers	Responsible Party	Ithaca (Section 18)
Client contact and account administration data	Client representatives, billing and support contacts	Responsible Party	Ithaca (Section 18)
Supplier and business contact data	Supplier representatives	Responsible Party	Ithaca (Section 18)
Marketing contact data	Subscribers, prospects	Responsible Party	Ithaca (Section 18)
Client Data inside ODIN, including patient clinical records	Client staff, patients, other Client data subjects	Operator	The Client

Information	Whose information	Our capacity	Who to contact
De-identified analytical data derived from ODIN	Not attributable to any person	Responsible Party	Ithaca (Section 18)

3.3 **The same person, two capacities.** A Client's employee may fall into more than one row above. Where we hold that person's name, work email address and role because they are our contact for the contract, for billing or for support, we decide why we hold that information and we are the Responsible Party. Where the same person's details sit inside the Client's ODIN account as a user record, a rostered crew member or the author of a clinical report form, we hold that information on the Client's instruction and we are the Operator. Which capacity applies depends on why we hold the information, not on who the person is.

3.4 **Where we are the Responsible Party**, we carry the full set of obligations under POPIA, including lawful processing, notification, security safeguards, and dealing with your access, correction and objection requests directly.

3.5 **Where we are the Operator**, we process only on the documented instruction of the Client, under a written contract that meets sections 20 and 21 of POPIA. If your information sits inside a Client's ODIN account, the Client is the Responsible Party and you should direct your request to that Client. If you contact us instead, we will refer you to the Client and tell you that we have done so, unless the Client's instructions or the law require otherwise.

4. Information We Collect

4.1 **Information you give us.** We may collect:

(a) your name and contact details, including email address, telephone number and company details, submitted when you interact with the Website or with us;

(b) information you provide when you enquire about, negotiate for, or use our services; and

(c) any information that is the subject of a contract or service agreement between us.

4.2 **Information we collect automatically.** When you use the Website, our server logs automatically record information from your browser or mobile platform, including approximate location, IP address, cookie identifiers, device and browser type, and the pages you requested. Where this information relates to an identifiable person, we treat it as Personal Information and apply this Policy to it. We use it in aggregate form to measure Website use, maintain security, and improve content.

4.3 **Cookies.** We use cookies on the Website. Cookies are small files stored on your device that allow the Website to recognise a returning visitor. We use cookies that are necessary for the Website to function, and cookies that measure how the Website is used. Cookie information is aggregated to measure the number of visits, the

average time spent on the Website and the pages viewed, and is not used to identify you personally. You can block or delete cookies through your browser settings, although parts of the Website may not work correctly if you do.

4.4 **Information from other sources.** We may collect information about you from your employer or the organisation you represent, from public registers and public sources, and from Clients where you are their nominated contact.

4.5 **Voluntary or mandatory.** Supplying your information to us is voluntary, except where a law requires the collection or where the information is necessary to conclude or perform a contract with you. If you do not give us information we need, we may be unable to provide our services to you or to respond to your request.

4.6 **Third-party information you give us.** Where you give us the Personal Information of another person, you must have a lawful basis to do so and must tell that person that their details have been given to us. We will process their information in accordance with this Policy.

5. Why We Process Your Information

5.1 We process Personal Information to:

(a) provide the services you have requested and notify you of material changes to them;

(b) respond to your enquiries, requests and complaints;

(c) conclude, administer and perform contracts, including billing and account management;

(d) maintain internal records and follow up as part of our customer care processes;

(e) operate, secure, monitor and improve the Website, ODIN and our other systems, including detecting faults and investigating incidents;

(f) prevent, detect and investigate fraud and other criminal activity;

(g) comply with our obligations under South African law and respond to lawful requests from regulators, courts and law enforcement;

(h) conduct research, training and statistical analysis aimed at improving our services; and

(i) send direct marketing, subject to Section 9.

6. Our Lawful Basis for Processing

6.1 We process Personal Information only where section 11 of POPIA permits it. We rely on the following grounds:

(a) **Consent.** Where you have given voluntary, specific and informed consent to the processing, or a competent person has consented on behalf of a child.

(b) **Contract.** Where processing is necessary to conclude or perform a contract to which you are a party, or to take steps at your request before entering into a contract.

(c) **Legal obligation.** Where processing is necessary to comply with an obligation imposed on us by law.

(d) **Your legitimate interest.** Where processing protects a legitimate interest of yours.

(e) **Our legitimate interest.** Where processing is necessary for the legitimate interests we or a third party pursue, provided those interests are not overridden by your rights.

