Policy

Information Security, GDPR, POPIA

Last Updated: October 2024

Sendmarc
sendmarc.com | info@sendmarc.com

| **North America**
Raleigh

| **Netherlands**
Amsterdam

| **Argentina**
Buenos Aires

| **South Africa**
Johannesburg

| **Canada**
Toronto

| **Australia**
Brisbane

Contents

Sendmarc: is a global company and its affiliates, including and limited to

- Sendmarc Inc, Registration Number SR# 20230211167, 2020 Progress Suite 100-139, Raleigh, North Carolina, 27608
- Sendmarc Europe B.V, Registration Number RSIN 864234818, Keizersgracht 555, Amsterdam 1017 DR, Netherlands.
- Sendmarc (Pty) Limited, Registration Number 2018/336082/07, 1 Sturdee Avenue, Rosebank, South Africa, 2196.

Chief Information Security Officer:

Sam Hutchinson

Overview

Sendmarc's purpose is to make email a secure & legitimate communication channel. We achieve this by enabling organizations to protect their staff, customers and suppliers from email phishing and spoofing attacks originating from their own domain which is achieved using the global standard of DMARC.

This document presents Sendmarc's Information Security Policy and governs all information security procedures & processes.

Sendmarc is a SaaS web application and service provider that processes the following data:

- Personal Information relating to its Customer/s and any staff as required by it;
- DMARC reports from reporters about a Customer's domain. Approval is necessary by the domain owner for Sendmarc to receive DMARC reports;
- Intellectual Property submitted by the Customer, with its approval;
- Domain reports from reporters about a Customer's domain. Approval is necessary by the domain owner for Sendmarc to receive Domain reports;
- Data retrieved from the web as to publicly registered domains;
- Dark Web scan reports from reporters about a Customer's email address;

In compliance with the relevant data protection legislation, Sendmarc has two distinct responsibilities:

- We are the Responsible Party/Controller regarding customers Personal Information, including but not limited to: company details, user details, such as email addresses, phone numbers, billing details and any other information required to perform the Services.
- We are the Operator/ Processor of the Personal Information that the customer provides to us, pursuant to rendering services, as we process the personal information on your behalf.

The following terms shall have the meaning as set out hereunder:

“Data Subject” means an identifiable, living natural person or an existing, juristic person as is relevant ;

“Personal Information” means any personal information, otherwise called personal data, relating to a living, identifiable natural person and where it is applicable under the relevant isolation, and existing, juristic person.

“Responsible Party” means a public or private body any person who, alone or in conjunction with any other party determines the purpose of and the means for processing the personal information;

“Operator” means a person who processes personal information for responsible party in terms of a contract or mandate, without coming under the direct authority or control of that party;

1.1. Purpose

The purpose of this Policy is to define Sendmarc's Information Security Policy in respect of the following:

Part A: The Sendmarc Platform

The Sendmarc Platform manages the Customer's DMARC data, DMARC Policy, SPF, DKIM and BIMI entries. No other systems have access to this data or policies.

Part B: Employee Access Controls

Access to a client's Sendmarc services is limited to approved staff that are required to access our Platform and Administration Systems. Sendmarc has taken to ensure client data is kept safe even within the walls of Sendmarc's offices.

Part C: Business Administration Systems

Business Administrations Systems (BAS) are the supporting systems that Sendmarc Pty Ltd uses to operate the business. Examples of such systems are financial processing, tickets systems, CRM and others. None of the BAS has access to the data managed by The Sendmarc Platform.

1.2. Scope

Sendmarc's Information Security Policy contained within this document applies to all Sendmarc employees, affiliates and contractors.

1.3. Legal, Regulatory and Governance

Sendmarc is compliant with the following legislative, regulatory or good governance requirements:

1. Protection of Personal Information Act, 4 of 2013 (POPIA);
2. Electronic Communications and Transactions Act, 25 of 2002 (ECTA);
3. The Consumer Protection Act, 68 of 2008 (CPA);
4. The EU General Data Protection Regulation 2016/679 (EU-GDPR);
5. The UK General Data Protection Regulation (UK-GDPR);

Part A: The Sendmarc Platform

The Sendmarc Platform may manage a Customer's DMARC data, DMARC Policy, SPF, DKIM, MTA-STS, TLS-RPT and BIMI entries. The data to which the Platform has access to is described in Section 4, and no other system has access to this data or policies unless directly authorized by the Customer via the Sendmarc Platform API.

