PoliteMail

Data Protection Impact Assessment

Privacy & Security Considerations for the Global Enterprise

MK-GN06 2302

Contents

Privacy by Design.

It's your data, we process and protect it.

Internal & Analytics Use

PoliteMail is designed to support internal email broadcasts and analytics, not external email. All personal data processed will be of employees.

Email analytics tools function in a very similar way to web analytics tools. If your company's internet use policy allows the company to log data and collect web analytics, this likely applies to email analytics data collection.

Email measurement primarily utilizes beacon images (tiny transparent images) to measure opens and URL redirects to measure clicks. PoliteMail's integration with M365 also enables authentication data to be used for measurement. These measurement devices do not require any special technology or software installed on the recipient devices, the analytics tools simply capture data present in the standard web or authentication requests.

Personal Information

A name and business email address are often considered personal information. To process and send email and provide an audit trail, PoliteMail processes and stores the sender's and recipient's email address and name.

All http/https requests contain data from the originating device known as a user agent string which includes IP address and potentially device identification data and data such as OS and browser version. PoliteMail processes incoming https user agent string data to perform a reverse IP look-up for geographic location to city level, and to determine device type (desktop or mobile, by OS).

No Sensitive Information

No sensitive information is processed or stored by PoliteMail by default. This is no reason to process or store any sensitive data or financial data on our system. PoliteMail does provide tools to support the import of additional data fields related to an employee email address, and this is generally list segmentation data such as department, division, location (building or country), etc. Importing such data requires user action, and additions or removal of such data is within user control.

Content is Processed, Not Stored

PoliteMail does not control the content of the broadcast email, but when email is processed to add the analytics encoding, the messages are only on the Services for the duration of the send process, and once sent by the SMTP service are no longer stored. In the event the user schedules a send for future or time-zone delivery, some messages will be held on the server until such delivery schedule time. Those files will be stored using AES-256 encryption, and on AES-256 encrypted storage. PoliteMail does provide tools to save email templates and drafts on the services. When sending using PoliteMail online (verses the Outlook add-in) interface, the system will store the content as a sent item. The user is in control of these templates, drafts and sent items and may delete them at any time.

Cookie-less

PoliteMail may write temporary, expiring first-party session cookies with device identifiers, and does not store third-party cookies, persistent cookies, or share any cookie-data with any other party.

Intent

PoliteMail is a third-party provider processing email on your behalf, adding analytics functionality for statistical analysis. The intent of such statistical analysis is to monitor communication performance metrics such as reach, attention, readership and engagement, in order to make improvements to the internal communications programs. The data analytics are not intended to support individual behavior modification or corrective actions.

Legal Basis

Your company issues the email addresses to employees with the expectation they will receive company email, and your company already processes email and email data, therefore no explicit content is required as this is a legitimate interest of the business.

Consent

Because PoliteMail receives this personal data from the company, by way of distribution group membership or via import of list data and does not collect such personal information direct from an individual person, no consent is required. Because the interaction data is collected for first-party statistical analysis, no consent is required.

Privacy Compliance

Privacy by Design and Default

When developing our software products and services, we consider both our customer and the data subjects (typically employees). PoliteMail has designed methods to provide accurate, yet anonymous, statistical email analytics.

PoliteMail's SaaS services architecture is designed to provide completely segregated data processing and storage for each customer. We provide dedicated cloud services and databases, to prevent intermingling. While virtualized services may run on the same physical hardware, logical isolation and storage segregation maintains clear separation. All data in transit is encrypted using the HTTPS TLS1.2 protocols and at rest with AES-256 encryption.

We consider privacy and security when developing our products. We follow a security development lifecycle to address privacy and security concerns up front, code against the SANS/CWE Top 25 most dangerous software errors, conduct static and dynamic vulnerability scanning on every pre-release build, and conduct annual third-party application penetration testing.

Anonymous Measurement

Anonymization means the measurement data cannot be identified to a person, and pseudonymization or encryption means no individual can be identified without a specific "key" and such key is kept separate from the data. For privacy compliance, PoliteMail's anonymous tracking mode is configured and locked on the server application by an authorized administrator and cannot be changed by any user. The effect of anonymous tracking is to break the direct relationship between the personal data and the interaction data. The data about an employee being sent an email is always known, by the sender, by the recipient, by the Microsoft Office email system, and when using PoliteMail to process and measure email broadcasts.

How PoliteMail Anonymization Works, Technically

To maintain privacy, email interactions are related to an anonymized record, and not the individual recipient's email address record, which contains personal data in the form of name and company provided email address.