6.2 **Our legitimate interests.** Where we rely on clause 6.1(e), our interests are operating and improving our business and services, securing our networks and information, preventing fraud and criminal activity, managing supplier and business partner relationships, and establishing, exercising or defending legal claims.

6.3 **Objection.** You may object to processing based on clause 6.1(d) or 6.1(e) on reasonable grounds, in the manner set out in clause 15.4.

7. Special Personal Information and Children's Information

7.1 **Special Personal Information.** We do not process Special Personal Information as a Responsible Party except where sections 27 to 33 of POPIA permit it, most commonly with your consent or where processing is necessary to establish, exercise or defend a right in law.

7.2 **Health information in ODIN.** Clinical report forms and related patient records inside ODIN are Special Personal Information concerning health. We process this information only as an Operator, on the instruction of the Client. The Client is the Responsible Party and is responsible for establishing the authorisation for that processing under section 32 of POPIA, and for giving notice to patients. We treat this information as confidential and do not use it for any purpose other than delivering the services, except in de-identified form under clause 8.4.

7.3 **Children's information.** We do not knowingly collect the Personal Information of a child as a Responsible Party without the prior consent of a competent person. Where information about a child is processed inside ODIN, that processing takes place under the Client's authority and section 35 of POPIA authorisation, not ours. If you believe we hold a child's information without proper authorisation, contact the Information Officer and we will investigate and, where required, delete it.

8. ODIN and Client Data

8.1 **Our role.** ODIN is the platform our Clients use. Information processed through ODIN is subject to the terms of the agreement concluded between us and the Client. In respect of that information the Client is the Responsible Party and we are the Operator.

8.2 **What ODIN holds.** ODIN records:

(a) Client organisation data;

(b) Client business asset data, including employee information;

(c) clinical report forms and the information contained in them; and

(d) usage data.

8.3 **What we do with it.** We process Client Data only for the purposes recorded in the Client's agreement, being the provision and maintenance of ODIN, technical support and troubleshooting, storage and backup, system monitoring, security and performance optimisation, account communications, and the collection of analytical data. We do not process Client Data for our own purposes, and we do not disclose it to third parties except to sub-operators engaged under our agreement with the Client, or as required by law.

8.4 **De-identified analytics.** Where we use ODIN data to produce analytics and statistical insights, we de-identify it first in accordance with POPIA so that individual Data Subjects cannot be identified or re-identified. Special Personal Information is anonymised before any analytical processing. Once de-identified to the standard in section 6(1)(b) of POPIA, the resulting data falls outside POPIA and we process it as a Responsible Party for our own account, including to improve ODIN and develop new features.

8.5 **Notices to patients and Client staff.** Giving privacy notices to patients, employees and other Data Subjects whose information a Client places into ODIN, and recording consent where consent is the applicable ground, is the Client's obligation as Responsible Party. We do not deal directly with those Data Subjects.

9. Direct Marketing

9.1 **Consent.** Where we send you direct marketing by electronic communication and you are not an existing customer, we will first obtain your consent using the form prescribed by section 69(2) of POPIA and Regulation 6 (Form 4). We will only ask you once.

9.2 **Existing customers.** Where you are an existing customer, we may send you direct marketing about our own similar products and services on the basis of section 69(3) of POPIA. We obtain your details in the course of a sale, give you the opportunity to object at the time of collection, and give you that opportunity again in every communication we send.

9.3 **Opting out.** You may object or withdraw consent at any time, at no cost, using the unsubscribe mechanism in the communication or by contacting the Information Officer. We will stop sending marketing on request.

10. Sharing Your Information

10.1 **Who we share with.** We may disclose Personal Information to:

(a) operators and service providers who process it on our behalf, including hosting providers, Website analytics providers, communication and support tooling providers, and providers engaged to market and distribute our services;

(b) our professional advisers, including auditors, attorneys and insurers;

(c) judicial, regulatory and law enforcement bodies, where the law requires or permits it; and

(d) a third party that acquires all or part of our shares or assets, or that succeeds us in carrying on all or part of our business, whether by merger, acquisition, reorganisation or otherwise. Where this happens we will notify you by way of a banner on the Website.

10.2 **Operator obligations.** Every operator we engage is bound by a written contract that requires it to process Personal Information only on our instruction, to establish and maintain the security measures required by section 19 of POPIA, and to notify us immediately of any Security Compromise. We remain responsible for their performance.

10.3 **No sale.** We do not sell, rent or otherwise commercially exploit Personal Information for monetary consideration.

11. Cross-Border Transfers

11.1 **When transfers happen.** Some of the operators and service providers we use process Personal Information outside South Africa. Where that occurs, we transfer Personal Information only where section 72 of POPIA permits it.