1. Platform Environment

The Sendmarc Platform and its services are hosted in Microsoft Azure using their high-availability, highly scalable platforms. Sendmarc's production environment is designed for maximum security, uptime, scalability and performance.

1.1. Server Setup

All Sendmarc Platform services exist on a virtual private network and are not accessible outside of the Sendmarc Azure environment. Traffic on the private VLAN is fully encrypted using SSL and TLS.

Only the web application's interface is accessible publicly to authorized users through a load-balancer and firewall. The firewall has intrusion prevention technology and inspects all traffic passed onto the web application service.

The web application has built-in DDoS protection to ensure we prevent attacks on the customer portal.

Sendmarc's Azure services include the following:

- Azure Kubernetes Service (AKS) instance to run the application portal and associated workloads. https://azure.microsoft.com/en-in/services/kubernetes-service
- MariaDB Database Service to store the structured application data. https://azure.microsoft.com/en-in/services/mariadb
- Redis Caching service for message brokering between job queues and for in-memory storage. https://azure.microsoft.com/en-in/services/cache
- Azure DNS service provides the backend to host system-generated DNS records. https://azure.microsoft.com/en-in/services/dns
- File storage for file access and management – see Section 1.3

Sendmarc also makes use of Cloudflare (https://www.cloudflare.com/application-services/products/dns/) for the hosting of system-generated DNS records.

1.2. Server Access Control

Sendmarc ensures that access to services is strictly controlled. Sendmarc uses Microsoft's Active Directory to manage employee access, and all sever access is controlled using 2FA.

This is consistently audited and maintained to remain in line with our internal policies. Only approved staff have access to our server infrastructure for maintenance and client service purposes.

1.3. Data Storage

All data is stored using Azure General Purpose V2 storage as described here:

- https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview

Azure General Purpose V2 ensures the security of customer data and has redundant infrastructure which encrypts the data-at-rest as well as in-transit.

When Sendmarc transfers Personal Information we will ensure that any organization with whom we share it, outside the Republic of South Africa will treat it with the same level of protection that we are obliged to, in accordance with the relevant legislation.

For data subjects in the EEA or Switzerland : Where Personal Information is transmitted from a location within the EEA or Switzerland to a country or international organization outside of the EEA or Switzerland and that country does not provide a level of protection for Personal Information which the European Data Commission ("the Commission") deems adequate, we use and adhere to the standard contractual clauses ("SCC's") approved by the Commission to legitimately transfer Personal Information.

1.3.1.Data Encryption

All data-at-rest in our file storage and databases is encrypted using managed private keys. This data is decrypted when accessed and then encrypted during transit using SSL and TLS protocols.

1.3.2.Logical Separation

Data is logically separated both in the file store and the database. The application has strict controls in place to ensure that all data is segregated correctly and there is no possibility of a crossover.

1.3.3.Backups

All backups are encrypted using AES 256-bit encryption.

2. Application Security

Sendmarc has been designed and developed from the ground up with the strictest security standards in mind. Principles common to web-based applications are built into every layer of the software. Industry-leading technology is used to ensure resilience to attacks and malicious use.

2.1. Attack Mitigation

The following are just some of the attacks we protect against:

- Distributed Denial of Service (DDoS) attacks – This is built into our network layer and sits in front of the public IP address to access the application.
- Cross-Site Scripting attacks – all user data displayed in the user interface is escaped to ensure that scripts cannot be executed in the browser.
- Cross-Site Request Forgery attacks – All forms contain a special key to ensure that attackers cannot attempt requests to the system outside of the product.
- SQL Injection attacks – The application validates all input for data type and structure. On top of this, all data sent to the database is escaped to prevent query execution.

