GoLogic Privacy Policy

PUBLIC

ISO 27001 HIPAA

Our Organization

Across our organization and brands, we value collaboration, communication and trust. Our policies are an important foundation in providing clear expectations and guidelines to ensure success for our customers, for our people, for our products and as an organization to maintain standards, security and compliance.

Our policies cover the following entities and/or brands: *GoFax, GoLogic, Faxaroo, Notifyre, Notifyre LLC, Stirdie and GoEmail*. We refer to these entities and/or brands as ‘our organization’.

Purpose

At GoLogic we are strongly committed to maintaining the privacy of our customers' and users' personal information. We strictly comply with the Australian Privacy Principles (APPs) under the Privacy Act 1988 (Cth), as amended. We will not sell or disclose your information to any other organisation unless required by law. This policy explains how and why we collect, use, hold and disclose your personal information.

Information Collection and Use

At GoLogic, to provide our services and/or to improve our users' and visitors' experience, we may collect personal information from visitors, enquiries and customers on our website. Personal information such as (but not limited to) name, company name, email, contact numbers and credit card details may be requested through relevant and suitable channels such as telephone, email, website enquiry forms, website free trial offers or general account registration forms. Account usernames and passwords for relevant services may also be collected and stored, enabling users to access our secure sites. If you do not provide us with your personal information, we may not be able to provide you with our services, communicate with you or respond to your enquiries.

To access and/or improve our services, cookies (a piece of text placed or stored by a user's web browser for record keeping) may be used. Cookies are generally used to enable our online services, to manage and improve our visitors' experiences, and to improve our advertising and/or web traffic monitoring. Depending on a user's web browser and settings, computers can be configured to accept or reject cookies, or they can be deleted and/or may expire after a period of time. In some instances, if cookies are disabled, it may affect access to some of the content and facilities on our website.

For GoLogic to provide its services, information on account usage, reports and transmission/document history may be stored securely online for a limited period of time or as required by law. See the Terms and Conditions of the relevant service. Such information will only be used to provide users' relevant GoLogic services and/or to provide support or to improve our services to our customers. We will also take reasonable steps to destroy or de-identify personal information once we no longer require it for the purposes for which it was collected, when a default or configured retention period has passed or for any secondary purpose permitted under the APPs. In accordance with the Telecommunications (Interception and Access) Act 1979 (Cth), customer metadata will be stored for two years after cancellation of the account with GoLogic.

We will be open and clear about the information we collect and what we do with information you provide. If you do not wish to receive information from GoLogic, unless required to use our services, you can opt out at any time.

We will use your personal information to offer you products and services we believe may interest you, but we will not do so if you tell us not to. Where you receive electronic marketing communications from us, you may opt out of receiving further marketing communications by following the opt-out instructions provided in the communication.

Anonymity and Pseudonymity

Where it is lawful and practicable to do so, you have the option of not identifying yourself, or of using a pseudonym, when dealing with us, for example for general enquiries that do not

require us to act on your behalf. However, in most cases we need to verify your identity to provide our services, such as account creation, billing, and fax, SMS or email transmission services, so it will often not be practicable for us to deal with you anonymously or under a pseudonym. Where this is the case, we will tell you why at the time.

Sensitive Information

Sensitive information is a special category of personal information under the APPs and includes information such as health information, and information about racial or ethnic origin. GoLogic does not seek to collect sensitive information as part of its ordinary services. Where sensitive information is incidentally contained within content that customers choose to send, store or transmit using our services, for example the content of a fax, SMS or email, we collect and hold that information only as a service provider acting on the customer's instructions, and we do not use or disclose it for any purpose other than providing the service, unless required or authorised by law. Where GoLogic itself needs to collect sensitive information directly from an individual for its own purposes, we will only do so with that individual's consent, or where an exception under APP 3.4 applies.

Unsolicited Personal Information

If we receive personal information that we did not solicit, we will assess whether we could have lawfully collected it had we sought it. If we could not have, and the information is not contained in a Commonwealth record, we will destroy or de-identify that information as soon as practicable, provided it is lawful and reasonable to do so.

Security of Information

Strict guidelines are followed to ensure our users' and customers' information is protected. These guidelines include, but are not limited to, secure websites for collecting and storing information, secure hosting sites requiring authorised access, dedicated processes for information collection and data management, and strict employee training and confidentiality obligations.

All information will be kept confidential to the best of our ability. However, due to the nature of online communication, we cannot guarantee the security of transmissions that occur beyond our security control, such as transmissions across the open internet.

In line with the Terms and Conditions of GoLogic services, account holders and users are responsible for securely managing their account access and login details. GoLogic will take no responsibility for the mismanagement or disclosure of account access or login details on the customer's behalf.