11.2 **Basis for transfer.** We rely on one or more of the following:

(a) the recipient is subject to a law, binding corporate rules or a binding agreement that provides an adequate level of protection, including provisions on onward transfer substantially similar to section 72;

(b) you have consented to the transfer;

(c) the transfer is necessary to conclude or perform a contract between you and us, or between us and a third party in your interest; or

(d) the transfer is for your benefit, it is not reasonably practicable to obtain your consent, and you would be likely to give it if it were.

11.3 **ODIN hosting.** The hosting location for Client Data, and any change to it, is recorded in the Client's agreement. We do not transfer Client Data across a border without giving the Client prior written notice and complying with section 72 of POPIA.

11.4 **Details on request.** You may ask the Information Officer for details of the countries to which your Personal Information is transferred and the safeguards applied.

12. How We Secure Your Information

12.1 **Measures.** We take appropriate, reasonable technical and organisational measures to prevent loss of, damage to, or unauthorised destruction of Personal Information, and unlawful access to or processing of it, as required by section 19 of POPIA. These include access controls and authentication, encryption of data in transit and at rest, network and application monitoring, logging, backup and recovery procedures, and staff confidentiality obligations and training.

12.2 **Ongoing review.** We identify reasonably foreseeable internal and external risks to Personal Information in our possession or under our control, maintain safeguards against those risks, verify that the safeguards are effectively implemented, and update them in response to new risks or identified deficiencies. We have regard to generally accepted information security practices.

12.3 **Limits.** No system is immune to compromise. We do not warrant that our security measures will prevent every incident, and Section 14 sets out what we do if one occurs.

13. How Long We Keep Your Information

13.1 **General rule.** We keep Personal Information only for as long as necessary for the purpose for which it was collected, unless a law requires or authorises us to retain it for longer, we need it to establish, exercise or defend a legal claim, you have consented to longer retention, or it is retained in de-identified form for statistical or research purposes.

13.2 **Contract records.** Where we have contracted with you, we keep the information for the duration of the contract and thereafter for the period required by applicable law, including the retention periods under the Companies Act 71 of 2008 and tax legislation.

13.3 **Website and enquiry data.** Enquiry and marketing contact records are kept for 12 (twelve) months after your last interaction with us, unless you ask us to delete them sooner.

13.4 **Client Data.** Retention and deletion of Client Data inside ODIN is governed by the Client's agreement, including its backup retention period and its post-termination export and deletion terms. Clinical records carry statutory and professional retention obligations that rest with the Client as Responsible Party.

13.5 **Security Compromise records.** We keep records of Security Compromises, including the facts, effects and remedial action taken, for at least 5 (five) years.

13.6 **Your query.** You may ask us at any time whether we hold information about you, how long we intend to keep it, and to request its deletion.

14. Security Compromises

14.1 **Response procedures.** We maintain procedures to detect, investigate, assess and respond to any actual or suspected Security Compromise. On becoming aware of one, we contain and secure the affected systems, assess the scope, nature and

impact of the incident, and document the nature of the compromise, the categories of Personal Information involved, the number of Data Subjects affected, and the likely consequences.

14.2 **Notification where we are the Responsible Party.** Where there are reasonable grounds to believe that Personal Information for which we are the Responsible Party has been accessed or acquired by an unauthorised person, we notify the Regulator and the affected Data Subject as soon as reasonably possible after discovering the compromise. In setting that timing we take account of the legitimate needs of law enforcement and any measures reasonably necessary to determine the scope of the compromise and restore the integrity of our systems. Where a Data Subject's identity cannot be established, notification to that Data Subject is not required.

14.3 **Delay.** We may only delay notifying a Data Subject where a public body responsible for the prevention, detection or investigation of offences, or the Regulator, determines that notification will impede a criminal investigation.

14.4 **Content of the notification.** A notification to a Data Subject is made in writing and provides sufficient information to allow protective measures to be taken, including a description of the possible consequences of the compromise, a description of the measures we intend to take or have taken to address it, a recommendation on steps you can take to mitigate the possible adverse effects, and, if known to us, the identity of the unauthorised person.

14.5 **Method.** We communicate the notification by email to your last known address, by post to your last known physical or postal address, by a prominent notice on the Website, by publication in the news media, or as the Regulator directs.

14.6 **Where we are the Operator.** Where the compromise affects Client Data, we notify the affected Client immediately, and in any event within 24 (twenty-four) hours of becoming aware of it, and give the Client reasonable assistance to meet its own obligations under section 22 of POPIA. The Client, as Responsible Party, is responsible for notifying the Regulator and the affected Data Subjects.