2.2. HTTPS

All Sendmarc web traffic is transmitted using HTTPS. The certificates used for this encryption are automatically rotated every three months.

2.3. Application Access Control

Access to the Sendmarc application is controlled using a combination of secure user logins and user roles. The users, as well as their associated permission levels, can be controlled by an account administrator using the user management built into to application.

2.3.1. Passwords

All passwords in Sendmarc are encrypted using strong, one-way encryption algorithms. Passwords are salted before being run through the encryption algorithms to ensure that the encrypted password values are unique and protected against attacks on hashed passwords. Passwords are required to have a minimum length and complexity.

2.3.2. User Roles & Access Control

Sendmarc users can be limited to certain functions and areas of the product. This is done using role-based controls. The access rights are controlled by the account administrator nominated by your company.

2.3.3. Event & Activity Logging

All updates to Sendmarc data are logged with a timestamp and user identifier to allow us to build an audit trail of modifications.

Sendmarc tracks and monitors user login and password resets to detect any activity that is out of the ordinary. This allows us to prevent attacks on the system and ensure data integrity.

System errors are logged, and those logs are analyzed to create reports on system health as well as potential bugs. These errors are fixed and shipped daily, maintaining the quality and dependability of the application.

2.4. Change & Quality Control

Sendmarc has services that monitor performance, health, status and availability of the application. These systems automatically alert our administrators of any downtime, malicious attacks, or spikes in server load. With this real-time monitoring runs around the clock to keep the application online.

2.5. Quality Assurance

Sendmarc ships updates and bug fixes into production daily. In order to do this, while ensuring no downtime, there are several quality assurance practices that we follow.

2.5.1.Code Reviews

All code that is added to our version control system is reviewed before it can be shipped live. When performing a review, we look at the quality of the code to prevent bugs as well as ensuring the code is secure and not open to abuse.

2.5.2.Automated Testing

Our code and systems are run through a series of automated unit tests and quality assurance pipelines. If any of these fail at any point in time, the process is stopped, and administrators are alerted about the problem. Steps are then taken to resolve the issue and a post-mortem performed to prevent similar errors from occurring again.

2.5.3.System Rollback

Azure Kubernetes Service (AKS) allows us to rollback any update to the system at any point in time. If there is a problem with an update, we can revert to a prior version at the click of a button.

3. Disaster Recovery & Backups

Sendmarc is hosted on Microsoft Azure hosting environment and is designed for high availability. However, there is always the possibility of a system or data center outage. Sendmarc has implemented a fully geo-redundant system in Azure that can recover from an outage in a short amount of time. DR testing is performed every six months.

3.1. Application Redundancy

The application itself runs inside of an Azure Kubernetes Service (AKS) cluster with multiple nodes. This allows us to scale up the individual parts of the system during periods of high workloads. In addition to this, the multiple node configuration means that if one node goes down, there are additional nodes in place to take over.

3.2. Geo-Redundant Infrastructure

Sendmarc has built a fully redundant setup with failover across geographic regions. All persistent data is replicated across at least two Azure regions ensuring availability if one data center goes down. Along with this, our infrastructure configuration is version controlled and scripted, allowing us to ensure an exact copy of our deployment during disaster recovery.

3.3. Backups

Our database service takes full, differential, and transaction log backups which are also geo-redundant. The backups allow us to restore the server to any point in time within a 7-day period.

4. Data Processing

The Sendmarc Platform does not have any access to customer email boxes, servers or data, except for and in the course and scope of its Breach Detection Services and product. Sendmarc generally collects data by processing the incoming DMARC reports that are generated globally by other DMARC reporting servers. Within the DMARC specification, there are two types of reports:

- Aggregate reports; and
- Forensic reports

The terms of use and retention periods Sendmarc will retain Aggregate & Forensic Reports for 5 years. If a customer cancels their Sendmarc services, all Personal Information and any other data will be destroyed within 14 days of cancellation and rotated out of backups within 21 days.