You may access or request correction of the personal information that we hold about you by contacting us using the details set out below. There are some circumstances in which we are

not required to give you access to your personal information, and if this applies, we will tell you why.

There is no charge for requesting access to your personal information, but we may require you to meet our reasonable costs in providing you with access, such as the cost for time spent collating large amounts of material.

We will respond to your requests to access or correct personal information within a reasonable time and will take all reasonable steps to ensure that the personal information we hold about you remains accurate, up to date and complete.

Cross-Border Disclosure of Personal Information

GoLogic may use suppliers, hosting providers, routing carriers or other contractors located outside Australia to help deliver our services, for example alternate telecommunications routing providers that use gateways located overseas.

Before we disclose your personal information to an overseas recipient, we will take reasonable steps to ensure that the recipient does not breach the APPs in relation to that information, for example by requiring the recipient to comply with the APPs or an equivalent privacy law under contract. Where an exception under APP 8.2 applies, such as your express consent or a requirement of law, we may disclose personal information overseas without taking those steps. We will not otherwise disclose your personal information to overseas recipients.

Accuracy of Information

We will, where possible, keep all information about our users and account holders up to date and relevant. However, in many instances, users can control and update their own information online via their secure web account access. We may also, from time to time, contact you through various methods to request up-to-date information.

External Links

Where there are links to external sites, unless through direct supply of our services, GoLogic is not responsible for the information or data collection processes these external sites manage.

Customer Access

Customers are secured by a personal username and password, and where activated, other controls made available, such as multi-factor authentication. No details are accessible regarding passwords by any employee, and information is stored with secure access only by the individual creator. Customers can request a change of password or a new password via their registered email address. Account change requests will require verification; no information or account transfers will be undertaken without the authorised consent of the account owner or admin user.

Customer Information Obtained for Account Management

Due to the nature of the services provided, there are minimum details required to gain access to GoLogic services, including but not limited to:

- First Name
- Last Name
- Company Name
- Email
- Phone
- Country

How We Disclose Your Information

We may disclose your information to third parties who provide services to us, including organisations and contractors that assist us with the purposes for which we use your information. These services include:

- customer enquiries
- mailing operations, billing, and debt-recovery functions
- information technology and network services

We may also disclose your information:

- to your authorised representatives or advisers, or when you ask us to do so
- to other telecommunications and information service providers to provide porting and/or information regarding your existing contracts or services
- to the manager of the Integrated Public Number Database (IPND), the Australian Communications and Media Authority (ACMA) and other organisations as required or authorised by law
- to law enforcement and national security agencies, and other government and regulatory authorities as required or authorised by law
- to third parties who assist us to manage or develop our business and corporate strategies and functions, including our corporate risk or funding functions
- for the purposes of facilitating or implementing a transfer or sale of all or part of our assets or business
- where you have expressly consented to the disclosure, or the consent may be reasonably inferred from the circumstances
- where we are otherwise permitted to disclose the information under the Privacy Act

Some of the third parties described above may be located overseas. See Cross-Border Disclosure of Personal Information above.

Notifiable Data Breaches

GoLogic has processes in place to identify, assess and respond to data breaches in accordance with Part IIIC of the Privacy Act 1988 (Cth), the Notifiable Data Breaches scheme.

If we become aware of, or reasonably suspect, a data breach involving personal information we hold, we will promptly investigate and assess whether the breach is an eligible data breach, that is, whether it is likely to result in serious harm to any individual to whom the information relates.

Where we determine that an eligible data breach has occurred, we will, as soon as practicable:

- notify affected individuals of the breach, including the information involved and our recommended steps for them to take in response; and
- notify the Office of the Australian Information Commissioner (OAIC).

Our internal breach response procedures set out the detailed steps our employees must follow when a suspected breach is identified. This policy is to be read together with, and does not replace, those internal procedures.

Where a breach involves protected health information (PHI) that GoLogic processes on behalf of a U.S. HIPAA covered entity or business associate, we will additionally comply with the HIPAA Breach Notification Rule (45 CFR 164.400-414) and the notification obligations set out in the applicable Business Associate Agreement, including notifying the affected covered entity or business associate without unreasonable delay and no later than 60 days after discovery of the breach.

Complaints

If you have a complaint about the way in which we have handled any privacy issue, including your request for access to or correction of your personal information, you should contact us using the details set out below.

We will consider your complaint and determine whether it requires further investigation. We will acknowledge your complaint, investigate it, and notify you of the outcome within a reasonable time.