14.7 **Publication.** The Regulator may direct us to publicise a Security Compromise, and we will comply with any such direction.

14.8 **Review.** After a Security Compromise we review our security measures and procedures to identify improvements and reduce the likelihood of recurrence. We may engage external cybersecurity specialists, legal counsel or other third parties to assist with response, investigation and remediation.

15. Your Rights

15.1 **What you can do.** Subject to POPIA, you have the right to:

(a) be notified that we are collecting your Personal Information, and that it has been accessed or acquired by an unauthorised person;

(b) confirm free of charge whether we hold Personal Information about you, and request a record or description of it;

(c) request that we correct or delete Personal Information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully;

(d) request that we destroy or delete a record of Personal Information that we are no longer authorised to retain;

(e) object, on reasonable grounds, to the processing of your Personal Information under clause 6.1(d) or 6.1(e);

(f) object at any time to processing for direct marketing purposes;

(g) withdraw consent, where processing is based on consent, without affecting the lawfulness of processing before withdrawal;

(h) not be subject to a decision based solely on automated processing, as set out in Section 16;

(i) submit a complaint to the Regulator; and

(j) institute civil proceedings regarding an alleged interference with the protection of your Personal Information.

15.2 **Access requests.** Requests for access are dealt with under PAIA. The fees for obtaining a copy or description of Personal Information held about you are prescribed by PAIA. Confirmation of whether or not we hold your Personal Information is free. Our PAIA Manual is available at www.ithaca.co.za.

15.3 **Correction and deletion.** Requests to correct or delete must be made to the Information Officer on the form prescribed by Regulation 3 to POPIA (Form 2).

15.4 **Objections.** Objections must be made to the Information Officer on the form prescribed by Regulation 2 to POPIA (Form 1), setting out the reasonable grounds relied on. Once you object, we stop processing the information concerned unless the law requires or permits us to continue.

15.5 **Verification and timing.** We may ask you for proof of identity before acting on a request, so that we do not disclose information to the wrong person. We respond to requests within the timeframes prescribed by POPIA and PAIA and, where no timeframe is prescribed, within a reasonable time.

15.6 **Requests about ODIN data.** If your request concerns information held inside a Client's ODIN account, direct it to that Client. See clause 3.5.

16. Automated Decision-Making

16.1 **We do not do this.** We do not make decisions about you that produce legal consequences for you, or that affect you to a substantial degree, based solely on the automated processing of Personal Information intended to provide a profile of you.

16.2 **If this changes.** We will update this Policy before introducing any such processing, and will comply with section 71 of POPIA, including by providing you with sufficient information about the underlying logic of the automated processing and an opportunity to make representations about the decision.

17. No Sale of Personal Information

17.1 We do not sell, rent or otherwise commercially exploit Personal Information to third parties for monetary consideration.

18. Contact Us

18.1 **Information Officer.** We have designated an Information Officer in accordance with POPIA, registered with the Regulator, who is responsible for ensuring compliance with our data protection obligations and for handling privacy enquiries. You may contact us on any privacy matter, including exercising your rights under this Policy or POPIA, using the following details:

Item	Detail
Information Officer	Niel Sadie
Email address	info@ithaca.co.za
Registered address	485 on Dawn Street, Lynnwood, Pretoria

18.2 **Specific enquiries.**

(a) **General privacy questions.** Use the contact details in clause 18.1.

(b) **Access requests.** Submit a written request to the Information Officer using the details in clause 18.1, in the manner set out in our PAIA Manual.

(c) **Correction, deletion and objection.** Submit the prescribed form to the Information Officer using the details in clause 18.1.

19. Complaints

19.1 **Raising a complaint with us.** Any complaint may be made by contacting the Information Officer using the details in clause 18.1. We ask that you raise your complaint with us first so that we have an opportunity to resolve it. You are under no obligation to do so, and you remain free to approach the Regulator directly at any time, whether or not you have raised the matter with us.

19.2 **Complaints to the Regulator.** If we cannot resolve your complaint, or you are unsatisfied with how we handled it, you have the right to complain to the Regulator. Complaints must be made in the manner and form prescribed by Regulation 7 to POPIA (Form 5), available on the Regulator's website.

19.3 **Regulator contact details:**

Item	Detail
Physical address	Woodmead North Office Park, 54 Maxwell Dr, Woodmead, Sandton, 2191
Phone number	010 023 5200

Item	Detail
Toll free number	0800 017 160
General enquiries	enquiries@inforegulator.org.za
POPIA complaints	POPIAcomplaints@inforegulator.org.za
PAIA complaints	PAIAcomplaints@inforegulator.org.za
Website	www.inforegulator.org.za