4.1. Aggregate Reports

Aggregate Reports contain metadata on the email traffic of your domain(s) and do not contain any personal information. The meta-data is received in an XML file format and can include:

4.2. Summary of authentication results

- 4.2.1. IP identified in the email
- 4.2.2. Total of IP addresses identified
- 4.2.3. Disposition of the message, to show if the Policy was applied
- 4.2.4. DKIM authentication result, the domain and result
- 4.2.5. SPF authentication result, the domain and result

4.3. Receiving ISP information

- 4.3.1. Report ID number
- 4.3.2. Reporting Organization Name
- 4.3.3. Reporting Organization sending email address and additional contact information
- 4.3.4. Beginning and ending data range in seconds

4.4. Description of a DMARC record

4.4.1. Header domain/from domain

4.4.2. Alignment settings for both DKIM and SPF

4.4.3. Domain policy (reject)

4.4.4. Subdomain policy (reject)

4.4.5. Percentage of messages to which the DMARC policy is to be applied

Sendmarc collects these reports and converts the raw data into reporting that is easier to read, analyze and use as an action list.

4.2. Forensic Reports

Forensic reports are optional and sent by a limited number of DMARC report senders. These are parts or copies of specific messages that failed the DMARC checks. The contents of these messages could contain Personally Identifiable Information (PII). Sendmarc offers three methods on storing these messages:

1. **Default**: We store the message encrypted and the message is only viewable by the client, the domain owner.
2. **Encrypted**: Sendmarc can provide the client with a PGP key and only the client can decrypt the Forensic Report using their private key and password,
3. **No Storage**: The client can request that Sendmarc does not receive or store forensic reports.

4.3. Breach Detection

In the course and scope of delivering the Services as required for the Breach Detection, Sendmarc may also process the following Personal Information, including but possibly not limited to the following. This Processing is undertaken in the pursuit of the detection and prevention of cyber fraud, which is in the legitimate interests of the Data Subject and the Customer and takes into account the three-part test, constituting purpose, necessity and balancing.

- Full names of Data Subjects;
- Email Addresses;
- Financial information;
- Employment related usernames and passwords;
- Employment Information;
- Geographic location based information.

5. Incident Management process

5.1. Reports & Incidents

We have a breach management plan to follow should an incident occur. There are five elements:

- Identification and Classification
- Containment and Recovery
- Risk Assessment
- Notification of Breach
- Evaluation and Response

5.2. Identification and Classification

Though Sendmarc does everything technologically to ensure data security, we have also put in place procedures that will allow any staff member to report an information security incident. Staff are aware they should report such an incident to the Information Officer. This allows for early recognition of the incident so that it can be dealt with in the most appropriate manner. The report is then reviewed by the Information Officer to confirm if a breach has actually occurred.

5.3. Containment and Recovery

This step limits the scope and impact of the breach of data protection procedures. If a breach occurs, the Information Officer:

- Investigates the breach and ensures that the appropriate resources are made available for the investigation.
- Establishes who in the Organization needs to be made aware of the breach and begins the containment exercise.
- Establishes whether there is anything that can be done to recover losses and limits the damage the breach can cause.

5.4. Risk Assessment

In assessing the risk arising from a data security breach, the Information Officer will consider what would be the potential adverse consequences for Data Subjects, i.e., how likely it is that adverse consequences will materialize and, in the event of materializing, how serious or substantial are they likely to be.

5.5. Notification of Breaches

5.5.1. In the event of a loss of Personal Information on the unauthorized access thereto, occurs it is reported immediately, both internally and to the Information Officer or appropriate supervisory authority. It is also reported, in the appropriate circumstances, to the Data Subject and the Information Officer or appropriate supervisory authority, as soon as reasonably possible within a period of 72 hours. When notifying individuals, Sendmarc will consider using the most appropriate medium to do so in terms of the relevant legislation.

5.5.2. Such notification shall only be made where Sendmarc can identify the Customer to which the Personal Information relates. Where it is not possible, website publication will be considered and any other steps prescribes by the relevant supervisory authority and/or the Information Regulator.