When PoliteMail processes an email broadcast for sending, it inserts the name and email address record and the anonymized ID record into separate database tables for each recipient of the message. In this way we maintain both an audit trail of who was sent what email from whom, as well as the method to depersonalize the relationship of email interactions to receipts, as those interactions are related to the anonymized ID.

Within each email message it processes, PoliteMail inserts measurement encoding (alphanumeric unique identifiers) including encoded Secure Hypertext Transfer Protocol (HTTPS) references to small, transparent pixel beacon images and encoded URLs rewrites (encoded URL addresses to web pages

which will redirect to the actual destination URL). When a recipient interacts with an email message, both M365 authentication data as well as any encoded https requests made to the PoliteMail application are processed and the email interaction data is stored and associated to the anonymized ID record, keeping those interactions anonymous without the use of additional information.

Any analytical data or reports pulled from PoliteMail would reveal the number (or percentages) of unique recipients who interacted with that specific email message, but not whom. Therefore, with Anonymized sending, the analytical and statistical interaction information does not relate to an identified or identifiable natural person. To prevent against the rare case where a sparsely populated segment might be linked to other easily available information (such as the number of employees within a specified geographic area), PoliteMail will produce a null result for any segments of data less than 5 individual records.

Within the PoliteMail application and database system, the email address records and the anonymized ID records do have a relationship which would require specialized technical knowledge and authenticated access to reassociate. Under Article 4(3b) PoliteMail's *Anonymous* send mode would be classified as pseudonymization, as the interaction analytics data can no longer be attributed to a specific data subject without the use of such additional information, which is kept separately and is subject to technical and organizational measures to ensure against re-attribution.

IP and Geolocation Privacy

To prevent IP processing by the PoliteMail application, a proxy server can be configured. As all http/https traffic gets routed through the proxy, without enabling the use of x-forward-for (XFF) headers, the proxy server is effectively an anonymizing service, as any https request would only reveal the IP of the proxy server.

A blind proxy service makes detection and prevention of abusive system access significantly more difficult, increasing risk. When network control groups, logging, and DDoS services are enabled on the proxy, the PoliteMail Services will still process IP addresses and store IP address in log files, but for technical and security purposes only, not for use within the analytics application.

Employee Privacy

Access to your employee personal data, including name and email address, is limited to PoliteMail system administrators according to least privilege principles. All data is AES-256 encrypted at rest. An authorized PoliteMail user within your organization will be able see the recipients of their email distributions, not unlike what can be done without PoliteMail. Within analytics reports, email sent using anonymous measurement will prevent the identification of the individuals

Data Retention

Generally, email data including email addresses and analytics is stored for the Term of the contract. Name and email address records may be deleted and removed from the system by PoliteMail users, but if or when that address is sent an email in future using PoliteMail, a new record containing that information will be created.

You are Controller, We are a Processor

As a PoliteMail customer, you are the data controller and data owner. PoliteMail is a processor. As a processor, we have an obligation to secure and protect this data and take responsibility by providing technical safeguards, access restrictions, policies and practices to protect the data privacy of individual data subjects.

How We Manage Your Data

We use your customer data only to provide the services we have agreed on, and never share it with third parties for any purpose. We make contractual data security and privacy commitments for the software and services we agree to provide. We strive to maintain transparent policies and processes, so our customers and their employee data subjects are fully aware of the data being collected, its purpose, and what operations are being performed on that data. We provide ready access to your data, so you may extract data or delete data as desired and fulfill any data subject requests. If and when you leave our service, we follow specific protocols to permanently remove your data from our systems.

How We Limit Access to Your Data

We have implemented technical and organizational measures to protect your data from unauthorized or inappropriate access and use. While certain PoliteMail administrators and technical support engineers do require data access in order to provide the services, we employ role-based security group controls, IP restrictions and multifactor authentication for all PoliteMail personnel. All PoliteMail employees are required to sign confidentiality agreements and attend data security and privacy awareness training upon hire and at least annually.

Data Location

PoliteMail partners with Microsoft Azure and Amazon AWS to provide tier 1 cloud hosting services, maintaining agreements which are at least as stringent as our own data-processing terms. PoliteMail maintains several Virtual Private Networks and Virtual Private Cloud (VPC) environments, and customers may select a specific geographic location (US, EU, ASIAPAC) for their data processing and storage to occur. All technical services and administration are provided from the USA.

Requests for Data

How We Respond To Legal Requests For Customer Data

In the event of a legal hold or government request for data, we follow our standardized, contractual processes to provide you with notice and a copy of such request, unless legally prohibited from doing so.

How We Respond To Data Subject Requests

In the event a data subject makes a request for data, we follow our standardized processes to provide you with notice and a copy of such request, and do not provide data to, or interact directly with, the data subject.