If you are not satisfied with our response to your complaint, or with how we have handled it, you may complain to the Office of the Australian Information Commissioner (OAIC):

- Website: OAIC
- Phone: 1300 363 992

- Post: GPO Box 5288, Sydney NSW 2001

United States - HIPAA (Health Insurance Portability and Accountability Act)

Where GoLogic creates, receives, maintains or transmits protected health information (PHI) on behalf of a U.S. HIPAA covered entity or another business associate, for example health-related content sent via fax, SMS or email through GoFax, Faxaroo or Notifyre, GoLogic acts as a business associate under HIPAA and enters into a Business Associate Agreement (BAA) with that covered entity or business associate before processing PHI on its behalf.

As a business associate, GoLogic:

- uses and discloses PHI only as permitted or required by the applicable BAA, or as otherwise permitted or required by law;
- applies the minimum necessary standard, using, disclosing and requesting only the minimum amount of PHI needed for the purpose (45 CFR 164.502(b), 164.514(d));
- maintains administrative, physical and technical safeguards for electronic PHI consistent with the HIPAA Security Rule (45 CFR Part 164, Subpart C);
- reports any impermissible use or disclosure of PHI, and any breach of unsecured PHI, to the affected covered entity or business associate without unreasonable delay, consistent with the applicable BAA and 45 CFR 164.410 and 164.408, generally no later than 60 days after discovery;
- where GoLogic holds PHI in a designated record set on a covered entity's behalf, assists that covered entity or business associate in responding to an individual's request to: access PHI (45 CFR 164.524); amend PHI (45 CFR 164.526); receive an accounting of disclosures of PHI (45 CFR 164.528); restrict certain uses or disclosures of PHI (45 CFR 164.522(a)); or receive confidential communications of PHI (45 CFR 164.522(b));
- flows these same obligations down to any subcontractor that creates, receives, maintains or transmits PHI on GoLogic's behalf (45 CFR 164.502(e)(1)(ii)).

Individuals seeking to exercise the HIPAA rights listed above, or to obtain a copy of a covered entity's Notice of Privacy Practices (45 CFR 164.520), should contact the covered entity that provided their health information to GoLogic's services, as that entity - not GoLogic - is responsible for responding to such requests. GoLogic will support that entity's response where GoLogic holds the relevant PHI.

In addition to the complaint rights described above, individuals may lodge a complaint about a potential HIPAA violation directly with the U.S. Department of Health and Human Services, Office for Civil Rights (OCR):

- Online: the OCR Complaint Portal at U.S. Department of Health & Human Services - Office for Civil Rights
- Phone: 1-800-368-1019 (TDD: 1-800-537-7697)
- Email: OCRMail@hhs.gov

No individual will be subject to retaliation, intimidation or any other adverse action for filing a complaint or exercising any right under HIPAA (45 CFR 164.530(g)).

GoLogic's Privacy Officer is the individual designated as responsible for HIPAA compliance, including developing and implementing this policy, receiving HIPAA-related complaints, and workforce training on the handling of PHI (45 CFR 164.530(a)-(b)). Workforce members who fail to comply with this policy or an applicable BAA are subject to sanctions under GoLogic's internal disciplinary procedures (45 CFR 164.530(e)).

Contact Details

If you have any questions, comments, or concerns, please contact us at:

GoLogic

ABN: 53 105 263 974

100/1 Gardak St, Alexandra Headland, QLD. 4572. Australia

Phone: 1300 667 355 / +61 (0)7 5227 8300

Fax: 1300 764 413 / +61 7 4051 3399

Attention: Privacy Officer compliance@gologic.com.au

Changes to This Policy

From time to time, we may change our policy on how we handle personal information or the types of personal information which we hold. Any changes to our policy will be published on our website. You may obtain a copy of our current policy by downloading a copy from our website or by contacting us at the contact details above.

Document Information

Document Number:	GG-POL-051
Classification:	Public
Version Number:	1.9
Last Update:	10 August 2026

Next Review Date:	10 August 2027
Review Frequency:	Annually
Author:	Mali Harpur
File Name:	GoLogic Privacy Policy.docx
Document Title:	Privacy Policy
Policy Owner:	Privacy Officer
Standard:	ISO 27001:2022 A5.33, A5.34; HIPAA Privacy Rule 45 CFR 164.502(b), 164.506, 164.514(d), 164.520, 164.522, 164.524, 164.526, 164.528, 164.530; HIPAA Security Rule 45 CFR 164.312; HIPAA Breach Notification Rule 45 CFR 164.400-414; Privacy Act 1988 (Cth) Schedule 1 (APPs), Part IIIC (Notifiable Data Breaches)