5.5.3. Notification will be provided in writing by means of either:

5.5.3.1. Email;

5.5.3.2. Electronic communications;

5.5.3.3. registered mail;

5.5.3.4. on the Organization’s website;

5.5.4. The notification shall provide the following information where possible:

5.5.4.1. Description of possible consequences of the breach;

5.5.4.2. Measures taken to address the breach;

5.5.4.3. Recommendations to be taken by the Customer and/or Data Subject to mitigate adverse effect; and

5.5.4.4. The identity of the party responsible for the breach.

5.6. Evaluation and Response

Subsequent to any information security breach a thorough review of the incident will occur. The purpose of this review is to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.

Part B: Employee Access Control

Access to a client's Sendmarc services is limited to approved staff that are required to access our systems for client service or maintenance purposes. This section outlines the measures that Sendmarc has taken to ensure client data is kept safe even within the walls of Sendmarc's offices.

1. Identity Access

Sendmarc employs the following physical safety measures within the Sendmarc Offices

1.1. Gated security;
1.2. Key Card entry;
1.3. Biometric scanners;
1.4. A receptionist to identify/welcome anyone who does not have access; and
1.5. CCTV.

These access records and procedures are reviewed by management regularly.

2. Employees

Sendmarc employees can only access client data if they have permission to do so.

All Sendmarc staff attest to terms and conditions that specifically outline privacy, information security, and confidentiality. Sendmarc staff are also trained regularly on the following:

2.1. General procedures;
2.2. Paper records;
2.3. Email and personal productivity software;
2.4. Electronic remote access;
2.5. Laptops/Notebooks;
2.6. Mobile storage devices;
2.7. Data transfer; and
2.8. Breach management.

3. Employee & Contractors

Background checks that include a criminal record and credit checks are conducted on all employees before they are hired. New employees are carefully coached and trained before being allowed to access confidential or personal files.

Employees ensure that callers to the office or other unauthorized persons are unable to view personal or sensitive information, whether held on paper documents or information displayed on PC monitors, etc.

All employees ensure that PCs are logged off or 'locked' when left unattended for any period of time. Where possible, staff are restricted from saving files to the local disk. Users are instructed to only save files to their allocated cloud drive.

Personnel who retire, transfer from any internal department, resign etc. are removed immediately from mailing lists and access control lists. Relevant changes also occur when staff transfer to other internal assignments.

Negligence or malicious behavior are required to be dealt with as follows:

3.1. In the case of contractors or service provider representatives, such shall immediately be escorted off-site and remediation sought in line with any contractual agreement or binding usage policy.

3.2. In the case of employees, the Disciplinary Process shall be invoked.

3.3. Law enforcement shall be informed where required, or legal action may be instituted where deemed necessary.

4. Network Security

Sendmarc IT Network Administrators are responsible for ensuring network infrastructure is securely designed, deployed and maintained, by adhering to all the requirements of the Sendmarc information security documentation, including the System Security Policy, and security configuration standards.

Network segregation is a key design principle that shall be implemented between networks that have different trust levels. Segregation includes appropriate segmentation of networks and implementation of network filtering, such as implemented through network filtering (firewall) access rules, between network segments of different trust levels.

Systems that have access to and are used to manage network infrastructure shall be appropriately secured and should be segmented on a network level.

5. WIFI

Wireless networks shall adhere to current best practice and enterprise-class configuration which includes:

Using an appropriately secure wireless security protocol to ensure the confidentiality of information transmitted over wireless networks.

Appropriately authenticating users and/or devices to wireless networks. Authentication mechanisms such as pre-shared keys (PSK) were designed for use in-home or small office environments and are not considered suitably secure for use in an enterprise environment.

Network infrastructure should appropriately log activity, including security events.

6. Paper Records

- Papers with confidential data are locked away when not in use.
- Paper records and files containing personal data are handled in such a way as to restrict access to only those persons with business reasons to access them.
- Sendmarc shreds all paper records that contain confidential information. Other secure disposal methods are in place and properly used for confidential material, not on paper.
- Sendmarc does not make use of facsimile technology (fax machines) for transmitting documents containing personal data.