What Data Does PoliteMail Process and Store?

The following table details all the data PoliteMail processes and stores. A User is defined as a PoliteMail for Outlook application end user. A Recipient is an employee email address a message has been sent to.

PoliteMail User/Sender Data

DATA ELEMENT	REQUIRED	STORED	PROCESSING	STORAGE ENCRYPTION
User Email Address	Yes	Yes	User Authentication	AES256
User Role	Yes	Yes	Data Access	AES256
User Password	Optional	Yes (Not with SSO)	User Authentication	SHA256
User Title	Optional		User Identity	AES256
User Address	Optional		User notifications	AES256
User Phone	Optional		User notifications	AES256
User Group	Optional		User Identity, user segmentation	AES256
User Region	Optional		User Identity, user segmentation	AES256

Mailing List & Recipient Data

DATA ELEMENT	REQUIRED	STORED	PROCESSING	STORAGE ENCRYPTION
Recipient Email Address	Yes	Yes	Email addressing, list membership, subscription management, reporting segmentation	AES256
Recipient Name	Yes	Yes	Email addressing/personalization, list membership	AES256
Recipient Timezone	Yes	Yes	AD working hours for scheduled sends	AES256
Recipient Default Language	Optional		*Browser Setting translation	AES256
Department	Optional		List management, reporting segmentation	AES256
Division	Optional		List management, reporting segmentation	AES256
Campus	Optional		List management, reporting segmentation	AES256
Building	Optional		List management, reporting segmentation	AES256
Manager	Optional		List management, reporting segmentation	AES256
Other HR Attributes If/As Required by Customer	Optional		List management, reporting segmentation	AES256

Message Data

DATA ELEMENT	REQUIRED	STORED	PROCESSING	STORAGE ENCRYPTION
Email Message	Yes	Optional and temporary (as draft or scheduled send)	Composing and sending email message	AES256
Sent Time/Date	Yes	Yes	Reporting & analysis	SHA256
Time Zone	Yes	Yes	List management, reporting segmentation	AES256
To:	Yes	Yes	Reporting & analysis	SHA256
From:	Yes	Yes	Reporting & analysis	AES256
Subject:	Yes	Yes	Reporting & analysis	AES256
URL's	Yes	Yes	Click reporting	AES256
Word Count	Yes	Yes	Reporting	AES256
Image Count	Yes	Yes	Reporting	AES256
Image Sizes (Pixel Dimensions)	Yes	Yes	Reporting	AES256

We optionally gather the following data via the PoliteMail archive service to support working hours sending:

- contact_email (string): The email address of the user's contact information.
- time zone (string): The time zone of the user's calendar.
- workdays (int): A bitmask representing the workdays of the week for the user.
- day_start (TimeSpan): The start time for the user's workday.
- day_end (TimeSpan): The end time for the user's workday.
- mailbox_language (string): The language of the user's mailbox.

When sending to a list using Graph Expansion for each group member we pull:

- smtp (string): The SMTP address of the user.
- display_name (string): The display name of the user.
- mailbox_type (int) : The mailbox type of the user, represented as an integer value.

Email Interaction Data

MESSAGE DATA	REQUIRED	STORED	PROCESSING	STORAGE ENCRYPTION
Device OS	Yes	Yes	Reporting Analytics	AES256
Browser Ver	Yes	Yes	Reporting Analytics	AES256
Date & Time	Yes	Yes	Reporting Analytics	AES256
Message ID	Yes	Yes	Reporting Analytics	SHA256
Recipient ID	Optional individual or anonymized	Yes	Reporting Analytics	AES256
User Agent	Yes	Partial	Reporting Analytics	AES256
IP	Yes	Optional via proxy	Reporting Analytics	AES256
Geolocation	Yes	Yes	IP reverse lookup to ascertain region (state/province)	SHA256
URL Clicked	Yes	Yes	Reporting Analytics	AES256
Link ID	Yes (Reverse IP lookup) to state/prov level	Yes	Reporting Analytics	AES256
View Time	Yes	Yes	Reporting Analytics	AES256

Data by Measurement Mode

Data Collected / Stored	Individual Mode	Anonymous Mode	Aggregate Mode
Sender Email	✓	✓	✓
Distribution List Name	✓	✓	✓
Nested DL / Subgroup	✓		
Subject, Date, Time	✓	✓	✓
Recipient Name, Email	✓	Anonymized	
Recipient IP	✓	Geoloc only	Geoloc only
Recipient User Agent	✓	✓	✓
Open Date, Time, Device	✓	✓	✓
Read Time (secs open)	✓	✓	✓
Clicks (link name and url)	✓	✓	✓