7. Email & Personal Productivity Software

- Standard unencrypted email is never used to transmit any data of a personal or sensitive nature. Clients that wish to use email to transfer such data must ensure that personal or sensitive information is encrypted, either through file encryption or through the use of a secure email facility which will encrypt the data (including any attachments) being sent.
- Where personal or sensitive data is held on applications and databases with relevant security and access controls in place, additional controls prevent such data from being copied to personal productivity software (i.e., Dropbox, Drive etc.).
- Sendmarc scans outgoing emails and attachments for keywords that would indicate the presence of personal data and, if appropriate, prevent its transmission.

8. Remote Access

When accessing this data remotely, it is done via a secure encrypted link via an SSL VPN tunnel with relevant access controls in place. Stringent security and access controls, such as strong passwords, are used for an additional layer of protection.

Sendmarc utilizes technologies that will provide for the automatic deletion of temporary files which may be stored on remote machines by its operating system.

Sendmarc ensures that only known machines (whether desktop PC, laptop, mobile phone, PDA, etc.) configured appropriately with up-to-date anti-virus and anti-spyware software are allowed to remotely access centrally-held personal or sensitive data.

9. Laptops & Mobile Storage

All portable devices are password-protected to prevent unauthorized use of the device and unauthorized access to information held on the device. Passwords used to access PCs, applications, databases, etc. are of sufficient strength to deter password cracking or guessing attacks. We instruct employees to create a password that includes numbers, symbols, upper and lowercase letters. Passwords are changed every 90 days.

Personal, private, sensitive, or confidential data are not stored on portable devices.

Laptops are physically secured if left in the office overnight. When out of the office, the device is kept secure at all times.

Staff-owned devices, such as portable media players (e.g., iPods, etc.), digital cameras, USB sticks, etc. are technologically restricted from connecting to Sendmarc-owned computers. Sendmarc implements procedures that will ensure that personal data held on mobile storage devices is fully deleted when the data is no longer required.

When replacing or selling laptops, hard drives are formatted and sanitized with a hard drive degausser program.

10. Data Transmissions

Data transfers only take place via secure on-line channels where the data is encrypted rather than copying to media for transportation. In general, we do not employ manual data transfers using removable physical media (e.g., memory sticks, CDs, tapes, etc.).

However, in the event it is absolutely necessary, any such encrypted media will be accompanied by a member of Sendmarc staff delivered directly to, and be signed for, by the intended recipient.

Part C: Business Administration Systems

Business Administrations Systems (BAS) is all the supporting systems that Sendmarc Pty Ltd uses to support customers. This includes systems like billing processing, support tickets systems, CRM systems and others. None of the NBAS have access to the data managed by The Sendmarc Platform.

1. Personal Data Access

Sendmarc's Business Administration Systems (BAS) do not have access to the data managed by the Sendmarc Platform. The BAS will Process Personal Information of its customers for the following purposes:

1.1. To provide or manage any information and services requested by the Customer;

1.2. To establish the Customer's needs in relation to specific instructions to Sendmarc;

1.3. To identify the identity of the Customer;

1.4. To facilitate the delivery of services to Customer. This includes normal business operations such as billing and invoicing, support tickets, CRM;

1.5. To send newsletters;

1.6. To comply with FICA and any other relevant anti-bribery or anti money-laundering requirements;

1.7. For general administration purposes;

1.8. For legal and / or contractual purposes;

1.9. To enter into negotiations and / or transact with third parties; and

1.10. To carry out analysis and customer profiling, including but not limited to identifying the full names, identity number, physical and postal addresses, contact numbers and email address of natural persons, and in the case of juristic persons, to identity the registration number, directors, shareholders, physical and postal addresses, contact numbers and email address of such juristic person, its directors and / shareholders.

2. Suppliers

Sendmarc makes use of the following suppliers for Normal Business Administration. None of the services have access to the data managed by the Sendmarc Platform.

2.1. Operations

Name	Purpose	More Information
Docusign	Document Approval	https://www.docusign.com/trust/privacy/gdpr
Google Apps	Productivity	https://policies.google.com/privacy?hl=en-US
Miro	Collaboration	https://miro.com/legal/privacy-policy
Microsoft 365	Email, Documents, Storage	https://www.microsoft.com/en-gb/privacy/privacystatement
Payspace	HR	https://www.payspace.com/privacy-policy
HubSpot	CRM	https://www.hubspot.com/data-privacy/gdpr
Sendgrid	Email Delivery	https://www.twilio.com/legal/privacy
Telviva	Telecommunications	https://telviva.co.za/data-privacy-statement/
WhatsApp	Communication	https://www.whatsapp.com/legal/updates/privacy-policy-eea
Entrust	Certificate Provider	https://www.entrust.com/legal-compliance/data-privacy/privacy-statement
XERO	Billing	https://www.xero.com/uk/campaigns/xero-and-gdpr
1Password	Password Manager	https://1password.com/legal/privacy

Acronis	Backup & Patch Management	https://www.acronis.com/en-us/company/privacy/
Adobe	Creative Design	https://www.adobe.com/privacy/policy.html
BambooHR	Employee Management Tool	https://www.bamboohr.com/legal/privacy-policy
Chargebee	Subscription Management	https://www.chargebee.com/privacy/
Cledara	SaaS Management Platform	https://www.cledara.com/privacy-policy#:~:text=We%20share%20information%20at%20your,you%20and%20obtaining%20your%20consent.
Deel	Payroll Platform	https://www.deel.com/legal/privacy-policy/
Dext	Expense Management Platform	https://dext.com/en/privacy-policy
Grammarly	Writing Assistant	https://www.grammarly.com/privacy-policy
Gusto	Recruiting and HR Platform	https://gusto.com/legal/privacy
Loom	Screen Recording Software	https://support.loom.com/hc/en-us/articles/10017863878557-Privacy-and-Security
Monday.com	Project Management Software	https://monday.com/trustcenter/privacy
Slack	Internal communication	https://monday.com/trustcenter/privacy
Syft Analytics	Financial Analytics Platform	https://www.syftanalytics.com/privacy-policy
Upflow	Accounts Receivable Platform	https://upflow.io/privacy-policy
Postscanmail	Mail Management	https://www.postscanmail.com/privacy.html
Vanta	Compliance Management	https://www.vanta.com/privacy
Thinkific	Learning Management System	https://www.thinkific.com/privacy-policy/

2.2. Website

Name	Purpose	More Information
Upcloud	Hosting	https://upcloud.com/privacy-policy
Runcloud	Provisioning	https://runcloud.io/legal/privacy-policy
Zapier	Automation	https://zapier.com/privacy
Cloudflare	DNS & DDoS protection	https://www.cloudflare.com/privacypolicy
Google Ads	Advertising	
Godaddy	DNS Hosting	https://za.godaddy.com/help/privacy-center-27875

2.3. Engineering

Name	Purpose	More Information
PHPStorm	IDE	https://www.jetbrains.com/legal/docs/privacy/privacy.html
API Layer	IP address enrichment	https://ipstack.com/privacy
Github	Source Control	https://docs.github.com/en/github/site-policy/github-privacy-statement
Sentry	Error, Performance monitoring	https://sentry.io/privacy

ClickUp	Project Management Software	https://clickup.com/terms/privacy
Datadog	Monitoring and Analytics	https://www.datadoghq.com/legal/privacy/
Entri	Domain Management Automation	https://entri.app/privacy-policy/#:~:text=Data%20Protection%20Rights,-We%20would%20like&text=Every%20user%20is%20entitled%20to,information%20you%20believe%20is%20inaccurate.
Figma	Design Collaboration Tool	https://www.figma.com/legal/privacy/
Instatus	Status Page Builder	https://instatus.com/policies/privacy
Intruder	Online Vulnerability Scanner	https://www.intruder.io/privacy
IPStack	IP Information and Management	https://ipstack.com/privacy#:~:text=General%3A%20We%20process%20such%20personal,browser%20communicates%20to%20our%20server.
JetBrains	Developer Tools	https://www.jetbrains.com/legal/docs/privacy/privacy/
Mailtrap	Email Testing Software	https://mailtrap.io/privacy/
Pulsedive	Cybersecurity	https://pulsedive.com/privacy/
Sonarcloud	Code Review	https://www.sonarsource.com/company/privacy/

3. Data Collection

3.1. When Sendmarc collects Personal Information directly from a Data Subject it is done so in line with Articles 5- 14 of the GDPR and/or Section 18 of POPI, as and when required for a defined purpose, unless an exception is applicable.

3.2. Sendmarc will always collect Personal Information in a fair, lawful, transparent and reasonable manner to ensure that it protects the Data Subject's privacy and will Process the Personal Information based on legitimate grounds in a manner that does not adversely affect the Data Subject in question.

3.3. Sendmarc often collects Personal Information directly from the Data Subject and/or Customer and/or in some cases, from Third Parties. Where Sendmarc obtains Personal Information from Third Parties, it will ensure that it so informs the Data Subject and/or Customer or will only Process the Personal Information without consent where it is permitted to do so in terms of an exception as referred to in clause 3.1 above or the applicable legislation.

3.4. The Personal information Sendmarc collects in the ordinary course of business includes:

3.4.1. only information that is adequate, necessary, and relevant to enable it to effectively render the Service or assist in any manner required, such as the Customer's name, identity or registration number, Customer's employees or its director's Personal information, contact information etc.;

3.4.2. electronic communications sent to Sendmarc;

3.4.3. technical information;

3.4.4. information from the Data Subject and/or Customer's visits to the Sendmarc website, including the type of browser and operating system that the Customer uses, access times, pages viewed, URLs clicked on, his IP address and the pages visited before and after navigating the Sendmarc website;

3.4.5. social media tracking pixels that allow platforms such as Facebook and Twitter to interact with the Sendmarc website and give feedback on the Customer's actions;

3.4.6. device information, including the unique device identifier, hardware model, operating system and version and mobile network information;

3.4.7. The Sendmarc website uses various technologies including "cookies" which allow the website to recognize and respond to the Data Subject and/or Customer as an individual. The Data Subject and/or Customer can elect to accept or decline cookies. If a Data Subject and/or Customer elects to decline cookies, not all elements of the website may function as intended, so his website experience may be affected.

4. Retention of Records

4.1. Sendmarc may keep records of the Personal Information it has collected, correspondence, or comments in an electronic or hardcopy file format.

4.2. Sendmarc will not retain personal information for a period longer than is necessary to achieve the purpose for which it was collected or processed and is required to delete, destroy (in such a way that it cannot be reconstructed) or de-identify the information as soon as is reasonably practicable once the purpose has been achieved. This prohibition will not apply in the following circumstances –

4.2.1. where the retention of the record is required or authorized by law;

4.2.2. Sendmarc requires the record to fulfil its lawful functions or activities;

4.2.3. retention of the record is required by a contract between the parties thereto;

4.2.4. the Customer (or competent person, where the Customer is a child) has consented to such longer retention; or

4.2.5. the record is retained for historical, research or statistical purposes provided safeguards are put in place to prevent use for any other purpose.

4.3. Accordingly, Sendmarc will, subject to the exceptions noted herein, retain Personal Information for as long as necessary to fulfil the purposes for which that Personal Information was collected and/or as permitted or required by applicable law.

4.4. Where Sendmarc retains Personal Information for longer periods for statistical, historical or research purposes, Sendmarc will ensure that appropriate safeguards have been put in place to ensure that all recorded Personal Information will continue to be Processed in accordance with this Policy and the applicable laws.

4.5. Once the purpose for which the Personal Information was initially collected and Processed no longer applies or becomes obsolete, Sendmarc will ensure that the Personal Information is deleted, destroyed or de-identified sufficiently so that a person cannot re-identify such Personal Information.

4.6. In instances where we de-identify the Personal Information, Sendmarc may use such de-identified information indefinitely.